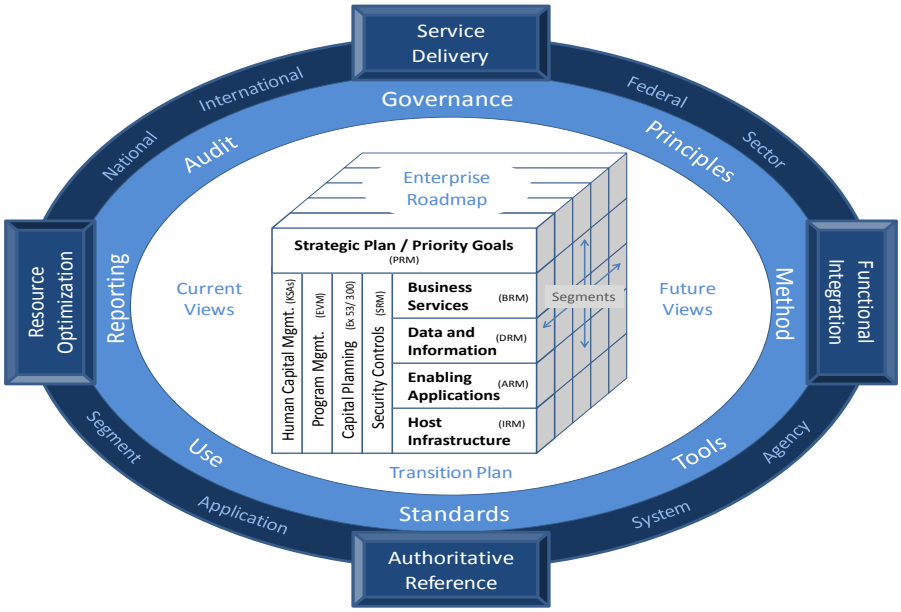
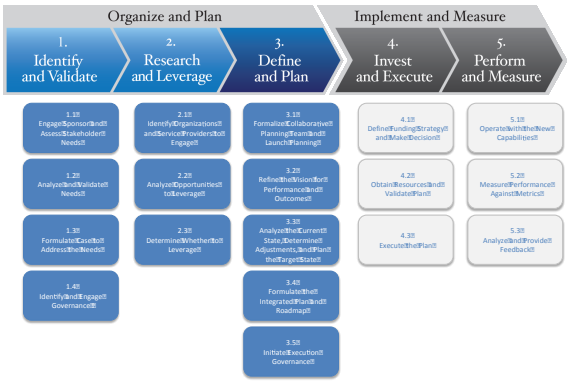
January 29, 2013

Federal Enterprise Architecture Framework

Version 2





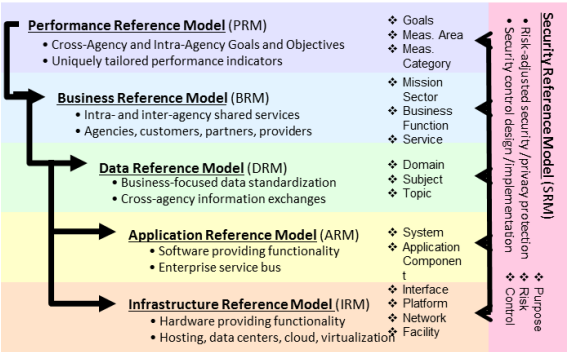


Table of Contents

1 Introduction to the Federal Enterprise Architecture Framework (FEAF) v2 11

2 Overview of the Collaborative Planning Methodology 13

3 Step 1: Identify and Validate 15

3.1 Purpose 15

3.2 The Planner's Role 15

3.3 Outcome 16

4 Step 2: Research and Leverage 16

4.1 Purpose 16

4.2 The Planner's Role 16

4.3 Outcome 16

5 Step 3: Define and Plan 17

5.1 Purpose 17

5.2 The Planner's Role 17

5.3 Outcome 17

6 Step 4: Invest and Execute 18

6.1 Purpose 18

6.2 The Planner's Role 18

6.3 Outcome 18

7 Step 5: Perform and Measure 18

7.1 Purpose 18

7.2 The Planner's Role 18

7.3 Outcome 19

8 Overview of the Consolidated Reference Model 20

9 Introduction to the Performance Reference Model 23

9.1 Purpose of the Performance Reference Model 23

9.2 Structure of the Performance Reference Model 23

10 Using the Performance Reference Model Taxonomy 24

10.1 Integrating CPIC (Exhibit 300) Performance Reporting with the FEA PRM 24

11 PRM Touchpoints with other Reference Models 25

12 Associated Methods/Best Practices for the PRM 25
12.1 Line of Sight 25
12.2 Selecting a Balanced Set of Exhibit 300 Performance Measures 28
13 PRM Summary 28
14 Introduction to the Business Reference Model 30
14.1 Purpose of the Business Reference Model 30
14.2 Structure of the Business Reference Model 30
15 Using the Business Reference Model Taxonomy 31
15.1 Identifying opportunities to share services government-wide 31
15.2 Reducing costs by eliminating duplication within the enterprise 31
16 BRM Touchpoints with other Reference Models 32
17 Associated Methods/Best Practices for the Business Reference Model 33
17.1 Business Architecture for Decision Support 33
17.2 Business Process Modeling 34
18 BRM Summary 34
19 Introduction to the Data Reference Model 35
19.1 Purpose of the Data Reference Model 35
19.2 Structure of the Data Reference Model 35
20 Using the Data Reference Model Taxonomy 36
20.1 Using the DRM to Compare Data Sources across Federal Agencies 36
20.2 Using the DRM to Create a Standardized Information Exchange 36
21 DRM Touchpoints with other Reference Models 37
22 Associated Methods/Best Practices for the Data Reference Model 37
22.1 Data Description 37
22.2 Data Context 38
22.3 Data Sharing 39
23 DRM Summary 39
24 Introduction to the Application Reference Model 41
24.1 Purpose of the Application Reference Model 41
24.2 Structure of the Application Reference Model 41
25 Using the Application Reference Model 42
25.1 IT Cost Reduction through IT/ Application Portfolio Management 42

25.2 Using the ARM with the entire Consolidated Reference Model (CRM) 43
26 ARM Touchpoints with other Reference Models 43
27 Associated Methods/Best Practices for the Application Reference Model 44
27.1 Capability Modeling and Analysis 44
27.2 Service Oriented Architecture 44
27.3 Portfolio Management 45
28 ARM Summary 45
29 Introduction to the Infrastructure Reference Model 46
29.1 Purpose of the Infrastructure Reference Model 46
29.2 Structure of the Infrastructure Reference Model 46
30 Using the Infrastructure Reference Model Taxonomy 47
30.1 Using the IRM to Create an IT Asset Management (ITAM) 47
30.2 Using the IRM to Identify Opportunities for Shared Services 48
31 IRM Touchpoints with other Reference Models 48
32 Associated Methods/Best Practices for the Infrastructure Reference Model 49
32.1 Methods 49
32.2 Best Practices 49
33 IRM Summary 50
34 Introduction to the Security Reference Model 51
34.1 Purpose of the Security Reference Model 51
34.2 Structure of the Security Reference Model 51
35 Using the Security Reference Model Taxonomy 52
35.1 Using Standards to classify Policy at the International, National, Federal, Sector, Enterprise or Department Level 52
35.2 Using Policy to select Controls at the Agency or Segment Level 53
35.3 Enforcing Design with Controls at the System or Application Level 53
36 SRM Touchpoints with other Reference Models 54
37 Associated Methods/Best Practices for the Security Reference Model 54
37.1 Risk Based Design 54
37.2 Security Controls 55
38 SRM Summary 55
39 Artifacts 57

39.1 Strategy Sub-Architecture Domain 58
39.2 Business Sub-Architecture Domain 59
39.3 Data Sub-Architecture Domain 60
39.4 Applications Sub-Architecture Domain 62
39.5 Infrastructure Sub-Architecture Domain 63
39.6 Security Sub-Architecture Domain 64
Appendix A: Collaborative Planning Methodology Guidance Document 65
A.1 Overview of the Collaborative Planning Methodology 65
A.1.1 Step 1: Identify and Validate 67
A.1.2 Step 2: Research and Leverage 68
A.1.3 Step 3: Define and Plan 68
A.1.4 Step 4: Invest and Execute 69
A.1.5 Step 5: Perform and Measure 70
A.2 Step 1: Identify and Validate 71
A.2.1 Step At-a-Glance 72
A.2.2 A Note on Core Artifacts 73
A.2.3 Activity 1.1: Engage Sponsor and Assess Stakeholder Needs 73
A.2.4 Activity 1.2: Analyze and Validate Needs 76
A.2.5 Activity 1.3: Formulate case to address the needs 78
A.2.6 Activity 1.4: Identify and Engage Governance 81
A.3 Step 2: Research and Leverage 85
A.3.1 Step At-a-Glance 86
A.3.2 A Note on Core Artifacts 87
A.3.3 Activity 2.1: Identify Organizations and Service Providers to Engage 87
A.3.4 Activity 2.2: Analyze Opportunities to Leverage 89
A.3.5 Activity 2.3: Determine Whether to Leverage 92
A.4 Step 3: Define and Plan 94
A.4.1 Step At-a-Glance 95
A.4.2 A Note on Core Artifacts 97
A.4.3 Activity 3.1: Formalize Collaborative Planning Team and Launch Planning 97
A.4.4 Activity 3.2: Refine the vision for performance and outcomes 100
A.4.5 Activity 3.3: Analyze the Current State, Determine Adjustments, and Plan the Target State ... 104

A.4.6 Activity 3.4: Formulate the Integrated Plan and Roadmap 125
A.4.7 Activity 3.5: Initiate Execution Governance 131
A.5 Step 4: Invest and Execute 135
A.5.1 Step At-a-Glance 137
A.5.2 A Note on Core Artifacts 137
A.5.3 Activity 4.1: Define Funding Strategy and Make Decision 138
A.5.4 Activity 4.2: Obtain Resources and Validate Plan 139
A.5.5 Activity 4.3: Execute the Plan 139
A.6 Step 5: Perform and Measure 141
A.6.1 Step At-a-Glance 142
A.6.2 A Note on Core Artifacts 142
A.6.3 Activity 5.1: Operate with the New Capabilities 142
A.6.4 Activity 5.2: Measure Performance Against Metrics 143
A.6.5 Activity 5.3: Analyze and Provide Feedback 143
Appendix B: Business Reference Model (BRM) 144
B.1 Business Reference Model Overview 144
B.1.1 BRM Structure 145
B.2 Using the BRM Taxonomy 147
B.2.1 Inter-Agency 147
B.2.1.1 Office of Management and Budget 147
B.2.2 Intra-Agency 147
B.2.2.1 Agency Executives and Business Managers 147
B.2.2.2 Agency CIOs 148
B.2.2.3 Portfolio Managers 149
B.2.2.4 Architects 149
B.2.2.5 Project Managers 151
B.2.2.6 Development Teams 151
B.3 Associated Methods 152
B.3.1 Business Architecture for Decision Support 152
B.3.2 Business Process Modeling 153
B.3.3 Business Process Modeling Notation (BPMN) 154
B.4 BRM Taxonomy 155

Appendix C: Data Reference Model (DRM) 156
DRM Executive Summary 156
C.1 Introduction 157
C.1.1 FEA DRM Focus 157
C.1.2 DRM as Federal Guidance 157
C.1.3 What the DRM Is and Is Not 158
C.1.4 The DRM and Knowledge Management 158
C.1.5 FEA DRM Meta-Model 159
C.1.6 DRM Fundamental Methods 161
C.1.7 DRM Overview 162
C.2 Associated Methods and Data Standards 163
C.2.1 Data Description 163
C.2.1.1 Overview of Metadata 163
C.2.1.2 Data Description Methods 164
C.2.2 Data Context 166
C.2.2.1 Role of Data Context in Governance 166
C.2.2.2 Data Categorization Methods 167
C.2.2.3 Usage Context 168
C.2.3 Data Sharing 170
C.2.3.1 Sharing Data through Data Exchange Services 170
C.2.3.2 Data Sharing through Data Access Services 173
C.2.3.3 Information Sharing 174
C.3 DRM Examples of Use 176
C.3.1 Use Case Example One: Comparing Data Sources across Federal Agencies 176
C.3.2 Use Case Example Two: Standardized Information Exchange for Suspicious Activity Reporting 176
C.4 Measurement Success Factors 177
C.5 Summary 179
Appendix C.i: List of Acronyms 180
Appendix D: Application Reference Model (ARM) 182
D.1 Introduction to the Application Reference Model (ARM) 182
D.1.1 Purpose 183

D.1.1.1 ARM Guiding Principles 184
D.2 Associated Methods / Best Practices 184
D.2.1 Capability Modeling and Analysis 185
D.2.2 Service Oriented Architecture 185
D.2.3 Portfolio Management 185
D.3 Using the Application Reference Model 186
D.3.1 Use Case: IT Cost Reduction through IT / Application Portfolio Management 186
D.3.1.1 Synopsis 186
D.3.1.2 Challenge 186
D.3.1.3 Solution 187
D.3.1.4 Possible Results 187
D.3.2 Use Case: Using the ARM with the entire Consolidated Reference Model (CRM) 187
D.3.2.1 Synopsis 187
D.3.2.2 Challenge 188
D.3.2.3 Solution 188
D.3.2.4 Results 189
Appendix E: Infrastructure Reference Model (IRM) 191
E.1 Introduction to the IRM 191
E.1.1 Purpose 191
E.1.1.1 Guiding Principles 191
E.1.1.2 IRM Outcomes 192
E.1.1.3 Stakeholder Usage 192
E.1.2 IRM Structure 193
E.1.2.1 IRM Taxonomy 194
E.1.2.2 IRM Relationships 195
E.2 Using the IRM Taxonomy 197
E.2.1 Use Case: IT Asset Management (ITAM) 198
E.2.1.1 Goal 198
E.2.1.2 Challenges 199
E.2.1.3 How the IRM Helps 199
E.2.2 Use Case: Shared Services – Cloud First 200
E.2.2.1 Goal 200

E.2.2.2 Challenges 200
E.2.2.3 How the IRM Helps 201
E.3 Associated Methods/Best Practices 203
E.3.1 Methods 203
E.3.2 Best Practices 205
Appendix F: Security Reference Model (SRM) 207
F.1 Approach to Security Architecture 207
F.1.1 The Security Reference Model 207
F.1.2 SRM Approach to Security 208
F.1.2.1 What is a Risk? 209
F.2 Design Compliance for Architectural Layers 211
F.2.1 International, National, Federal, Sector, Enterprise or Department -> Standards set Policy 211
F.2.1.1 Architecture Guidance 211
F.2.2 Agency or Segment -> Policy influences Controls 212
F.2.2.1 Architecture Guidance 213
F.2.3 System or Application -> Controls enforce Design 213
F.2.3.1 Architecture Guidance: 214
F.3 Relationship to other Reference Models 215
F.4 Optimal Risk Based Design 218
F.5 Security Controls and Metrics 222
F.5.1 Purpose of Controls 222
F.5.1.1 Managing Risk as Part of the Control Strategy 222
F.5.1.2 Security Value Chain 224
F.5.1.3 Control Selection 225
F.5.1.4 Defense in Depth 225
F.5.1.5 How to use Control Appendices 225
F.5.2 Metrics 226
F.5.2.1 Performance and Compliance 226
F.5.2.2 PRM 226
F.5.2.3 Metrics Maturity 227
F.5.2.4 How to use Performance Metrics 227

Appendix F.i: Ontology List of Methods 229
Appendix F.ii: Controls and Metrics Mapping 233
Appendix F.iii: Security Reference Document Mappings 274
Appendix F.iv: Links to Lists of Threat Sources and Vulnerabilities 281
Appendix G: Performance Reference Model Taxonomy with Definitions 283
Appendix H: Business Reference Model Taxonomy with Definitions 311
Appendix I: Data Reference Model Taxonomy with Definitions 360
Appendix J: Application Reference Model Taxonomy with Definitions 380
Appendix K: Infrastructure Reference Model Taxonomy with Definitions 401
Appendix L: Security Reference Model Taxonomy with Definitions 427

1 Introduction to the Federal Enterprise Architecture Framework (FEAF) v2

Enterprise Architecture (EA) supports planning and decision-making through documentation and information that provides an abstracted view of an enterprise at various levels of scope and detail. The Common Approach to Federal Enterprise Architecture, released in May 2012 as part of the federal CIO's policy guidance and management tools for increasing shared approaches to IT service delivery, presents an overall approach to developing and using Enterprise Architecture in the Federal Government. The Common Approach promotes increased levels of mission effectiveness by standardizing the development and use of architectures within and between Federal Agencies. This includes principles for using EA to help agencies eliminate waste and duplication, increase shared services, close performance gaps, and promote engagement among government, industry, and citizens.

The *Federal Enterprise Architecture Framework v2* describes a suite of tools to help government planners implement the Common Approach. At its core is the Consolidated Reference Model (CRM), which equips OMB and Federal agencies with a common language and framework to describe and analyze investments. It consists of a set of interrelated "reference models" that describe the six sub-architecture domains in the framework:

- Strategy
- Business
- Data
- Applications
- Infrastructure
- Security

These are designed to facilitate cross-agency analysis and the identification of duplicative investments, gaps and opportunities for collaboration within and across agencies. Also, by applying all six reference models, agencies can establish a line of sight from the strategic goals at the highest organizational level to the software and hardware infrastructure that enable achievement of those goals. Collectively, the reference models comprise a framework for describing important elements of federal agency operations in a common and consistent way.

To apply the framework to an agency's specific environment, the agency should develop a set of "core" artifacts to document its environment within the framework presented by the CRM. Each sub-architecture domain represents a specific area of the overall framework and has particular artifacts, based on EA best practices, which are described and recommended in the Framework and Artifacts document. The type and depth of documentation actually used by the agency should be guided by the need for detail and answers to questions about requirements, applicable standards, timeframes, and available resources.

The real value to the agency of developing an Enterprise Architecture is to facilitate planning for the future in a way that transforms the government while making it more efficient. The agency can use the

EA process to describe the enterprise as it currently is and determine what the enterprise should look like in the future, so that it can make plans to transition from the current state to the future state. The *Collaborative Planning Methodology* provides steps for planners to use throughout the planning process to flesh out a transition strategy that will enable the future state to become reality. It is a simple, repeatable process that consists of integrated, multi-disciplinary analysis that involves sponsors, stakeholders, planners, and implementers.

The agency will create an Enterprise Roadmap to document the current and future architecture states at a high level and presents the transition plan for how the agency will move from the present to the future in an efficient, effective manner. The agency's Enterprise Roadmap combines the artifacts developed for the EA, both current and future state versions, with a plan developed through the Collaborative Planning Methodology. This creates awareness, visibility and transparency within an organization to facilitate cross-organization planning and collaboration. It maps strategy to projects and budget and helps identify gaps between investment and execution, as well as dependencies and risks between projects.

All in all, the *Federal Enterprise Architecture Framework v2* helps to accelerate agency business transformation and new technology enablement by providing standardization, analysis and reporting tools, an enterprise roadmap, and a repeatable architecture project method that is more agile and useful and will produce more authoritative information for intra- and inter-agency planning, decision-making, and management.

2 Overview of the Collaborative Planning Methodology

Planning is done to affect change in support of an organization's Strategic Plan, and the many types of planners (e.g., architects, organization and program managers, strategic planners, capital planners, and other planners) must work together to develop an integrated, actionable plan to implement that change. Planning should be used to determine the exact changes that are needed to implement an organization's Strategic Plan, enable consistent decision-making, and provide measurable benefits to the organization. In short, an organization's Strategic Plan should be executed by well-rounded planning that results in purposeful projects with measurable benefits.

In today's environment, which demands more efficient government through the reuse of solutions and services, organizations need actionable, consistent, and rigorous plans to implement Strategic Plans and solve priority needs. These integrated plans should support efforts to leverage other Federal, state, local, tribal, and international experiences and results as a means of reusing rather than inventing from scratch. Plans should be consistent and rigorous descriptions of the structure of the organization or enterprise, how IT resources will be efficiently used, and how the use of assets such as IT will ultimately achieve stated strategies and needs.

The role of planners is to help facilitate and support a common understanding of needs based on the organization's Strategic Plan, help formulate recommendations to meet those needs, and facilitate the development of a plan of action that is grounded in an integrated view of not just technology planning, but the full spectrum of planning disciplines to include, but not limited to, mission/business, IT resources, capital, security, infrastructure, human capital, performance, and records planning.

Planners provide facilitation and integration to enable this collaborative planning discipline, and work with specialists and subject matter experts from these planning groups in order to formulate a plan of action that not only meets needs but is also implementable within financial, political, and organizational constraints. In addition, planners have an important role to play in the investment, implementation, and performance measurement activities and decisions that result from this integrated planning process.

The *Collaborative Planning Methodology*, shown in Figure 1, is a simple, repeatable process that consists of integrated, multi-disciplinary analysis that results in recommendations formed in collaboration with sponsors, stakeholders, planners, and implementers. This methodology includes the master steps and detailed guidance for planners to use throughout the planning process. Architecture is but one planning discipline included in this methodology. Over time the methods and approaches of other planning disciplines will continue to be interwoven into this common methodology to provide a single, collaborative approach for organizations to use.

The *Collaborative Planning Methodology* is the next generation replacement for the *Federal Segment Architecture Methodology (FSAM)*. As the replacement for the *FSAM*, the *Collaborative Planning Methodology* has been designed to be more flexible, more widely applicable, and more inclusive of the larger set of planning disciplines.

The *Collaborative Planning Methodology* is intended as a full planning and implementation lifecycle for use at all levels of scope defined in the *Common Approach to Federal Enterprise Architecture*: International, National, Federal, Sector, Agency, Segment, System, and Application.

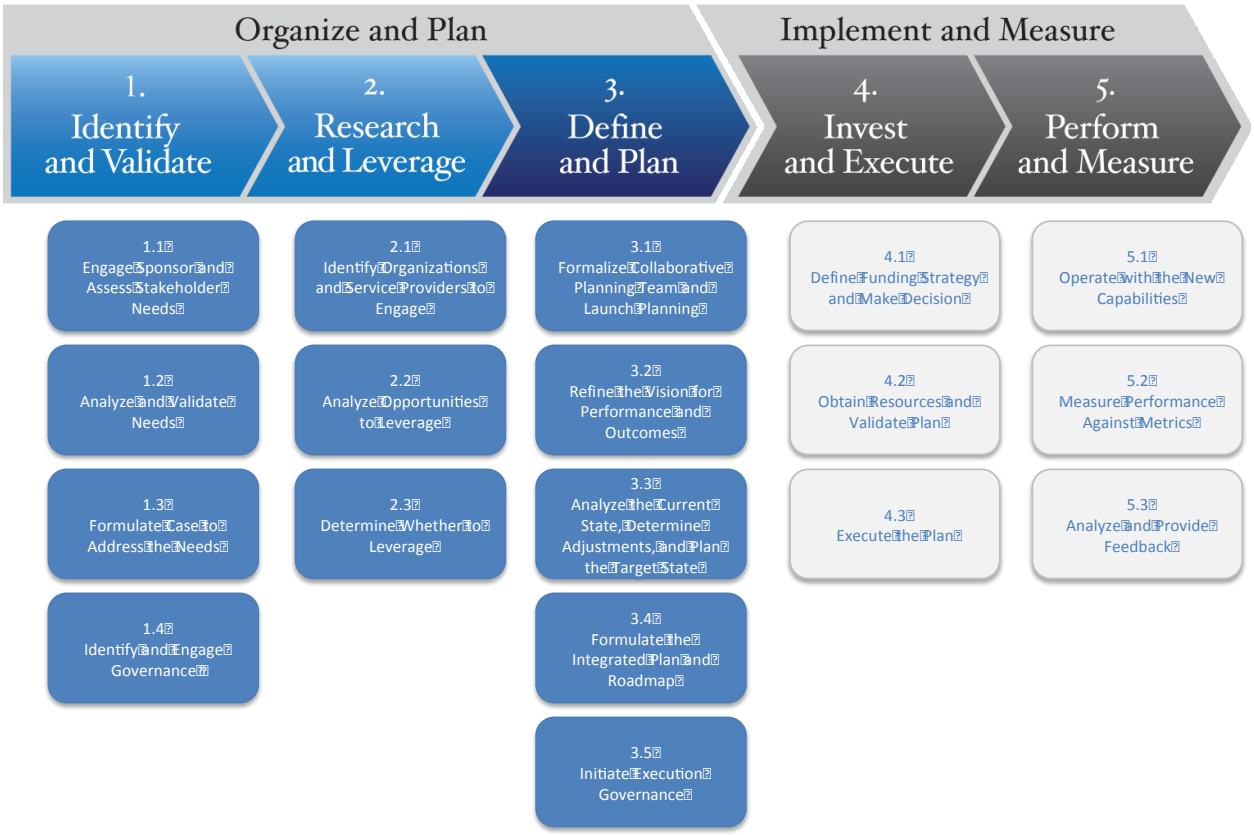


Figure 1: Collaborative Planning Methodology (CPM)

The *Collaborative Planning Methodology* consists of two phases: (1) *Organize and Plan* and (2) *Implement and Measure*. Although the phases are shown as sequential, in fact there are frequent and important iterations within and between the phases. In the first phase, planners serve a key role facilitating the collaboration between sponsors and various stakeholders to clearly identify and prioritize needs, research other organizations facing similar needs, and formulate the plans to address the stated needs. In the second phase, planners shift into a participatory role, supporting other key personnel working to implement and monitor change related activities. As part of the second phase of the methodology, planners specifically support investment, procurement, implementation, and performance measurement actions and decisions.

The *Collaborative Planning Methodology* is stakeholder-centered with a focus on understanding and validating needs from sponsor and stakeholder perspectives, planning for those needs, and ensuring that what is planned ultimately results in the intended outcomes (Step 1). Additionally, this methodology is structured to embrace the principles of leverage and reuse by assisting planners in determining whether there are other organizations that have previously addressed similar needs, and

whether their business model, experiences, and work products can be leveraged to expedite improvement (Step 2).

Ultimately, the *Collaborative Planning Methodology* helps planners work with sponsors and stakeholders to clearly articulate a roadmap that defines needs, what will be done to address those needs, when actions will be taken, how much it will cost, what benefits will be achieved, when those benefits will be achieved, and how those benefits will be measured (Step 3). The methodology also helps planners support sponsors and stakeholders as they make decisions regarding which courses of action are appropriate for the mission, including specific investment and implementation decisions (Step 4). Finally and perhaps most importantly, the methodology provides planners with guidance in their support of measuring the actual performance changes that have resulted from the recommendations, and in turn, using these results in future planning activities (Step 5).

The five steps of the *Collaborative Planning Methodology* are detailed in the following sections.

3 Step 1: Identify and Validate

3.1 Purpose

The purpose of this step is to identify and assess what needs to be achieved, understand the major drivers for change, and then define, validate, and prioritize the mission and goals with stakeholders and operational staff. During this step, the stakeholder needs and the operational requirements are validated so that ultimately, all stakeholder groups are working towards the same, well understood, validated outcome. Initial performance metrics are created to begin focusing the measurement of success to be consistent across stakeholder groups. In this step, a sponsor for the planning effort is identified. The sponsor can range in levels of scope from an executive leader to a functional leader or even an application owner.

An additional purpose of this step is to identify and engage appropriate governance.

3.2 The Planner's Role

In this step, planners (architects and other planners) facilitate a direct collaboration between the sponsor and stakeholders as they work together to define, validate, and prioritize their needs, and build a shared vision and understanding. In doing so, planners analyze stated needs in the context of overarching drivers to help aid decision makers in their assessment of whether stated needs are feasible and realistic. Since these needs shape the scope and strategic intent for planning, it is imperative that the sponsor and stakeholders agree on the needs before beginning subsequent planning steps.

In addition to identifying needs, planners work with the sponsor and stakeholders to establish target performance metrics that will ultimately be used to determine if the planned performance has been achieved.

Once needs are identified and validated, planners support the sponsor in identifying and initiating appropriate governance. Who makes the decisions and when those decisions will be made is important to the timing and buy-in of recommendations for change.

3.3 Outcome

At the end of Step 1, the key outcomes are (1) identified and validated needs, (2) an overarching set of performance metrics, and (3) a determination of who (governance) will ultimately oversee and approve recommended changes to meet those needs.

4 Step 2: Research and Leverage

4.1 Purpose

The purpose of this step is to identify organizations and service providers that may have already met, or are currently facing needs similar to the ones identified in Step 1, and then to analyze their experiences and results to determine if they can be applied and leveraged or if a partnership can be formed to address the needs together. In alignment with the "Shared First" principle, it is at this point that planners consult both internal and external service catalogs for pre-existing services that are relevant to the current needs. In some instances, an entire business model, policy, technology solution, or service may be reusable to address the needs defined in Step 1 – an important benefit in these cost-constrained, quickly evolving times. Based on this analysis, sponsors and stakeholders determine whether or not they can leverage the experiences and results from other organizations.

4.2 The Planner's Role

Planners facilitate the research of other organizations and service providers to assess whether they have similar needs and whether these organizations have already met these needs or are currently planning to meet these needs. Planners lead the assessment of the applicability of the other organizations' experiences and results and help determine whether there are opportunities to leverage or plan together. Once these organizations and their needs and experiences have been identified and assessed, planners formulate a set of findings and recommendations detailing the applicability and opportunity for leverage. These findings and recommendations are submitted to the sponsor who engages governance with this information as appropriate.

4.3 Outcome

At the conclusion of Step 2, planners, the sponsor, and stakeholders have a clear understanding of the experiences and results of other organizations, and the sponsor and / or governance have determined whether or not these experiences should be leveraged to meet the needs being considered as part of the planning effort. In some instances, another organization may be currently planning for similar needs and a partnership can be formed to collectively plan for these needs. The decision to leverage or not has a significant impact on the planning activities in Step 3. For instance, if the organization determines

that it can leverage policies and systems from another organization in order to meet its own needs, these policies and systems become a critical input to planning in Step 3.

5 Step 3: Define and Plan

5.1 Purpose

The purpose of this step is to develop the integrated plan for the adjustments necessary to meet the needs identified in Step 1. Recommended adjustments could be within any or all of the architecture domains: strategy, business, data, applications, infrastructure, or security.

The integrated plan defines what will be done, when it will be done, how much it will cost, how to measure success, and the significant risks to be considered. Additionally, the integrated plan includes a timeline highlighting what benefits will be achieved, when their completion can be expected, and how the benefits will be measured. It is during this step that analysis of current capabilities and environments results in recommended adjustments to meet the needs identified in Step 1. The formal design and planning of the target capabilities and environment is also performed during this step.

In addition to the integrated plan, the architecture, capital planning, security, records management, budget formulation, human capital, and performance compliance documents are developed based on the analysis performed in Step 3. The end outcome is an integrated set of plans that can be considered and approved by the sponsor and governance.

5.2 The Planner's Role

Architects lead the development of the architecture by applying a series of analysis and planning methods and techniques. Through this process, planners work on each of the architecture domains (strategy, business, data, applications, infrastructure, and security) and produce artifacts to capture, analyze, and visualize the plans for change. Most important is the architect's efforts to synthesize the planning into recommendations that can be considered and approved by the sponsor and governance.

During the development of the architecture, architects facilitate the interaction with other planning disciplines (e.g., budget, CPIC, security) so that each discipline's set of plans is incorporated into a cohesive set of recommendations to meet the needs stated in Step 1. Throughout these efforts, planners develop the integrated plan and roadmap to reflect the course of action that has been determined through these planning activities.

5.3 Outcome

At the end of Step 3, the sponsor and stakeholders will possess an integrated set of plans and artifacts defining what will be done, when it will be done, what and when benefits will be achieved, and an estimated cost. This set of plans should be synthesized into discrete decision-making packages for the appropriate sponsor and governance given financial, political, and organizational constraints.

6 Step 4: Invest and Execute

6.1 Purpose

The purpose of this step is to make the investment decision and implement the changes as defined in the integrated plan. Many groups participate in this step, however, it is important to note that these groups will need to work as a coordinated and collaborative team to achieve the primary purpose of this step: to successfully implement the planned changes.

6.2 The Planner's Role

In this step architects are in a support role, assisting in investment and implementation activities by providing information to aid in decisions, and to support interpretation and revision of plans from Step 3. Architects may be required to continue research and analysis into other organizations and their experiences (Step 2), update plans (Step 3), or re-engage stakeholders for feedback on desired outcomes (Step 1). Throughout the investment and implementation, architects provide continuing support such as interpreting the plans, making changes to the plans, supporting decision-making, and ensuring that plans are followed and architectural requirements are met. The involvement of architects does not cease at the conclusion of planning in Step 3.

6.3 Outcome

During Step 4, a decision is made concerning the investment in the changes that were planned in Step 3. At the end of Step 4 the recommendations for addressing the defined needs have been implemented. If the investment is not approved, planners, sponsor, and stakeholders return to previous steps to alter the recommendations and plans for future consideration. It is important to reiterate that during the implementation (Step 4) there could be a variety of changes to the integrated plans (Step 3) including, but not limited to, policy changes, organizational changes, technology changes, process changes, and resource changes.

7 Step 5: Perform and Measure

7.1 Purpose

During Step 5 the mission is operated with the new capabilities planned in Step 3 and implemented in Step 4. The purpose of Step 5 is to operate the mission and measure performance outcomes against identified metrics (Step 1).

7.2 The Planner's Role

Planners may not be the keeper of the actual performance data, but they leverage available performance data to assess whether the implemented capabilities achieve desired and planned performance. Feedback from this step can feed into future planning efforts as well as immediate planning and implementation adjustments as necessary. Feedback may also impact more immediate changes in plans that may be considered by governance, including configuration management.

7.3 Outcome

At the end of Step 5, the new capabilities as planned in Step 3 and implemented in Step 4 will be operational. The key outcome of this step is measured performance outcomes against identified metrics from Step 1.

8 Overview of the Consolidated Reference Model

The Consolidated Reference Model of the Federal Enterprise Architecture Framework (FEAF) equips OMB and Federal agencies with a common language and framework to describe and analyze investments. It consists of a set of interrelated "reference models" designed to facilitate cross-agency analysis and the identification of duplicative investments, gaps and opportunities for collaboration within and across agencies. Collectively, the reference models comprise a framework for describing important elements of federal agency operations in a common and consistent way. Through the use of the FEAF and its vocabulary, IT portfolios can be better managed and leveraged across the federal government, enhancing collaboration and ultimately transforming the Federal government.

The five reference models in version 1 the Federal Enterprise Architecture have been regrouped and expanded into six in the current version of the Federal EA.

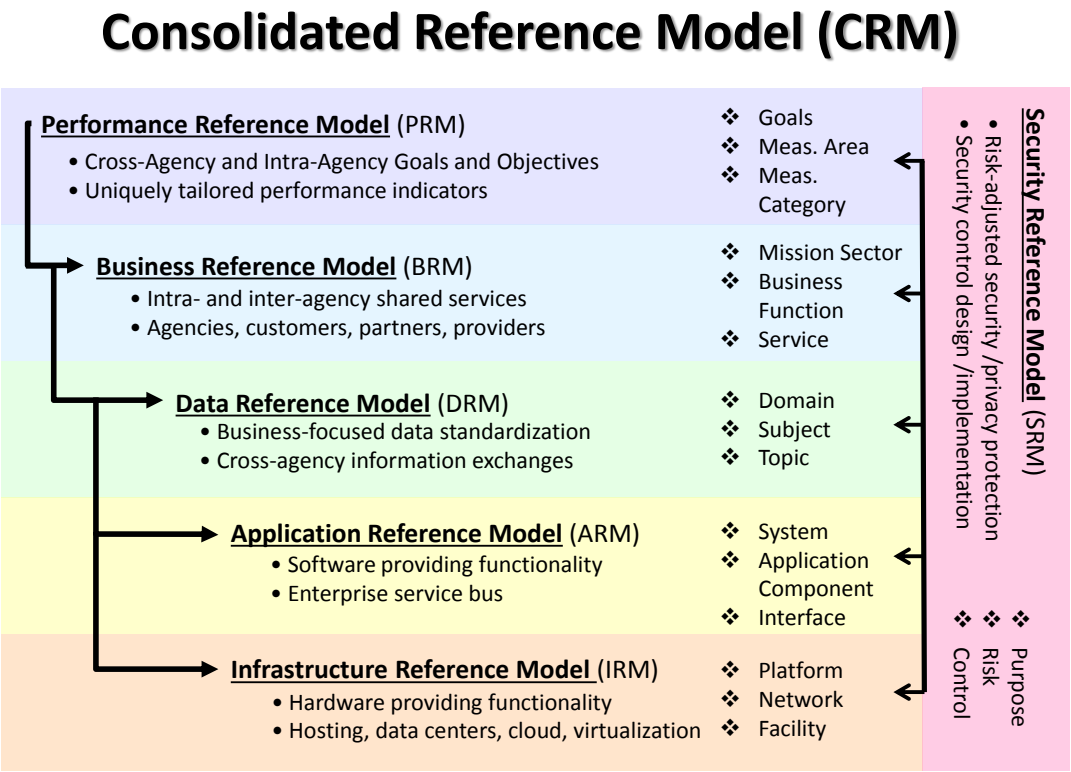


Figure 2: Consolidated Reference Model

The **Performance Reference Model (PRM)** links agency strategy, internal business components, and investments, providing a means to measure the impact of those investments on strategic outcomes.

The **Business Reference Model (BRM)** describes an organization through a taxonomy of common mission and support service areas instead of through a stove-piped organizational view, thereby promoting intra- and inter-agency collaboration.

The **Data Reference Model (DRM)** facilitates discovery of existing data holdings residing in "silos" and enables understanding the meaning of the data, how to access it, and how to leverage it to support performance results.

The **Application Reference Model (ARM)** categorizes the system- and application-related standards and technologies that support the delivery of service capabilities, allowing agencies to share and reuse common solutions and benefit from economies of scale.

The **Infrastructure Reference Model (IRM)** categorizes the network/cloud related standards and technologies to support and enable the delivery of voice, data, video, and mobile service components and capabilities.

The **Security Reference Model (SRM)** provides a common language and methodology for discussing security and privacy in the context of federal agencies' business and performance goals.

These reference models provide standardized categorization for strategic, business, and technology models and information. Using a common language to describe investments supports analysis and reporting across agency Enterprise Architectures and facilitates identification of opportunities for sharing and reuse of services and applications across agencies. Each reference model has its own taxonomy, methods, touch points, and use cases that provide examples of how the reference model can be applied.

The relationships between the reference models are important to understanding the overall CRM and its ability to provide value to the Federal Government. This is illustrated through the entity diagram of the meta-model below. The PRM is initiates the line of sight from the agency strategic plan, through the BRM, to the rest of the Enterprise Architecture. The SRM is ubiquitous, informing decisions made throughout the other sub-architectures to ensure that security is baked into IT systems from the beginning.

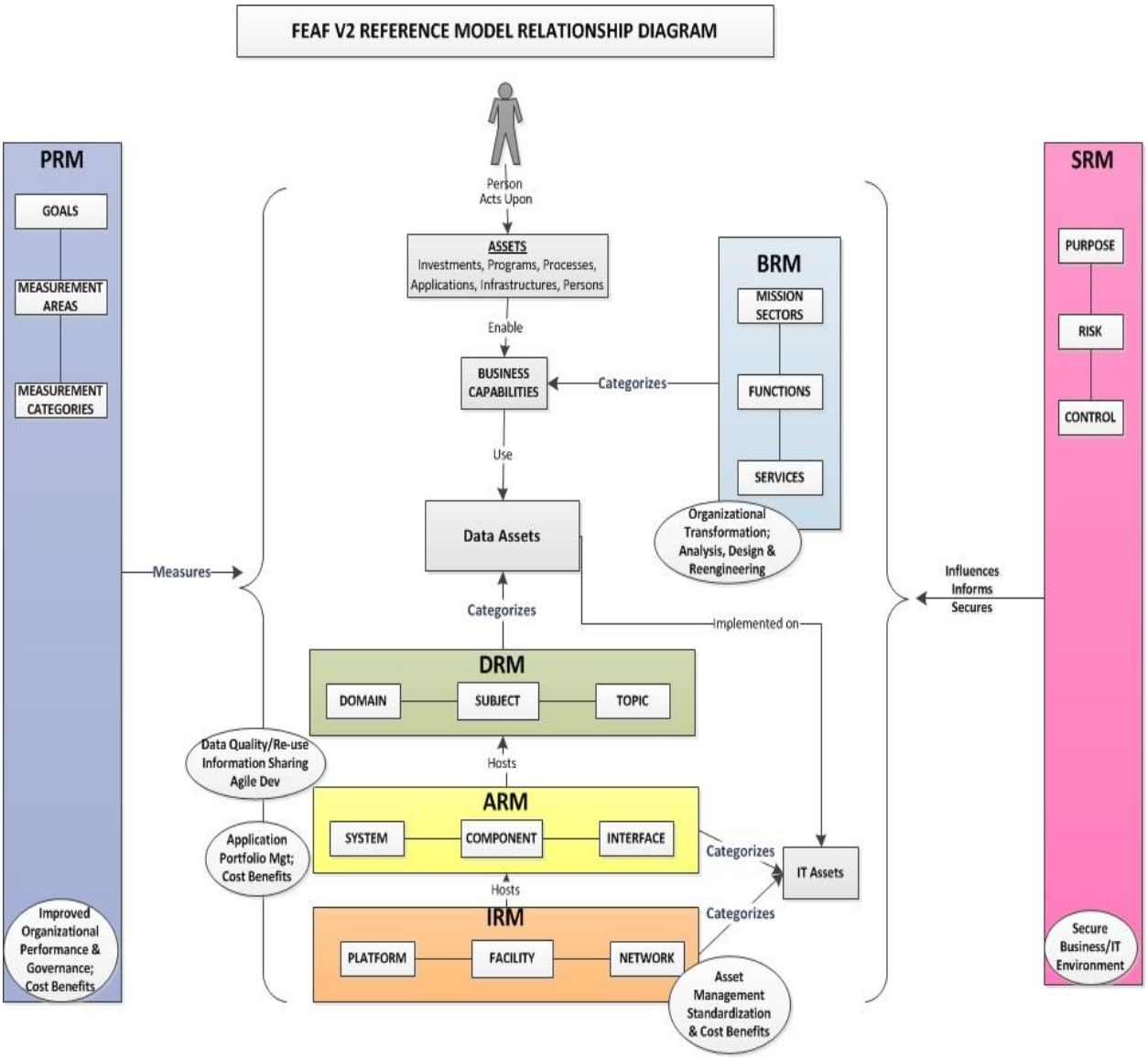


Figure 3: Consolidated Reference Model Relationship Diagram

9 Introduction to the Performance Reference Model

9.1 Purpose of the Performance Reference Model

The Performance Reference Model (PRM) is designed to provide linkage between investments or activities and the strategic vision established by agencies and the Federal government. Historically, linking information management investments and activities has been anecdotal due to a lack of standard approach to describing Agency and cross agency performance attributes. The GPRA Modernization Act of 2010 requires the government to publish performance information through a central web site and make strategic plans and performance reports available in machine readable formats. This advance enables more comprehensive and consistent linking of investments and activities to Agency strategic goals and objectives, Agency priority Goals, Cross Agency Priority goals and management areas of focus. The PRM leverages the requirements of the GPRA Modernization Act to establish mechanisms to link directly to the authoritative performance elements published in compliance with the law and provides the means for use of future developments in the mandated central performance website Performance.gov.

9.2 Structure of the Performance Reference Model

There are three areas to the Performance Reference Model. The first is the Goal. This enables grouping of investments and activities through a common and authoritative framework established by agencies in compliance with OMB direction and the GPRA Modernization Act. It allows the identification of common performance elements across investments or activities, and in the future will enable cross-platform information linkages between systems such as Performance.gov and the IT Dashboard. This linkage provides the logical relationships necessary to consistently provide much richer insights into details of the supported performance areas than previously feasible.

The second area of the Performance Reference Model is Measurement Area. This describes the manner in which the investment or activity supports the achievement of the supported performance element identified by the Agency Goal. Measurement Areas apply to the more detailed performance indicators associated with the investment of activity rather than the functions of the investment or activity. Investment or activity performance indicators should have a clear linkage to the activities, of course, but it is important to recognize that investments or activities may align to multiple measurement areas.

The third area, Measurement Category, refines Measurement Area. Any Measurement Category may be applied to any Goal.

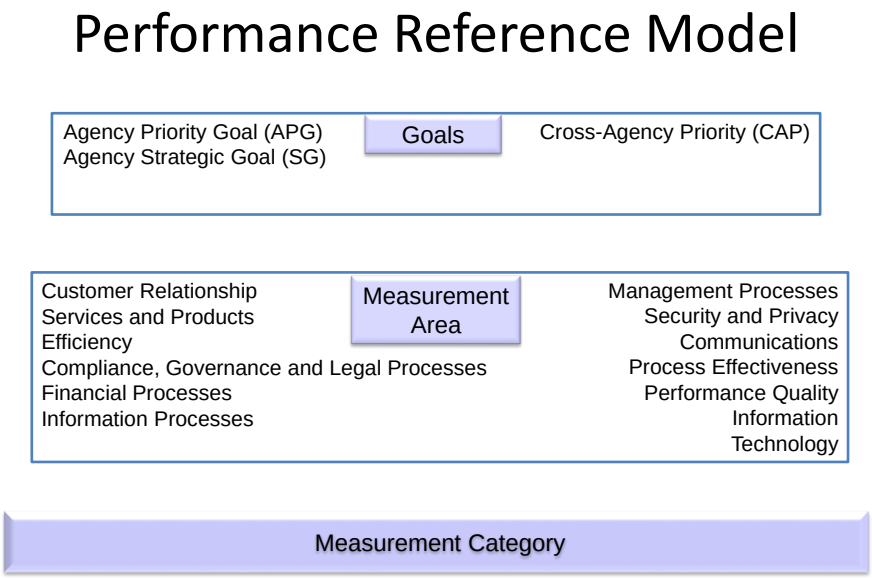


Figure 4: High Level PRM Taxonomy

10 Using the Performance Reference Model Taxonomy

10.1 Integrating CPIC (Exhibit 300) Performance Reporting with the FEA PRM

As part of Exhibit 300 investment proposals, federal agencies are required to:

Describe the relationship between investment and agency strategic goals. A narrative explanation of the investment's specific contribution to mission delivery and management support functions is required in Section B for the Exhibit 300A. Investment owners must identify how the investment contributes to the agency target architecture and links to performance objectives in the published agency strategic plan. The PRM code for the most closely associated performance objective is required.

Provide investment-specific performance measures that quantify the intended performance benefits. Each measure must be categorized using a FEA Performance Measurement Category, and investment owners must ensure that the measures are balanced and drawn from multiple measurement categories. Performance metrics will be reported on the IT Dashboard.

Report on investment results using these measures monthly, quarterly, semi-annually and annually.

11 PRM Touchpoints with other Reference Models

The PRM, like all other reference models, is intended to work in concert with other reference models. The combined descriptive qualities of the multiple perspectives afforded by assigning different reference model perspectives to investments or activities can provide rich insights into what, why and how the investments or activities are undertaken. Previous versions of the PRM included mission function characteristics that were redundant to the BRM. In this version of the PRM the Measurement Category codes have been streamlined to better identify the means by which performance is achieved. Including BRM and PRM mappings with an investment or activity provides information about the strategic basis (why) through the Agency Goal, the means (how) through the measurement category, and the mission functions involved (what) through the BRM taxonomy. Additional mappings to other reference models provide further context for the investment or activity with the SRM providing information about risk, the DRM about the information involved and the ARM and IRM providing the technical details about the implementation.

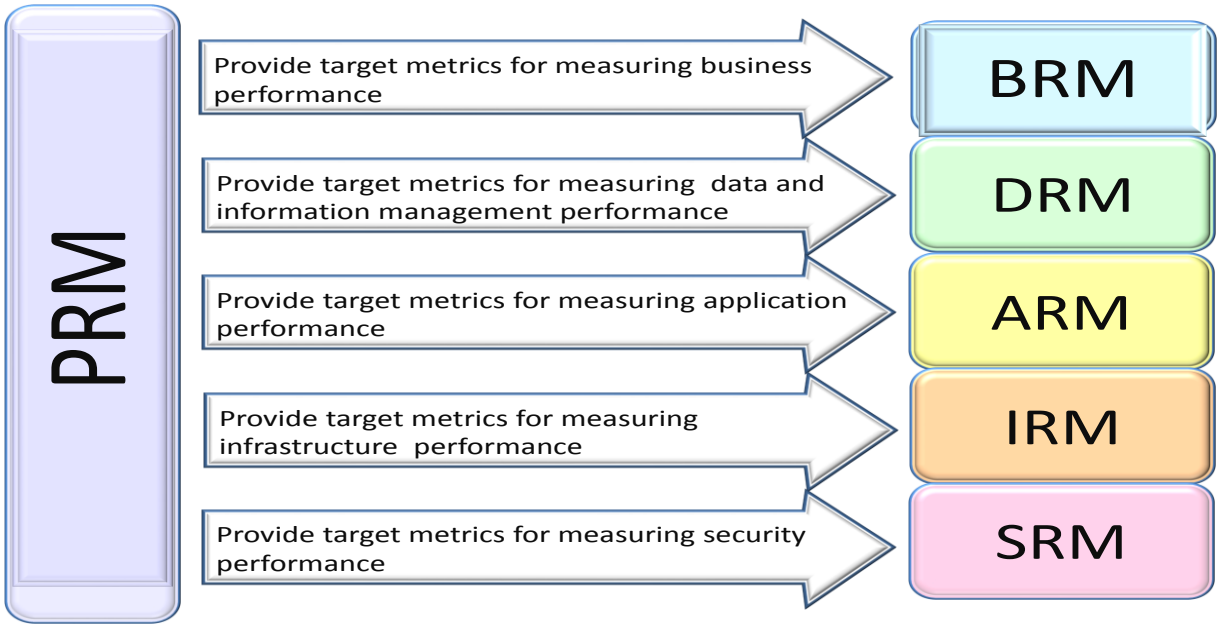


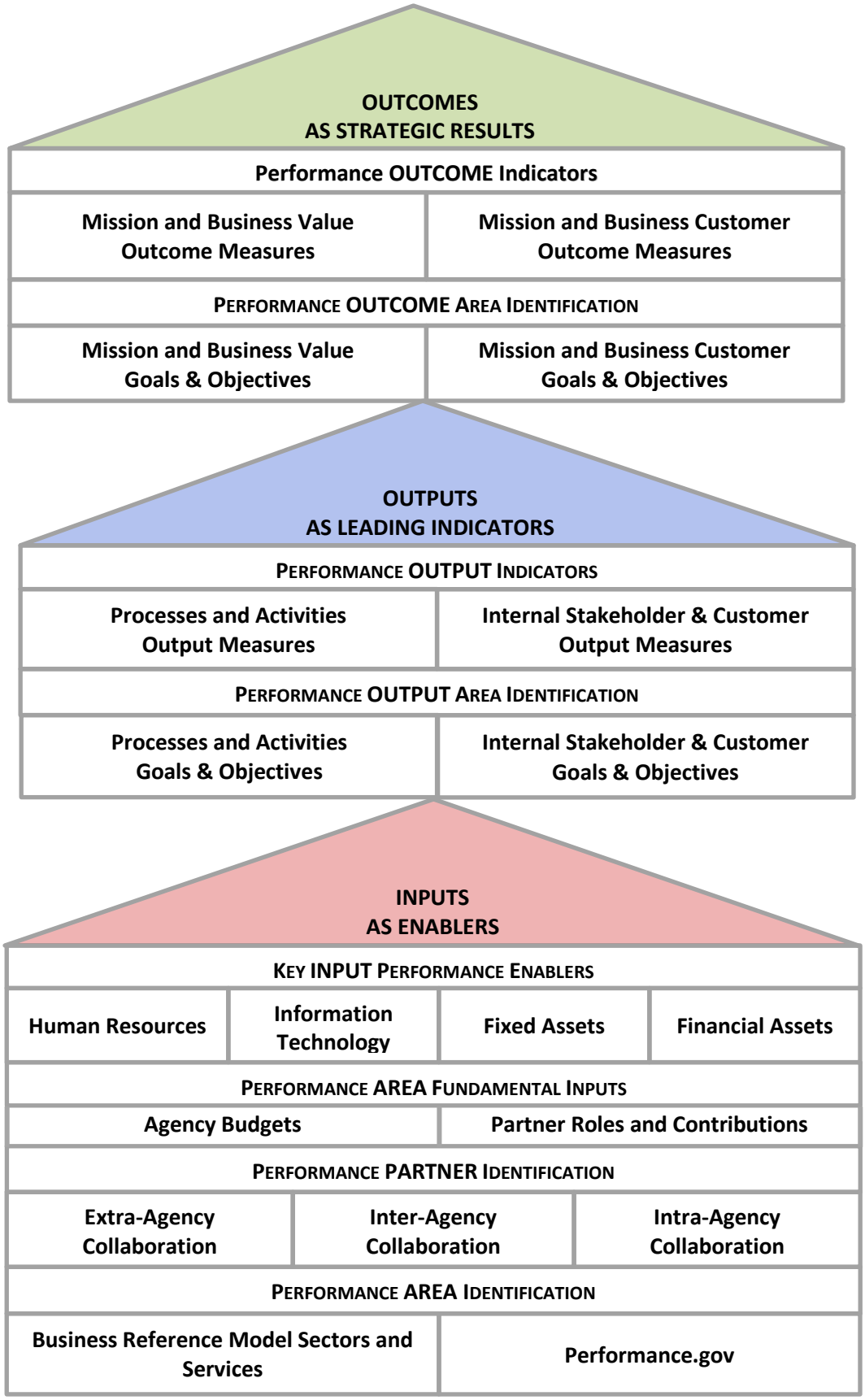
Figure 5: PRM Touchpoints with other Reference Models

12 Associated Methods/Best Practices for the PRM

12.1 Line of Sight

Central to the value of the PRM is the concept of line of sight. Line of sight is the idea that the work done at lower levels of detail has a clear path to the outcomes of the agency. The PRM Line of Sight essentially forms a value chain for tracing lower level investments and activities to higher level

outcomes. The PRM provides significant capability in regard to line of sight. The illustration below demonstrates the key components of the PRM Line of Sight.


OUTCOMES
AS STRATEGIC RESULTS
Performance OUTCOME Indicators
Mission and Business Value Outcome Measures
Mission and Business Customer Outcome Measures
PERFORMANCE OUTCOME AREA IDENTIFICATION
Mission and Business Value Goals & Objectives
Mission and Business Customer Goals & Objectives
OUTPUTS
AS LEADING INDICATORS
PERFORMANCE OUTPUT INDICATORS
Processes and Activities Output Measures
Internal Stakeholder & Customer Output Measures
PERFORMANCE OUTPUT AREA IDENTIFICATION
Processes and Activities Goals & Objectives
Internal Stakeholder & Customer Goals & Objectives
INPUTS
AS ENABLERS
KEY INPUT PERFORMANCE ENABLERS
Human Resources
Information Technology
Fixed Assets
Financial Assets
PERFORMANCE AREA FUNDAMENTAL INPUTS
Agency Budgets
Partner Roles and Contributions
PERFORMANCE PARTNER IDENTIFICATION
Extra-Agency Collaboration
Inter-Agency Collaboration
Intra-Agency Collaboration
PERFORMANCE AREA IDENTIFICATION
Business Reference Model Sectors and Services
Performance.gov

12.2 Selecting a Balanced Set of Exhibit 300 Performance Measures

With the revision of the FEA PRM, there is now a requirement to reclassify Exhibit 300 performance measures based on the revised FEA PRM measurement categories. The overall purpose of performance measures is to provide detailed insight into the value proposed and realized by the investment. When measures intuitively align with milestones and narrative, the reviewer can more easily envision what value the investment achieves or will achieve, as well as when proposed enhancements in benefits will come on line and begin to realize value.

A methodology for selecting and classifying a balanced set of Exhibit 300 performance measures using the revised FEA PRM is provided below.

The first step in selecting performance measures, or in reviewing the current performance measures for an investment, is to compare investment narrative, milestones, and measures with each other to ensure that they are mutually reinforcing, that is, that they tell the same story. Part I, specifically in the narrative blocks, presents the overall context in which the investment will be understood by reviewers. The language used to describe milestones and performance measures, as well as the performance measures themselves, provided in Part X Section C, should be designed to reinforce the relevance of planned spending to Part I narrative and to showcase achievements to date.

In the Exhibit 300B, Section C, investment owners are required to provide operational performance metrics of two essential types: *Results Specific* and *Activities and Technology Specific*.

Results-specific measures should reinforce the benefits summarized in the narrative or substantiate technology cost requirements. If a new capability will result in a significant reduction in the time required to complete a particular customer service, for example, the planned business cycle time reductions need to be emphasized in the narrative and reinforced in the investment performance measures. If a new technology capability will result in a significant increase in electronic workload, then the corresponding needed increases in infrastructure should be described as well as included in the budget.

Technology-specific measures should provide insight into the technology cost drivers for the investment or provide information about the soundness of its performance. For example, a capability that requires an investment in full fault tolerance during periods of high demand would indicate the importance of performance measures to show whether the investment is performing at the required extremely high availability standard.

13 PRM Summary

Simply put, the Agency Goal provides the means to identify the strategic element supported by the activity or investment while the Measurement Category identifies how the activity or investment supports that goal. Using these two aspects of the Performance Reference Model it is now possible to understand how multiple investments or activities work in complementary fashion to support Agency or cross-agency performance. This combined structure is useful for focusing investment or activity purpose

on larger strategic contexts. Performance indicators at the investment or activity level should clearly align with the strategic elements identified in the Agency Goal and Measurement Category.

The detailed taxonomy with definitions is available in Taxonomy G.

14 Introduction to the Business Reference Model

14.1 Purpose of the Business Reference Model

The Business Reference Model (BRM) is a classification taxonomy used to describe the type of business functions and services that are performed in the Federal Government. By describing the Federal Government using standard business functions rather than an organizational view, the BRM promotes cross-government collaboration. It enables business and IT leaders to discover opportunities for cost savings and new business capabilities that help to achieve strategic objectives. The BRM describes the "What we do" of the Federal enterprise through the definition of outcome-oriented and measurable functions and services.

While the BRM provides a standardized way of classifying government functions, it is only a model; its true utility and value is realized when it is applied and effectively used in business analysis, design and decision support that help to improve the performance of an agency, bureau or program.

14.2 Structure of the Business Reference Model

The BRM taxonomy is structured as a three-layer hierarchy representing Executive Branch Mission Sectors, Business Functions and Services.

> **Mission Sector** – Identifies the ten business areas of the Federal Government in the *Common Approach to EA*
>
> **Business Function** – Describes what the Federal government does at an aggregated level, using the budget function classification codes provided in OMB Circular A-11
>
> **Service** – Further describes what the Federal government does at a secondary or component level

The choice of these particular three layers for the taxonomy enables aggregation and analysis of IT investments and applications for a variety of different purposes. Including budget function classification codes in the reference model enables detailed analysis of IT investments along the same lines as budget analysis is performed for all other government investments. Including services in the reference model facilitates the search for reusable or sharable applications or components to reduce redundancy and costs for providing services to agencies and citizens.

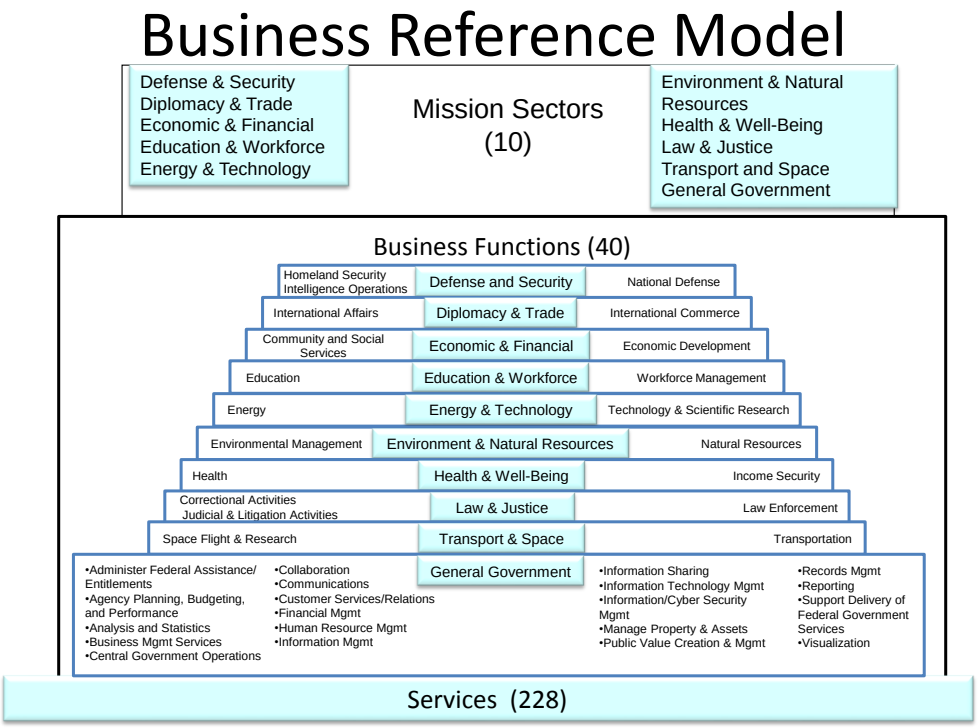


Figure 6: High Level BRM Taxonomy

15 Using the Business Reference Model Taxonomy

One of the primary purposes of enterprise architecture is to support and improve organization-wide strategic planning and decision-making. The BRM is designed to provide agencies with a standard means to categorize their capital investments, identify areas for collaboration, consolidation and reuse based on the business functionality being delivered, and help improve the overall IT architecture to better enable mission outcomes. The BRM also provides decision-support capabilities to stakeholders and different levels of staff, within and between agencies.

15.1 Identifying opportunities to share services government-wide

The BRM allows agencies and the Office of Management and Budget (OMB) to identify projects and investments across the Federal Government that support a common business purpose, highlighting opportunities for collaboration and reuse of shared services government-wide.

15.2 Reducing costs by eliminating duplication within the enterprise

The BRM benefits the agency at all organizational levels, from executives to developers.

> **Executives and Managers**: Use of a standardized business taxonomy such as the BRM enables executives and managers to see the gaps and redundancies within their enterprise. These gaps

and redundancies are opportunities for cost savings and new business capabilities that help achieve the organization's strategic objectives.

Portfolio Managers: Use of the BRM as a framework for IT portfolio management ensures proper alignment of IT projects and investments to the business needs of the organization. It will also help guide the development of business cases to request and justify funding for future development and maintenance of programs, systems, and applications.

Project Managers: During the concept and planning phase of a project, the BRM allows project managers to identify current business capabilities and determine if or how the proposed project fits into the existing architecture. Project managers can also use the BRM to streamline common business processes to reduce or avoid cost, improve cycle time, and improve customer satisfaction and value. Additionally, application performance may be enhanced by finding better ways of doing business, such as sharing data sources, and developing common data retrieval and storage services.

Developers: From a development perspective, the BRM will enhance the ability for project teams to work towards a common, shareable solution for satisfying business needs. The costs associated with maintaining duplicative applications and services can be reduced by developing sharable services that can be used by more than one application or organization. Integrated service delivery approaches can also reduce the burden on the public by collecting data once and sharing it among systems, thereby reducing the burden on users of those systems.

16 BRM Touchpoints with other Reference Models

BRM is informed by the PRM and informs the other reference models. At the high level, the BRM relationship and tie-in to the other reference models is illustrated in the following table:

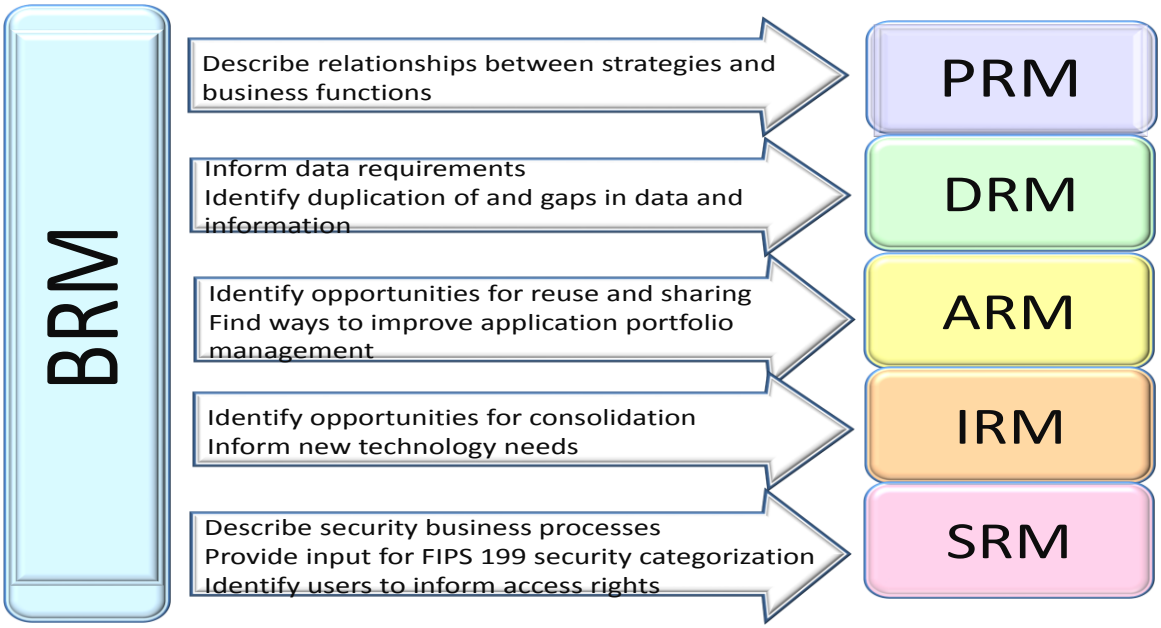


Figure 7: BRM Touchpoints with the other Reference Models

17 Associated Methods/Best Practices for the Business Reference Model

The Business Reference Model can be used in conjunction with various architecture, development, and analysis methods to provide comprehensive and standardized design, development, and governance capabilities. This section illustrates a few examples of associating the BRM with other methods.

17.1 Business Architecture for Decision Support

The BRM provides the functional foundation used in developing the business architecture. The business architecture contains information about and relationships between organizational goals, objectives, policies, organizational structures, business functions, and processes as well as business rules and policies. It may also include relationships with other architectural layers – such as data, application, technology, and security – to compose the comprehensive enterprise architecture. This enables the development of a "line of sight" (inputs – outputs – outcomes) that is used to analyze how the organization achieves its business objectives and determine where there may be gaps and redundancies in delivering the services needed to achieve strategic goals.

By defining the relationship between strategy, performance and business functions for a specific organization, the business architecture can show the relative performance of functions and whether or not each organization's function supports a strategic objective.

17.2 Business Process Modeling

Business process modeling is a central part of all the activities that lead to effective and efficient management of Federal functions. Modeling is a proven and well-accepted engineering technique. Because a model is a simplification of reality, a model can provide greater understanding of the system being developed.

Business Process Modeling and Notation (BPMN) and the Unified Modeling Language (UML) are examples of "open" industry standard notational formats that support model-based systems engineering. BPMN allows business analysts to create process diagrams that are expressive and rich enough to address complex business issues such as exception handling. As an extension of UML, BPMN has traditionally been viewed as a modeling tool, but the executable aspect of it is also highly important.

The executable counterpart to the BPMN is Business Process Execution Language (BPEL), which may be generated from BPMN. BPEL enables organizations to run business processes in an automated environment. BPEL also enables process choreography and orchestration. Business process "choreography" is the execution of independent business processes in an automated fashion using XML and web services, while orchestration is the arrangement and synchronization of those automated processes.

18 BRM Summary

The Business Reference Model (BRM) forms a key part in delivering expected outcomes and business value to an organization. By using a standard taxonomy to classify functions, investments, programs, services and other elements across the Federal Government, the BRM is useful in identifying opportunities for cost reduction, collaboration, shared services, and solution reuse in agency IT portfolios and intra- and inter-agency collaboration.

Significantly more detail about the structure, taxonomy, and associated methods of the Business Reference Model is available in Appendix B. The detailed taxonomy with definitions is available in Taxonomy H.

19 Introduction to the Data Reference Model

19.1 Purpose of the Data Reference Model

The Data Reference Model's (DRM) primary purpose is to promote the common identification, use, and appropriate sharing of data/information across the federal government. The DRM is a flexible and standards-based framework to enable information sharing and reuse via the standard description and discovery of common data and the promotion of uniform data management practices. The DRM provides a standard means by which data may be described, categorized, and shared, and it facilitates discovery and exchange of core information across organizational boundaries.

As a reference model, the DRM is presented as an abstract framework from which concrete implementations may be derived. The DRM's abstract nature will enable agencies to use multiple implementation approaches, methodologies and technologies while remaining consistent with the foundational principles of the DRM.

19.2 Structure of the Data Reference Model

The Data Reference Model taxonomy is defined by a hierarchy in three layers, as illustrated below. The top rank of the hierarchy consists of four Domains. The middle layer of the hierarchy contains twenty-two Subject elements and the lowest rank of the hierarchy includes one hundred and forty-four Topic elements. The DRM provides a structure and vocabulary for agencies to form a consensus as to how, at a Federal level, to categorize, describe, and share data.

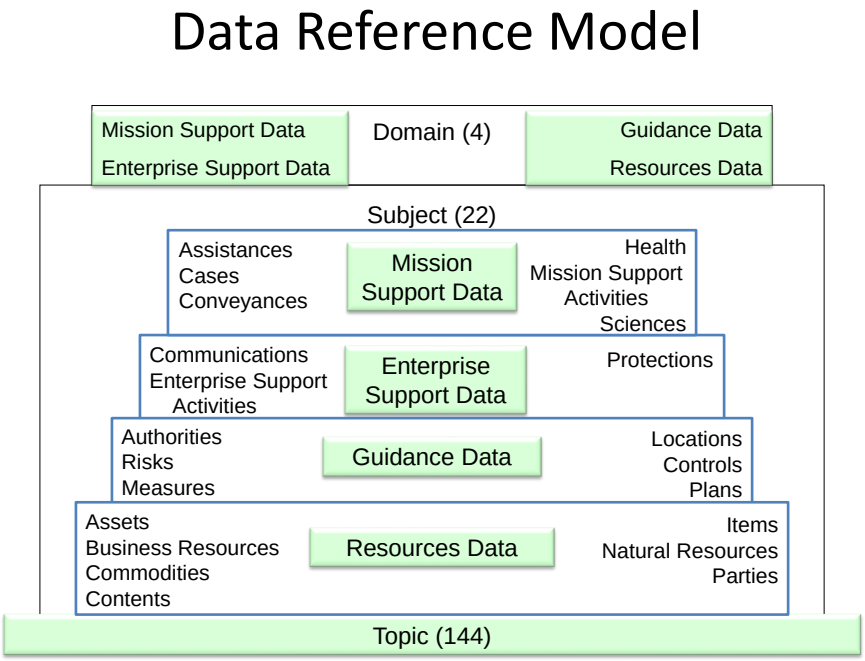


Figure 8: High Level DRM Taxonomy

As illustrated, the topic element is open and requires use of Tree Diagrams to identify how the Topic elements in the DRM taxonomy relate to the Subject and Domain elements. In the Appendix, each Domain is shown as a tree diagram, followed by definitions of the taxonomy elements in the corresponding tree.

20 Using the Data Reference Model Taxonomy

20.1 Using the DRM to Compare Data Sources across Federal Agencies

Goal: Improve the quality and depth of information available for mission performance.

Method: Compare data sources containing similar data, though possibly used for a different purpose.

Challenges:

- Finding data sources that are worth comparing
- Identifying what information is common between data sources, and thus usable for correlation

How the DRM Helps: The DRM taxonomy identifies data categories, regardless of usage context. Used in concert with the Business Reference Model (BRM) taxonomy, we can classify the data that is managed in a given data source by the mission or business context in which that data is used. Classifying a set of data sources by the DRM and BRM taxonomies produces a data set that can be searched to determine, for example, which data sources contain a common data class but use it for different business contexts. For a large set of data sources, that search capability saves considerable time over manually examining each data source to see if it contains what is required.

20.2 Using the DRM to Create a Standardized Information Exchange

Goal: Facilitate a standardized information exchange across a Community of Interest.

Method: Model the exchange and build exchange schemas using available data standards, such as NIEM.

Challenges:

- Federal, state, local, and tribal organizations typically use different data definitions and structures in the storage and exchange of like data across a community of interest.
- As data is exchanged between organizations within or across these domains, transformations or interfaces must be created for each new data source.

How the DRM Helps: Creating a standardized information exchange with agreed upon data descriptions enables each participating organization to create the necessary interface to receive or provide data only once. Existing exchange partners can use a new participant's data without having to write any interface or transformation. Also, it improves the quality of information exchange by ensuring that the source and target mapping is accurate, through the exchange model and standardized data definitions.

21 DRM Touchpoints with other Reference Models

The DRM is closely linked with the other five reference models of the Consolidated Reference Model Framework. At the high level, the DRM relationship and tie-in to the other reference models is illustrated in the following table:

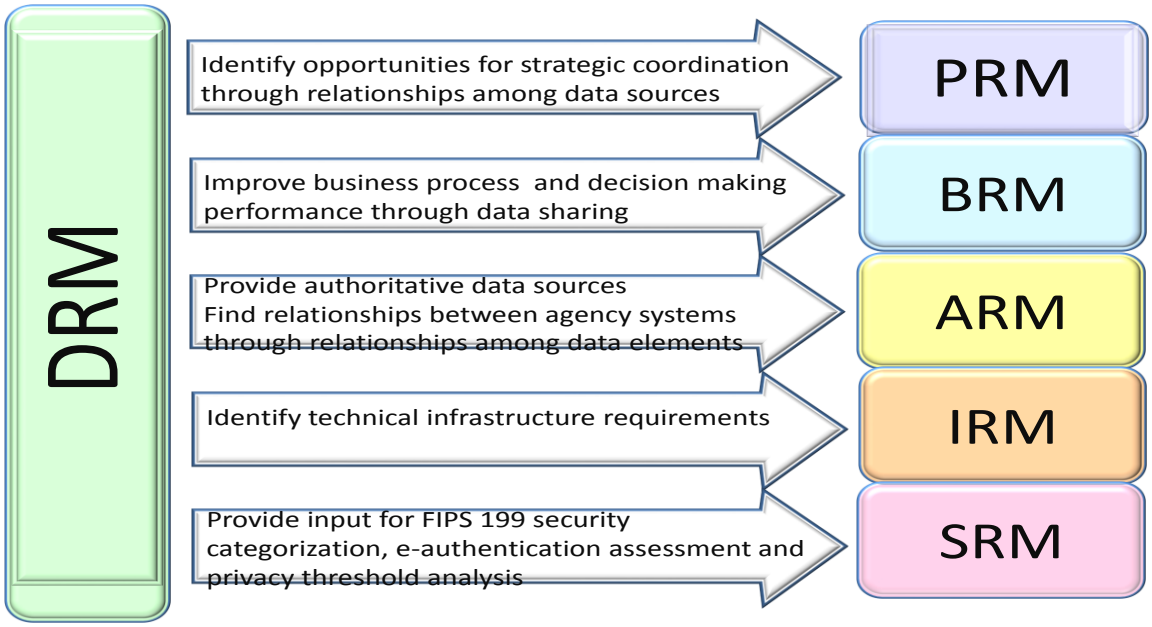


Figure 9: DRM Touchpoints with the other Reference Models

22 Associated Methods/Best Practices for the Data Reference Model

The DRM describes data and information needed to perform Federal business and mission functions by use of collective methods. There are three fundamental method areas associated with the DRM to help agencies consistently categorize, describe, and share their data: Data Description, Data Context, and Data Sharing.

22.1 Data Description

Data Description provides a means to uniformly describe data, thereby supporting its discovery and sharing. Traditionally, data description was solely focused on organizing and describing structured data. With unstructured data as the largest focus of agencies' data management challenges, the DRM Description component has been revised to focus on the larger topic of metadata, which includes both traditional structured data and unstructured data description.

The methods listed below explain best practice examples meant to inform and enhance an agency's data description processes and to align agency data practices with the FEA DRM.

- Integration Definition for Function Modeling (IDEF). The model IDEF1X is used to define a logical data model when the target deployment is known to be a relational database. www.itl.nist.gov/fipspubs/idef1x.doc
- The Open Government Group Architecture Framework (TOGAF). TOGAF® defines an Architecture Development Method (ADM) that uses the four business, application, data, and technical architecture domains. http://www.opengroup.org/togaf
- Unified Modeling Language™ (UML). UML is a mature and widely adopted technology-independent, modeling language that supports the application development life cycle. http://www.omg.org/spec/UML/
- Department of Defense Architecture Framework v2.02 (DoDAF v2.02). The DoDAF v2.02 provides detailed guidance for "fit-for-purpose" architecture development. http://dodcio.defense.gov/sites/dodaf20/
- ISO/IEC 11179. An international standard that specifies the kind and quality of metadata needed to describe data and that specifies how to manage metadata in a metadata registry. http://www.iso.org/iso/home.htm
- Dublin Core. A core metadata vocabulary intended to facilitate discovery and management of resources. http://dublincore.org/

22.2 Data Context

Context often takes the form of a set of terms (i.e., words or phrases) that are, themselves, organized in lists, hierarchies, or trees. Data Context is any information that provides additional meaning to data and an understanding to the purposes for which it was created. The Data Context method can also be called "categorization" or "classification".

Agencies and organizations participating in COIs are called upon to categorize their data. Once shared in data registries, these categorizations become vehicles for discovering data that offer value for data sharing. For an agency, the DRM taxonomy can be used to categorize core data sources (e.g., data bases, data warehouses, files) that support a particular business function.

The DRM taxonomy is not meant to be fixed and unchanging. Rather, it is flexible and scalable so that new Subjects and Topics can be added as the business model for the Federal government changes. The core categorization provided by the DRM not only includes Domains, Subjects and Topics, but also allows agencies to decompose Topics further into Agency-specific entities, as needed, for their respective business processes.

The methods listed below explain best practice examples that can be used by an agency to categorize its data and align its data practices with the FEA DRM.

- Data Asset Catalog. An agency can create a data catalog with the following steps: 1) Inventory data assets and collect the data model or structure for each asset, 2) Map the asset characteristics to the DRM Taxonomy, 3) Preserve the results in a data catalog. A data asset catalog reduces time and cost to implement change by reducing the time to locate needed data, identifying redundant data assets for decommissioning, and identifying opportunities to reuse or extend a data asset rather than creating a new data asset. The data asset catalog also

provides the foundation of an enterprise data inventory, which lists and describes all agency data sets used in the agency's information systems and is required by OMB's Policy on *Managing Government Information as an Asset*.

- Information Discovery and Search. By mapping each data asset in the agency's data asset catalog to the agency's data categorization taxonomy, an agency can enable users to discover the information they need without having to know in advance where it is or even if the particular information exists. The discovery and search capability uses the data categorization taxonomy to identify the data assets that satisfy the search criteria of the user.

22.3 Data Sharing

Data Sharing is the use of information by one or more consumers that is produced by another source other than the consumer. It supports the access and exchange of data and is enabled by capabilities provided by both the Data Context and Data Description standardization areas.

The methods listed in the table below describe the best practices used for information sharing. This guidance is meant to inform and enhance effective agency information sharing processes.

- National Information Exchange Model (NIEM). In 2005, the Department of Justice (DOJ) and the Department of Homeland Security (DHS) partnered with the Global Justice Information Sharing Initiative (Global) to develop the NIEM. NIEM is a federated information exchange framework which enables interoperability across multiple mission areas or "domains", with each domain managing its data models and content standards separately, while benefiting from central investment in tools, training, model management, and governance. See www.NIEM.gov.
- Data.gov. The purpose of Data.gov is to increase public access to high value, machine-readable datasets generated by the Executive Branch of the Federal Government. It provides descriptions of the Federal datasets (metadata), information about how to access the datasets, and tools that leverage government datasets. See www.data.gov.
- Linked Data, or Linked Open Data (LOD). The Web enables us to link related documents. Similarly it enables us to link related data. The term Linked Data, or Linked Open Data (LOD) refers to a set of best practices for publishing and connecting structured data on the Web. Key technologies that support Linked Data are URIs (a generic means to identify entities or concepts in the world), HTTP (a simple yet universal mechanism for retrieving resources, or descriptions of resources), and RDF (a generic graph-based data model with which to structure and link data that describes things in the world). See http://linkeddata.org/home.
- Information Sharing Environment Building Blocks. The Information Sharing Environment Building Blocks guidance helps organizations promote responsible information sharing. See http://ise.gov/building-blocks.

23 DRM Summary

The DRM provides guidance for agencies to leverage existing Data Assets across the government. The DRM increases the Federal government's agility in drawing out the value of information as a strategic

asset. This reference-able, conceptual approach facilitates information sharing and reuse across the Federal government.

Significantly more detail about the structure, taxonomy, and associated methods of the Data Reference Model is available in Appendix C. The detailed taxonomy with definitions is available in Taxonomy I.

24 Introduction to the Application Reference Model

24.1 Purpose of the Application Reference Model

The purpose of the Application Reference Model (ARM) is to provide the basis for categorizing applications and their components. As agencies map their current and planned Information Systems to the ARM categories, gaps and redundancies will become evident, which will aid in identifying opportunities for sharing, reuse, and consolidation or renegotiation of licenses. This information may be used in conjunction with the other Reference Models to identify these opportunities.

For the purposes of the CRM, **Application** is defined as: *Software components (including websites, databases, email, and other supporting software) resting on Infrastructure that, when aggregated and managed, may be used to create, use, share, and store data and information to enable support of a business function.*

The ARM is a categorization of different types of software, components and interfaces. It categorizes software that supports or may be customized to support business. It does not include operating systems or software that is used to operate hardware (e.g. firmware) because these are contained in the IRM. It also does not contain mission-specific categorizations for systems because that information can be obtained from mappings to the BRM.

24.2 Structure of the Application Reference Model

As seen in Figure 1, the ARM consists of three levels: Systems, Application Components, and Interfaces.

- **Systems** are discrete sets of information technology, data, and related resources, organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information in support of a specific business process. The ARM Systems category does not include mission-specific systems.
- **Application Components** are self-contained software that can be aggregated or configured to support, or contribute to achieving, many different business objectives. For example, workflow management, document management, records management and many other types of components can support multiple IT Systems and business processes.
- **Interfaces** are protocols used to transfer information from system to system.

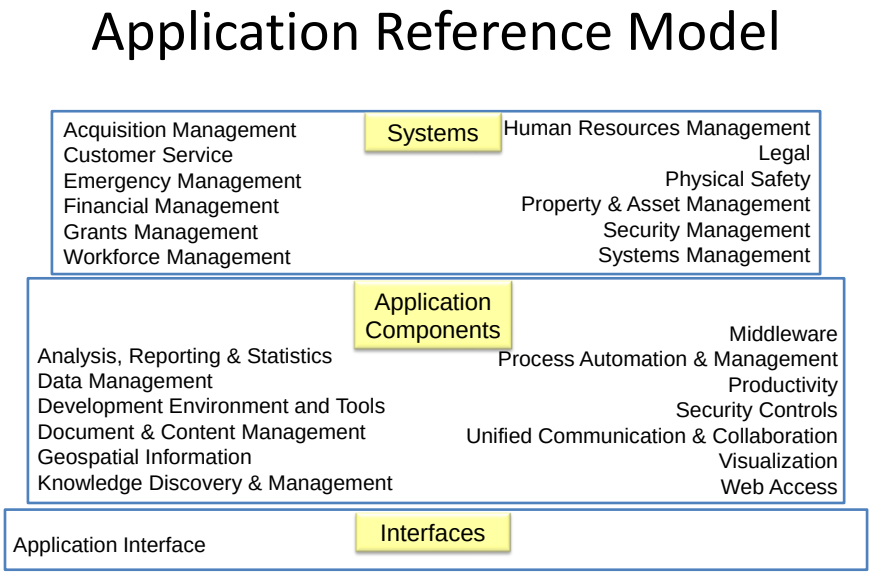


Figure 10: High Level ARM Taxonomy

25 Using the Application Reference Model

25.1 IT Cost Reduction through IT/ Application Portfolio Management

Goal: Find opportunities to reduce the cost of IT within a government agency

Method: Upon mapping systems to the ARM, look for redundancy to find opportunities to share, reuse, or consolidate information systems; or to consolidate licenses and negotiate reduced pricing. Review the mappings from across the Federal Government, if they are available, to identify opportunities for sharing and reuse that span agencies.

Challenges:

- Each agency has its own portfolio of legacy and modern information systems.
- Although the general consensus is that duplicates of information systems exist, they are difficult to identify.

How the ARM Helps: By mapping agency systems and application components to the ARM, a searchable dataset is produced so that manual information gathering is not needed. This analysis may result in consolidating instances of the same application, consolidating licenses into an agency-wide license when they are up for renewal, selecting a single new agency-wide solution that will be hosted in the cloud, or even changing business processes to enable sharing a system.

25.2 Using the ARM with the entire Consolidated Reference Model (CRM)

Goal: Determine the correct technologies to meet a well understood business need, while supporting the OMB Shared-First approach.

Method: The architects supporting the agency's efforts work with the solution team to map the project elements to the FEA CRM. Using this mapping, the architects use the repository of organizational and governmental CRM mappings to find systems, services and solutions that might meet their needs.

Challenge: Both within the agency and across the federal government, there are many existing solutions that might be potential candidates, so being able to quickly and easily navigate such information is critical.

How the CRM Helps: By using the same taxonomies to map both project needs and existing solutions across the six reference models, extensive and comprehensive information can be searched easily to identify opportunities for reuse or sharing. Then the solution team, including the business owners, can use industry standard methods to perform an objective, data-driven analysis and determine whether an existing solution is a sufficiently good fit for the environment and purpose, and if so, which one.

26 ARM Touchpoints with other Reference Models

The ARM is closely linked with the other five reference models of the Consolidated Reference Model Framework. At the high level, the ARM relationship and tie-in to the other reference models is illustrated in the following table:

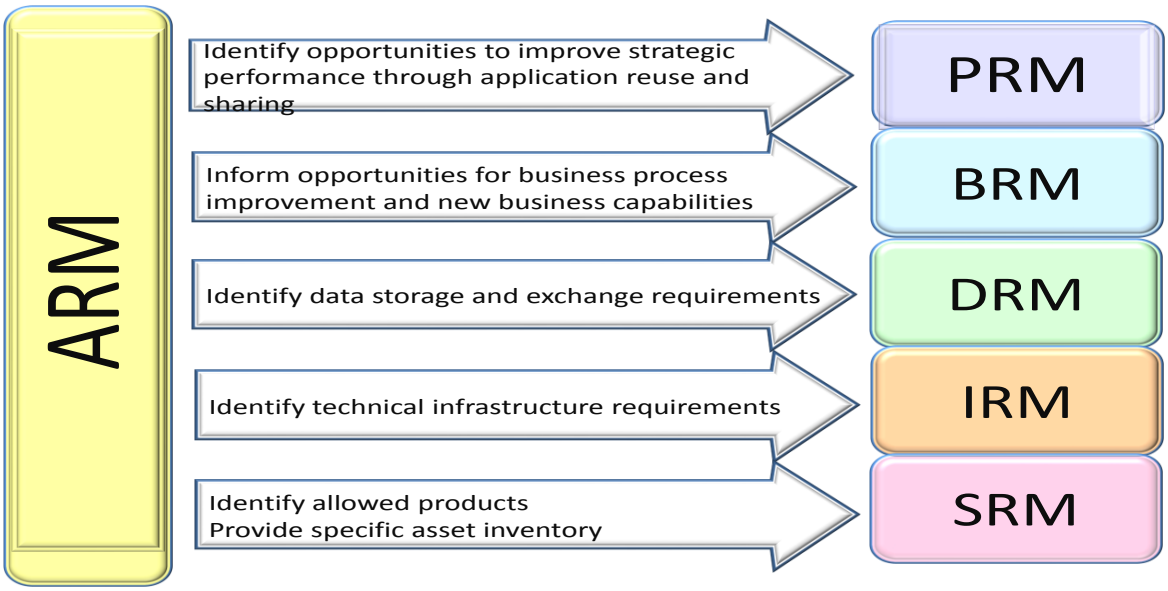


Figure 11: ARM Touchpoints with the other Reference Models

27 Associated Methods/Best Practices for the Application Reference Model

This section presents three emerging approaches that can be used in conjunction with each other to exploit the information in the implemented ARM (i.e., the ARM structure plus the agency mapping of applications and investments to it), as well as the other Reference Models. These methods are: Capability Modeling and Analysis; Service Oriented Architecture; and Portfolio Management. The sharing and reuse objectives of the FEA Reference Models are facilitated by using these methods to solve enterprise problems. In addition, the three methods enable modularization and improve the flexibility of applications and the IT acquisition process.

27.1 Capability Modeling and Analysis

Capability Modeling and Analysis is a Requirements Analysis technique that facilitates the translation of business/mission and technical requirements into discrete capabilities that lend themselves to sharing and reuse analysis (Shared-First). By casting requirements as capabilities at various levels of abstraction (meaning they may be decomposed into more detailed capabilities) and with capability dependencies modeled, the commonality across requirements is more obvious than with standard requirements analysis or business process analysis techniques. Within the context of the FEA Reference Models, capability requirements can be associated with elements and categories of the BRM for functional capabilities, the ARM for back-office and software support capabilities, and the IRM for infrastructure capabilities.

Capability Modeling and Analysis also has the advantage of modularizing the requirements so that capabilities can be combined in new ways to meet new business/mission and technical objectives. This method is a natural outgrowth of the Service Oriented Architecture (SOA) direction of OMB, the Federal CIO Council, and many Agencies. The method provides a direct analogy to the services that can be provided to meet the capability requirements – as discussed in the next section.

27.2 Service Oriented Architecture

Service Oriented Architecture (SOA) is an architectural style in which IT solutions are assembled from a collection of interacting services. This method not only provides more application flexibility because services can be more easily modified or replaced, but also reduces the cost of developing and maintaining applications because the solution design is better understood and the impact of changes is isolated. The key to success with SOA is the development of an architecture of services – a layered diagram that depicts the services and their dependencies. This is critical in the consumption/reuse of services because it establishes the boundaries between services and indicates the relationships among them.

Services can be mapped to the appropriate FEA Reference Models to assist in identifying candidate services for use in particular applications. For example, if a solution requires a document management

service, the ARM will identify other applications that have this capability or services that can satisfy this requirement. Services contained in registries or repositories should be mapped to the ARM and other reference models to facilitate the discovery process.

27.3 Portfolio Management

In the Federal Government, portfolio management is widely applied to IT investments and programs. This method has significant benefits when applied to all IT assets – in particular services and applications. To promote reuse or sharing of services, portfolio management techniques should be used to assess assets for viability into the future and to develop a service lifecycle plan for each asset. For example, to continue the use of the document management application component, each existing (legacy or COTS) document management component should be mapped to the ARM so that the reuse potential can be evaluated by potential consumers. However, if the legacy document management service is to be deprecated in the near future, this information should be associated with the service. In this way, potential consumers of the service will be informed of the lifecycle plans for the service.

Portfolio Management techniques can also be used to support application functionality consolidation by analyzing the mappings to the ARM with the associated lifecycle information. In addition, this method may facilitate the analysis for shifting application components from legacy hosting to the Cloud Computing environment (Cloud-First) as well as the analysis for moving to open-source software.

28 ARM Summary

Significantly more detail about the structure, taxonomy, and associated methods of the Infrastructure Reference Model is available in Appendix D. The detailed taxonomy with definitions is available in Taxonomy J.

29 Introduction to the Infrastructure Reference Model

29.1 Purpose of the Infrastructure Reference Model

The Infrastructure Reference Model (IRM) is the taxonomy based reference model for categorizing IT infrastructure and the facilities and network that host the IT infrastructure. The IRM supports definition of infrastructure technology items and best practice guidance to promote positive outcomes across technology implementations.

For the purposes of the CRM, **Infrastructure** is defined as: The generic (underlying) platform consisting of hardware, software and delivery platform upon which specific/customized capabilities (solutions, applications) may be deployed.

The IRM implementation enables sharing and reuse of infrastructure to reduce costs, increase interoperability across the government and its partners, support efficient acquisition and deployment, and enable greater access to information across enterprises.

In addition to providing a categorization schema for IT infrastructure assets, the IRM enables analysis of IT infrastructure assets at a Department or Agency level as well as at a Federal Government level. In the Federal context, the IRM is adopted and used to conduct Government-wide analysis of IT infrastructure assets and to identify consolidation initiatives. In the Department or Agency context, the IRM is used to drive good IT infrastructure asset management practices such as identifying end-of-life assets before they affect the mission of an organization and to identify opportunities for sharing and consolidating infrastructure.

29.2 Structure of the Infrastructure Reference Model

The IRM taxonomy is intended to provide a categorization scheme for physical IT assets, the operating systems and firmware that run them, and the locations or facilities that host the physical IT assets. The IRM is divided into three levels as shown in the figure below.

Level 1 of the hierarchy, called “Domain”, consists of three entities, Platform, Network and Facility, which are linked and related to each other to enable analysis of IT assets across the three dimensions.

Level 2 of the hierarchy, called “Area”, consists of 13 total Areas (for example, “Hardware”) linked to the three Domains in Level 1. Level 3 of the hierarchy, called “Category”, consists of 90 total Categories (for example, “Personal Computer – Laptop”) linked to the 13 Areas in Level 2.

The adaptive and loosely coupled approach of the IRM supports multiple levels of executive management, capital planning and architecture stakeholders and their analytical needs.

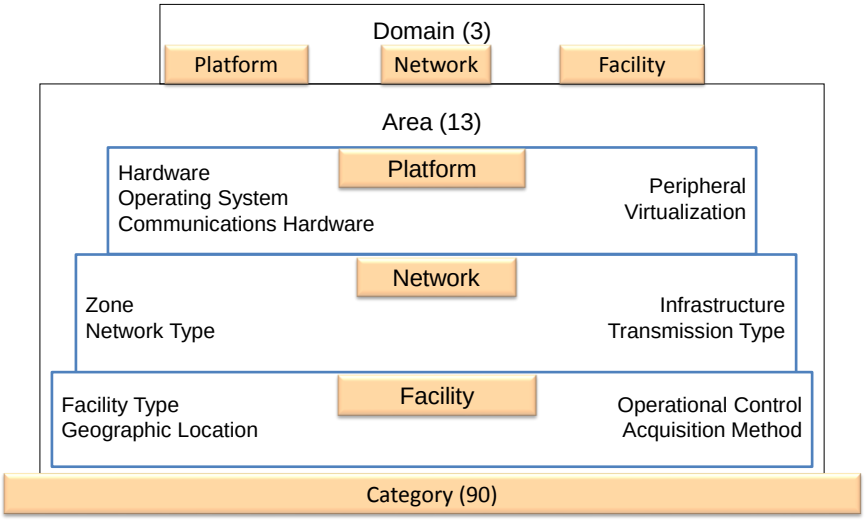


Figure 12: High Level IRM Taxonomy

30 Using the Infrastructure Reference Model Taxonomy

The Use Cases described within this section present examples of how the IRM is used to solve enterprise issues. Fundamental to using the IRM as a decision making tool is an IT infrastructure asset inventory that is categorized using the IRM.

These Use Cases provide approaches for applying the taxonomy and accompanying reference model materials to: (1) complete an IT asset management inventory; and (2) evaluate whether to consolidate infrastructure to the cloud, using the IT infrastructure asset inventory.

30.1 Using the IRM to Create an IT Asset Management (ITAM)

Goal: Improve IT resource decision-making, delivering cost efficiencies, reducing duplication/redundancy and promoting information sharing across communities of interest.

Method: Inventory, manage and refresh IT assets over their entire lifecycle (from acquisition to disposal) according to an IT Asset Management (ITAM) strategy.

Challenges:

Many information technology (IT) organizations, especially within the federal, state and local sectors, are faced with the on-going challenges of providing and managing IT services that are responsive to the ever-changing demands and needs of diverse business customers.

How the IRM Helps: Mapping an organization's IT assets to the Infrastructure Reference Model (IRM) and Application Reference Model (ARM) provides a robust technical definition, categorized by a common taxonomy, which will harmonize the islands of IT asset information collected by proprietary IT management sensor/discovery tools. ITAM provides the foundation for the infrastructure architecture consisting of computing devices, peripherals, systems, applications and IT capital investments, interwoven with the other EA architectural layers, to render a "line of sight" that equates to measurable value chains (e.g. Return on Investment (ROI) and Total Cost of Ownership (TCO)) incorporating all associated costs.

30.2 Using the IRM to Identify Opportunities for Shared Services

Goal: Identify candidates for consolidation of intra-agency commodity IT services.

Method: After developing an IT asset inventory, quantify, categorize and cross-walk the results to the reference models' taxonomy of infrastructure services and back-office application systems.

Challenges:

- Massive IT costs due to legacy and antiquated systems, as well as traditional data center and server infrastructure
- Lack of standards or lack of application of standards for sharing data and services.

How the IRM Helps: Using the IT asset inventory and IRM categorization, the agency was able to see a clear picture of duplicative infrastructure components and services in data centers that were owned and operated by the agency. Not only did the agency identify component services for internal private cloud implementation, due to security and information sensitivity requirements, but they also identified public cloud solutions that sustained their existing re-hosting and O&M needs while enabling a migration towards their emerging technology and standards-based service model.

31 IRM Touchpoints with other Reference Models

The IRM is closely linked with the other five reference models of the Consolidated Reference Model Framework. At the high level, the IRM relationship and tie-in to the other reference models is illustrated in the following table:

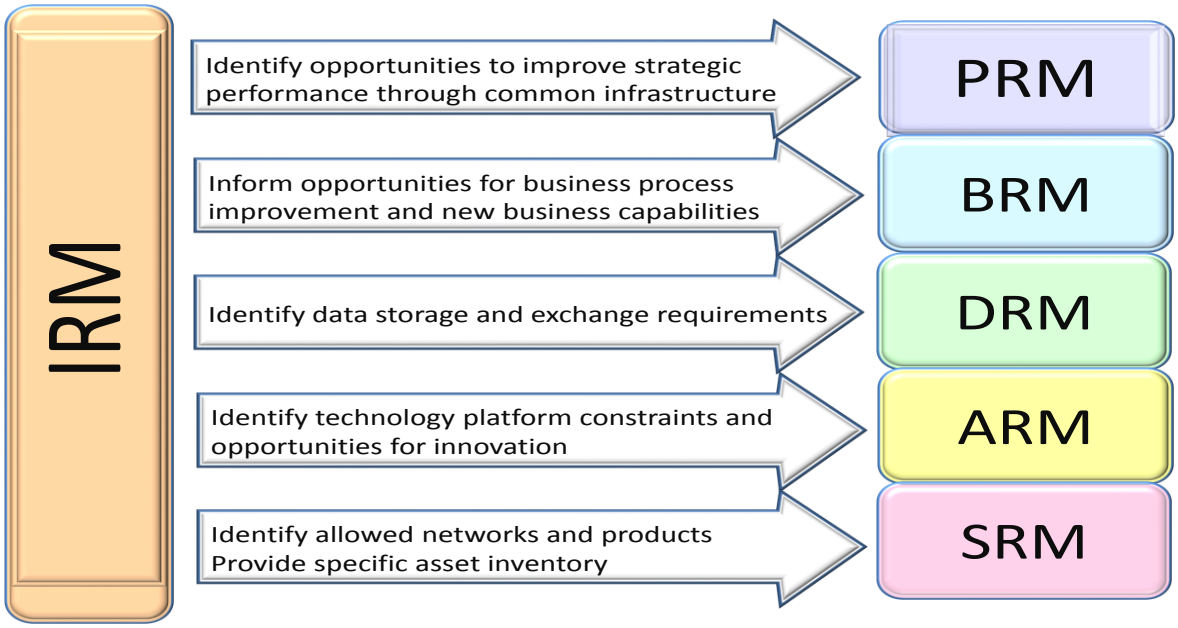


Figure 13: IRM Touchpoints with the other Reference Models

32 Associated Methods/Best Practices for the Infrastructure Reference Model

The Methods section presents how to quickly apply the IRM to the Use Cases discussed in Section 2 to solve enterprise problems.

32.1 Methods

Fundamental to using the IRM as a decision making tool is an IT infrastructure asset inventory that is categorized using the IRM. For this to be useful, additional data points including the manufacturer of the asset, cost, end-of-life/end-of-support dates, mapping to the Security Reference Model (SRM), etc., should be captured. A sample template, based on the NIST SP 800-128 specification, is given in Appendix E and is meant to be *extended* per the requirements of an agency's situation.

32.2 Best Practices

Apart from the above basic IT infrastructure asset inventory template, the following are widely accepted best practices, guidance and standards in the public and private sector that can adopt the IRM categorization as part of their implementation.

- ***Control Objectives for Information and related Technology (COBIT)*** – is an internationally accepted framework that provides an end-to-end business view of the governance of enterprise IT that reflects the central role of information and technology in creating value for enterprises

(i.e., COBIT helps to define *what* should be done). The principles, practices, analytical tools and models found in COBIT embody thought leadership and guidance from business, IT and governance experts around the world. COBIT is aligned with COSO, ITIL, ISO 27000, CMMI, TOGAF and PMBOK . The IRM is applied primarily in the Deliver and Support control domain.

- ***Information Technology Infrastructure Library (ITIL) v3*** – is the most widely accepted approach to IT Service Management in the world. ITIL provides a cohesive set of best practices, drawn from the public and private sectors internationally (i.e. ITIL helps provide the *how* for service management aspects). ITIL is aligned with various international quality standards including international standard ISO/IEC 20000 (IT Service Management Code of Practice).
- ***Object Management Group (OMG)*** is an international, open membership, not-for-profit computer industry consortium with members worldwide, including government agencies, small and large IT users, vendors and research institutions. OMG is most known for their standards development work. Over time, OMG has evolved to meet the changing business needs of IT by playing a strong role as a builder of practitioner-driven Communities of Practice focused on Green/Sustainability, Service Oriented Architecture, BPM, Cyber Security and Event Processing, while staying true to its standards development roots.
- ***Federal Shared Services Strategy -*** provides Federal Agency Chief Information Officers and key stakeholders guidance on the implementation of shared services as a key part of their efforts to eliminate waste and duplication and reinvest in innovative mission systems. A shared service is defined as a function that is provided by one or more service providers for the use and consumption by one or more customers. There are three **general categories** of *IT shared services*: **commodity, support, and mission**. These are delivered through cloud-based or legacy infrastructures.
- ***NIST Cloud Computing Reference Architecture (CCRA) and Taxonomy (Tax)***, NIST SP 500-292 - communicates the components and offerings of cloud computing. Guiding principles for the creation of CCRA were that it had to be a *vendor-neutral architecture* that did not stifle innovation by defining a prescribed technical solution (i.e. the "how").
- ***Related NIST Standards and Specifications*** are available at csrc.nist.gov.

33 IRM Summary

Significantly more detail about the structure, taxonomy, and associated methods of the Infrastructure Reference Model is available in Appendix E. The detailed taxonomy with definitions is available in Taxonomy K.

34 Introduction to the Security Reference Model

34.1 Purpose of the Security Reference Model

Security is integral to all architectural domains and at all levels of an organization. As a result, the Security Reference Model (SRM) must be woven into all of the sub-architectures of the overarching EA across all the other reference models and it must be considered up and down the different levels of the Enterprise. Enterprise Architecture Governance is the perfect place for security standards, policies, and norms to be developed and followed, since it is an enforcement point for Information Technology investments.

The SRM allows architects to classify or categorize security architecture at all scope levels of the Federal Architecture: International, National, Federal, Sector, Agency, Segment, System and Application. At the highest levels, the SRM is used to transform federal laws, regulations, and publications into specific policies. At the segment level, the SRM is used to transform department specific policies into security controls and measurements. At the system level, it is used to transform segment controls into system specific designs or requirements. Each level of the SRM is critical to the overall security posture and health of an organization and/or system.

34.2 Structure of the Security Reference Model

The Federal Security Reference Model (SRM) has three areas: Purpose, Risk, and Controls; these are divided into six total subareas (see figure below). Each one of these subareas must be addressed at the enterprise, agency, and system level. The SRM uses the information from the purpose and risk at each level of the enterprise to find and classify the correct controls to secure the environment.

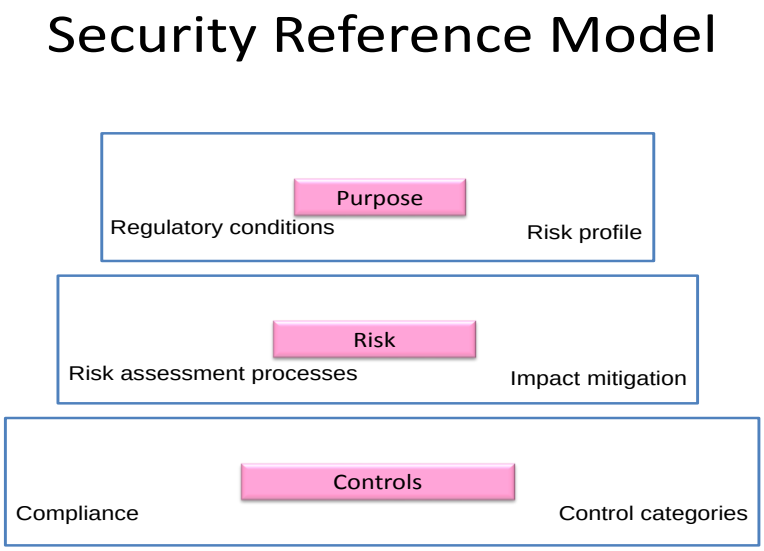


Figure 14: High Level SRM Taxonomy

Purpose: Security practices must balance both risk reduction and regulatory compliance. The SRM incorporates regulatory compliance at the enterprise level with risk profiles at the system and application levels to drive security choices.

Risk: Risk reduction is the ultimate reason for the application of security controls. According to NIST SP 800-30, risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Risk is reduced through exercising control over the potential impact and/or likelihood of a vulnerability being exploited or through elimination of a threat source.

Controls: The SRM uses the policies in place from the enterprise level to classify controls for a specific agency or segment. The SRM allows the architect to choose controls based on the purpose of an agency as well as by the risks faced by that particular agency. Controls maintained or satisfied at the agency level can then be inherited at lower system or application levels and to facilitate the design and/or requirements of the specific system. While the FISMA controls in use across the federal government allow agencies and security personnel to audit or review a system, the SRM uses the controls selected by the agency or segment to actually "bake" security into a system or application.

35 Using the Security Reference Model Taxonomy

35.1 Using Standards to classify Policy at the International, National, Federal, Sector, Enterprise or Department Level

At the enterprise level, the key tenet of the SRM is to use the standards in place across the federal or national IT security space to classify policy for a specific enterprise or agency. These standards include FISMA, HIPAA, FISCAM, and other security and privacy laws and regulations enacted by the US Government to control information and IT infrastructure. The SRM can then identify overlap between standards and policies within an enterprise. The policies must also be balanced with appropriate requirements so as not to preclude the organization achieving its business objectives.

Considerations at the Enterprise Level:

- What is the enterprise/department's primary business?
- With what other departments/agencies would it be logical to share services?
- What effect will a minimum policy statement have on subordinate agency business requirements? At the enterprise level all lower level architectures must be considered and layered into considerations.

Appendix C contains several mappings of the various reference documents regarding security in the Federal IT space as they relate to policy, legal and OMB requirements. It can be used for reference to gauge completeness of agency policies and guidance.

35.2 Using Policy to select Controls at the Agency or Segment Level

At the agency or segment level, the SRM uses the policies in place from the enterprise level to classify controls for a specific agency or segment. These controls can then be inherited or used at lower system or application levels.

While the FISMA specific controls (such as those from NIST SP-800-53 and 53a) are a crucial part of the SRM, they are not the only controls. Appendix F.ii includes these and controls from HIPAA, FISCAM, and the Privacy Act so many sources of Federal security and privacy requirements can be viewed at once. This allows the SRM to encompass all of an agency's security.

Considerations at the Agency Level (in addition to considerations at the Enterprise Level):

- What types of information (e.g. health, personal, classified) are processed and is there regulatory guidance specific to those information types?
- What controls are required based on the types of information, and how might they limit business processes?
- Does this create a risk to the business goal/objective? If so, is it greater than the risk of not implementing the control? (Risk Assessment)

35.3 Enforcing Design with Controls at the System or Application Level

At the system or application level, the SRM uses the controls in place at the agency or segment level to facilitate the design and/or requirements of the specific system. It is critical for architects to be involved in the earliest stages of planning a system or application in order to minimize the impact sometimes involved if security is added or addressed at a later stage. It is also crucial to understand the business goals and processes that are driving decisions for a particular system or application, in addition to knowing what policies and controls will be inherited.

Also, it is critical for the architect to use the SRM to ensure that proper security controls are placed at each level. *Security flows down;* but if no agency or segment provides or defines the control, the system architect must put them in place, creating extra effort and inconsistency between systems. If a Federal law specifies certain action, the system level must comply whether or not an agency capability or policy has been developed to support that law.

Considerations at the System/Application Level (in addition to those at the Enterprise and Agency Levels):

- Are there pre-defined controls required for this type of information?
- Are there risk concerns not covered by predefined controls?

36 SRM Touchpoints with other Reference Models

The SRM helps business owners with risk-based decision-making to achieve security objectives by understanding the purpose and impact of security controls on business processes or IT systems. Security integration across layers of the architecture is essential to ensure the protection of information and IT assets. Security must start at the business layer and work its way down to the application and infrastructure layers.

At the high level, the SRM relationship and tie-in to the other reference models is illustrated below:

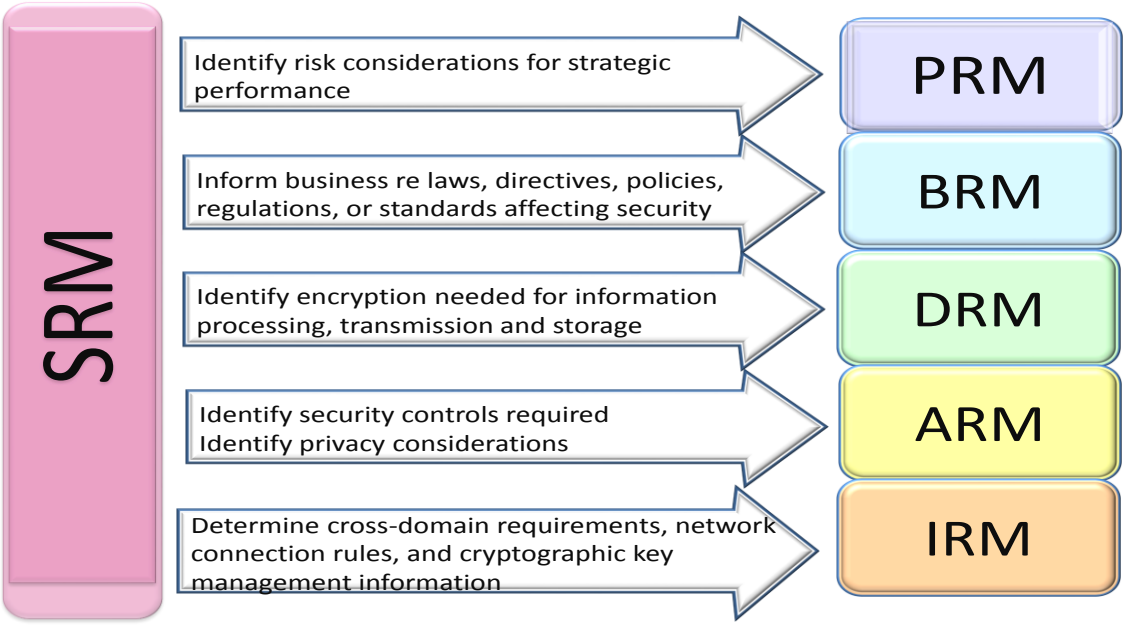


Figure 15: SRM Touchpoints with the other Reference Models

37 Associated Methods/Best Practices for the Security Reference Model

37.1 Risk Based Design

Government Agencies all strive for the best solutions to identify, assess, and manage risks to their systems, applications, and infrastructures. The National Institute of Standards and Technology (NIST) is at the forefront of risk guidance for the public sector.

The Risk Management Framework (RMF), as described in NIST SP 800-30 rev 1, provides a process that integrates information security and risk management activities into the system development life cycle.

The RMF steps include system categorization, selection of security baseline controls, control implementation, control assessment, system authorization, and system monitoring.

Security controls, policy, and processes must be built into the systems development life cycle (SDLC) for information security to be implemented successfully and cost-effectively. Each organization should have a mechanism by which risk and security concerns inform the design and implementation of systems and applications, to avoid creating cost and schedule impacts due to security requirements being added at the operations and maintenance stage of the SDLC. The continuous assessment of risk and the effectiveness of controls are required throughout the entire lifecycle of the IT system.

37.2 Security Controls

Implementing controls is not the primary goal of security. Rather, controls are an indispensable part of achieving the goal of reducing risk through layered security measures. There are some standard controls for the Federal Executive Branch flowing from various sources, including NIST 800-53, DoDI 8510, and public laws such as HIPAA and the Privacy Act. Appendix F.ii also lists commonly implemented controls.

Risk management relies on the ability to identify risk and select an appropriate control set to reduce that risk to acceptable levels. The primary ways to deal with risk include:

- Mitigate Risk (such as by hardening software and closing back doors). NIST security controls are primarily directed towards risk mitigation. The control set implemented within an organization should be tailored for that specific organization's needs.
- Avoid Risk (such as by not implementing particular solutions with known vulnerabilities). Architects can identify where certain configurations are unacceptable and use the Agency IRM and ARM to disallow particular standards, technologies and vendors from use.
- Transfer Risk (such as by contractually obligating vendors to assume risk). Agency policy should mandate certain risk related assurances when leasing contracts to third parties. If no Agency policies exist, the architect should work with contracting officials to achieve a balance where the government is not unduly carrying risk. This is particularly important when implementing infrastructure and platform as a service, and all cloud services.
- Accept Risk (such as deciding not to build reinforced bunkers to protect against meteor showers)

38 SRM Summary

Linking security and privacy to agency enterprise architecture, including agency performance objectives, business processes, data flows, applications and infrastructure technologies, ensures that each aspect of the business receives appropriate security and privacy considerations. Additionally, addressing security and privacy through enterprise architecture promotes interoperability and aids in the standardization and consolidation of security and privacy capabilities.

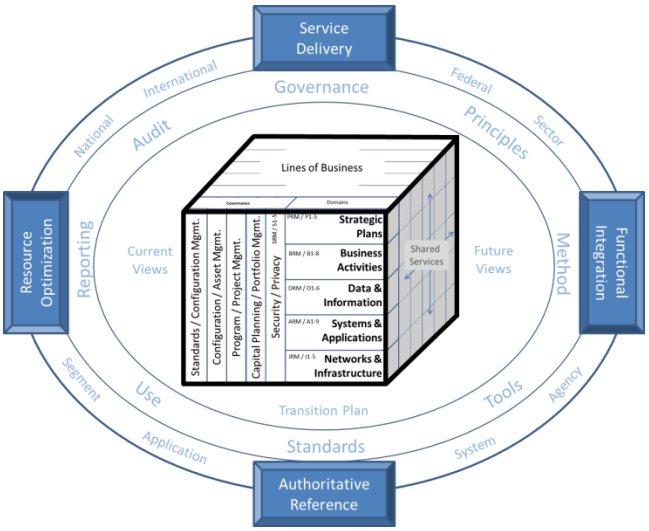
Significantly more detail about the structure, taxonomy, and associated methods of the Security Reference Model is available in Appendix F. The detailed taxonomy with definitions is available in Appendix L.

39 Artifacts

EA supports planning and decision-making through documentation and information that provides an abstracted view of an enterprise at various levels of scope and detail.

There are six sub-architecture domains in the *Common Approach to Federal Enterprise Architecture*:

- Strategic
- Business Services
- Data and Information
- Enabling Applications
- Host Infrastructure
- Security



These six sub-architecture domains delineate the types of analysis and modeling that are necessary to meet stakeholder requirements.

Based on EA best practices, the *Common Approach to Federal EA* lists one required core documentation artifact for each of the six sub-architecture views. This serves to promote consistent views within and between architecture as well as promoting interoperability within and between government organizations.

Sub-Architecture Domain	Required Core Artifact
Strategy	Concept Overview Diagram
Business	High-Level Process Diagram
Data	High-Level Logical Data Model
Applications	Application Interface Diagram
Infrastructure	High-Level Network Diagram
Security	Control List

Table 1. Required Core Artifacts List

There are also several dozen elective artifacts identified in the *Common Approach to Federal EA* to support additional analysis if that is needed. The type and depth of documentation should be guided by the need for detail and answers to questions about requirements, applicable standards, timeframes, and available resources.

39.1 Strategy Sub-Architecture Domain

PRM Artifact		Description	Other Framework Names
S-1	Concept Overview Diagram (core)	The high-level graphical/textual description of the operational concept	DoDAF OV-1 (Operational Concept)
S-2	Strategic Plan	A description of the organization's vision, strategic objectives, a prioritization of the desired outcomes from achieving those objectives, the measurements that will demonstrate achievement, and the resources to be used to achieve them	DoDAF CV-1, 2, 3, 5, 6 (Capability Effects, Hierarchy, Schedules, Deployments, and Activities)
S-3	Concept of Operations Scenarios	Organizes Business Process Sequences into scenarios	DoDAF OV-6c (Operational Activity Sequences)
S-4	SWOT Analysis	Presents the Strengths, Weaknesses/Limitations, Opportunities, and Threats involved in a project or in a business venture including risks and impacts	
S-5	Performance Measures Scorecard	A strategic performance management tool that can be used by managers keep track of the Performance Metrics associated with the execution of activities by the staff within their control and to identify the Performance Gaps and consequences arising from these gaps	Balanced Scorecard (BSC)

Table 2. Strategy Domain Artifacts

39.2 Business Sub-Architecture Domain

BRM Artifact		Description	Other Framework Names
B-1	Business Process Diagram (core)	Presents the hierarchical structure of organizational activities and activities performed by organizational performers to consume and produce resources	DoDAF OV-5a&b (Operational Activities), Operational Activity Diagram, Business Process Model
B-2	Business Operating Plan	Describes, from a timeline perspective, the changes to the Business Service Catalog, Organizational Chart, and Business Process Model to transition from the current state to the objective state	DoDAF PV-2 (Project Schedules), Business Transition Plan
B-3	Business Service Catalog	Presents the business services, taken from the BRM, that are provided within the scope of the architecture and may also indicate business services that are consumed or used internally within the architecture	DoDAF SvcV-1 (Service Composition)
B-4	Organization Chart	Presents the composition and relationships among organizational performers	DoDAF OV-4 (Organizational Relationships)
B-5	Use Case Narrative and Diagram	Describes a set of possible sequences of interactions between systems and users in a particular environment and related to a particular goal	
B-6	Business Case / Alternatives Analysis	A summary of the planning, budgeting, acquisition, and management of federal capital assets sufficient to determine if investment funding should be recommended or continued	OMB Exhibit 300

Table 3. Business Domain Artifacts

39.3 Data Sub-Architecture Domain

DRM Artifact		Description	Other Framework Names
D-1	Logical Data Model (core)	Presents data requirements that reify the information concepts identified by corresponding Conceptual Information models	DoDAF DIV-2 (Data Requirements)
D-2	Knowledge Management Plan	Provides a detailed description of how knowledge, information, and data are shared across the enterprise between systems, applications, knowledge warehouses, and databases	
D-3	Data Quality Plan	A systematic approach to data quality assurance	
D-4	Data Flow Diagram	The functions (activities) performed by systems or services, their hierarchical structure, and their resource flows	DoDAF SV/SvcV-4 (System Functions and Service Activities and Resource Flows)
D-5	Physical Data Model	Presents data-elements and data-structures that reify the data requirements specified by corresponding logical data models	DoDAF DIV-3 (Data Implementation)
D-6	CRUD Matrix	Presents resources that are consumed and produced by activities performed by organizational performers	DoDAF OV-3 (Organizations, Activities, and Resources), Business Data Mapped to Key Business Processes (CRUD)
D-7	State-Transition Diagram	The states systems transition to in response to events	DoDAF SV/SvcV-10b (System and Service State Transitions)
D-8	Event Sequence Diagram	A sequence of triggering events associated with resource flows and systems	DoDAF SV/SvcV-10c (System and Service Activity Sequences)
D-9	Data Dictionary	A centralized repository of information about data such as name, type, range of values, source, and authorization for access for each data element in the organization's files and databases	

DRM Artifact		Description	Other Framework Names
D-10	Object Library	A collection of computer programs in the form of relocatable instructions, which reside on, and may be read from, a mass storage device	

Table 4. Data Domain Artifacts

39.4 Applications Sub-Architecture Domain

ARM Artifact		Description	Other Framework Names
A-1	Application Interface Diagram (core)	The identification of application resource flows and their composition	DoDAF SV-1 (System Composition and Interfaces)
A-2	Application Communication Diagram	The means by which resource flows between applications occur	DoDAF SV/SvcV-2 (Systems and Services Interface Means)
A-3	Application Interface Matrix	The interface relationships among systems	DoDAF SV-3 (System - System Interfaces)
A-4	Application Data Exchange Matrix	The details of resource flows among systems; the activities performed; the resources exchanged; and the attributes (rules and measures) associated with these exchanges	DoDAF SV/SvcV-6 (System and Service Resource Flows)
A-5	Application Service Matrix	Interface relationships between services and applications	DoDAF SvcV-3a&b (Service Interfaces to Services and Systems)
A-6	Application Performance Matrix	The measures (metrics) of applications	DoDAF SV/SvcV-7 (System and Services Measures)
A-7	System / Application Evolution Diagram	The planned incremental steps toward migrating a suite of systems and/or applications to a more efficient suite, or toward evolving a current system or application to a future implementation	DoDAF SV/SvcV-8 (System and Service Evolution)
A-8	Enterprise Service Bus Diagram	Describes the interaction and communication between mutually interacting software applications in service-oriented architecture (SOA)	
A-9	Application Maintenance Procedure	Describes how to modify software to provide error corrections, enhancements of capabilities, deletion of obsolete capabilities, and optimization	
A-10	Application Inventory	A registry of applications and services, the system functions or service activities they perform, and, optionally, prioritized or ranked.	

ARM Artifact		Description	Other Framework Names
A-11	Software License Inventory	A list of Commercial-off-the-Shelf (COTS) and open source software assets with details about each (installation date, original cost, condition and such).	

Table 5. Application Domain Artifacts

39.5 Infrastructure Sub-Architecture Domain

IRM Artifact		Description	Other Framework Names
I-1	Network Diagram (core)	Describes the means by which resource flows between systems occur	DoDAF SV/SvcV-2 (Systems and Services Interface Means)
I-2	Hosting Concept of Operations	Presents the high level functional architecture, organization, roles, responsibilities, processes, metrics and strategic plan for hosting and use of hosting services	
I-3	Technical Standards Profile	Collects the various systems standards rules that implement and sometimes constrain the choices that can be made in the design and implementation of an architecture	DoDAF StdV-1 (Standards Profile)
I-4	Technology Forecast	The emerging technologies, software/hardware products, and skills that are expected to be available in a given set of time frames and that will affect future infrastructure development	DoDAF SV/SvcV-9 (System and Service Technology and Skills)
I-5	Cable Plant Diagram	Diagrams the wires and connectors used to tie a network together	
I-6	Wireless Connectivity Diagram	Diagrams a communications network that provides connectivity to wireless devices	
I-7	Rack Elevation Diagrams (front and back)	Two-dimensional elevations, drawn to scale and showing everything that needs to be placed in a certain area, that describe the organization of specific equipment on a rack	
I-8	Data Center / Server Room Diagram	Diagrams the layout and contents of a data center or server room	

IRM Artifact		Description	Other Framework Names
I-9	Wiring Closet Diagram	Diagrams the layout and contents of a wiring closet	
I-10	Point of Presence Diagram		
I-11	Asset Inventory	A list of assets with details about each (installation date, original cost, condition and such)	Asset register
I-12	Facility Blueprints	Technical drawings of the facility	

Table 6. Infrastructure Domain Artifacts

39.6 Security Sub-Architecture Domain

SRM Artifact		Description	Other Framework Names
SP-1	Security Controls Catalog (core)	Describes the total set of security controls from which the developer may choose those that are applicable for the effort	NIST SP 800-53, SP 800-37, CNSSI-4009, FIPS 200
SP-2	Security and Privacy Plan	A description of the enterprise security and privacy programs, policies and procedures for the agency	
SP-3	Security Authorization Documentation	Compilation of security documents relevant to each system such as: System Security Plan, Risk Analysis, Security Requirements Traceability Matrix, System Security Authorization Agreement, Authority to Operate, etc.	C&A Documentation
SP-4	Continuous Monitoring Plan	Describes the organization's process of monitoring and analyzing the security controls and reporting on their effectiveness	Continuous Monitoring Procedures
SP-5	Disaster Recovery Plan	A plan that describes all aspects of recovery from an incident that temporarily disables the operational capabilities of the enterprise, but does not entail re-location	
SP-6	Continuity of Operations Plan	A plan that describes all aspects of recovery from an incident that temporarily disables the operational capabilities of the enterprise, and does require re-location	

Table 7. Security Domain Artifacts

Appendix A: Collaborative Planning Methodology Guidance Document

A.1 Overview of the Collaborative Planning Methodology

Planning is done to affect change in support of an organization's Strategic Plan, and the many types of planners (e.g. architects, organization and program managers, strategic planners, capital planners, and other planners) must work together to develop an integrated, actionable plan to implement that change. Planning should be used to determine the exact changes that are needed to implement an organization's Strategic Plan, enable consistent decision-making, and provide measurable benefits to the organization. In short, an organization's Strategic Plan should be executed by well-rounded planning that results in purposeful projects with measurable benefits.

In today's environment, which demands more efficient government through the reuse of solutions and services, organizations need actionable, consistent, and rigorous plans to implement Strategic Plans and solve priority needs. These integrated plans should support efforts to leverage other Federal, state, local, tribal, and international experiences and results as a means of reusing rather than inventing from scratch. Plans should be consistent and rigorous descriptions of the structure of the organization or enterprise, how IT resources will be efficiently used, and how the use of assets such as IT will ultimately achieve stated strategies and needs.

The role of planners is to help facilitate and support a common understanding of needs based on the organization's Strategic Plan, help formulate recommendations to meet those needs, and facilitate the development of a plan of action that is grounded in an integrated view of not just technology planning, but the full spectrum of planning disciplines to include, but not limited to, mission/business, IT resources, capital, security, infrastructure, human capital, performance, and records planning.

Planners provide facilitation and integration to enable this collaborative planning discipline, and work with specialists and subject matter experts from these planning groups in order to formulate a plan of action that not only meets needs but is also implementable within financial, political, and organizational constraints. In addition, planners have an important role to play in the investment, implementation, and performance measurement activities and decisions that result from this integrated planning process.

The *Collaborative Planning Methodology*, shown in Figure 1, is a simple, repeatable process that consists of integrated, multi-disciplinary analysis that results in recommendations formed in collaboration with sponsors, stakeholders, planners, and implementers. This methodology includes the master steps and detailed guidance for planners to use throughout the planning process. Architecture is but one planning discipline included in this methodology. Over time the methods and approaches of other planning disciplines will continue to be interwoven into this common methodology to provide a single, collaborative approach for organizations to use.

The *Collaborative Planning Methodology* is the next generation replacement for the *Federal Segment Architecture Methodology (FSAM)*. As the replacement for the *FSAM*, the *Collaborative Planning Methodology* has been designed to be more flexible, more widely applicable, and more inclusive of the larger set of planning disciplines.

The *Collaborative Planning Methodology* is intended as a full planning and implementation lifecycle for use at all levels of scope defined in the *Common Approach to Federal Enterprise Architecture*: International, National, Federal, Sector, Agency, Segment, System, and Application.

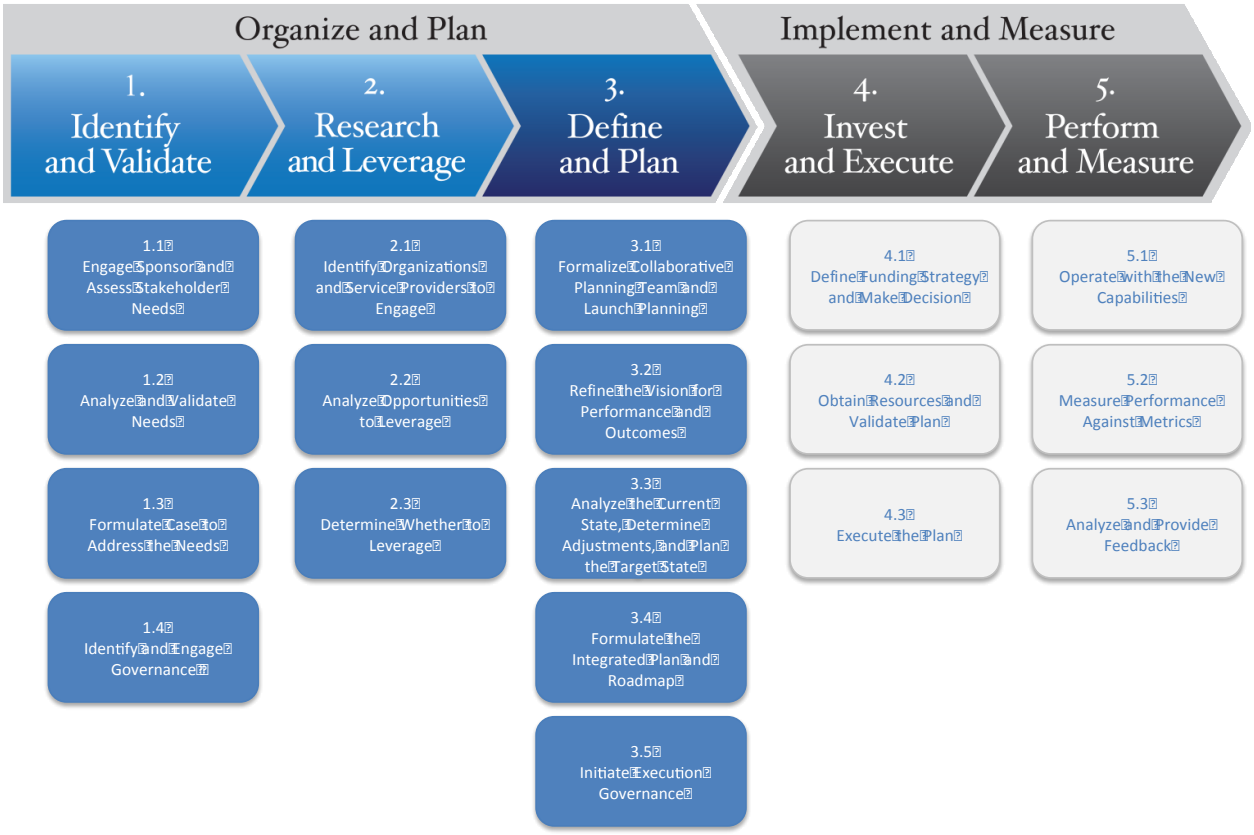


Figure A.2: Collaborative Planning Methodology (CPM)

The *Collaborative Planning Methodology* consists of two phases: (1) *Organize and Plan* and (2) *Implement and Measure*. Although the phases are shown as sequential, in fact there are frequent and important iterations within and between the phases. In the first phase, planners serve a key role facilitating the collaboration between sponsors and various stakeholders to clearly identify and prioritize needs, research other organizations facing similar needs, and formulate the plans to address the stated needs. In the second phase, planners shift into a participatory role, supporting other key personnel working to implement and monitor change related activities. As part of the second phase of the methodology, planners specifically support investment, procurement, implementation, and performance measurement actions and decisions.

The *Collaborative Planning Methodology* is stakeholder-centered with a focus on understanding and validating needs from sponsor and stakeholder perspectives, planning for those needs, and ensuring that what is planned ultimately results in the intended outcomes (Step 1). Additionally, this methodology is structured to embrace the principles of leverage and reuse by assisting planners in determining whether there are other organizations that have previously addressed similar needs, and whether their business model, experiences, and work products can be leveraged to expedite improvement (Step 2).

Ultimately, the *Collaborative Planning Methodology* helps planners work with sponsors and stakeholders to clearly articulate a roadmap that defines needs, what will be done to address those needs, when actions will be taken, how much it will cost, what benefits will be achieved, when those benefits will be achieved, and how those benefits will be measured (Step 3). The methodology also helps planners support sponsors and stakeholders as they make decisions regarding which courses of action are appropriate for the mission, including specific investment and implementation decisions (Step 4). Finally and perhaps most importantly, the methodology provides planners with guidance in their support of measuring the actual performance changes that have resulted from the recommendations, and in turn, using these results in future planning activities (Step 5).

The five steps of the *Collaborative Planning Methodology* are detailed in the following sections.

A.1.1 Step 1: Identify and Validate

Purpose: The purpose of this step is to identify and assess what needs to be achieved, understand the major drivers for change, and then define, validate, and prioritize the mission and goals with stakeholders and operational staff. During this step, the stakeholder needs and the operational requirements are validated so that ultimately, all stakeholder groups are working towards the same, well understood, validated outcome. Initial performance metrics are created to begin focusing the measurement of success to be consistent across stakeholder groups. In this step, a sponsor for the planning effort is identified. The sponsor can range in levels of scope from an executive leader to a functional leader or even an application owner.

An additional purpose of this step is to identify and engage appropriate governance.

The Planner's Role: In this step, planners (architects and other planners) facilitate a direct collaboration between the sponsor and stakeholders as they work together to define, validate, and prioritize their needs, and build a shared vision and understanding. In doing so, planners analyze stated needs in the context of overarching drivers to help aid decision makers in their assessment of whether stated needs are feasible and realistic. Since these needs shape the scope and strategic intent for planning, it is imperative that the sponsor and stakeholders agree on the needs before beginning subsequent planning steps.

In addition to identifying needs, planners work with the sponsor and stakeholders to establish target performance metrics that will ultimately be used to determine if the planned performance has been achieved.

Once needs are identified and validated, planners support the sponsor in identifying and initiating appropriate governance. Who makes the decisions and when those decisions will be made is important to the timing and buy-in of recommendations for change.

Outcome: At the end of Step 1, the key outcomes are (1) identified and validated needs, (2) an overarching set of performance metrics, and (3) a determination of who (governance) will ultimately oversee and approve recommended changes to meet those needs.

A.1.2 Step 2: Research and Leverage

Purpose: The purpose of this step is to identify organizations and service providers that may have already met, or are currently facing needs similar to the ones identified in Step 1, and then to analyze their experiences and results to determine if they can be applied and leveraged or if a partnership can be formed to address the needs together. In alignment with the "Shared First" principle, it is at this point that planners consult both internal and external service catalogs for pre-existing services that are relevant to the current needs. In some instances, an entire business model, policy, technology solution, or service may be reusable to address the needs defined in Step 1 – an important benefit in these cost-constrained, quickly evolving times. Based on this analysis, sponsors and stakeholders determine whether or not they can leverage the experiences and results from other organizations.

The Planner's Role: Planners facilitate the research of other organizations and service providers to assess whether they have similar needs and whether these organizations have already met these needs or are currently planning to meet these needs. Planners lead the assessment of the applicability of the other organizations' experiences and results and help determine whether there are opportunities to leverage or plan together. Once these organizations and their needs and experiences have been identified and assessed, planners formulate a set of findings and recommendations detailing the applicability and opportunity for leverage. These findings and recommendations are submitted to the sponsor who engages governance with this information as appropriate.

Outcome: At the conclusion of Step 2, planners, sponsor, and stakeholders have a clear understanding of the experiences and results of other organizations, and the sponsor and / or governance have determined whether or not these experiences should be leveraged to meet the needs being considered as part of the planning effort. In some instances, another organization may be currently planning for similar needs and a partnership can be formed to collectively plan for these needs. The decision to leverage or not has a significant impact on the planning activities in Step 3. For instance, if the organization determines that it can leverage policies and systems from another organization in order to meet its own needs, these policies and systems become a critical input to planning in Step 3.

A.1.3 Step 3: Define and Plan

Purpose: The purpose of this step is to develop the integrated plan for the adjustments necessary to meet the needs identified in Step 1. Recommended adjustments could be within any or all of the architecture domains: strategy, business, data, applications, infrastructure, or security.

The integrated plan defines what will be done, when it will be done, how much it will cost, how to measure success, and the significant risks to be considered. Additionally, the integrated plan includes a timeline highlighting what benefits will be achieved, when their completion can be expected, and how the benefits will be measured. It is during this step that analysis of current capabilities and environments results in recommended adjustments to meet the needs identified in Step 1. The formal design and planning of the target capabilities and environment is also performed during this step.

In addition to the integrated plan, the architecture, capital planning, security, records management, budget formulation, human capital, and performance compliance documents are developed based on the analysis performed in Step 3. The end outcome is an integrated set of plans that can be considered and approved by the sponsor and governance.

The Planner's Role: Architects lead the development of the architecture by applying a series of analysis and planning methods and techniques. Through this process, planners work on each of the architecture domains (strategy, business, data, applications, infrastructure, and security) and produce artifacts to capture, analyze, and visualize the plans for change. Most important is the architect's efforts to synthesize the planning into recommendations that can be considered and approved by the sponsor and governance.

During the development of the architecture, architects facilitate the interaction with other planning disciplines (e. g. budget, CPIC, security) so that each discipline's set of plans is incorporated into a cohesive set of recommendations to meet the needs stated in Step 1. Throughout these efforts, planners develop the integrated plan and roadmap to reflect the course of action that has been determined through these planning activities.

Outcome: At the end of Step 3, the sponsor and stakeholders will possess an integrated set of plans and artifacts defining what will be done, when it will be done, what and when benefits will be achieved, and an estimated cost. This set of plans should be synthesized into discrete decision-making packages for the appropriate sponsor and governance given financial, political, and organizational constraints.

A.1.4 Step 4: Invest and Execute

Purpose: The purpose of this step is to make the investment decision and implement the changes as defined in the integrated plan. Many groups participate in this step, however, it is important to note that these groups will need to work as a coordinated and collaborative team to achieve the primary purpose of this step: to successfully implement the planned changes.

The Planner's Role: In this step architects are in a support role, assisting in investment and implementation activities by providing information to aid in decisions, and to support interpretation and revision of plans from Step 3. Architects may be required to continue research and analysis into other organizations and their experiences (Step 2), update plans (Step 3), or re-engage stakeholders for feedback on desired outcomes (Step 1). Throughout the investment and implementation, architects provide continuing support such as interpreting the plans, making changes to the plans, supporting

decision-making, and ensuring that plans are followed and architectural requirements are met. The involvement of architects does not cease at the conclusion of planning in Step 3.

Outcome: During Step 4, a decision is made concerning the investment in the changes that were planned in Step 3. At the end of Step 4 the recommendations for addressing the defined needs have been implemented. If the investment is not approved, planners, sponsor, and stakeholders return to previous steps to alter the recommendations and plans for future consideration. It is important to reiterate that during the implementation (Step 4) there could be a variety of changes to the integrated plans (Step 3) including, but not limited to, policy changes, organizational changes, technology changes, process changes, and resource changes.

A.1.5 Step 5: Perform and Measure

Purpose: During Step 5 the mission is operated with the new capabilities planned in Step 3 and implemented in Step 4. The purpose of Step 5 is to operate the mission and measure performance outcomes against identified metrics (Step 1).

The Planner's Role: Planners may not be the keeper of the actual performance data, but they leverage available performance data to assess whether the implemented capabilities achieve desired and planned performance. Feedback from this step can feed into future planning efforts as well as immediate planning and implementation adjustments as necessary. Feedback may also impact more immediate changes in plans that may be considered by governance, including configuration management.

Outcome: At the end of Step 5, the new capabilities as planned in Step 3 and implemented in Step 4 will be operational. The key outcome of this step is measured performance outcomes against identified metrics from Step 1.

A.2 Step 1: Identify and Validate

Purpose

The purpose of this step is to identify and assess what needs to be achieved, understand the major drivers for change, and then define, validate, and prioritize the mission and goals with stakeholders and operational staff. During this step, the stakeholder needs and the operational requirements are validated so that ultimately, all stakeholder groups are working towards the same, well understood, validated outcome. Initial performance metrics are created to begin focusing the measurement of success to be consistent across stakeholder groups. In this step, a sponsor for the planning effort is identified. The sponsor can range in levels of scope from an executive leader to a functional leader or even an application owner.

Major Participants

In this step, planners (e.g. architects, organization and program managers, capital planners, and other planners) facilitate a direct collaboration between the sponsor and stakeholders as they work together to define, validate, and prioritize their needs, and build a shared vision and understanding. In doing so, planners analyze stated needs in the context of the overarching drivers to help aid decision makers in their assessment of whether stated needs are feasible and realistic. Since these needs shape the scope and strategic intent for planning, it is imperative that the sponsor and stakeholders agree on the needs before work begins on subsequent planning steps. Additionally, it is important that planners work with the sponsor and stakeholders to establish target performance metrics that must ultimately be used to determine if the planned performance has been achieved.

Once needs are identified and validated, planners support the sponsor in identifying and initiating appropriate governance. It is important for governance to be understood up front so that there is a body of people that can be leveraged for feedback, oversight, and for decision-making throughout the planning process.

Outcome

At the end of Step 1, the key outcomes are (1) identified and validated needs, (2) an overarching set of performance metrics, and (3) a determination of who (governance) will ultimately oversee and approve recommended changes to meet those needs.

A.2.1 Step At-a-Glance

Step 1 At-a-Glance	Step 1 Activities: Identify and Validate			
	Engage Sponsor and Assess Stakeholder Needs	**Analyze and Validate Needs**	**Formulate case to address the needs**	**Identify and Engage Governance**
Who Participates in This Activity?	• Planners • Stakeholders • Sponsor • Governance	• Planners • Stakeholders	• Planners • Stakeholders • Sponsor	• Planners • Sponsor • Governance
What Are The Inputs to This Activity?	• Interest from someone with a need to plan and affect change	• Risks and Impacts • Performance Gaps • Draft List of Stakeholder Needs	• Applicable Drivers, Assumptions, and Constraints • Validated List of Stakeholder Needs	• Vision, Goals and Objectives, Purpose Statement, and Scope
What Are The Outputs from This Activity?	• Leadership Team Roster • Risks and Impacts • Performance Gaps • Draft List of Stakeholder Needs	• Applicable Drivers, Assumptions, and Constraints • Validated List of Stakeholder Needs	• Target Performance Metrics • Impacts, Value, Risk, and Dependencies • Vision, Goals and Objectives, Purpose Statement, and Scope	• Governance Structure
What Is The Relative Complexity of This Activity?				

A.2.2 A Note on Core Artifacts

Like any methodology, the *Collaborative Planning Methodology* is designed for each step to be followed and each Activity Output to be produced. The use of "Core" and "Not Core" to describe these outputs is meant as the first set of tailoring guidance if an organization has constraints of time, budget or resources. As the CPM is tested and refined, feedback from organizations will improve this assignment and generate templates that help to scale outputs according to scope or size.

As described earlier, the goal in using this methodology is to encourage collaboration for high priority projects. This increases the awareness of solutions and services whose reuse can result in efficiencies. The CPM also provides the framework for organizations to generate actionable, consistent and rigorous plans that can lead to improved solutions.

A.2.3 Activity 1.1: Engage Sponsor and Assess Stakeholder Needs

In this activity, planners engage with stakeholders who are facing a challenge or have an opportunity that they would like help to address. This may be through stakeholders reporting a need or planners eliciting needs from the stakeholders. During this activity, planners interview stakeholders to get a more clear understanding of their needs including the risks and impacts of the needs not being addressed. The risks and impacts are an important factor in determining the quantity and timing of resources required to plan and address the stated needs. The impacts in particular are often a strong motivator for action, as they communicate what happens if action is not taken. For instance, if an organization does not commit to a standard approach for information exchanges, custom interfaces may cost more to develop and decision makers may be delayed in receiving timely information.

Knowledge of the needs, risks, and impacts helps the planners determine the actual performance gaps that need to be resolved. Performance gaps may vary from details like slow server response times for an application to very broad gaps like being unable to share information between Departments with shared missions. These performance gaps are a start to stakeholders focusing on outcomes that are targeted, quantified, and able to be positioned as the focus of the planning effort at hand.

In this activity, tasks begin with engaging the sponsor, business owners, and other stakeholders. These are the individuals that planners must interview to gather information about challenges, risks, and overall performance in order to formulate the needs that are common between individuals. These conversations result in stakeholder needs and a determination of the most appropriate sponsor to address those stakeholder needs.

The following visual illustrates the tasks within this activity.

Activity 1.1: Engage Sponsor and Assess Stakeholder Needs

Tasks:

1.11 Engage the sponsors, business owners, and other stakeholders

Planners use this CPM when there is an individual or group with a need that they would like to have addressed. The first order of business is to engage with this individual or group to understand more about their needs. Once a better understanding of the needs has been gathered, it is important to identify the stakeholders (e.g. sponsors, leaders, customers) that appear to be associated with this stated need. Each stakeholder may have a different perspective on how to address the stated need; the applicability of those suggestions is assessed in future steps. In this task the stakeholders must be engaged, either by planners or the originator of the need, to explain the role of planners and to schedule time to meet with the stakeholders. In the following tasks, the stakeholders must provide their perspectives to better shape the articulation of needs.

1.12 Discuss the business challenges, risks, and performance with Stakeholders

It is critical to engage stakeholders to identify their key business needs, challenges, risks, and their desired objectives and outcomes. Stakeholders must be engaged and planners may use the most appropriate method for the project. For instance, stakeholders could be engaged in working sessions that are scripted and include prepared materials. Also, stakeholders could receive data calls to collect their key business needs, objectives, and desired outcomes. In many instances, an interview or facilitated session is an ideal way to extract from the stakeholders their perspectives. A communications plan for the project may be appropriate to define the tactics for reaching stakeholders or others for these early discussions and all communications through all steps of the CPM.

Prior to the stakeholder conversations, customer, business process, and technology performance information must be collected to identify, quantify, and prioritize performance gaps between current and target performance metrics. Identifying performance gaps includes a review of any pre-existing performance information, oversight reports, customer surveys, or known deficiencies in achieving stated performance metrics. This pre-review of performance

information will help in facilitating the stakeholder conversations and will help more quickly evolve the focus of the stakeholders from challenges and risks to performance gaps.

During stakeholder interviews there may be several prominent issues beyond the original project need that arise. It is important to understand not just the originally stated need, but to also evolve the thinking around other stated needs by gaining the perspectives of the larger stakeholder community. Focusing on business challenges and risks generally elicits the most robust feedback that can then be translated into performance gaps.

1.13 Identify the common business challenges to determine stakeholder needs

In most cases, the stakeholders will have very similar issues or priorities. The fact that the stakeholders are affiliated in the previous steps with the originally stated need means a high probability that the stakeholders face common challenges. Whether there is immediate consensus or not, it is ultimately important for stakeholders to recognize and identify with the business challenges that are common to the group so that planning activities can be performed as a group, to ultimately address the challenges in unison.

The stakeholder conversations in the previous task resulted in documented risks, impacts, and performance gaps. Creating major categories from this feedback and organizing the feedback within those categories is useful for looking at trends and commonality of opinions. It is also useful to look at the feedback from the dimensions of geography, seniority, employment role, and other factors that might lead to trends that are not universal but are noticeable within a cross section of the stakeholder community.

1.14 Assign the Sponsor with the appropriate authorities

There are positive and negative aspects to being the sponsor for a planning effort. The most significant positive aspect is to be in a position of leadership for the planning itself. The leadership position affords the sponsor with a unique opportunity to shape the future. The most significant negative aspect is the dedication of time to the effort. The sponsor must be current on the actions and recommendations of planners and the stakeholders in order to represent the project interests as required.

Generally, if the focus is on a single organizational group, selection of the sponsor is a straightforward decision. If, however, the focus of the planning includes multiple organizational groups within the same organization, the representatives from each organizational group must select the single sponsor. Note that in cases involving multiple discrete and separate organizations, there must be several sponsors at peer levels.

It is important to educate the stakeholders and even the sponsor on the role of the sponsor. Some sponsor candidates will be more qualified than others based on the time and leadership requirements of the position. Optimally, the sponsor must provide visionary leadership and play an active role in shaping the direction of the planning.

Overall, a sponsor must have the following characteristics: effective communicator, qualified decision maker, talented leader, respected within the affected organizations, visionary, good political skills, energetic, and excited about opportunities for change.

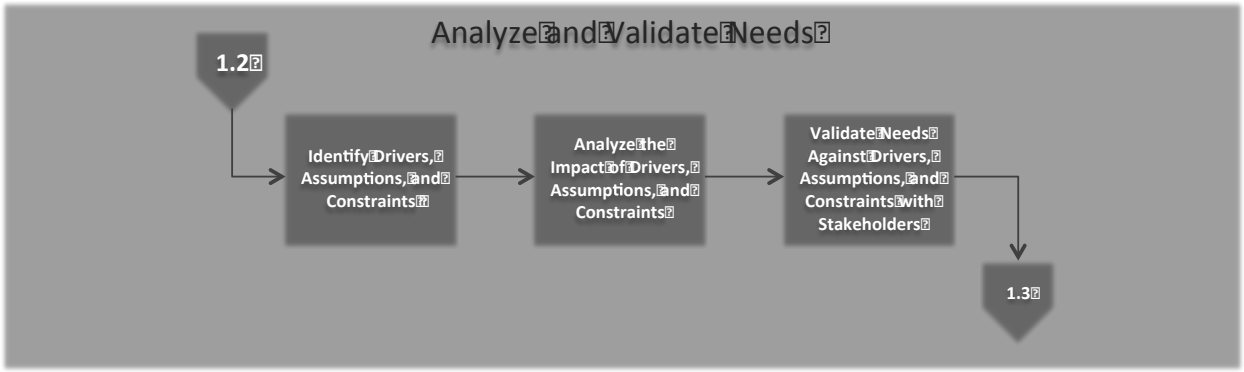
1.1 Activity Outputs:

Output	Core	FEA Layers
Leadership Team Roster	Y	n/a
Project Communication Plan	N	n/a
Risks and Impacts	N	S
Performance Gaps	Y	S
Draft List of Stakeholder Needs	Y	S
Key to FEA Layers: S = Strategy, B = Business, D = Data, A = Application, I = Infrastructure, SP = Security		

A.2.4 Activity 1.2: Analyze and Validate Needs

In this activity, the draft needs from the previous activity are analyzed in the context of drivers, assumptions, and constraints. The purpose of this activity is to validate the needs including the feasibility of addressing the needs given constraints as well as the validity of needs given other drivers. Additionally, the needs from the previous activity are validated to ensure that they are adequately addressing the performance gaps and risks that were also identified in the previous activity. Ultimately this activity yields a finalized list of needs that the stakeholders and sponsor agree are to be the focus of the planning.

The following visual illustrates the tasks within this activity.



Activity 1.2: Analyze and Validate Needs

Tasks:

1.21 Identify drivers, assumptions, and constraints

The previous activity yielded a draft list of stakeholder needs as well as the risks of not addressing these needs and the performance gaps associated with these needs. In this task the drivers, assumptions, and constraints associated with the needs are defined for use in the next tasks.

Drivers are forces like people, knowledge, and conditions that impact the need in focus. Drivers can be financial, political, legal, organizational, or cultural in nature, to name a few. In this task planners need to identify the drivers that impact this need or that could potentially have an influence on the need.

Assumptions are accepted cause and effect relationships, or estimates of the existence of a fact from the known existence of other fact(s). In this task planners need to identify the assumptions that are of significant impact on the need.

Constraints are elements or factors that work as a bottleneck. Constraints restrict an entity from achieving its potential with reference to its goal. In this task planners need to identify the constraints that have a significant influence on the need in focus or could potentially have an influence on this need.

The planner must also be aware of inter-related drivers, assumptions or constraints so the impact of responding to one is assessed against the others.

1.22 Analyze the impact of drivers, assumptions, and constraints

Having a consistently understood set of assumptions about the needs is an important part of maintaining a common understanding among the stakeholder community throughout the planning effort. Needs, performance gaps, and risks have been defined but inconsistency in the assumptions within the stakeholder community can result in a fragmented planning effort.

Likewise, consistently understanding the drivers and constraints that act upon the needs is important in that needs might be dynamic to the point of rendering the planning effort not useful.

Outputs from previous tasks provide planners with the required drivers, assumptions, and constraints. In this task the analysis is performed to determine impacts of those drivers, assumptions, and constraints on the stated needs. Planners need to assess each specific need against each specific driver, assumption, and constraint to determine validity of the need as it is stated. A list of the impacts and / or reactions of the needs in the context of the drivers, assumptions, or constraints is one good way of documenting the analysis.

1.23 Validate needs against drivers, assumptions, and constraints with stakeholders

The analysis from the previous task is the significant input to this task as planners look to validate the needs. In this task planners are validating that the stated needs are appropriate given the known drivers, assumptions, and constraints.

If, for instance, a major driver for a need is a law that might be repealed, then the validity of planning for this need at this time might be called into question.

In another example, if a need will obviously have a large scale cost impact and there are significant cost constraints on the organization, then the validity of the need being part of the planning could be called into question.

Planners need to also review the assumptions and ensure that there is consistency of assumptions within the stakeholder community. If, for instance, there are differences in assumptions between two groups, this could greatly reduce the likelihood of successfully plan for the stated needs.

1.2 Activity Outputs:

Output	Core	FEA Layers
Applicable Drivers, Assumptions, and Constraints	N	S
Validated List of Stakeholder Needs	Y	S, B
Key to FEA Layers: S = Strategy, B = Business, D = Data, A = Application, I = Infrastructure, SP = Security		

A.2.5 Activity 1.3: Formulate case to address the needs

Ultimately even the most well-constructed list of needs will need to be prioritized and set into a scope so that planning can be appropriately managed and performed. In this activity planners work with stakeholders to evaluate the relative priority of each need and then establish the scope of the planning effort.

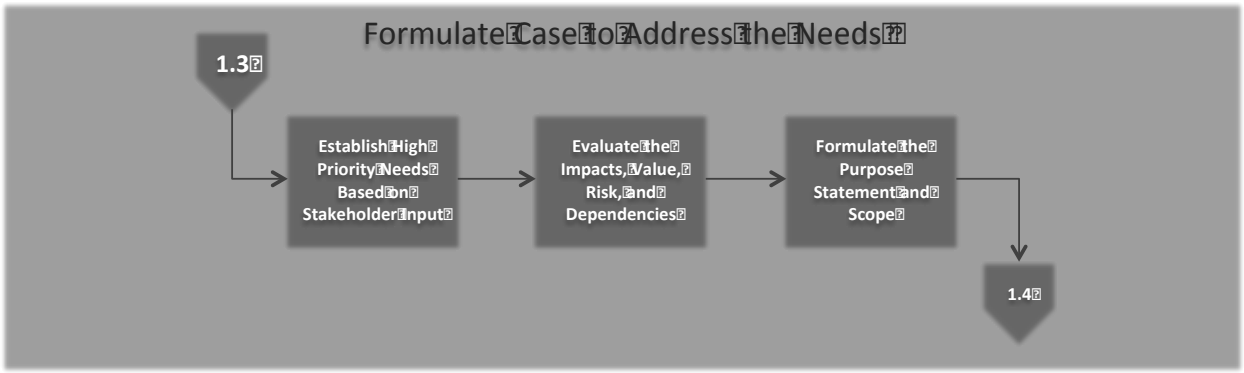
The prioritization of needs is another opportunity for the stakeholder community to have a dialogue that will ultimately bring the community together in a consistent line of thinking. The many factors that are weighed in prioritization and how members of the stakeholder community relate to (or resonate with) those factors are an important discovery. Put more plainly, it is important to understand how each stakeholder views the needs and sets the priorities of the needs differently than their peers. Planners facilitate the stakeholder community in a dialogue to discover how needs will be prioritized and how the scope of planning will be set.

In addition to the prioritization of needs, planners engage the stakeholder community to initiate performance planning. Planners, with their awareness of the high priority needs, focus on performance

metrics that are aligned to those high priority needs. This precision of focus on priority needs allows for more time and concentration to be put on planning for those needs that are most critical.

Planners leverage the high priority needs and performance metrics to develop a vision, purpose statement and scope for planning. The vision for planning is the stakeholder community's single voice as to what must be accomplished in planning given the high priority needs and emerging operational requirements. The purpose statement synthesizes this content into a statement as to why the planning must be done. This purpose statement is authored and signed by the sponsor. The scope of planning is a more detailed look at the boundaries of the planning effort given the prioritized needs, the performance metrics, the vision, and the purpose statement.

The following visual illustrates the tasks within this activity.



Activity 1.3: Formulate Case to Address the Needs

Tasks:

1.31 Establish high priority needs based on stakeholder input

The planning effort must be focused on needs that are commonly determined to be of high priority and realistic within defined drivers, assumptions, and constraints. Planners engage the stakeholder community to determine, in a structured way, the relative priority of the defined needs.

There are several ways to accomplish a prioritization of needs. In most instances it is important to evaluate the relative degree of association between the stated need and the defined performance gaps. Needs that are more closely associated with performance gaps are generally of higher priority.

In some instances, the performance gaps themselves might need to be prioritized in order to better target the intent of the planning effort. In such instances, revisiting performance gaps with the stakeholders is important to gain consensus as to which performance gaps are higher priority. After this is accomplished, the needs can be associated to the high priority performance gaps to determine the high priority needs.

One method that could be used to determine this relative importance is pairwise comparison, in this case balancing the priority of drivers against the ability of a project to address them. Methods like the Value Measuring Methodology (VMM) could also be used, although this may be more appropriate to CPM Task 3.41: Identify alternatives for transition and perform cost / value / risk analysis to compare transition alternatives.

1.32 Evaluate the impacts, value, risk, and dependencies

Finalizing the list of high priority needs cannot be done without first considering the impacts, value, risks, and dependencies associated with each need. The intent is to look more closely at each high priority need from the previous task to determine that the list of high priority needs has been defined appropriately.

Planners must evaluate each high priority need to determine the impact and value of meeting the need. During this task, planners evaluate the significance of meeting the need and specifically the degree of value and impact on stated performance gaps. This approach allows planners to begin formulating the intended or projected effects of addressing each need. This analysis is a significant start to the formulation of the performance and outcomes expectations associated with the planning effort. The planning effort must only be considering needs that are of significant impact and value to stated performance gaps.

Planners also must consider significant dependencies associated with each need. There will be instances where a need is highly aligned to a performance gap and will almost certainly provide value in relation to that performance gap, however the need may not be feasible to address due to other dependencies. These dependencies could be financial, social, political, technological, or organizational to name a few. Planners need to consider significant dependencies associated with each need and then determine if any of the dependencies render it impractical to immediately plan to address the need.

1.33 Formulate the Vision, Goals and Objectives, Purpose Statement, and Scope

After identifying the high priority needs, planners can leverage the impact and value assessment from the previous step to formulate the vision, goals and objectives, purpose statement, and scope for what is to be achieved through the planning effort. It is important to note that the performance related items are highly iterative and must continue to develop throughout the planning process. That being said, it is critical to begin the planning activities with a defined and documented vision, goals and objectives, purpose statement, and scope. These performance-related items are the guiding light for the planning process and for decision making with the stakeholder community.

Planners must leverage the stated performance gaps and high priority needs to craft a vision for what is expected as outcomes of the planning. Even at the point of having defined performance gaps and high priority needs, the stakeholder community can still have significant differences in opinion as to the vision for the future. The vision is a summary

description and illustration that captures how the world might look if the needs are appropriately addressed. At this point in the planning process, this vision and its depiction will likely be very high level. However, having this documented vision is useful to continuing to coalesce the stakeholders.

The vision is further defined by developing goals and objectives. These goals and objectives are a more detailed representation of the vision. This level of precision and detail continues to bring the stakeholders into a common alignment with a stated intent for the future. Like the vision, the goals and objectives must continue to be developed throughout the planning process. Ultimately what is planned must be evaluated against the vision, goals and objectives to determine if the planning was effective in addressing these performance intentions.

The vision, goals, and objectives must be drafted with stakeholder input and presented to the sponsor for review and approval. The sponsor then can produce a succinct, sponsor level statement that defines the purpose of the planning effort. This purpose statement must be a succinct but meaningful articulation of the major challenges or issues that the sponsor would like to see addressed, based on the vision, goals, and objectives. This purpose statement provides planners and stakeholders with a consistent, sponsor level mandate to perform the planning. The purpose statement must be direct enough to ensure that planners and stakeholders understand the sponsor level expectations and can develop an actionable, integrated plan based on those expectations.

The vision, goals and objectives, and purpose statement must be packaged into a formal scope for the planning effort. The inclusion of the priority performance gaps, the priority needs, and the intended performance metrics from previous tasks will complete the formal scope. The scope sets the boundaries for the planning effort, based on the analysis and stakeholder consensus achieved in the previous tasks.

1.3 Activity Outputs:

Output	Core	FEA Layers
Target Performance Metrics	Y	S
Impacts, Value, Risk, and Dependencies	N	S
Vision, Goals and Objectives, Purpose Statement, and Scope	Y	S
Key to FEA Layers: S = Strategy, B = Business, D= Data, A = Application, I = Infrastructure, SP = Security		

A.2.6 Activity 1.4: Identify and Engage Governance

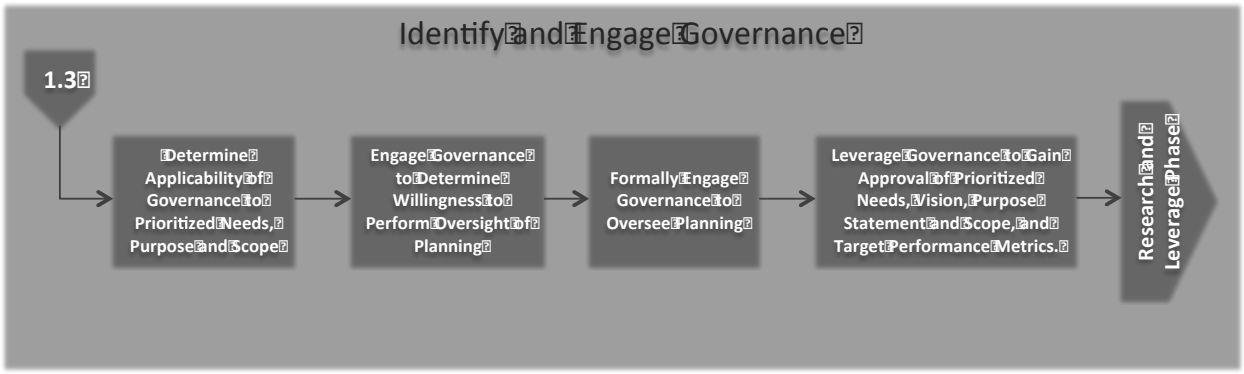
The establishment of the vision, goals and objectives, purpose statement, and scope helps shape the governance required for this planning effort. It is critical that the analysis and plans that result from the

planning effort have a defined audience with the role of reviewing and governing the decisions being made. This formalized identification of applicable governance reduces risks and provides for more clearly defined decision making authorities.

Planners work with the sponsor to develop a governance framework that forecasts the appropriate level of governance. The governance framework must identify the key roles for the planning development and show the relationships to existing governance bodies that may have operational oversight related to the scope of planning. The governance framework must include not only internal governance groups but also external groups that must be engaged for more broadly grounded governance. In establishing the governance framework with representatives from all planning disciplines, the project is alerted to the required approvals well ahead of when they take place.

Planners and sponsor can use the governance framework to illustrate the relative accountability and authority for decision-making, ensure a consistent and well-defined approach for decision-making, provide a mechanism for adjudicating disagreements or differences in perspective, and provide a definition of roles and responsibilities to ensure performance metrics are met. While the roles and responsibilities of each group or individual are described in the governance framework, many existing governance bodies will likely have existing governing charters that establish overall authority, roles and responsibilities, and decision-making processes. The governance structure must align with existing governance processes including the management of the overall enterprise architecture, capital planning process, security and privacy management processes, human capital management process, quality assurance processes, and the systems development lifecycle processes to name a few.

The following visual illustrates the tasks within this activity.



Activity 1.4: Identify and Engage Governance

Tasks:

1.41 Determine applicability of existing governance to prioritized needs, purpose and scope

Most organizations have governance teams that cover a variety of planning and execution activities. In many instances, there are teams that govern investments, projects, architectures, and other group decision activities. As previously stated, it is imperative that

the planning effort involves governance throughout the process so that incremental decisions are agreed upon and the end result is in alignment with the expectations of the governance teams.

In this task, planners review the existing governance structure and specifically look at the charters of the existing teams to determine which, if any, teams are aligned to the planning effort at hand. Planners must leverage the prioritized needs, purpose statement, and scope and find the governance team(s) with the proper alignment. It is certainly possible that none of the existing governance teams are appropriate or fully cover governance responsibilities for the planning effort at hand. In these instances, establishment of a new governance team is an appropriate course of action. The recommendations for governance team alignment must be presented to the sponsor.

1.42 Engage existing governance to determine willingness to perform oversight of planning

The sponsor is the appropriate person, in most cases, to engage directly with the chairs of the governance teams in an effort to confirm that the recommended teams are in fact appropriate for the planning effort at hand. The sponsor is seeking confirmation from the governance team chair that the governance team has appropriate charter authority and is willing to perform oversight throughout the planning process.

It is important to prepare the sponsor with a solid understanding of the planning process including the types of governance that will be required throughout the planning process. The sponsor must ensure that the governance team chair is fully aware of the scope and level of commitment that is being requested of the governance team.

1.43 Formally engage existing governance or initiate new governance to oversee planning

Through the previous tasks, either planners will have not been able to identify appropriate governance teams, or they will have found appropriate governance teams and those teams have either accepted or rejected the invitation to govern the planning at hand.

If the governance team has accepted the request to govern the planning then it is important to meet with the complete governance team, at their next meeting perhaps, and walk them through the planning approach as well as the vision, goals and objectives, purpose statement, and scope.

If the governance team has not accepted the request or no appropriate governance team has been identified, then planners must support the sponsor in formulating a new, perhaps temporary, governance team for the planning effort, including formulation of the processes and workings of that team. The formation of new governance for planning will depend on whether there is a temporary or ongoing need for this form of governance.

In some instances there is a recognized need for governance to oversee planning on a continuing basis. In these instances, a governance team must be formed and chartered with responsibilities that cover not only the planning at hand, but also to include other current and future planning efforts. In other instances it is appropriate to simply stand up a temporary governance team with responsibilities for the planning at hand.

In either instance, it is important to meet with the complete governance team, at their next (or first) meeting perhaps, and walk them through the planning approach as well as the vision, goals and objectives, purpose statement, and scope.

1.44 Leverage governance to gain approval of prioritized needs, vision, purpose statement and scope, and target performance metrics

Now that the governance team has been engaged or new governance has been initiated, it is a good idea to engage the team immediately in reviewing and approving the prioritized needs, vision, goals and objectives, purpose statement, scope, and target performance metrics.

If the governance team is new then planners must provide an environment where the governance team dynamics can form a bit prior to this approval process. If the governance team is new, or if it exists but has never performed such a review and approval, planners must help the governance team become familiar with the items under consideration, how these items set the stage for the larger planning process, and how these items will be used throughout the rest of the planning process.

1.4 Activity Outputs:

Output	Core	FEA Layers
Governance Structure	Y	S
Key to FEA Layers: S = Strategy, B = Business, D= Data, A = Application, I = Infrastructure, SP = Security		

A.3 Step 2: Research and Leverage

Purpose

The purpose of this step is to identify organizations and service providers that may have already met, or are currently facing needs similar to the ones identified in Step 1, and then to analyze their experiences and results to determine if they can be applied and leveraged or if a partnership can be formed to address the needs together. In alignment with the "Shared First" principle[1], it is at this point that planners consult both internal and external service catalogs for pre-existing services that are relevant to the current needs and can bring efficiencies in both cost and productivity. In some instances, an entire business model, policy, technology solution, or service may be reusable to address the needs defined in Step 1 – an important benefit in these cost-constrained, quickly evolving times. Based on this analysis, sponsors and stakeholders determine whether or not they can leverage the experiences and results from other organizations.

Major Participants

Planners (e.g. architects, organization and program managers, capital planners, and other planners) facilitate the project's research into other organizations and service providers to assess whether they have similar needs and whether these organizations have already met these needs or are currently planning to meet these needs. Planners lead the assessment of the applicability of the other organizations' experiences and results and help to determine whether there are opportunities to leverage or work together to plan. Once these organizations and their needs and experiences have been identified and assessed, planners formulate a set of findings and recommendations detailing the applicability and opportunity for leverage. These findings and recommendations are submitted to the sponsor who engages governance with this information as appropriate.

Outcome

At the conclusion of Step 2, planners, the sponsor, and stakeholders have a clear grasp on the experiences and results of other organizations, and the sponsor and / or governance have determined whether or not these experiences will be leveraged to meet the needs being considered as part of the planning effort. In some instances, another organization may be currently planning for similar needs and a partnership can be formed to collectively plan for these needs. The decision to leverage or not leverage has a significant impact on the planning activities in Step 3. For instance, if the organization determines that it can leverage policies and systems from another organization in order to meet its own needs, these policies and systems become a critical input to planning in Step 3. Furthermore, a detailed analysis of alternatives is part of Step 3 during Activity 3.34 and is used to confirm the choice to leverage existing solutions or services.

[1] http://www.cio.gov/pages.cfm/page/OMB-Launches-Federal-IT-Shared-Services-Strategy

A.3.1 Step At-a-Glance

Step 2 At-a-Glance	Step 2 Activities: Research and Leverage		
	Identify Organizations and Service Providers to Engage	**Analyze Opportunities to Leverage**	**Determine Whether to Leverage**
Who Participates in This Activity?	• Planners • Sponsor	• Planners • Sponsor • Organizations and Service Providers to Engage	• Planners • Sponsor • Organizations and Service Providers to Engage
What Are The Inputs to This Activity?	• Target Performance Metrics • Vision, Goals and Objectives, Purpose Statement, and Scope • Validated Register of Stakeholder Needs	• Target Performance Metrics • Vision, Goals and Objectives, Purpose Statement, and Scope • Validated Register of Stakeholder Needs • Organizations and Service Providers to Engage	• Target Performance Metrics • Vision, Goals and Objectives, Purpose Statement, and Scope • Validated Register of Stakeholder Needs • Partnership Risk and Benefits Analysis
What Are The Outputs from This Activity?	• Organizations and Service Providers to Engage	• Partnership Risk and Benefits Analysis	• Partnership Feasibility Report • Memorandum of Understanding
What Is The Relative Complexity of This Activity?			

A.3.2 A Note on Core Artifacts

Like any methodology, the *Collaborative Planning Methodology* is designed for each step to be followed and each Activity Output to be produced. The use of "Core" and "Not Core" to describe these outputs is meant as the first set of tailoring guidance if an organization has constraints of time, budget or resources. As the CPM is tested and refined, feedback from organizations will improve this assignment and generate templates that help to scale outputs according to scope or size.

As described earlier, the goal in using this methodology is to encourage collaboration for high priority projects. This increases the awareness of solutions and services whose reuse can result in efficiencies. The CPM also provides the framework for organizations to generate actionable, consistent and rigorous plans that can lead to improved solutions.

A.3.3 Activity 2.1: Identify Organizations and Service Providers to Engage

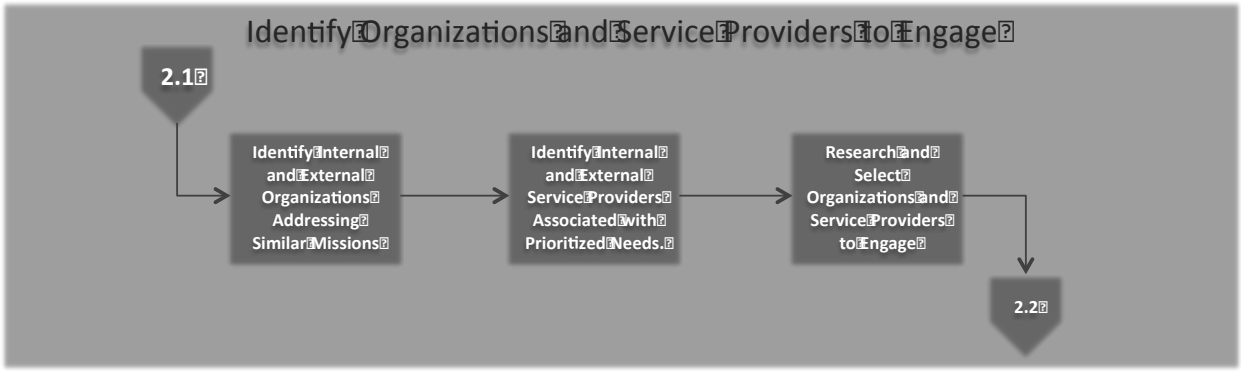
In Step 1, planners, stakeholders, sponsors, and governance have worked together to develop a validated set of stakeholder needs and the target performance, vision, goals and objectives, purpose statement, and scope associated with those validated needs. Prior to launching into full scale planning in Step 3, it is important to prepare by researching organizations and service providers that might have experiences that could be leveraged to help address the stated needs.

In this activity, planners identify organizations and service providers that have experiences that might be relevant to the needs being planned. For example, if an organization's mission is focused on water quality then perhaps another organization with a water quality related mission might have faced similar needs. Likewise, if the need at hand is focused on case management then perhaps another organization has faced a similar case management need, despite the two organizations having dissimilar missions. In other scenarios, there might be service providers that are already offering solutions related to the needs at hand. In such scenarios, planners can learn from the service providers to understand more about how the marketplace is addressing similar needs.

In each of these instances, planners are identifying which organizations and service providers will be engaged in order to determine the actual relevancy of their experiences. In Step 2, the term "experiences" can mean lessons learned, reusable requirements, reusable solutions, planning that can be done in partnership, and other experiences from which planners can learn or leverage prior to beginning the significant planning in Step 3.

To be clear, Step 2 is not about identifying solutions or performing any form of alternatives analysis. The rigor of the planning in Step 3 is required to perform such evaluations. Step 2 is about planners performing the research to determine whether there are experiences that can be considered as inputs to the planning efforts in Step 3, and to determine whether there are other organizations facing similar needs with whom it would be appropriate to plan as a team.

The following visual illustrates the tasks within this activity.



Activity 2.1: Identify Organizations and Service Providers to Engage

Tasks:

2.11 Identify internal and external organizations addressing similar missions

Planners must look broadly to find organizations that may have experiences that could relate to the needs being planned. In this task, planners look both internally and externally to the organization to find other organizations that may have similar missions. The logic in this task is that organizations with a similar mission may be facing similar needs.

For instance, if the organization has water quality as a mission then perhaps a water quality agency in another country might be a relevant organization to identify for engagement. Similarly, if a government organization processes student loans, then perhaps an external private sector organization that processes financial loans might be a relevant organization to identify for engagement.

Planners must develop a list of potential organizations to engage including how those organizations are related to the needs at hand. The concept of engaging these organizations might be abstract or foreign to some individuals, and the reasons for engagement may need to be explained in detail prior to getting approval to move forward with that engagement.

2.12 Identify internal and external service providers associated with prioritized needs

Service providers are an important element of Step 2. Service providers represent what is currently feasible within the marketplace or within a government institution. If there is a need and a business model, a service provider has often emerged to try to meet that need, in the private or public sector. Increasingly, there are service providers that offer not only technology solutions but also full scale mission solutions that can be procured.

Step 2 is not about evaluating service providers. However, performing research on service providers will provide critical information about whether a service provider has already met the needs at hand, or whether the planning in Step 3 is truly breaking new ground.

Planners must look broadly to find service providers that have experiences that could relate to the needs being planned. In this task, planners look both internally and externally to the organization to find service providers that may offer services related to the needs at hand. The logic in this task is that prior to planning, it is important to understand the needs that have already been met by service providers, and how those needs have been met.

In more plain speak, planners are trying to determine if the wheel has already been invented, or if it needs to be invented. Planners are trying to avoid re-inventing the wheel during the detailed planning in Step 3. If, for instance, the organization at hand has needs associated with payroll, then perhaps external payroll service providers would be relevant to identify for engagement or outsourcing.

Planners must develop a list of potential service providers to engage including how those service providers are related to the needs at hand.

2.13 Research and select organizations and service providers to engage

Planners have a list of internal and external organizations and service providers but need to narrow this list to a manageable collection of organizations to engage. In this task, planners must research the organizations and service providers to more accurately prioritize the targets for engagement.

Planners must perform a qualitative analysis on each organization and service provider to determine relative applicability to the needs at hand. Additionally, planners must consider the accessibility of the organizations and service providers so that engagement can be reasonably assured to be feasible. Planners must present their list of prioritized target organizations and service providers to the sponsor, prior to beginning any form of engagement activity.

2.1 Activity Outputs:

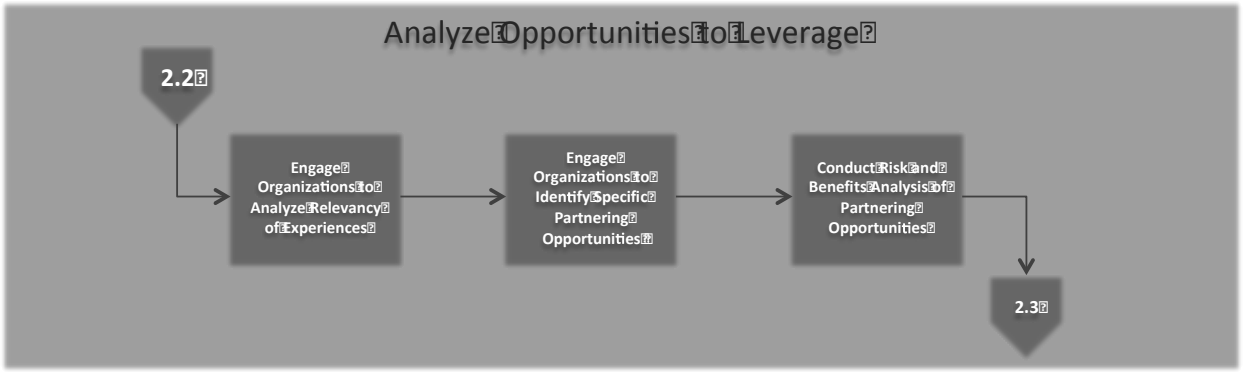
Output	Core	FEA Layers
Organizations and Service Providers to Engage	Y	S
Key to FEA Layers: S = Strategy, B = Business, D= Data, A = Application, I = Infrastructure, SP = Security		

A.3.4 Activity 2.2: Analyze Opportunities to Leverage

Once the potential organizations and service providers have been identified, planners can formally engage these groups to determine what experience is relevant to the needs at hand. Specifically, planners must engage these organizations to determine the relevancy of their experiences as well as to determine whether there are partnership opportunities with these organizations when appropriate. In

each instance, the risks and benefits of partnering must be carefully considered before establishing a partnering relationship.

The following visual illustrates the tasks within this activity.



Activity 2.2: Analyze Opportunities to Leverage

Tasks:

2.21 Engage organizations to analyze relevancy of experiences

Planners must begin by engaging their prioritized targets for engagement, identified in the previous activity. In many instances, a formal outreach from the sponsor is a good way of performing the introduction to the organizations and service providers that planners seek to engage. This outreach could be a formal email or letter or even perhaps a quick phone call to set the stage.

Planners then can perform a more tactical outreach, preferably by phone, to discuss the scope, the nature of questions, the forthcoming read-ahead materials, and to schedule the formal meeting. Whenever possible, face-to-face interaction will be the preferred method of engagement. Data calls are not an ideal mechanism for engaging with other organizations or service providers.

Planners must prepare a simple, succinct read-ahead package that includes an overview of the planning effort, the vision, goals and objectives, purpose statement, and scope. Additionally, it must be made clear to the audience why the organization or service provider was selected for engagement.

At the engagement meeting(s), planners must focus on the experiences at that target organization, including the relevancy of those experiences to the needs at hand and any architecture data that may be available from the organization. Planners must keep a record of the specific experiences, and any similarities and differences in the operating environment, constraints, and drivers that the organization faces in comparison to the organization planning for the needs. Planners must seek to identify specific experiences that could be leveraged.

2.22 Engage organizations to identify specific partnering opportunities

Upon engaging with the organizations, it may become apparent that some of the organizations are facing similar needs but have not yet planned for those needs. For instance, you may be focusing on a payroll need and may find three other organizations facing a similar payroll need. In these instances, there is an opportunity to "partner" with these other organizations to either plan together towards a common set of recommendations (perhaps shared services) or to agree on planning with parallel timelines where planning information could be shared.

In instances where the stated needs may be addressed in Step 3 with commodity type services, partnering with other organizations that are facing similar needs is a good path towards leveraging services or shared investments.

Planners must engage with the organizations to determine the interest in partnering for the planning in Step 3 and to document how that planning might be conducted should a partnership be formed.

2.23 Conduct risk and benefits analysis of partnering opportunities

If multiple partnership opportunities are available, planners need to conduct an analysis of the partnership opportunities to determine which are best in alignment with the stated needs. Planners need to consider the risks and benefits associated with partnering. For instance, risks could include a longer planning timeline, organizational differences, or a lack of leadership support for planning. Benefits could include a plan that results in a more cost effective shared service, shared cost of planning, and the ability to get fresh ideas from outside the organization.

Planners must analyze the risks and benefits of each partnering opportunity and then document the similarity in needs between the organization, the level of interest in partnering, the level of financial or resource commitment from the other organizations, the desired timeline of the other organizations, and any other facts that will help the sponsor determine whether partnering is a good decision. The risks, benefits, and other tasks must be presented to the sponsor.

2.2 Activity Outputs:

Output	Core	FEA Layers
Partnership Risk and Benefits Analysis	Y	n/a
Key to FEA Layers: S = Strategy, B = Business, D= Data, A = Application, I = Infrastructure, SP = Security		

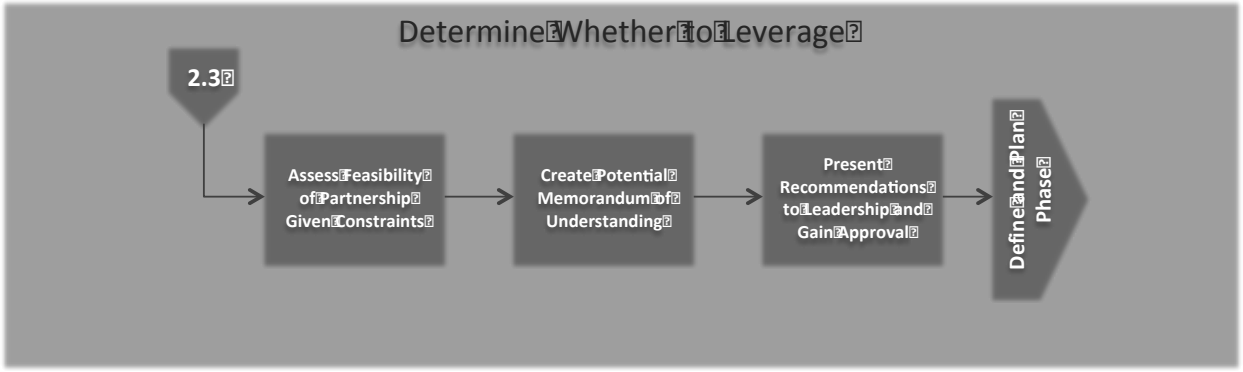
A.3.5 Activity 2.3: Determine Whether to Leverage

It is important to make a formal decision as to whether the experiences from the researched organizations and service providers should be leveraged or a partnering relationship can be established. In this activity, planners support the sponsor and governance in assessing the feasibility of leveraging experiences or partnering and then making a decision as to how that relationship will be established.

In some instances, it may be appropriate to draft a memorandum of understanding to document the terms of the relationship between the groups. This formal document will serve as a written understanding as to what each group expects including timing, financial consideration, and other important relationship matters.

Ultimately, the recommendation to leverage or partner must be presented to the sponsor and governance for formal consideration and approval. A formally approved recommendation to leverage or partner is an important input into the detailed planning in Step 3.

The following visual illustrates the tasks within this activity.



Activity 2.3: Determine Whether to Leverage

Tasks:

2.31 Assess feasibility of partnership given constraints

The risks and benefits of partnership have been considered but it is still important to evaluate the actual feasibility of a partnership given constraints on any of the relevant parties. Constraints could be financial, organizational, political, or other forms of constraints that would hold back a partnership from either being formed or being successful. Planners must analyze the partnership risks and benefits from the previous activity in the context of whether the risks are increased due to constraints, the benefits are reduced due to constraints, or whether there are constraints that make partnering difficult to the point of not being useful.

2.32 Create potential memorandum of understanding

It is important to formally document how the relevant organizations may work together. In this task, planners develop a draft memorandum of understanding to document how the experiences from another organization might be leveraged or to document how the multiple organizations would like to form a partnership for planning.

A memorandum of understanding is an important mechanism for beginning a positive working relationship with the other organizations. The memorandum of understanding does not need to be ratified during this step, however it will be a useful tool for communicating intent to the sponsor and governance.

2.33 Present recommendations to leadership and gain approval

The final decision as to whether to leverage, partner, or do neither is up to the sponsor and governance. Planners will formally package recommendations for sponsor and governance consideration. The opportunities for leverage or partnership, the related risks and benefits, the analysis of constraints, and the memorandum of understanding must be presented to the sponsor and governance.

2.3 Activity Outputs:

Output	Core	FEA Layers
Partnership Feasibility Report	Y	n/a
Memorandum of Understanding	N	n/a
Key to FEA Layers: S = Strategy, B = Business, D= Data, A = Application, I = Infrastructure, SP = Security		

A.4 Step 3: Define and Plan

Purpose

The purpose of this step is to develop the integrated plan for the adjustments necessary to meet the needs identified in Step 1. Recommended adjustments could be within any or all of the architecture domains: strategy, business, data, applications, infrastructure, and security. The integrated plan defines what will be done, when it will be done, how much it will cost, how to measure success, and the significant risks to be considered. Additionally, the integrated plan includes a timeline highlighting what benefits will be achieved, when their completion can be expected, and how the benefits will be measured. It is during this step that analysis of current capabilities and environments results in recommended adjustments to meet the needs identified in Step 1. Also during this step, the formal design and planning of the target capabilities and environment is performed. In addition to the integrated plan, the full complement of architecture, capital planning, security, records, budget, human capital, and performance compliance documents is developed based on the analysis performed in Step 3. The end outcome is an integrated plan that can be considered and approved by the sponsor and governance.

Major Participants

Planners (e.g. architects, organization and program managers, capital planners, and other planners) lead the development of the integrated plan (to include the architecture) by applying a series of analysis and planning methods and techniques. Through this process, planners plan for each of the architecture domains (strategy, business, data, applications, infrastructure, and security) and produce data as well as artifacts to capture, analyze, and visualize the plans for change. Most important is the planners' efforts to synthesize the planning into recommendations that can be considered and approved by the sponsor and governance.

During the creation of the integrated plan, planners facilitate interaction between the planning disciplines (e.g. architecture, budget, CPIC, security) so that each discipline's set of plans is integrated into a cohesive set of recommendations to meet the needs stated in Step 1. Throughout these efforts, planners maintain the integrated plan and roadmap to reflect the course of action that has been determined through these planning activities.

Outcome

At the end of Step 3, the sponsor and stakeholders will possess an integrated plan and artifacts defining what will be done, when it will be done, what benefits will be achieved and when, and an estimate of cost. This integrated plan must be synthesized into discrete decision-making packages for the sponsor and governance that are appropriate given financial, political, and organizational constraints.

A.4.1 Step At-a-Glance

Step 3 At-a-Glance	Step 3 Activities: Define and Plan				
	Formalize Collaborative Planning Team and Launch Planning	**Refine the vision for performance and outcomes**	**Analyze the Current State, Determine Adjustments, and Plan the Target State**	**Formulate the Integrated Plan and Roadmap**	**Initiate Execution Governance**
Who Participates in This Activity?	• Planners • Stakeholders • Sponsor • Governance	• Planners • Stakeholders • Sponsor • Governance	• Planners • Stakeholders • Sponsor • Governance	• Planners • Stakeholders • Sponsor • Governance	• Planners • Sponsor • Governance
What Are The Inputs to This Activity?	• Validated Register of Stakeholder Needs • Vision, Goals and Objectives, Purpose Statement, and Scope	• Validated Register of Stakeholder Needs • Vision, Goals and Objectives, Purpose Statement, and Scope • Partnership Feasibility Report • Memorandum of Understanding • Communication Strategy	• Validated Register of Stakeholder Needs • Vision, Goals and Objectives, Purpose Statement, and Scope • Partnership Feasibility Report • Memorandum of Understanding • Affected organizations and stakeholders • Prioritized strategic improvement Opportunities • Communication Strategy	• Business, data, enabling applications, and infrastructure artifacts from previous task • Architecture, Capital Planning, Security, Records, Budget, Human Capital, Section 508 Accessibility and Performance Compliance Documents from previous task	• Integrated Plan Document • Record of Decision • Recommendation Implementation Sequencing Plan

Step 3 At-a-Glance	Step 3 Activities: Define and Plan				
	Formalize Collaborative Planning Team and Launch Planning	**Refine the vision for performance and outcomes**	**Analyze the Current State, Determine Adjustments, and Plan the Target State**	**Formulate the Integrated Plan and Roadmap**	**Initiate Execution Governance**
What Are The Outputs from This Activity?	• Collaborative Planning Team (CPT) Roster • Collaborative Planning Team Formation Memorandum • Collaborative Planning Team Charter • Project Plan • Communication Strategy	• Affected organization and stakeholders • Refined Vision, Goals and Objectives, Purpose Statement, and Scope • Performance scorecard • Prioritized strategic improvement Opportunities • Presentation on Vision for Performance and Outputs	• Artifacts and Data (Appropriate Level of Specificity) for the Integrated Plan • Architecture Development Project Plan • Business, data, enabling applications, and infrastructure artifacts • Business and Data Architecture Adjustment Profiles • Business and Data Environment Presentation • Enabling Applications and Infrastructure Presentation • Architecture, Capital Planning, Security, Records, Budget, Human Capital, and Performance Compliance Documents	• Transition Recommendation Profile • Transition Recommendation Sequencing Diagram • Recommendation Sequencing Milestones • Proposed Implementation Recommendations • Analysis of Cost, Value, and Risk for Transition Options • Recommendation Implementation Sequencing Plan • Transition Plan Milestones • Application Migration / Sequencing Overview • Document Review Log • Feedback Tracking Document and Action Report • Integrated Plan Document • Executive Summary Presentation • Record of Decision • Policy, Procedures, and Guidance	• Governance Structure (Project Governance)
What Is The Relative Complexity of This Activity?					

A.4.2 A Note on Core Artifacts

Like any methodology, the *Collaborative Planning Methodology* is designed for each step to be followed and each Activity Output to be produced. The use of "Core" and "Not Core" to describe these outputs is meant as the first set of tailoring guidance if an organization has constraints of time, budget or resources. As the CPM is tested and refined, feedback from organizations will improve this assignment and generate templates that help to scale outputs according to scope or size.

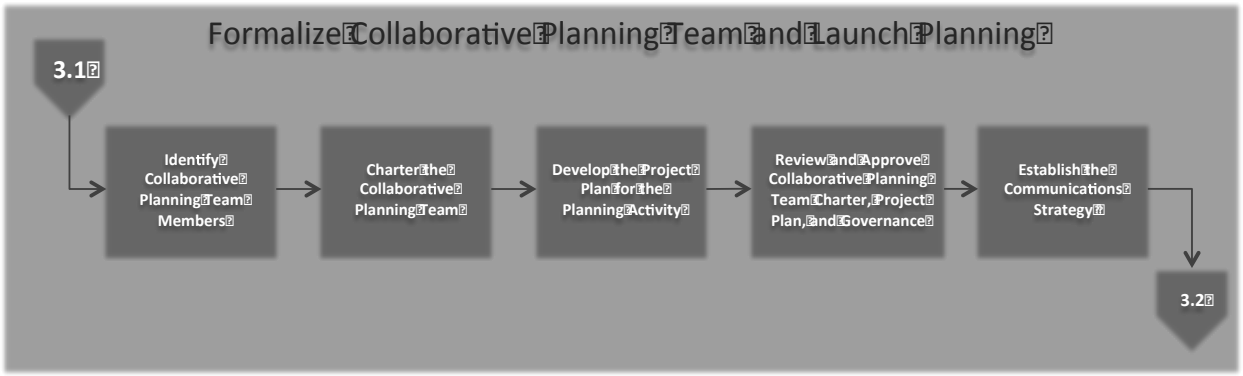
As described earlier, the goal in using this methodology is to encourage collaboration for high priority projects. This increases the awareness of solutions and services whose reuse can result in efficiencies. The CPM also provides the framework for organizations to generate actionable, consistent and rigorous plans that can lead to improved solutions.

A.4.3 Activity 3.1: Formalize Collaborative Planning Team and Launch Planning

Step 3 begins with the formation of the *collaborative planning team*. The collaborative planning team is a working level body of individuals that represent and can make decisions on behalf of the key stakeholder groups. Additionally, the collaborative planning team includes planners themselves. The collaborative planning team is an important group, as these representatives will guide the development of the planning in Step 3. During this activity, the sponsor solicits key personnel from each affected stakeholder group to form the collaborative planning team that will remain as a standing body throughout the planning process. The formation of the collaborative planning team includes the development of the charter that bonds the team members into active and constructive participation throughout the planning process. The charter formalizes the team's participation in developing the integrated plan in the context of the purpose statement crafted by the sponsor.

Lastly, this activity is intended to start the planning off on a solid project management foundation. This activity includes guidance for developing the project plan and communication strategy; both will be used throughout the planning process.

The following visual illustrates the tasks within this activity.



Activity 3.1: Formalize Collaborative Planning Team and Launch Planning

Tasks:

3.11 Identify Collaborative Planning Team Members

It is important to educate the sponsor on the role of the collaborative planning team. The collaborative planning team is the key group of working level resources that will help shape and develop the integrated plan to meet the prioritized needs. Overall, the collaborative planning team members should expect to contribute a significant amount of time thinking about and meeting on the formation of the integrated plan.

In most cases, the sponsor will appoint the collaborative planning team. The appointment of the team members usually involves an assessment of personnel to ensure that desired personnel are available and can contribute time to the development of the plan.

Once appointments have been determined, a formal outreach to the appointed individuals is a good way to bring those individuals into the planning process. Sometimes a one on one conversation with each appointed individual is better than a group introduction to the process and the role of a collaborative planning team member.

Although the communication strategy has not yet been developed, this task produces a communications item in the form of a collaborative planning team formation memorandum to communicate the existence of the collaborative planning team, its members, and its purpose.

3.12 Charter the Collaborative Planning Team

The collaborative planning team charter must include the role of the collaborative planning team members, roster of the team, decision-making structure for the team, purpose statement, and the scope of the planning.

Although the collaborative planning team charter is an important document, it must not take months to develop. Each of the team members must sign the charter, including the sponsor.

3.13 Develop the Project Plan for the Planning Activity

Although the planning team is just being formed, a project plan must be developed to detail the milestones and proposed dates for the development of the integrated plan. In this task, the project plan must be based on the outline of activities and tasks within Step 3. It may seem early in the process for developing the project plan however the collaborative planning team has the advantage of a documented purpose statement, scope, and other strategic information from Step 1.

There is always a risk of the planning becoming a prolonged analytical exercise. The project plan will help ensure that the integrated plan is developed within an acceptable time frame. This project plan will be revised later in Step 3 when more is known about the nature of the planning at hand.

3.14 Review and approve Collaborative Planning Team charter, project plan, and governance

It is important that the development of the integrated plan begin with common intentions and a common understanding of expectations. The collaborative planning team charter and project plan must be reviewed and approved by the sponsor and governance to ensure approval of how the team has been formed, the chartered intent of the team, and the project plan for how the team intends to develop the integrated plan.

3.15 Establish the communication strategy

Successful communication requires the development of a communication strategy. The communication strategy must identify relevant stakeholders in the context of the purpose statement and the collaborative planning team's knowledge of the affected organizations. The communication strategy includes the necessary value-based messages for the respective types of stakeholders.

For effective communications and collaboration, the collaborative planning team must establish a web site to facilitate barrier-less information dissemination. The communication strategy must address the necessary targeting (stakeholder, timing, and delivery means) of the value messages that are important throughout the project. This targeting must be orchestrated with existing organizational and informational channels, behaviors, calendars, and events to optimize reach and usefulness.

Examples of key organizational events would be workshops, collaborative forums, communities of practice or interest (COP, COI), and the annual budget and CPIC cycles. The communication plan must identify the optimal formats and delivery channels (email, brochure, presentations, and web) to sustain effective communications.

First, it is important to consider what the collaborative planning team needs to accomplish with its communication strategy. A simple dialogue with the collaborative planning team can help determine objectives to be included in their communication efforts. The governance framework can also provide additional guidance as to the specific communication needs and requirements associated with key governance stakeholders. The effectiveness of communication efforts can be measured by the goals and objectives established.

Based on the vision, goals and objectives, and scope, a facilitated session with the collaborative planning team can help identify the audience groups to which communications must be directed. For each audience group, the communication strategy must capture the design themes and key messages that are relevant throughout the architecture development process.

The tactical communications vehicles must be determined based on the communication strategy. Since the collaborative planning team has already established the communication goals and objectives, audience groups, design themes and key messages, tactical

communications vehicles can be selected more intelligently as appropriate. Common vehicle types include print, web and multimedia. Within those vehicle types are tactical communications vehicles such as brochures (print), slick sheets (print), website (web), collaboration forums (web), videos (multimedia), microblogs (internet), blogs (web), and social media (internet).

Since there are many documents that will be formulated and reviewed during the planning process, a collaborative website improves communication and consensus building. Project websites are an ideal way of keeping collaborative planning team members and even audience groups abreast of meetings, presentations, decisions, and the overall planning progress.

3.1 Activity Outputs:

Output	Core	FEA Layers
Collaborative Planning Team Roster	N	n/a
Collaborative Planning Team Formation Memorandum	N	n/a
Collaborative Planning Team Charter	N	n/a
Project Plan	N	n/a
Communication Strategy	N	n/a

Key to FEA Layers: S = Strategy, B = Business, D= Data, A = Application, I = Infrastructure, SP = Security

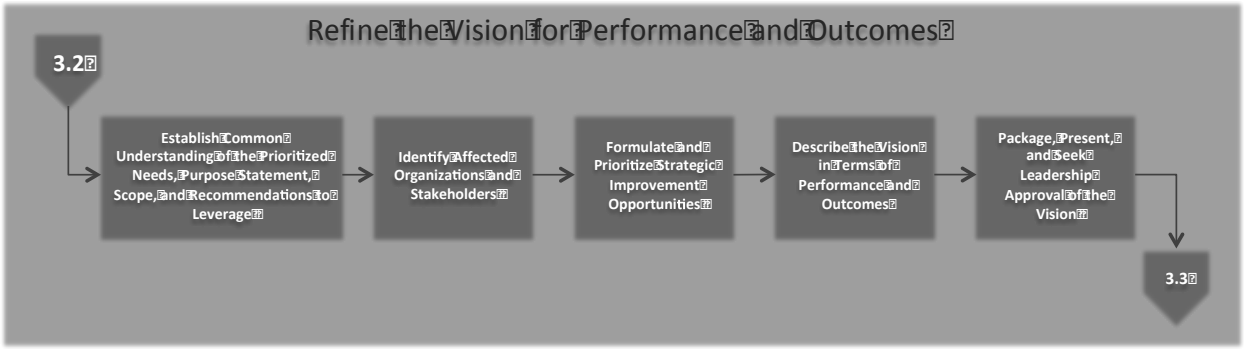
A.4.4 Activity 3.2: Refine the vision for performance and outcomes

The vision for performance and outcomes was developed in Step 1 however now that the collaborative planning team is formed it is important to revisit this information as a team. In Step 1, the needs were developed, validated, and prioritized and based on this the vision, goals and objectives, purpose statement, and scope were developed. The Step 1 activities were conducted with planners, the sponsor, and the stakeholder community so it is to be expected that these outcomes are very well representative of the vision for performance and outcomes.

Since the conclusion of Step 1, planners have actively engaged other organizations and service providers in Step 2 to research and perhaps leverage their experiences or partner with them to conduct coordinated planning. The outcomes of Step 2 as well as the experiences and perspectives of the individuals within the collaborative planning team will perhaps change some of the outputs from Step 1.

It is in this activity that the vision for performance and outcomes is revisited by the core team and the strategic improvement opportunities are formulated and prioritized from the perspective of the collaborative planning team.

The following visual illustrates the tasks within this activity.



Activity 3.2: Refine the Vision for Performance and Outcomes

Tasks:

3.21 Establish common understanding of the prioritized needs, purpose statement, scope, and recommendations to leverage

The collaborative planning team reviews the outputs of Steps 1 and 2 with planners and sponsor to establish a firm understanding of the planning challenge at hand. Specifically, it is important to bring each individual team member up to speed with the vision, goals and objectives, purpose statement, and scope; as well as the sources of this information within the stakeholder community.

The collaborative planning team needs to understand where the needs came from, why some needs were prioritized over others, how the needs translated into performance gaps and measures, how certain experiences were chosen to be leveraged, and how the sponsor has articulated the purpose of the team in its planning endeavor.

Planners must facilitate an open discussion of the Step 1 and Step 2 materials with the collaborative planning team to ensure that the materials are understood and embraced by the team as a starting point for planning.

3.22 Identify affected organizations and stakeholders

With a firm understanding of the vision, goals and objectives, purpose statement, and scope, the collaborative planning team identifies the organizations and stakeholders that are affected and their high-level relationships. Similar activities were conducted in Steps 1 and 2 for the purposes of identifying needs, leveraging experiences, and forming partnerships. In this task, the collaborative planning team is, for the first time, providing their specific knowledge and experiences to identify the affected organizations and stakeholders that may not yet have been identified.

Planners must review the newly updated list of affected organizations and stakeholders to determine if any of the Step 1 outputs must be revisited based on newly identified individuals to engage. In most instances, this task produces a list of additional people to engage for the purpose of validating the outputs from Steps 1 and 2 and to bring other key stakeholders along in the evolution of the planning. Key stakeholders or affected organizations on the list that are new and could provide new perspectives must be engaged in order to refine the outputs from Step 1.

3.23 Formulate and prioritize strategic improvement opportunities

Leveraging the needs, vision, goals and objectives, and scope developed in Step 1, the collaborative planning team needs to synthesize this information and formulate strategic improvement opportunities. The collaborative planning team is a working level team and this perspective will help to drill down into the outputs from Step 1 to identify specific strategic improvement opportunities.

The strategic improvement opportunities will be strongly related to the prioritized needs and will be developed as a means to achieve the vision. The list of strategic planning activities will be a succinct explanation of what strategic changes can be made to address the needs and achieve the vision.

The initial draft of the strategic improvement opportunities must be assessed to identify internal and external factors that may contribute to, or detract from, the achievement of the improvements identified. In doing so, the prioritization and selection of the strategic improvement opportunities must be grounded using the same validation process used to validate the needs in Step 1.

Once the strategic improvement opportunities have been developed and validated, they must be prioritized. Just as the needs were prioritized in Step 1, the list of strategic improvement opportunities must be prioritized to ensure that high priority strategic improvement opportunities are addressed first.

3.24 Refine the vision in terms of performance and outcomes

With a firm understanding of the prioritized strategic improvement opportunities, the collaborative planning team must revisit and refine the vision, goals and objectives, and performance measures that were output from Step 1. The new perspectives of the collaborative planning team, the new perspectives of newly identified organizations and stakeholders, and the process of developing and prioritizing strategic improvement opportunities can all influence modifications to the Step 1 outputs. This task is not as much about simply updating outputs as it is about being precise and accurate in the strategic intent of what is being planned.

The collaborative planning team must develop a simple one-page graphic illustrating the target state vision to meet the prioritized needs (e.g., Target Concept of Operations or DoDAF OV-1). The illustration must be a high-level description of the future once the strategic improvement opportunities have been addressed. This graphic is meant only to illustrate an early representation of the target state and will be enhanced, perhaps significantly, by additional analysis throughout Step 3. A summary vision statement describing the graphic and helping audiences understand the perspective of the collaborative planning team must complement the graphic.

This task also includes establishing the performance scorecard, which is focused on providing a complete picture of performance from the highest level of strategic performance down to business and investment performance to measure the success in achieving the target goals and vision. Note that when developing the performance scorecard, not all performance indicators, measures, and metrics will be known at this point. In subsequent activities planners will identify additional indicators, measures, and metrics through which the progress will be measured.

Performance indicators must be structured according to a balanced set of categories to ensure the targeted vision has a balanced set of outcomes. Ultimately these performance indicators will be used to understand the success the implementation of the plan has had in relation to the originally stated needs.

3.25 Package, present, and seek leadership approval of the vision

Planners must develop a package that summarizes the refined vision including the strategic improvement opportunities and the performance scorecard. Planners must prepare a presentation that includes the vision materials and present these materials in a decision-oriented format to the collaborative planning team for review and approval.

Planners must conduct a detailed workshop review of these vision materials so that the collaborative planning team members can feel comfortable articulating these materials within their respective organizations or stakeholder communities. The collaborative planning team then decides whether to proceed to presenting the materials to the sponsor and governance, or to refine the vision materials further.

It is recommended that there be a formal sign-off of the vision materials by the sponsor and governance. In order to solicit further support for the vision materials including the strategic improvement opportunities, optional sign-off of the materials must also include other key leadership roles such as the performance improvement officer (PIO), chief information officer (CIO), and the change management officer (CMO), when appropriate for the level of scope of the planning. The level of optional sign-off is defined at the discretion of the project sponsor.

3.2 Activity Outputs:

Output	Core	FEA Layers
Affected Organization and Stakeholders	N	n/a
Refined Vision, Goals and Objectives, Purpose Statement, and Scope	Y	S
Performance Scorecard	Y	S
Prioritized Strategic Improvement Opportunities	Y	S
Presentation on Vision for Performance and Outputs	N	S
Key to FEA Layers: S = Strategy, B = Business, D= Data, A = Application, I = Infrastructure, SP = Security		

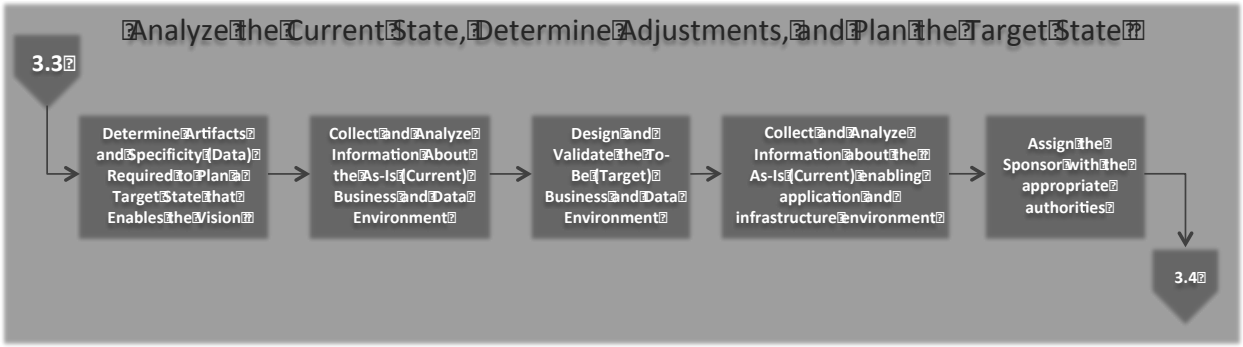
A.4.5 Activity 3.3: Analyze the Current State, Determine Adjustments, and Plan the Target State

This activity includes tasks that are very commonly related to architecture planning. Specifically, in this activity planners work with the collaborative planning team to assess the current business and data environment to form recommendations for how to change that environment to fulfill the strategic improvement opportunities. Then planners build from those recommendations to assess the current enabling application and infrastructure environment to form recommendations for how to change that environment to best enable the newly designed target business and data environment.

Planners are working on a set of inter-related views of the environments that ultimately make up the target or future state. Strategic improvement opportunities need to be fulfilled. These strategic improvement opportunities can be fulfilled by changes in the business and data environment. The changes in the business and data environment generally must be supported or enabled by changes in the enabling applications and infrastructure environment.

One key part of this activity is the first task where planners review the vision materials from the previous activity and determine what type and levels of planning are required to form recommendations for how the vision can be achieved. All planning efforts are not the same and therefore it is critical that planners first think about what needs to be planned, how it needs to be planned, what information and materials are required as inputs and outputs of the planning, and then to set a project plan based on these conclusions. The end result will be a more nimble planning exercise where the materials produced from the analysis will be “just enough”, and “just in time” for making decisions. This is a hallmark of the modern planning environment where nimble planning is critical to achieve results.

The following visual illustrates the tasks within this activity.



Activity 3.3: Analyze the Current State, Determine Adjustments, and Plan the Target State

NOTE: This is the only activity within the Collaborative Planning Methodology (CPM) that includes both tasks and sub-tasks within the activity. The tasks involved with analyzing the current state, determining adjustments, and planning the target state are complex and require a deeper level of methodology. As a result, the CPM has been created to include sub-tasks in this section to provide more detail.

Tasks:

3.31 Determine Artifacts and Data (Appropriate Level of Specificity) Required to Plan a Target State that Enables the Vision

As previously stated, each planning effort is different and most require some form of tailoring of the approach based on the nature of the planning at hand. For instance, in some cases the planning might be more business focused while in other cases the planning might require a stronger technology focus. Furthermore, in some cases the planning might be at an international level of scope while in other cases the planning might be at an application level of scope.

In addition to the area of emphasis and level of scope, there could possibly be mandated compliance documentation or other requirements that influence the nature of the planning. Compliance requirements such as architecture plans, capital plans, security plans, records plans, Section 508 accessibility standards and others must also be considered in this task. Information that is required for each of these required plans must be assembled as part of the planning tasks and sub-tasks.

In this task, planners consider the area of emphasis and the level of scope for the prioritized needs and vision. Additionally the other compliance requirements are considered for applicability. Planners use this information to determine which artifacts and data are required to plan for the vision.

Sub-Tasks

3.311 Determine Level of Scope from the Common EA Approach

The document titled *Common Approach to Federal Enterprise Architecture* has documented the "levels of scope" and these levels of scope must be considered in this sub-task. There are eight levels of scope described in the *Common Approach to Federal Enterprise Architecture*:

International
National
Federal
Sector
Agency
Segment
System
Application
These levels of scope promote consistency in planning as different approaches and techniques can be used for the varying levels of scope. The level of scope of a particular planning effort can range from high-level views of one or more organization, to detailed views of a single segment, system, or application.

For the planning at hand, planners must assess the needs, strategic improvement opportunities, and especially scope to determine which of the levels of scope apply.

3.312 Determine Sub-Architecture Domain/Viewpoint Emphasis

Just as the *Common Approach to Federal Enterprise Architecture* describes the levels of scope, it also describes the concept of sub-architecture domains or what are called viewpoints in some planning communities.

Planning supports decision-making through the creation of recommendations and support materials across various aspects of the problem set at hand. There are six "domains" within and across which planning is conducted. When planning for a need, planners must consider recommendations within the following domains:

Strategy
Business Services
Data and Information
Enabling Applications
Host Infrastructure
Security Controls

Note: Several of the items in the list of domains are particularly IT focused. In many planning scenarios there may be an even broader list of non-IT domains depending on the nature of the needs being addressed.

For the planning at hand, planners must assess the needs and strategic improvement opportunities to determine which of the domains are relevant and which are of particular emphasis. As previously stated, some planning efforts will have strategic improvement opportunities that are more focused on business services while other planning efforts might have strategic improvement opportunities more focused on security controls. It is generally the case that most if not all sub-architecture domains are relevant, in varying degrees.

3.313 Determine Relevant Artifacts and Data (Appropriate Level of Specificity) required for each Sub Architecture Domain

Based on the conclusions drawn in the previous two sub-tasks, planners must determine which artifacts and data are appropriate for the planning at hand. Specifically, planners must focus on the artifacts and data that are relevant for the level of scope and specifically the level of detail required for the level of scope. Additionally, planners must focus on the domains or viewpoints that are of emphasis given the planning at hand.

Planners must review the artifacts types described in the *Common Approach to Federal Enterprise Architecture* (Documentation, p26) to determine which are appropriate for the planning at hand. Beyond just the artifacts, planners must focus on the data within the artifacts. Planners need to determine which data and to what specificity is required so that recommendations can be formed to meet the needs and vision.

3.314 Determine other information required for the integrated plan

There are a wide variety of compliance or required planning artifacts and reports depending on the nature of the planning and the organizations, countries, companies, or industries involved with the planning. In many instances, architecture plans, capital plans, security plans, records plans, specific types of transition plans, business cases, and other such documents are required for investments to be made. In such instances, it is important for planners to consider the needs and vision at hand and then determine which of the compliance or required planning artifacts will need to be produced during this planning process.

The intent is that after concluding with the Collaborative Planning Methodology, an integrated plan would exist and this integrated plan would include all the compliance or required planning artifacts.

3.315 Tailor the remaining steps of the methodology based on the artifacts identified in the previous steps

Planners now know the level of scope, the domains of emphasis, and the compliance or required planning artifacts associated with the needs, vision, and scope of the planning at hand. Based on this information, planners must leverage the list of remaining activities, tasks and sub-tasks in Step 3 to refine the project plan based on the specific needs of the planning at hand.

This tailoring approach allows for more nimble, cost effective planning. This tailoring approach also helps to reduce the risk of burnout within the collaborative planning team or loss of political will for an overly elaborate planning effort.

Planners must refine the project plan and then ensure that it is appropriately communicated to the collaborative planning team members, the sponsor, and governance.

3.32 Collect and Analyze Information about the As-Is (current) business and data environment

Planners have a project plan that is tailored to include the specific analysis activities that are required for the planning at hand. Based on this project plan, planners begin the process of collecting information about the current or as-is business and data environment. The business environment includes business functions, processes, rules, logic, and resources. The data environment includes the data that is being used within the business processes, the flow of data between and throughout processes, and the transformation of data into information as an output of the processes. When appropriate, the Business Reference Model and Data Reference Model described in *A Common Approach to Federal EA* may be used to assist in reviewing the current environment.

Planners need to gather this information about the business and data environment so that they can analyze the environment and determine what is driving the performance gaps and needs identified in Step 1. Planners are seeking to identify the constraints that are driving the existence of the strategic improvement opportunities.

<u>Sub-Tasks</u>

3.321 Collect information on the business functions and interdependencies relevant to the prioritized needs

In this sub-task, planners are determining the business functions that are relevant to the needs and vision so that those functions can be analyzed and recommendations can be formed in subsequent sub-tasks. Planners must first determine the business services that are being performed in the business environment. For instance, a business service

could be payroll operations. Within the context of the needs and vision, there will be a few key business services that are important to the planning effort.

Once the key business services are identified, planners must map the needs and performance gaps to the services in order to determine a current level of service being provided. For instance, the payroll service might be lacking in advanced tax calculations and might take 50% too long to produce and process the payroll. This is the current level of service. This information is documented in the business services maturity matrix as the "level 0" or baseline level of maturity. In subsequent tasks planners will plan for incremental levels of business services maturity based on the level 0 maturity specifics.

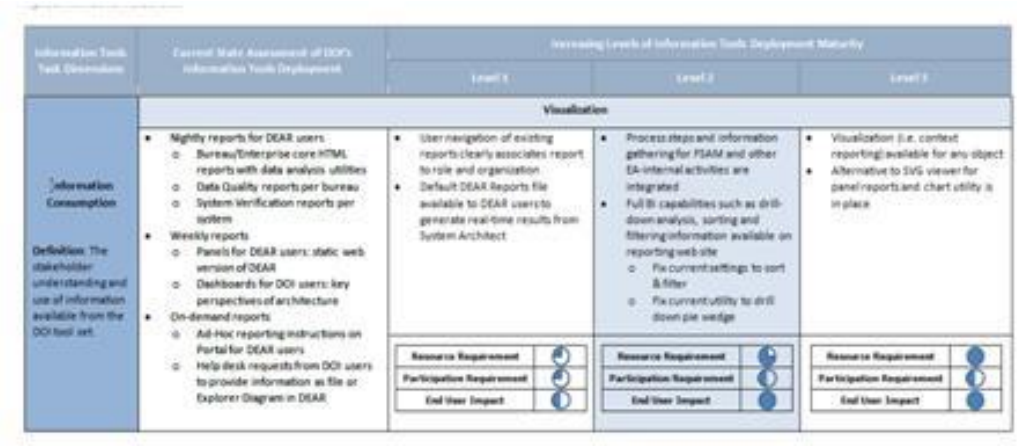


Figure A.3: Sample Maturity Matrix

Using the business services and the level 0 depiction in the maturity matrix, planners focus on the business processes that the organization must perform in order to deliver those business services. This analysis must begin with a high-level focus on the key business processes that deliver services, with the intent of identifying the critical chain of business processes that deliver value. The business services maturity matrix serves as a scoping tool to ensure that the planning effort maintains focus on the services that require attention, so the target vision, and goals and objectives can be achieved.

Each business service must be analyzed to determine the business area's *current* chain of business processes that deliver each service. The chain of business processes will be diagramed using a value chain drawing. The value chain drawing is a high-level logical ordering of business processes that provides an overview of how value (i.e., product or service) is produced. The collaborative planning team must not default to an "analysis paralysis" mode; if the current value chain of business processes is determined to be ad-hoc, or if consensus cannot be determined, this may highlight a major finding and result in a recommendation for business process definition, optimization, or standardization. The planning scope may contain several value chains. However, to maintain a manageable scope, the focus must be on the few that most require attention.

Documenting the value chains is an important mechanism for determining the elements of the business environment associated with the strategic improvement opportunities. By focusing on a specific value chain, planners can perform additional business environment analysis on the areas of impact, based on the needs and vision.

Next it is important to define the business function model and associate it to the value chain. Planners associate the business processes in the value chain to their associated business function(s) in order to identify the magnitude of the business functions that will be affected by potential business process improvements. In the case of business processes that deliver enterprise services (e.g., geospatial, infrastructure), a full mapping is not necessary, although understanding the magnitude of functions affected is helpful in determining future implementation level impacts (e.g. scalability).

To define the business function model, business areas must be decomposed to define a hierarchy that includes functions and business processes. A business function is a logical set of business processes performed on a continual basis that has no specific beginning or end point. Functions are decomposed into business processes, which are a group of related business activities usually executed in a sequential fashion to achieve an intermediate or end-result product or service.

The business function model is created to show the critical business processes identified in the value chain analysis in the context of the business area functions. Existing reference models that catalog enterprise business functions may be used in structuring the functional hierarchy, but the business processes in the business function model must be consistent with the business processes defined in the value chain models. The intent of this documentation is to ensure that the business processes are affiliated with the business functions.

The information collection during this sub-task must also identify the organizations that perform the business processes and activities. Interactions across organizational boundaries in performing the business processes must be described so that ownership and accountability can be analyzed in subsequent sub-tasks. These interactions can be described using swim-lane diagramming techniques. In many instances, the analysis of organizational relationships to business processes and activities can yield critical insight into the current state environment.

Overall, it is important to document business processes and activities to a level that is meaningful for identifying requirements that will help achieve the strategic improvement opportunities. Extended process modeling efforts are not recommended unless clearly warranted based on the strategic improvement opportunities or the value chain analysis. In this case where additional projects may emerge, it may benefit the organization to return to an earlier step within the CPM to reprioritize the projects and their strategic value.

3.322 Identify and assess high-level information/data, dependencies, and information sources associated with the relevant business functions

Through the business process and activity analysis, planners have become more familiar with the business's data environment. Although planners will document business modifications that can help achieve the strategic improvement opportunities, planners must re-use the business process and activity analysis to determine if there are information/data deficiencies that require adjustment to the current state.

For example, planners might have conducted business process analysis and determined that the business processes are sound but may also have noticed information-related deficiencies (e.g., insufficient data to make business decisions, redundant data entry between systems or manual routing of information that can be automated via information exchanges). In this case, planners may observe that there is an information collection and/or sharing deficiency whose resolution might lead to the achievement of a strategic improvement opportunity.

Planners must identify the high-level information requirements associated with the key business functions and processes identified in the previous sub-task. Planners need to determine where the data comes from, identify the major dependencies on the data besides the processes in focus for the planning, and define which information sources store the data.

Through the documentation of the business processes and information flows, planners must become familiar with the information requirements critical to the business. During this sub-task, planners must perform a qualitative analysis of the usefulness of key as-is information sources. The intent of this task is to document the sources of information in the current state before qualitatively assessing them along the key dimensions of accuracy, completeness, consistency, precision, timeliness, uniqueness, and validity. Part of the assessment of current data sources is the identification of existing security and privacy controls that are a part of the business's workflow, data management practices, system designs, infrastructure management, and other protective measures.

Part of the development of target information services in later tasks is identifying target authoritative data sources (ADS) for key shared information. In this sub-task planners need to collect information on the myriad data sources including whether the same information exists in multiple sources and whether this information has become inconsistent because of differences in data management practices. This can be a root cause of business process and information delivery issues.

3.323 Analyze the business and data environment and determine the required strategic and operational business and data adjustments to fulfill the vision

Planners must analyze the gap between the current and required business environment in the context of the strategic improvement opportunities. In this sub-task, planners must determine which elements within the current state business and data environment must change to meet the desired strategic improvement opportunities. Planners must describe the needed changes to the business and data environments and whether any of these changes are currently addressed with planned initiatives or investments. The result of this sub-task is an articulation of the changes that must be made within the target business and data environment.

In order to determine which elements of the business environment to analyze, planners need to map the strategic improvement opportunities to the key business processes previously documented. In many cases, business processes are defined at a level too high to determine where deficiencies in performance or service delivery are occurring and may need to be decomposed to the activity level. Critical business processes must be defined at the activity level to derive high-level information requirements for the service. Although this methodology does not prescribe a standard modeling notation for this task, at a minimum, business processes must be modeled to depict information inputs, outputs, and value-added activities to perform the business process.

Using the mapping of business processes to strategic improvement opportunities, planners must determine the elements of the business environment that need to be adjusted to achieve the strategic improvement opportunities. For example, if the analysis of the current business processes reveals business process efficiency opportunities and those business processes are tied to strategic improvement opportunities, planners must determine if the business process efficiencies will help achieve those strategic improvement opportunities and therefore must be recommended. The intent of this analysis is not to attempt to re-engineer business processes by recommending numerous changes to the business environment, but to determine the key business processes and critical adjustments necessary to achieve the strategic improvement opportunities.

Planners must also do the research required to determine if business and IT initiatives are currently planned that would support the required changes in the business environment, and whether these initiatives would, when implemented, fully or partially, address the required adjustments.

Planners must document potential changes to the business environment that could help achieve the strategic improvement opportunities. Planners must use a formal template to document the limitations of the current state, desired characteristics of the target

state, how the target state will help achieve the strategic improvement opportunities, and any known risk and cost considerations.

Once the business environment changes have been documented, it is important to also consider the data environment and changes that might be necessary. Just as with the business environment, planners must map the data environment to the strategic improvement opportunities to determine which elements of the data environment must be adjusted to achieve the strategic improvement opportunities. For example, if the analysis of the current business processes revealed information collection, storage, and sharing opportunities tied to strategic improvement opportunities, planners need to determine if the data environment opportunities will help achieve those strategic improvement opportunities and must therefore be recommended.

Part of the determination of adjustments to the data environment is the identification of existing security and privacy controls that will be a part of the business's workflow, data management practices, system designs, infrastructure management, and other protective measures. The intent of this analysis is not to re-design the full data environment by making numerous information related recommendations, but to determine the key high-level adjustments necessary to achieve the strategic improvement opportunities.

Creation of new authoritative data sources (ADS) may be required to achieve identified strategic improvement opportunities. Planners must also do the research required to determine if there are business and IT initiatives currently planned that would address the changes in the data architecture and whether these initiatives would, when implemented, fully or partially address the required adjustments.

Planners must document potential changes to the data environment that could help achieve the strategic improvement opportunities. Planners must use a formal template to document the limitations of the current state, desired characteristics of the target state, how the target state will help achieve the strategic improvement opportunities, and any known risk and cost considerations.

3.33 Design and Validate the To-Be (Target) Business and Data Environment

During this task, planners must define the optimal target business and data environment to reflect each of the business and data changes identified in the prior sub-tasks. During this task, planners will define the target business and data environment by developing target versions of the current state business and data artifacts previously developed. Note that where possible, efforts should be made to maintain common domain semantics to model and describe the components in the business and data environment.

The scope of this analysis must focus only on critical business processes and data at an appropriate level of detail and granularity so as to:

Identify the target state business processes and data
Facilitate the derivation of the data environment from the business environment
Maintain traceability between the business environment and data environment

In the end, the target business and data environment will be recommended for implementation in order to achieve the strategic improvement opportunities.

Sub-Tasks

3.331 Design target strategic and operational business environment, related performance, and organizational roles

Planners need to revisit the business services maturity matrix to design the maturity levels for the business services beyond level 0. In this sub-task, planners establish the target maturity levels that will contribute to achieving the vision while aligning to the desired performance metrics. With the establishment of these maturity levels, the collaborative planning team and sponsor can select target levels of business service maturity. This setting of maturity goals provides the information needed for planners to focus on specific business improvement targets.

For each target business service, planners must diagram the target chain of business processes in a value chain drawing describing the value that will be produced by the business processes. The target value chain might be identical to the current-state value chain because it is not uncommon for changes to be at the activity level rather than at the business process level. The intent of the target value chain analysis is to identify any differences in the business processes that are currently being provided, versus those that need to be provided in the target state. The value chain analysis will help determine where new business processes are required and where existing business processes may no longer be necessary.

Just as in the as-is analysis, the value chain must then be aligned to the target business function model. Planners must use the business function model to identify the critical business processes identified in the value chain analysis in the context of the business area functions. The business processes identified in the business function model must be consistent with the business processes identified in the value chain models. Additionally, it is necessary to ensure that the processes include built-in security and privacy controls, and compliance with Section 508 accessibility standards, that will provide proper levels of protection and accessibility that support effective business performance and which meet applicable laws, policies, directives, and guidance for the level of information criticality and sensitivity for the target business service.

For each key business process identified in the business function model and value chain models, it is necessary to define the target business processes and associated performance measures. The business and data changes defined in previous sub-tasks

are a major driver for the differences between the current and target state business process models. The business process models (e.g., IDEF0, BPMN) must be developed to describe the units of work, rules, guidance, enablers and performance measures for each key target business process.

Just as in the current state analysis, planners must understand the relationships between business processes and the organizations that perform or participate in those business processes. Using the business function model, value chain models, and business process models, planners must develop a target swim lane flow to describe a view of how organizational units interact in the context of the business processes that are delivering the services. Planners must make formal observations about accountability in the context of the organizations and their business processes.

3.332 Identify information/data, dependencies, and information sources associated with the target business environment

Using the target process models from the previous sub-task, planners must identify the information exchanged between key business processes along with the producers and consumers of that information and the mechanisms used to enable the exchange. Information access and exchange services must be summarized for information classes in a target information-sharing matrix.

Using the understanding of the key information flows developed in conjunction with the business process and activity analysis, planners must develop the target data model to provide a graphical representation of the data requirements and relationships. The data model will provide the structure and terminology for information and data in the target environment. The target data model must include subject areas, information classes, key entity types, and relationships.

The target data model must be used to update the data reference model (DRM) at the appropriate level. The target data model will be articulated to document data and its relationships to stewards and information sources. Planners must develop target data steward assignments by mapping each information class within the target data model to an organization that will be the data steward for that information class. The data steward is responsible for the creation, maintenance and quality of the data to support business activities in the target environment.

Based on the development of the target data steward assignments, planners must be able to communicate changes in stewardship and delivery of information. For instance, if two offices currently collect, store, and maintain the same data, and one office is designated as the steward, the other office could then become a customer of the steward office, rather than a second supplier of the same data.

In this sub-task planners must develop a matrix that documents how target business processes use the business information identified in the target data model (e.g., CRUD analysis). This matrix allows planners to map target business processes to core data entities to help identify candidate information services, including new authoritative data sources, and business processes that need to use these information services (preliminary requirements for orchestration). The matrix also helps identify producers and consumers of this information. At the end of this sub-task, the as-is key information sources must be updated with final recommendations concerning their designation as authoritative data sources.

The identification of information services is a key component to the target environment. This sub-task allows the planners to bridge the business and data domains by linking business processes and data. Through this analysis, planners must discover opportunities for re-use of information in the form of information sharing services. This analysis must also ensure that the information services include built-in security and privacy controls that will provide proper levels of protection that support effective business performance and which meet federal laws, policies, directives, and guidance for the level of information sensitivity. Planners must also look for information sharing service opportunities, within other parts of the enterprise and external to the enterprise.

3.333 Validate that the target business and data environment will fulfill the vision

Planners must review the outputs of the sub-tasks to ensure that the target business and data environments have adequately addressed the strategic improvement opportunities. During this sub-task, planners must review the business and data adjustment recommendations and the target business and data artifacts to ensure that there is full coverage of the strategic improvement opportunities.

Any strategic improvement opportunities that have not been addressed by the target business and data environments must be reviewed to ensure that the analysis is complete.

3.334 Package, present, and seek leadership approval of the business and data recommendations to achieve the vision

Planners must develop a package that describes the business and data environment and details recommendations for the collaborative planning team to review. This presentation must include a summary of how the business and data environment aligns with the needs, vision, goals and objectives, and performance metrics.

Planners must prepare a more detailed presentation that includes the business and data environments. The planners must conduct a detailed workshop review of the business and data environments with the collaborative planning team. The collaborative

planning team must decide at this point whether to proceed into the next set of analysis activities or to refine the plans for the business and data environment further.

It is recommended that there be a formal sign-off of the materials by the sponsor and governance.

3.335 Draft applicable portions of architecture, capital planning, security, records, budget, human capital, and performance compliance documents

In many organizations there are significant compliance or required documents associated with planning. At the start of this task planners determined which of these compliance or required items are applicable to the planning at hand.

Based on this assessment, planners should have been gathering the required data for the compliance documents throughout the sub-tasks. It is in this sub-task that planners leverage the information to begin creating the compliance documents.

Initial drafts of the relevant architecture, capital planning, security, records, budget, human capital, and performance compliance documents must be developed based on the guidance associated with those compliance documents. Note that at this stage of the CPM it is likely that more information will be needed to complete these compliance documents. As such, these compliance documents will be revisited in a later sub-task.

3.34 Collect and Analyze Information about the As-Is (Current) enabling application and infrastructure environment

This activity builds upon the analysis of the business and data environment performed in previous sub-tasks and is within the scope identified in Step 1. The focus of this task is to collect and analyze information pertaining to the as-is use of applications and infrastructure and how well those applications and infrastructure support the desired performance as well as how well they enable the business and data environment. Note that where possible, efforts should be made to maintain common domain semantics to model and describe the components in the enabling application and infrastructure environment. When appropriate, the Application Reference Model and Infrastructure Reference Model described in *A Common Approach to Federal EA* may be used to assist in this standardization.

This task includes assessing the applications and infrastructure across several dimensions, including business, data and technology alignment; service management; and maturity. This task also includes a high-level assessment of existing application interfaces and the data that is exchanged between those applications.

By performing an analysis of existing applications and infrastructure against the desired performance as well as the extent to which the business and data environment is enabled,

planners must be able to answer key questions related to the application and infrastructure environment including:

How well are the applications and infrastructure delivering business value in relation to the costs associated with operating and maintaining them?
What is the relationship between the existing applications, infrastructure, and technologies (i.e., as-is solution architecture)?
What existing applications are associated with authoritative data sources?
How efficient is my infrastructure?

Sub-Tasks

3.341 Collect and assess information on the enabling applications and infrastructure associated with the business and data environment

During this task, planners gather information that will be useful to conducting an analysis on how well the current applications and infrastructure support target business services. Information being gathered may include the applications currently in use, infrastructure currently in use, any known security issues or risks, and stakeholder feedback with regard to overall application performance and alignment to business needs. Performance information may also be derived from existing program performance assessments.

Information gathering can be performed using a variety of methods, including querying an existing repository of information and conducting interviews with key stakeholders (e.g., business owners, application owners) to understand the applications and infrastructure within a business service and to identify existing data sources. The information collected must be at a sufficient level of detail to assess the data fit, business fit, technology fit, service management, and maturity level of the application or infrastructure and must include the total cost to provide, deliver, support, and manage data, applications, and infrastructure in the portfolio.

The cost information gathered during this task must be leveraged to create required outputs for capital planning and investment control such as the cost-benefit analysis and return-on-investment analysis that will be utilized in the development of business cases. For example, if redundant applications and infrastructure are identified for decommissioning in subsequent activities, it will be helpful to have determined an estimated cost for the current environment.

The as-is solution architecture serves as a baseline for determining the required adjustments to the environment in order to align the strategic, business, and data improvements defined in previous tasks. Planners must develop an understanding of the current applications and infrastructure environment so subsequent analysis of the target applications and infrastructure architecture can be performed.

The as-is applications and infrastructure interface diagram(s) must be constructed to illustrate how the business functionality identified in the business model is associated with existing applications and infrastructure. This model shows the existing applications and infrastructure in the as-is state and identifies the relationships (e.g., data exchange packages) between them, but it may also include an overlay to show the boundaries of key business functions and external interfaces (e.g., organizational). The data depicted in the as-is applications and infrastructure interface diagram(s) must align with portions of the data model, and the applications and infrastructure depicted must be enablers of the business processes and activities already analyzed.

Unlike the description of the target solution architecture, the description of the as-is model must include only the as-is applications and infrastructure interface diagram(s) in order to limit the analysis of the as-is solution architecture to what is necessary to provide an adequate baseline. The subsequent development of the target solution architecture will include other artifacts.

3.342 Identify applicable technology, service, and information standards

High-level technology, service, and information standards for the target enabling applications and infrastructure environment must be specified with the goal of maintaining alignment with the desired performance as well as the enabling business and data requirements.

This sub-task begins with a review of the target business and data environments previously defined, along with the target maturity level for services. The purpose of this review is to ensure that the specification of high-level technology, service, and information standards are aligned with the overall strategic improvement opportunities defined in previous planning activities.

For each major business function, the required services and associated standards must be identified. This includes:

Identifying service interface needs
Defining high-level requirements related to security controls
Identifying information services required to support authoritative data sources
Identifying the maturity level for the underlying capabilities needed to deliver the service
Identifying technology standards or ensuring that existing technology standards are being adopted appropriately

3.343 Analyze the enabling applications and infrastructure environment and determine required adjustments to enabling applications and infrastructure to enable the target business and data environment

An assessment of the value and performance of as-is enabling applications and infrastructure within the defined scope of the planning is performed to determine where adjustments to the application and infrastructure environment must be investigated. This assessment is critical to ensure alignment to the strategic, business, and data requirements depicted in previous sub-tasks.

An overall assessment is performed for each as-is application and infrastructure component to determine how well the application or infrastructure component supports the vision previously developed. This assessment must also include an identification of the degree of functional overlap with other applications or infrastructure components and the extent to which the application or infrastructure components are associated with re-engineered or streamlined business processes (e.g., automated workflow).

The business value assessment must also take into consideration the overall efficiency of applicable investments (e.g., return on investment) relative to available alternatives to these investments in similar applications and infrastructure or to other enterprise services.

Results of the as-is applications and infrastructure analysis are compiled and evaluated using the as-is system and services scorecard, which produces a comprehensive scoring of the cost, fit, and value of as-is systems. The analysis results must be evaluated to answer key questions relative to the needs of the target application and infrastructure environment, including:

What existing investments are included in this portfolio?
What are the applications and infrastructure in the portfolio and how are they deployed?
How well are the applications and infrastructure able to deliver business value for the costs associated with operating and maintaining them?
What risks are associated with existing applications and infrastructure?
What applications or infrastructure must be considered for the target state?
What security and privacy continuous monitoring activities must be considered for the target state?
How efficient is my infrastructure?

3.35 Design and Validate the To-Be (Target) Enabling Applications, Services and Infrastructure Environment

In this task planners design and validate the to-be or target enabling applications and infrastructure environment to best enable the business and information environment. A complete depiction of the target state must include a depiction of the target applications and infrastructure that is consistent with the existing enterprise architecture and compliant with Section 508 accessibility standards. In addition to applications and infrastructure, planners need to define the technical and service standards used to automate and improve business functions within the scope of the planning. The scope of the target depiction in this task includes data sources, applications, and the interfaces between them. The target depiction in this task must also describe the boundaries defined by interfaces with external customers, applications, services, and organizations.

As a general rule, the specification of technical components must, in principle, be vendor-agnostic within the outputs of this task. As such, the depictions of applications and infrastructure must not be specific or unique to a particular solution or vendor. The key exceptions to this rule are where existing as-is systems, standard commercial off the shelf (COTS) solutions, and solutions purchased through enterprise license agreements (ELAs) are to be included as part of the target state. This integrated view will greatly improve the hand-off to implementers by providing a means for linking applications to data and their supporting technology components.

Sub-Tasks

3.351 Determine required target enabling applications and infrastructure to enable the target business and data environment

The result of completing this task is the selection of applications and infrastructure to be included in the target state, based on the desired performance as well as the enabling business and data environments. Planners must review the results of the business value analysis, combined with the specification of technology, service, and information standards in prior sub-tasks, to identify target applications that provide the necessary capabilities to support the target business and data environments. This analysis must also take into account how the existing applications and infrastructure are performing in terms of business value and cost. High business-value applications in the current state could be good candidates for the target state environment.

Selecting target-state applications may mean carrying forward an existing application to the target state, consolidation of multiple applications to reduce the total number of applications supporting a business function, and/or identification of a new high-level application requirement associated with automation of business processes.

As the development of the target application and infrastructure environment is tightly coupled with the business and data environment, this sub-task may become highly iterative as changes to the business and data environment are identified.

3.352 Identify the relationships and data exchange requirements between the target enabling applications

In this sub-task planners need to define the relationships between applications and infrastructure within the context of the overall boundaries. Planners must construct the target applications and infrastructure interface diagram(s) to illustrate how the business functionality identified in the business model is associated with target application and infrastructure components, including the definition of data exchange packages that need to exist between applications.

The target applications and infrastructure diagram(s) must show the applications and infrastructure in the target state and identify the data exchange relationships between them. This diagram may include an overlay to show the boundaries of key business functions and external interfaces. The diagram(s) must also depict the authoritative sources of record for data and how that data gets deployed in the applications view.

The planners could capture target application services in an application service component model (ASCM), an analytical technique that may be applied to business and enterprise application services to describe application service components and the mechanisms for providing application services to customers. This model, which provides a framework and vocabulary for guiding discussions between application service providers and consumers, is meant to be a catalyst for true cross-organization collaboration. Along with development of the ASCM, the technology model (TM) can be developed to show the technology components that support the business service delivery for each application service component defined in the ASCM.

3.353 Package, present, and seek leadership approval of the enabling applications and infrastructure recommendations to enable the target business and data environment

Planners must develop a package that summarizes the as-is and the to-be application and infrastructure environment and provide an overview of the benefits of this environment on desired performance and the vision. This must include the relevant artifacts describing the target application and infrastructure environment and how they enable the performance, business, and data environments.

Planners must conduct a detailed workshop review of these outputs for the collaborative planning team. The review must also include key IT personnel.

It is recommended that there be a formal sign-off of the materials by the sponsor and governance.

3.354 Update applicable portions of architecture, capital planning, security, records, budget, human capital, and performance compliance documents

In many organizations there are significant compliance or required documents associated with planning. At the start of this task planners determined which of these compliance or required items are applicable to the planning at hand.

Based on this assessment, planners should have been gathering the required data for the compliance documents throughout the sub-tasks. It is in this sub-task that planners leverage the information to update and potentially finalize the creation of the compliance documents.

Updated or potentially final drafts of the relevant architecture, capital planning, security, records, budget, human capital, and performance compliance documents must be developed based on the guidance associated with those compliance documents. Note that at this stage of the CPM, most of the information required for these documents must be gathered and ready to be used in the documents.

3.3 Activity Outputs:

Output	Core	FEA Layers
Common / Mission Services Target Maturity Levels	Y	B
As-Is Business Value Chain	Y	B
As-Is Business Function Model	Y	B
As-Is Key Business Process Model	N	B
As-Is Business Process Swim Lane Diagram	N	B
As-Is Key Information Sources and Qualitative Assessment	Y	D
As-Is Business Data Mapped to Key Business Processes (CRUD)	N	B,D
As-Is Data Model	Y	D
As-Is Data Steward Assignments	Y	D
Business and Data Architecture Adjustment Profiles	N	B,D
Target Business Value Chain Diagram	Y	B
Target Business Function Model	Y	B
Target Key Business Process Model	N	B
Target Business Process Swim Lane Diagrams	N	B
Target Business Data Mapped to Key Business Processes (CRUD)	N	B,D
Target Data Model	Y	D
Target Data Steward Assignments	Y	D
Business and Data Environment Presentation	N	B,D
Draft Architecture, Capital Planning, Security, Records, Budget, Human Capital, Section 508 Accessibility and Performance Compliance Documents	Y	n/a
As-Is Enabling Application and Infrastructure Architecture	Y	A, I
As-Is Application Scoring	N	A,I
Enabling Application and Infrastructure Architecture Adjustment Profiles	N	A,I

Target Enabling Application and Infrastructure Architecture	Y	A,I
Target Information Flow Diagram	Y	A,D
Target Information Sharing Matrix	N	A,D
Enabling Applications and Infrastructure Presentation	N	n/a
Updated Architecture, Capital Planning, Security, Records, Budget, Human Capital, Section 508 Accessibility and Performance Compliance Documents	Y	n/a

Key to FEA Layers: S = Strategy, B = Business, D= Data, A = Application, I = Infrastructure, SP = Security

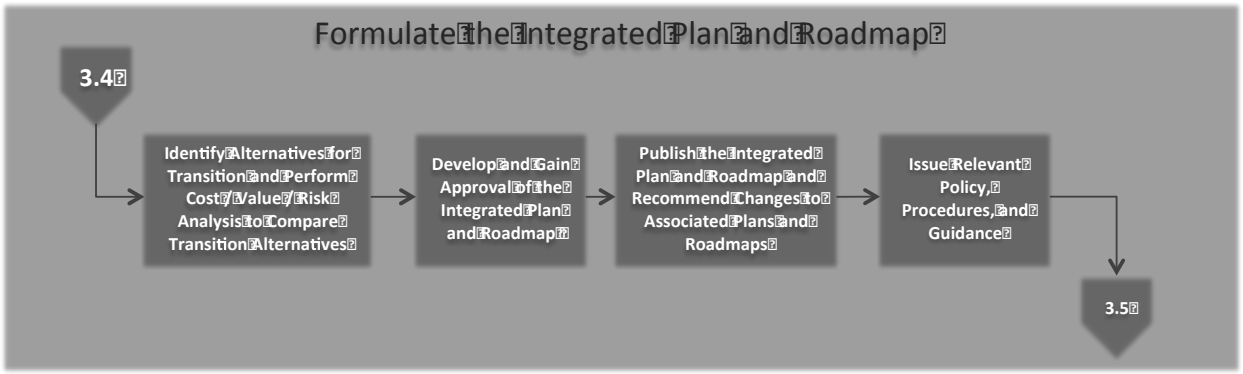
A.4.6 Activity 3.4: Formulate the Integrated Plan and Roadmap

This activity is the culmination of the analysis to create the integrated plan. The activity begins with the identification of transition options for the recommendations generated in previous activities. The business, data, enabling application, and infrastructure environment changes are considered in terms of transition options and timing. Each transition option must be assessed to determine the cost, value, and risk of each alternative. Planners complete this analysis and then author the integrated plan and roadmap.

The integrated plan consists of the full plan to include the architecture, recommendations for changes to environments, financial business case and budget requirements, performance expectations, and transition milestones. Unlike in many organizations where this information would be presented as separate and often times disjointed plans, the purpose of the Collaborative Planning Methodology is to produce an integrated plan to enable better decision making.

Once the plan is developed it must be presented for approval. The integrated plan must be formally presented for approval to the sponsor, relevant stakeholders, and the collaborative planning team. An approved integrated plan is ready for overall integration into enterprise transition planning, as well as to move forward into the implementation lifecycle.

The following visual illustrates the tasks within this activity.



Activity 3.4: Formulate the Integrated Plan and Roadmap

Tasks:

3.41 Identify alternatives for transition and perform cost / value / risk analysis to compare transition alternatives

In this task planners formalize the transition options for the sponsor and stakeholders to consider and make final decisions as to how the adjustments will be implemented. Transition options may be modular (i.e., stand-alone), in that they may be implemented independent of other transition options. Transition options may also share dependencies with each other. Such dependencies are likely to be identified as a consequence of the overall planning analysis performed in previous activities. In practice, it is a good idea to attempt to consolidate and de-couple transition options as much as possible in order to reduce the complexity of the cost / value / risk analysis.

It is important for planners to align and consider the transition options according to the strategic, business, data, application, and infrastructure adjustments defined in the previous activity. This provides line-of-sight of the recommendations and presents the transition options in a more actionable context for decision makers to evaluate and prioritize.

Note that throughout this activity, transition options that share dependencies with each other must be grouped into a higher-level transition option. This may especially be the case where there are dependencies between transition options that are derived based on different findings. In such cases, the opportunity to generalize the findings to encompass both sets of transition options may need to be considered.

Transition options are grouped and summarized as a set derived from the business, data, enabling application, or infrastructure findings. Typically, this will take form such as the following:

<u>Strategic Improvement Opportunity</u>

- Finding 1
  - Transition Option 1.1
  - Transition Option 1.2
- Finding 2
  - Transition Option 2.1
  - Transition Option 2.2

For each transition option, planners must assess the relative value being produced in relation to the strategic improvement opportunities and desired performance outcomes. This may require additional input from key stakeholders.

Additionally, an aggregate cost estimate must be prepared that includes the appropriate level of detail for weighing cost differences between transition options. Some more significant transition options may require more detailed system lifecycle cost estimates/total cost of ownership estimates prior to review and approval. Costs may also include decommissioning costs associated with transition options that eliminate a service or that result in system retirements.

In addition to cost and value, planners also need to consider the risks associated with the transition options. Planners need to perform an analysis to determine the top risks in terms of overall impact, per transition option. This involves assessing the likelihood of the occurrence of the risk, along with assessing the impact on both the cost and value of the transition option. Risks must then be rolled up to obtain an overall likelihood and cost / value impact.

Cost, value and risk estimates for each transition option must be analyzed using a quantitative approach such as the Value Measuring Methodology (VMM). Results of the analysis must be used to inform the selection of the most attractive transition option for implementation.

Results of the cost / value / risk analysis must be reviewed with the key stakeholders to gain buy-in to the proposed implementation recommendations. This review must include the value-to-cost comparison, an updated view of the transition sequencing details, and when appropriate a draft systems migration depiction. This is a critical task to ensure buy-in to the implementation recommendation proposals that are to be formalized in the integrated plan and roadmap.

3.42 Develop and Gain Approval of the Integrated Plan and Roadmap

The adjustments to the strategy, business, data, enabling application, and infrastructure environment and the related implementation transition options provide the basis for producing the detailed integrated plan and roadmap. The integrated plan summarizes the results of the planning analysis and provides an overview of the adjustments recommended to be made to the strategy, business, data, enabling applications, and infrastructure environment.

Using the adjustments to the strategy, business, data, enabling application, and infrastructure environment and the related implementation transition options, a draft sequencing work breakdown structure (WBS) must be developed. For each adjustment, a full representation of the deliverables that are required for implementation must be developed and described in the WBS. The WBS must incorporate deliverables associated with all aspects of the implementation, including technology, process, system, data, etc., along with any associated workforce development, communication and change management activities.

Based on the completed WBS, both a high-level implementation sequencing plan and an application migration / sequencing overview must be developed to summarize the sequencing plan for the integrated plan and roadmap. The implementation sequencing plan contains information regarding the timing and dependencies between those items identified in the WBS, including the technology, process, application, data, associated workforce development, communication, and change management activities. When applicable, the application migration / sequencing overview is developed to focus on the actual sequencing and transition of applications and infrastructure to achieve the target state.

Once the high-level sequencing is developed, a more detailed sequencing plan is developed in the form of a project schedule that includes all tasks associated with the overall implementation of adjustments to the environment. This sequencing plan details the sequenced tasks necessary to develop the elements of the WBS. Internal and external dependencies must also be included as either milestones or predecessor tasks.

Planners are now in a position to write the actual integrated plan based on the totality of analysis, recommendations, transition options, and sequencing plans developed. The integrated plan must be developed to describe findings, recommendations, and the overall transition plan. This document must be generated according to the outline provided in the following table.

Integrated Plan Sample Outline

Executive Overview: This brief (1-2 pages) overview describes the motivation behind the integrated plan. It is focused on providing clear, concise answers to key questions, such as:

- Where are we today? (Baseline)
- Why do we need to modernize? (Strategic Improvement Opportunities)
- What is our vision for modernization? (Vision, Goals and Objectives)
- How should we execute modernization? (Business, Data, Enabling Application, and Infrastructure Target Environments and Transition Options)
- When should we modernize and what are the relationships to other initiatives? (Sequencing Plan / Implementation Plan)
- Who needs to participate for this initiative to be successful? (Resource Plan)

Overview of Strategic Improvement Opportunities and Business Case: Provides a discussion of the scope, drivers, prioritized needs, and opportunities for improvement. Furthermore, the capital planning business case information should be in this section. This section further elaborates upon the following key questions:

- Where are we today? (Baseline)
- Why do we need to modernize? (Strategic Improvement Opportunities)

Recommendations for the Target State: Describes the existing environments and issues from a variety of perspectives that address the strategic improvement opportunities. The findings and recommendations are described in the context of the specific business services where improvements are recommended due to the drivers, prioritized needs, and desired target vision. All findings are associated to specific recommendations on how to proceed. Expected strategic improvement opportunities associated with the recommendations are also identified. Furthermore, the security, records, performance management, and human capital information should be in this section. This section further elaborates upon the following key question:

- What is our vision for modernization? (Vision, Goals and Objectives)

Target Business, Data, Enabling Application, and Infrastructure Environment: This should include a brief description of the business functions that are provided and the strategic objectives that are to be achieved by the transformation. It also describes the target state for the enabling application and infrastructure environment required to support the recommendations as well as the applications migration plan, and target data model. This section further elaborates upon the following key question:

- How should we execute modernization? (Business, Data, Enabling Application, and Infrastructure Target Environments and Transition Options)

Sequencing Plan: Describes the as-is state, target state, and the integrated steps required to transition from the as-is to the target environment based on the identified recommendations. Within the sequencing plan, performance improvements are also associated with transition milestones. The sequencing plan should also be tied to the business cases or investment proposals. This section further elaborates upon the following key questions:

- When should we modernize and what are the relationships to other initiatives? (Sequencing Plan / Implementation Plan)
- Who needs to participate for this initiative to be successful? (Resource Plan)

The integrated plan and roadmap must be distributed for review to the collaborative planning team, stakeholders, and the sponsor. Accompanying this distribution must be a cover letter that describes the highlights of the integrated plan. A separate executive summary document may also be necessary to facilitate review. During the review process, a document review form must be used to collect comments and change requests.

During the review process, all feedback must be recorded and cataloged. Follow-up actions must be documented and tracked through to completion. As feedback actions are documented and closed, comments and changes must be incorporated into the integrated plan and roadmap. This may also result in updates to other work products such as the sequencing WBS and project plan.

Once the final integrated plan is assembled based on feedback from the reviews, a formal approval meeting must be scheduled and conducted to obtain formal approval of the integrated plan by the collaborative planning team, stakeholders, and sponsor. A record of decision must be created to document the approval.

3.43 Publish the Integrated Plan and Roadmap and recommend changes to associated plans and roadmaps

Once the integrated plan and roadmap is approved, planners must publish the documents based on the communication strategy. In some instances, a variety of mechanisms must be used to communicate the plan contents and its impacts on the stakeholder community.

Furthermore, planners must work to identify other associated plans and roadmaps that have been previously published, and perhaps need to be updated based on the contents of this most recently published integrated plan and roadmap. Maintaining these collections of plans and roadmaps and ensuring that the changes find their way to the implementation teams and decision makers is critical to maintain a well-coordinated environment.

3.44 Issue relevant policy, procedures, and guidance

Planners must determine if there are policies, procedures, and/or guidance that are required based on the approval and publishing of the integrated plan and roadmap. In many instances, policies, procedures, and/or guidance are required in order to put the plan into action.

Behaviors that need to be changed based on the plan must be grounded in new policy, procedures, and/or guidance when needed.

3.4 Activity Outputs:

Output	Core	FEA Layers
Transition Recommendation Profile	N	n/a
Transition Recommendation Sequencing Diagram	N	n/a
Recommendation Sequencing Milestones	N	n/a
Proposed Implementation Recommendations	N	n/a
Analysis of Cost, Value, and Risk for Transition Options	Y	n/a
Recommendation Implementation Sequencing Plan	N	n/a
Transition Plan Milestones	Y	n/a
Application Migration / Sequencing Overview	Y	n/a
Document Review Log	N	n/a
Feedback Tracking Document and Action Report	N	n/a
Integrated Plan Document	Y	S,B,D,A,I,SP
Executive Summary Presentation	N	n/a
Record of Decision	Y	n/a
Policy, Procedures, and Guidance	N	n/a

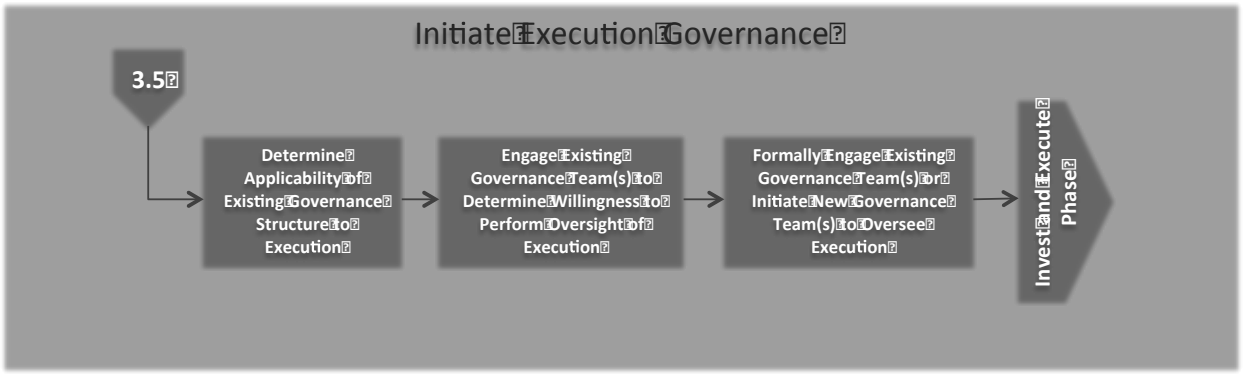
Key to FEA Layers: S = Strategy, B = Business, D= Data, A = Application, I = Infrastructure, SP = Security

A.4.7 Activity 3.5: Initiate Execution Governance

Activity 3.4 marks the conclusion of the significant planning as the integrated plan and roadmap has been completed, the reviews have been done, and the plan is approved. It is at this point in almost all planning efforts that individuals involved with the planning celebrate the completion of the planning and reflect on lessons learned. It is also at this point in many planning efforts that it is most critical to maintain momentum towards implementation and to not allow the conclusion of the planning to mean the end of the efforts towards achieving the vision.

The role of governance has been an important part of the planning oversight and decision-making and governance needs to maintain a strong role as Phase 2 of the Collaborative Planning Methodology, *Implement and Measure*, gets underway. It is important to consider the type of governance that will be needed during Phase 2 of the CPM. The investment, implementation, and performance measurement activities in Phase 2 of the CPM are distinctly different in nature than the planning activities in Phase 1 of the CPM. Because of these differences, planners need to assist the sponsor to determine the best governance relationships for Phase 2 of the CPM.

The following visual illustrates the tasks within this activity.



Activity 3.5: Initiate Execution Governance

Tasks:

3.51 Determine applicability of existing governance structure to execution

Most organizations have governance teams that cover a variety of investment and implementation activities. In many instances, there are teams that govern investments, other teams that govern projects, and still other teams that govern budget decision activities. As previously stated, it is imperative that the implementation effort involve governance throughout the implementation so that incremental decisions are agreed upon and the end result is in alignment with the expectations of the governance teams.

In this task, planners review the existing governance structure and specifically look at the charters of the existing teams to determine which, if any, teams are aligned to the investment and implementation effort at hand. Planners must leverage the integrated plan and roadmap to determine which governance teams are most closely aligned to the impending work. It is certainly possible that none of the existing governance teams are appropriate or fully cover governance responsibilities for the implementation effort at hand. In these instances, a new governance team might be an appropriate course of action. The recommendations for governance team alignment must be presented to the sponsor.

3.52 Engage existing governance team(s) to determine willingness to perform oversight of execution

The sponsor is the appropriate person, in most cases, to engage directly with the chairs of the governance teams in an effort to confirm that the recommended teams are in fact appropriate for the implementation effort at hand. The sponsor is seeking confirmation from the governance team chair that the governance team has appropriate charter authority and is willing to perform oversight throughout the implementation process. Of course, every organization is different in how governance boards operate; the objective in this task is to make a governance board aware of the project and confirm that they should have a part to execute the implementation.

It is important to prepare the sponsor with a solid understanding of the nature of the implementation and the types of activities in which governance will need to participate. The sponsor will want to ensure that the governance team chair is fully aware of the scope and level of commitment that is being requested of the governance team.

3.53 Formally engage existing governance team(s) or initiate new governance team(s) to oversee execution

Through the previous tasks, either planners will have not been able to identify appropriate governance teams, or they will have found appropriate governance teams and those teams have either accepted or rejected the invitation to govern the implementation at hand.

If the governance team has accepted the request to govern the implementation then it is important to meet with the complete governance team, at their next meeting perhaps, and walk them through what is being implemented, why it is being implemented, the milestones, and the risks.

If the governance team has not accepted the request or no appropriate governance team has been identified, then planners must support the sponsor in formulating a new, perhaps temporary, governance team for the implementation effort. The formation of new governance for implementation will depend on whether there is a temporary or ongoing need for this form of governance.

In some instances there is a recognized need for governance to oversee implementations on a continuing basis. In these instances, a governance team must be formed and chartered with responsibilities that cover not only the implementation at hand, but also to include other current and future implementation efforts. In other instances it is appropriate to simply stand up a temporary governance team with responsibilities only for the implementation at hand.

In either instance, it is important to meet with the complete governance team, at their next (or first) meeting perhaps, and walk them through the implementation details.

3.5 Activity Outputs:

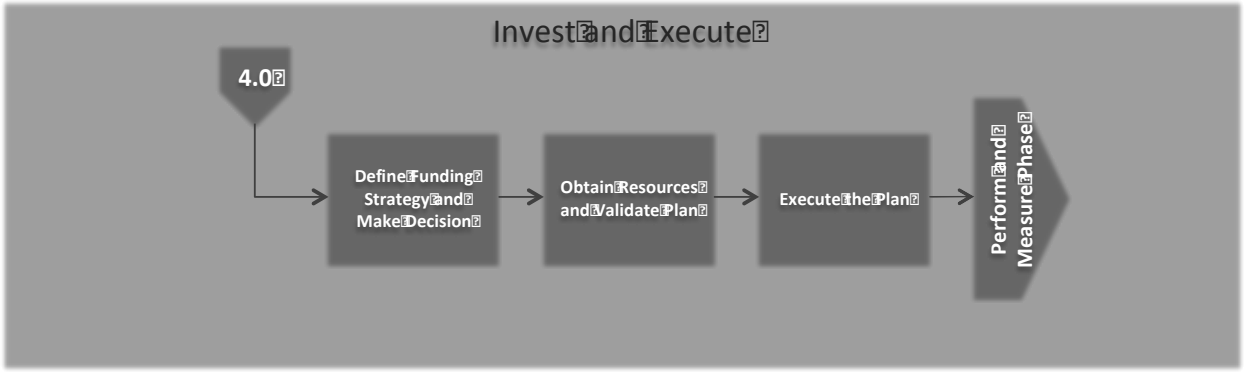
Output	Core	FEA Layers
Governance Structure (Project Governance)	N	S

Key to FEA Layers: S = Strategy, B = Business, D= Data, A = Application, I = Infrastructure, SP = Security

A.5 Step 4: Invest and Execute

Purpose

The purpose of this step is to make the investment decision and implement the changes as defined in the Integrated Plan produced in Step 3. Many groups participate in this step, however, it is important to note that these groups will need to work as a coordinated and collaborative team to achieve the primary purpose of this step: to successfully implement the planned changes.



Step 4 Activities

Role of Planners

In this step most planners (e.g. architects, performance planners, and other planners) are in a support role, assisting in investment and implementation activities by providing information to aid in decisions, and to support interpretation and revision of plans from Step 3. The exceptions to this statement are the capital planners and budget planners who are performing a primary and leadership role in the facilitation of investment decisions and budget formulation. The planners who performed primary and leadership roles in Steps 1-3, including the architects, may be needed to further research and analysis into other organizations and their experiences (revisiting Step 2), update plans (revisiting Step 3), or re-engage stakeholders for feedback (revisiting Step 1). The architects have a continuing support role (e.g. interpreting the plans, making changes to the plans, supporting decision making) throughout investment and implementation. The involvement of the planners, including the architects, does not cease at the conclusion of Step 3. As investment decision are made and changes are implemented the planners update the Integrated Plan. This step should not begin without the planning effort successfully navigating the management milestones, reviews and approval, and in cases of revisiting previous steps these same milestones, reviews and approvals must be achieved.

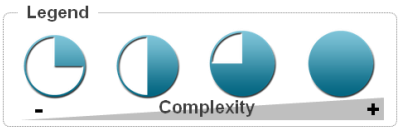
Outcome

During Step 4, a decision is made concerning the investment in the changes that were planned in Step 3. At the end of Step 4 the recommendations for addressing the defined needs have been implemented. If the investment is not approved, the planners, leadership, and stakeholders return to previous steps to

alter the recommendations and plans for another iteration of plans for consideration. It is important to reiterate that the Integrated Plan (Step 3) and the implementation (Step 4) could consist of a variety of changes to include, but not limited to, policy changes, organizational changes, technology changes, process changes, and skills changes. In many instances, the non-technology changes could be the most significant and impactful for an organization.

A.5.1 Step At-a-Glance

Step 4 At-a-Glance	Identify and Validate Activities		
	Define Funding Strategy and Make Decision	**Obtain Resources and Validate Plan**	**Execute the Plan**
Which Planners Participate in This Activity?	• Capital Planners (primary, lead) • Architects (review, interpretation) • Budget Planners (primary, lead)	• Capital Planners (primary, lead) • Architects (review, interpretation) • Budget Planners (primary, lead)	• Project Planners (primary, lead) • PMO (primary, lead) • Architects (review, interpretation) • Capital Planners (review, oversight) • Budget Planners (review, oversight)
What Are The Planning Inputs (from Steps 1-3) to This Activity?	• Governance Structure (Project Governance) • Integrated Plan Document • Analysis of Cost, Value, and Risk for Transition Options • Recommendation Implementation Sequencing Plan • Transition Plan Milestones • Transition Recommendation Sequencing Diagram • Recommendation Sequencing Milestones	• Integrated Plan Document • Recommendation Implementation Sequencing Plan • Transition Plan Milestones • Transition Recommendation Sequencing Diagram • Recommendation Sequencing Milestones	• Integrated Plan Document • Recommendation Implementation Sequencing Plan • Transition Plan Milestones • Transition Recommendation Sequencing Diagram • Recommendation Sequencing Milestones
What Is The Relative Complexity of This Activity?			



A.5.2 A Note on Core Artifacts

Like any methodology, the *Collaborative Planning Methodology* is designed for each step to be followed and each Activity Output to be produced. The use of "Core" and "Not Core" to describe these outputs is meant as the first set of tailoring guidance if an organization has constraints of time, budget or

resources. As the CPM is tested and refined, feedback from organizations will improve this assignment and generate templates that help to scale outputs according to scope or size.

As described earlier, the goal in using this methodology is to encourage collaboration for high priority projects. This increases the awareness of solutions and services whose reuse can result in efficiencies. The CPM also provides the framework for organizations to generate actionable, consistent and rigorous plans that can lead to improved solutions.

A.5.3 Activity 4.1: Define Funding Strategy and Make Decision

In this activity, the capital planners and budget planners are providing lead support services to the decision makers to determine whether to fund the Integrated Plan that was approved in Step 3 including the source of funds and timing of funds availability. The other planners, such as architects, provide support services during this activity including any required clarifications or interpretations of the Integrated Plan. The key output of this activity is a defined funding strategy and a decision to approve the investment of required funds.

Several of the outputs from Step 3 are critical to perform this activity. Specifically, in Step 3 the governance structure was defined for how the implementation would be governed. This governance structure is first put into use during this activity. However, most of the investment decision process will also involve the more established investment decision governance groups and processes within the organization.

In addition to the governance structure, there are additional Step 3 outputs that are used during this activity. The actual recommendations to be implemented, the sequencing plans and milestones, and the Integrated Plan all contain information that is essential for defining the funding strategy and performing the investment decision process to obtain a decision to proceed.

Within this activity, there are many groups that have important roles. These groups all must collaborate effectively to make decisions and proceed with implementation. The architects perform a support role in interpreting the Integrated Plan and explaining the sequencing of milestones. The governance and investment decision makers need to have a working and advisory relationship with the architects. Additionally, the performance planners need to be part of the governance advisory function to explain the performance improvements that are expected. The budget and capital planners need to work in an integrated manner to bring about a funding strategy that is grounded in the project and funding realities of the organization.

Throughout this activity, the role of governance is a critical component to establishing a funding strategy and making the investment decision. The project governance structure defined in Step 3 will represent the interests of the project to the investment governance structure. The investment and budget governance structure will make the ultimate decisions as to the investment and whether funds should be assigned so that the implementation can proceed.

A.5.4 Activity 4.2: Obtain Resources and Validate Plan

In this activity the resources (people, technologies, expertise) are obtained and tactical adjustments to the plan are made and validated as necessary. In many instances an organization may need to seek outside support to implement the Integrated Plan. In such instances, procurement activities are conducted as part of this activity. Resources are obtained by performing the procurement activities as defined by the organization's procurement office.

As with most procurements, a proposal from the winning bidder includes their technical approach for performing the implementation activities. In such instances, the technical proposal needs to be harmonized with the milestones and action plans defined in Step 3. Once the procurement is complete, the vendor will initiate implementation activities by refreshing the milestones and project plan associated with the Integrated Plan created in Step 3 and by harmonizing these materials with what was proposed during the procurement activities. These changes must be performed in conjunction with the planners and the project governance as appropriate.

Step 3 outputs include many variations of milestone and sequencing views to illustrate the intent of how the implementation will be conducted. These outputs are critical inputs to this activity, as the procurement leverages these items in any requests for proposal. Additionally, upon award the vendor will look to integrate these milestone and schedules with their technical approach and make adjustments as necessary. Any adjustments must be vetted through governance as appropriate.

Just as with any other procurement, there are a variety of interested and engaged parties that need to work together. The project governance team is the representative of the interests and needs of the project itself. These individuals will work closely with the procurement officials, legal officials, and with the winning vendor throughout this activity. The planners will be engaged with the vendor selection as well as the initial implementation start-up activities that begin during this activity.

Ultimately any procurement, adjustments to plans, and adjustments to timing will need to be vetted by both project and organization governance teams. The governance prior to the significant implementation activities is just as critical as the governance during the actual implementation itself. Beginning the implementation with a solid and timely procurement and vendor integration is just as critical to the success of the implementation as any other activities.

A.5.5 Activity 4.3: Execute the Plan

In this activity the significant implementation tasks are conducted. In the previous activities there have been decisions to invest, procurement activities have been performed, and the vendor teams have been integrated into a revised timeline. The execution of the timeline and the implementation of the Integrated Plan from Step 3 is the focus of this activity. Many organizations have their own system development lifecycle, configuration management processes, testing processes, change management processes, and decision gates for managing implementation activities. It is during this activity that these processes and decision gates are leveraged to ensure a successful implementation.

The planning outputs from Step 3 are once again leveraged in this activity. Items such as the milestones, the specific recommendations for change, and the project governance structure are critical to a successful implementation. As many organizations have their own project management standards, this activity will certainly also yield project artifacts such as project plans, project status reports, test plans, configuration management plans, and other project artifacts. The planners will engage throughout the implementation to ensure that the implementation matches the intent of what was planned. The planners perform an important role of representing end user intentions and needs, as defined in the Integrated Plan and the outputs of Steps 1-3.

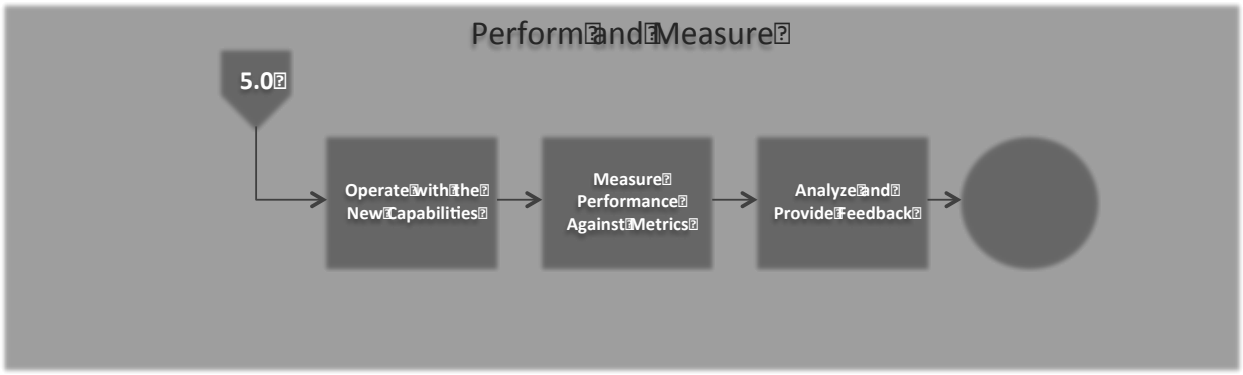
The project management office and the project governance structure are the primary participants in this activity along with the vendors that are performing the implementation tasks. The planners perform an advisory role to the vendors, the project management team, and the governance teams to ensure that everyone is operating from a common understanding of what was planned and documented in the Integrated Plan. The planners may also be engaged with other individuals based on the organization's system development lifecycle. For instance, the planners may need to engage with the organization's Chief Technology Officer, formal test lab, or formal configuration process, as necessary.

Throughout the implementation, the project management office performs the major coordination activities and reports into the project governance structure that was defined in Step 3. The project governance structure will in turn report into an organization specific governance structure or directly into the executive sponsor of the implementation. Governance at varying levels is critical to ensuring checks and balances throughout the implementation.

A.6 Step 5: Perform and Measure

Purpose:

The major outcome of Step 4 is that the recommendations in the Integrated Plan are implemented and operational within the affected organizations. During Step 5, the organization performs its operations while leveraging the newly implemented changes. The purpose of Step 5 is to perform operations and measure performance outcomes against identified metrics.



Step 5 Activities

Role of Planners

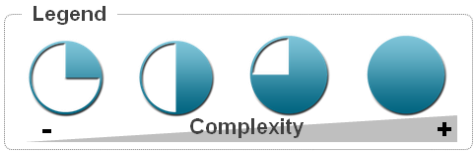
The planners are most in touch with the Integrated Plan, its genesis from the stakeholder outreach activities and the defined issues that were originally determined to be priority enough to address. During Step 5 the planners are in a role to observe and monitor the newly implemented changes and determine whether the intended impacts and outcomes have been realized or if further adjustments are needed. The planners may not be the keeper of the actual performance data, but they need to leverage available performance data to assess whether the implemented capabilities have helped to achieve planned performance metrics. Feedback from this step feeds into future planning efforts as well as immediate planning and implementation adjustments as necessary. Feedback may also necessitate more immediate changes in plans. Any additional changes that impact previously approved plans needs to be reviewed and approved by governance.

Outcome

The key outcome of Step 5 is measured performance outcomes against identified metrics. Step 5 may also produce important outcomes such as feedback into planning to make further adjustments beyond what was implemented in Step 4.

A.6.1 Step At-a-Glance

Step 5 At-a-Glance	Identify and Validate Activities		
	Operate with the New Capabilities	**Measure Performance Against Metrics**	**Analyze and Provide Feedback**
Which Planners Participate in This Activity?	• Architects (review, interpretation)	• Architects (primary, lead)	• Architects (primary, lead)
What Are The Planning Inputs (from Steps 1-3) to This Activity?	• Integrated Plan Document	• Integrated Plan Document • Analysis of Cost, Value, and Risk for Transition Options	• Integrated Plan Document • Analysis of Cost, Value, and Risk for Transition Options
What Is The Relative Complexity of This Activity?			



A.6.2 A Note on Core Artifacts

Like any methodology, the *Collaborative Planning Methodology* is designed for each step to be followed and each Activity Output to be produced. The use of "Core" and "Not Core" to describe these outputs is meant as the first set of tailoring guidance if an organization has constraints of time, budget or resources. As the CPM is tested and refined, feedback from organizations will improve this assignment and generate templates that help to scale outputs according to scope or size.

As described earlier, the goal in using this methodology is to encourage collaboration for high priority projects. This increases the awareness of solutions and services whose reuse can result in efficiencies. The CPM also provides the framework for organizations to generate actionable, consistent and rigorous plans that can lead to improved solutions.

A.6.3 Activity 5.1: Operate with the New Capabilities

In this activity the organization leverages the newly implemented changes as part of their operations. The new changes might be small or large but it is important to operate and monitor the impacts of the new changes. In this activity, the organization's operations staff performs regular operations with little outside involvement. The planners and specifically the architects are available to perform advisory services such as interpretation of intended outcomes as defined in the Integrated Plan.

The most significant output from Step 3 that is in use in this activity is the Integrated Plan. The Integrated Plan contains the recommended changes and the desired impacts of those changes. This

information is useful for the operations staff as they begin to perform regular operations using the new capabilities.

As was the case in Step 4, the planners are available in a support and advisory capacity throughout this activity. The planners engage with the operations end users to ensure that they understand what was intended by the changes and how those changes should be impacting operations.

A.6.4 Activity 5.2: Measure Performance Against Metrics

In this activity the performance of operations with the newly implemented changes is measured against the metrics defined in Steps 1 and 3. In the previous activity the operations are performed and in this activity the operations are measured against intended metrics. The planners are not likely the keeper of the performance data but are available to assist the operations staff in the interpretation and understanding of the data and to help coordinate the delivery of the performance data for interpretation and use. The data is an important input for the next activity where the data is analyzed and formal feedback is prepared.

The Integrated Plan from Step 3 is the primary input for this activity. Additionally, the Analysis of Cost, Value, and Risk for Transition Options is a useful input as the value information from this analysis can be useful to the gathering of performance data against the pre-defined metrics.

The planners continue to work closely with the operations staff to ensure that the metrics are understood and that the performance data is gathered accurately and in a timely manner.

A.6.5 Activity 5.3: Analyze and Provide Feedback

In this activity the performance metrics from the previous activity are analyzed and feedback is formally prepared. The performance data from the previous activity is analyzed to determine whether intended performance outcomes are being achieved or whether additional adjustments might be necessary. Engagement and interpretation with the operations staff is an important part of the analysis including the validation of the conclusions that are established based on the data.

Once the analysis is complete, formal feedback is prepared. This feedback is intended for leadership and governance audiences and is prepared to include any recommendations for further adjustments. Changes to planning documents are needed if additional adjustments are being recommended.

As in the previous activity, the Integrated Plan and the Analysis of Cost, Value, and Risk for Transition Options are important inputs from Step 3. These documents help shape the analysis and provide basis for the feedback.

It is important to engage actively with the operations staff to properly review the analysis and any feedback that is formally developed. The operations staff can provide thoughts and reviews of these materials to ensure that the analysis and feedback are both sound in thinking and practicality. Ultimately, the planners or in some cases the operations staff themselves will present the analysis and feedback to the project and organization's governance.

Appendix B: Business Reference Model (BRM)

B.1 Business Reference Model Overview

The Office of Management and Budget's (OMB) Common Approach to Federal Enterprise Architecture (EA) is based on standardizing the development, integration and use of strategic, business, data and technology architectures to promote increased levels of mission effectiveness. EA is intended to integrate with other management and technology governance areas including strategic planning, capital planning, project management, and cyber-security in order to deliver mission and support capabilities in shorter timeframes with more agility and responsiveness to stakeholders. The figure below depicts OMB's common approach to Federal EA.

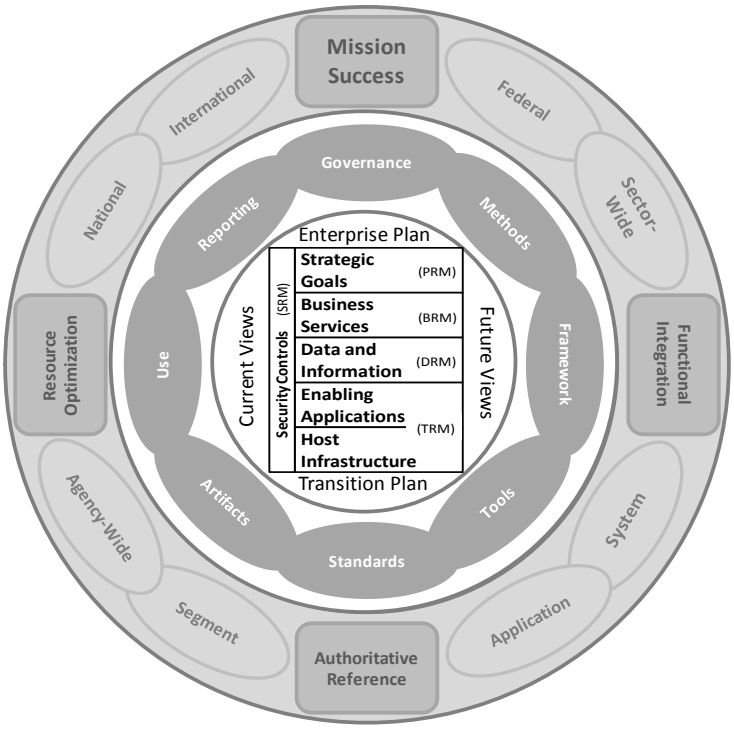


Figure B.4: OMB's Common Approach to Development of Federal EA

Primary Outcomes

EA development helps in enabling the following four primary outcomes:

- **Mission Success** – Provide a consistent view and accurate information across the enterprise to support planning and decision-making
- **Functional Integration** – Facilitate and encourage interoperability between programs and enhanced services by the use of EA standards

- **Authoritative Reference** – Provide an integrated, consistent view of strategic goals, business services (mission and support) and enabling technologies across the entire organization, including programs, services, and systems
- **Resource Optimization** – Provide a harmonized and consistent view of all types of resources in each functional area, program, and system area

The Business Reference Model (BRM) and its associated elements form a key part in delivering expected outcomes and business value to an organization The BRM is one of six reference models of the Federal Enterprise Architecture (FEA). It is a classification taxonomy used to describe the type of business functions at the system, segment, agency, sector, Federal, national, or international levels. The taxonomy identifies business functions and services that are performed in the Federal Government and between Executive Departments, subordinate agencies and with external partners. In using a standard taxonomy to classify functions, investments and other elements across the Federal Government, the BRM is useful in identifying opportunities for cost reduction, collaboration, shared services, and solution reuse in agency IT portfolios and intra- and inter-agency collaboration.

The BRM provides a framework enabling a functional (as opposed to organizational) perspective of the Federal Government, including its internal operations. By describing the Federal Government using standard business functions and services rather than an organizational view, the BRM promotes cross-government collaboration. It enables business and IT leaders to discover opportunities for cost savings and new business capabilities that help to achieve strategic objectives. The BRM describes the "What we do" of the Federal enterprise through the definition of outcome-oriented and measurable functions and services. While the BRM provides a standardized way of classifying government operations, it is only a model; its true utility and value are realized when it is applied and effectively used in business analysis and decision support that help to improve the performance of an organization.

B.1.1 BRM Structure

The BRM is composed of three products: a functional taxonomy, a visual representation of the taxonomy and this narrative that describes the reference model and how to use it.

The BRM taxonomy provides a common reference framework that Executive agencies can align their processes and activities internally and with the rest of the Federal Government. The purpose of the BRM taxonomy is to enable the classification of functions across the Federal Government. In doing so the taxonomy seeks to provide coherence and simplicity out of the complexity of the Federal Government.

The BRM taxonomy is structured as a three-layer hierarchy representing the business functions and services of the Executive Branch of the Federal Government. The highest level is the Mission Sector, followed by the Business Function, with the Business Sub-Function at the lowest level.

- **Mission Sector** – Identifies the ten business areas of the Federal Government in the *Common Approach to EA*

- **Business Function** – Describes what the Federal Government does at an aggregated level, using the budget function classification codes provided in OMB Circular A-11
- **Service** – Further describes what the Federal Government does at a secondary or component level

The table below identifies the ten Mission Sectors and their definitions.

Mission Sector	Definition
Defense and Security	Defined by the functions of national defense, homeland security, and intelligence operations and their associated services.
Diplomacy and Trade	Defined by the functions of international affairs and international commerce and their associated services.
Economic and Financial	Defined by the functions of economic development and community and social services and their associated services.
Education and Workforce	Defined by the functions of education and workforce management and their associated services.
Energy and Technology	Defined by the functions associated with energy, technology and scientific research and their associated services.
Environment and Natural Resources	Defined by the functions of environment and our natural resources and their associated services.
Health and Well-Being	Defined by the functions of health and well-being of the public and their associated services.
Law and Justice	Defined by the functions of with law enforcement and judicial activities and their associated services.
Transport and Space	Defined by the functions of transportation modes, including space exploration and their associated services.
General Government	Defined by the general functions and services associated with all levels of government.

Table B.1: Federal EA Mission Sectors

B.2 Using the BRM Taxonomy

One of the primary purposes of enterprise architecture is to support and improve the enterprise strategic planning and business decision making. The BRM is designed to provide agencies with a standard means to categorize their capital investments, identify areas for collaboration and reuse based on delivery of business capability, and help improve the overall IT architecture to better enable mission outcomes. The BRM also provides decision-support capabilities to stakeholders and different levels of staff, within an agency and externally across the Federal Government.

From a Federal perspective, the BRM allows the Office of Management and Budget (OMB) to identify opportunities for collaboration and reuse of shared services government-wide.

B.2.1 Inter-Agency

B.2.1.1 Office of Management and Budget

Each fiscal year, Federal Agencies are required to submit Exhibit 53s and Exhibit 300s to request funding for new major projects and on-going capital investments and align these projects and investments to the BRM. This enables OMB to identify projects and investments across the Federal Government that support a common business purpose, which further allows OMB to identify candidate shared services that more agencies can use, thereby reducing the number of redundant services throughout the Federal Government. Through the use of a standard classification scheme, the BRM functional taxonomy, opportunities for shared services and elimination of redundancies may be identified.

B.2.2 Intra-Agency

From an internal agency perspective, the BRM will offer support to the following areas:

- Agency Executives and Business Managers
- Agency CIOs
- Portfolio Managers
- Architects - (Chief) Enterprise and Solution Architects
- Project Managers
- Development Teams

B.2.2.1 Agency Executives and Business Managers

Agency executives and business managers include but are not limited to departmental Secretaries, Administrators, Business and IT Senior Executives and Managers. They want to know what value EA can bring to the bottom line of an organization. EA traditionally responds that value is delivered through:

- Improved organizational efficiency and effectiveness
- Cost reduction through standardization and reuse and
- New capabilities identified for strategic advantage

While these are achievable benefits, there is little discussion on how this value is achieved or delivered. The IT Governance Institute (ITGI) has developed an internationally accepted IT Value framework called

Val IT. Within the Val IT framework, value is defined as the total life-cycle benefits net of related costs, adjusted for risk and (in the case of financial value) for the time value of money. While the framework is focused on creating value for IT Investments, it also has a relationship to enterprise architecture.

The Val IT framework is summarized in what is called the "Four Ares". The Four Ares concept provides the basic "value" framework by asking simple questions whose detailed responses provide the path to "value" delivery. The Four Ares are:

- Are we doing the right things?
- Are we doing them the right way?
- Are we getting them done well?
- Are we getting the benefits?

The following figure illustrates the role of Enterprise Architecture in providing the data and analysis to answer these questions.

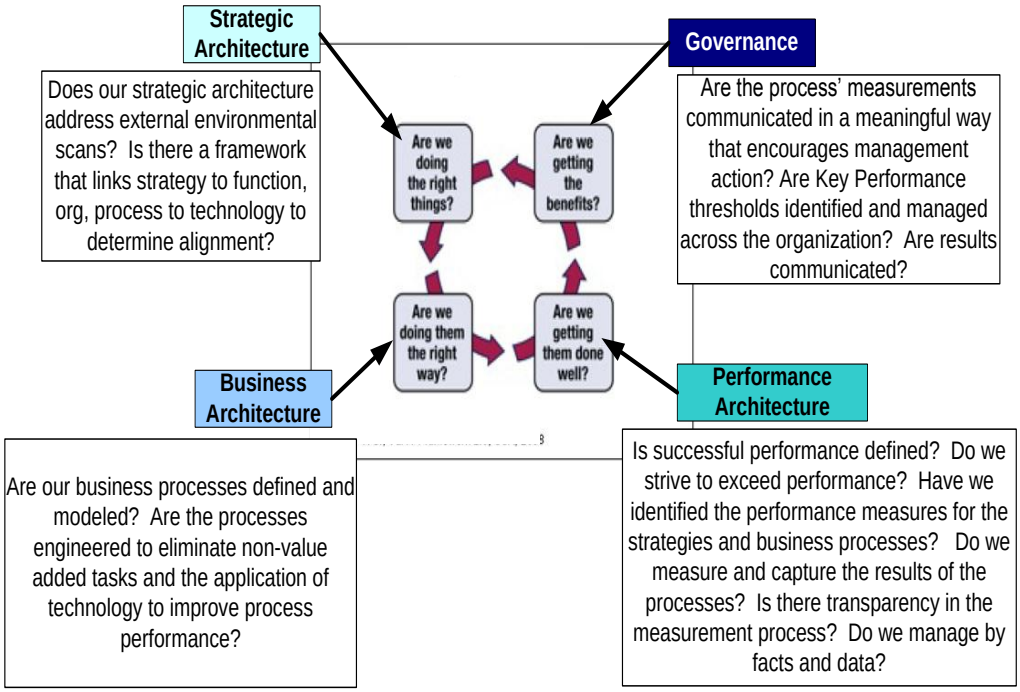


Figure B.5: IT Governance Institute's "Four Areas" and their intersection with EA

Using a standardized business taxonomy, such as the business reference model, enables executives and managers to see the gaps and redundancies within their enterprise and across similar or related organizations. These gaps and redundancies are opportunities for cost savings and new business capabilities that help achieve organizations' strategic objectives.

B.2.2.2 Agency CIOs

Agency CIOs are responsible for establishing and sustaining enterprise architecture management. The CIO understands how agency IT investments align to the organization's business architecture (based in part on the BRM functional taxonomy) in order to make informed decisions about future investments. The BRM includes functions performed throughout the Federal Government. Alignment of organization-specific business processes and applications to these standard functions and services will enable organizations to identify gaps and overlaps. Having established standard functions enables consistent analysis internally within an organization, and externally throughout the Federal Government. From an internal perspective, the analysis helps modify current and identify strategic future business direction.

B.2.2.3 Portfolio Managers

Information technology enables the achievement of business objectives of an organization through the automation of business processes and information services. As a result, it must be managed in a manner that provides a line of sight from the business strategy to the delivery of quality IT services. Enterprise architecture, capital planning, and IT portfolio management allow organizations to manage the delivery of IT solutions that most effectively enable business needs.

Enterprise architecture provides the information for business planning. Capital planners and portfolio managers must have a solid understanding of an organization EA to ensure that projects and investments are aligned appropriately. Working with the organization's EA program office, capital planners and portfolio managers should leverage the organization's EA information base to identify functional portfolios that align to the organization's lines of business. Using the BRM as a framework for IT portfolio management ensures proper alignment of IT projects and investments to the business needs of the organization. Using the CPIC process to select, control, and evaluate assets within a business-oriented portfolio structure ties a clear line-of-sight to the business needs and ensures IT projects and investments are delivering capability services as defined by the business architecture.

B.2.2.4 Architects

An enterprise architect is responsible for establishing and governing the implementation of EA principles based on the fundamental values and rules of an organization. There are two different types of EA principles: ones that govern the EA process and ones that govern the implementation of the architecture. Architectural principles for the EA process affect development, maintenance, and use of the EA. Architectural principles for the EA implementation establish the first tenets and related decision-making guidance for designing and developing business solutions and information systems.

The Federal standard Business Reference Model provides a common reference base for developing and sharing architectural principles. The business-derived architectural principles represent the fundamental business requirements and practices. Utilizing the brain power across the Federal Government, agency architects could identify the best-practice and most suitable architectural principles applicable to the business functions their organizations perform.

Another area of concern to the Architect is the definition and maintenance of the architectural layers of the EA. The BRM helps to identify common business functionality that should be part of the business architecture, and in turn implement that functionality through projects. The organization's business

architecture describes the operations, business functions and services supported by the organization. This business architecture will help guide the development of business cases to request and justify funding for future development and maintenance of programs, systems, and applications. This leads to the development and management of projects to implement these business architectures.

B.2.2.5 Project Managers

Project managers are responsible for managing all aspects of a project, including aligning the project with the business architecture. The BRM helps to identify the common business the project should contribute or support.

During the concept and planning phase of a project, the BRM allows project managers to identify current business capabilities and determine if or how the proposed project fits into the existing architecture. The BRM provides a classification schema to identify organizations, processes and applications that are associated with a given function as well as the up and down stream functions. Identifying and addressing duplicate functionality may result in improvements to the overall efficiency and effectiveness of an organization.

Project managers can also use the BRM to streamline common business processes based on best practices. Streamlining processes has many benefits including cost reduction, cost avoidance, improved cycle time, improved and customer satisfaction and value. Additionally, application performance may be enhanced by finding better ways of doing business, such as sharing data sources, and developing common data retrieval and storage services.

B.2.2.6 Development Teams

From a development perspective, the BRM will enable project teams to align applications and services to a standard set of business functions. Using a common set of business functions will enable internal as well as external analysis of the types of applications and services available throughout the Federal Government. Internally within the organization, it will enhance the ability for project teams to work towards a common solution for satisfying business needs. This will also enhance the ability for agencies to collaborate and identify common, shareable solutions.

Building applications and systems to support common business capabilities will streamline the development process. Identifying systems that, when properly built, can be shared among various applications and systems will make efficient use of resources that are already strained due to financial and budgetary restrictions. The costs associated with maintaining duplicative applications and services can be reduced by developing sharable services that can be used by more than one application or organization. For example, developing a sharable print service that can be used by many applications will reduce the costs associated with maintaining redundant code in individual applications. A shared service will require less workforce resources since the changes will be limited to the shared services and not every application that uses that service. Shared services can also reduce the burden on the public. A shared service may provide the ability to share data within and among systems. It also allows data to be collected once and used many times, thereby reducing the burden on users of the system. A shared service across government also enhances the users experience by providing a common look and feel to applications.

B.3 Associated Methods

The Business Reference Model can be used in conjunction with various architecture, development, or analysis methods to provide comprehensive and standardized design, development, and governance capabilities. This section illustrates a few examples of associating the BRM with other methods.

B.3.1 Business Architecture for Decision Support

The BRM provides the functional foundation used in developing business architectures. A Business Architecture (BA) provides a framework that relates business strategy with the organization structure, functions and processes. The relationships with these elements enable the development of a "line of sight" that is used to analyze how the organization achieves its business objectives and determine where there may be gaps and redundancies in delivering the services necessary to achieve strategic goals. A Business Architecture contains information and relationships to organizational goals, objectives, policies, organizational structures, business functions, and processes as well as business rules and policies.

The purpose of a Business Architecture is to provide accurate information that:

- Is the basis for strategic decision-making
- Is actionable and focused on achieving and improving business results
- Improves the performance and governance of business processes and outcomes
- Identifies and creates new capabilities that improve organization mission accomplishment
- Saves taxpayer funds through collaboration and reuse, productivity enhancements, and the elimination of redundancies
- Improves the quality, availability and sharing of data and information for decision making, and
- Drives the efficient use of IT Resources

Figure 3 below provides one possible illustrative view of the relationship of these elements and their relationships. Business Architectures may also include relationships with the data from other architectural layers – such as data, application, technology, and security – to compose the comprehensive enterprise architecture. Figure 3 indicates there is a relationship between strategy, performance and business functions. By defining that relationship for a specific organization, business architectures can show the relative performance of functions and whether or not each organization's function supports a strategic objective.

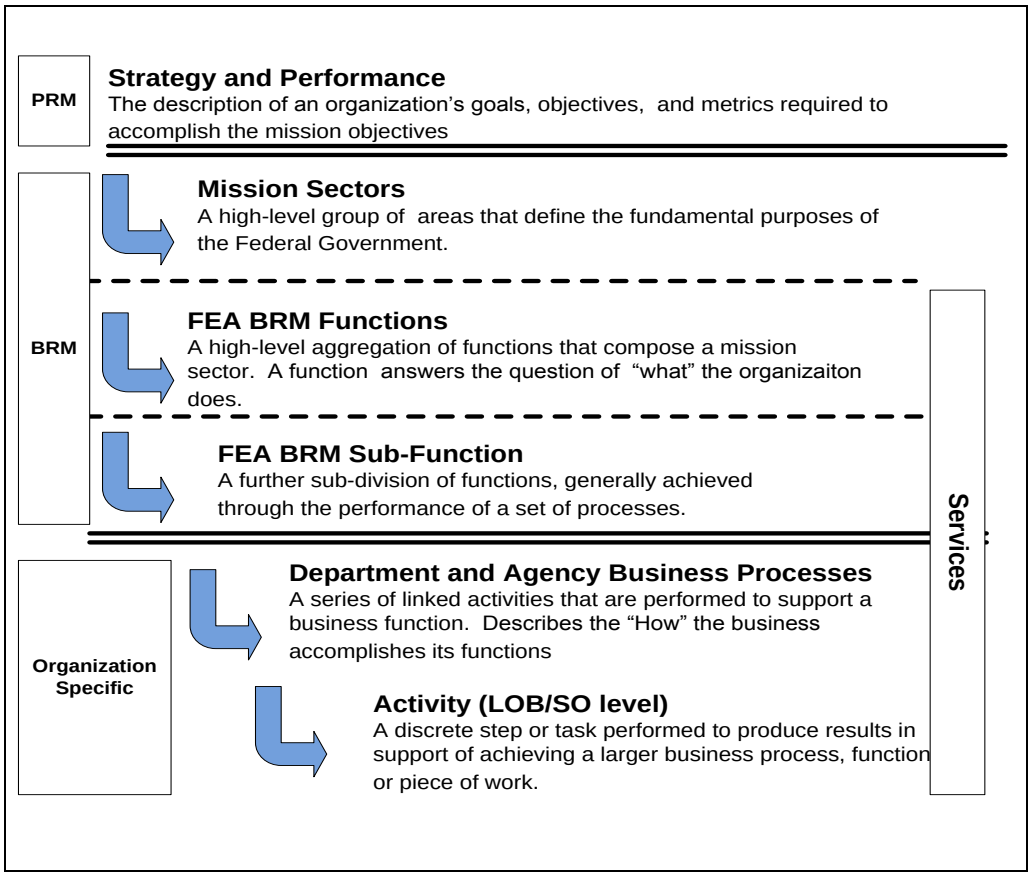


Figure B.6: Business Architecture framework

B.3.2 Business Process Modeling

One objective of the Business Reference Model is to depict a taxonomy of the Federal Government's fundamental business functions and services. This taxonomy serves to classify the complex federal functional environment in order to simplify, analyze and aid the streamlining of service provision to support those functions independent of the agency or agencies involved in the execution. To enable a vision of streamlining service-oriented, seamless functional execution performed by inter-agency and intra-agency collaboration, it is of paramount importance to facilitate precise, complete, consistent, coherent, and accurate communication to all stakeholders that articulates the requirements necessary to convey:

- What the intended outcome is for each function
- What must be accomplished to achieve that outcome
- How it is to be accomplished from its beginning to its end (end-to-end) regardless of the number of organizations involved in the completion of a function's execution

Business Process Modeling Notation (BPMN) and the Unified Modeling Language (UML) are examples of "open" industry standard notational formats that support model-based systems engineering. BPMN and UML govern and facilitate the selection of terms and symbols necessary to represent the complex logic requirements associated with semantic constructs (e.g., workflow sequences, functions, processes,

activities, tasks, dependencies, relationships, decision points, business entities, actors, scenarios, logical decomposition, inheritance).

Business process modeling is a central part of all the activities that lead effective and efficient management of Federal functions. Models are built to:

- Communicate the desired structure and behavior of our capability increment (e.g., system)
- Visualize and control the system's architecture or even the architecture for the system of systems
- Better understand the system we are building within a defined context, often exposing opportunities for simplification and reuse as a by-product of the modeling process
- Manage risk

Modeling is a proven and well-accepted engineering technique. Because a model is a simplification of reality by definition, a model can provide greater understanding of the system or system of systems that are being developed. Models of complex systems that are intended to solve complex problems allow humans to comprehend such a system in its entirety.

Through modeling, we achieve four aims. Applied to systems oriented to automating business processes these aims are:

- Models help us visualize a business process as it is or as we want it to be
- Models permit us to specify the structure or behavior of the process
- Models give us a template that guides us in constructing a system, or more formally a business process capability increment in automated form
- Models document the decisions we made (Booch, 1999)

B.3.3 Business Process Modeling Notation (BPMN)

BPMN allows business analysts to create process diagrams that are expressive and rich enough to address complex business issues such as exception handling. As an extension of UML, BPMN has traditionally been viewed as a modeling tool, but the executable aspect of it is also highly important. BPMN extends the more traditional UML activity diagram by the addition of a wealth of process oriented semantic constructs. BPMN has matured over time to the point that some organizations have full process execution based on Business Process Execution Language (BPEL).

The executable counterpart to the BPMN is BPEL which may be generated from BPMN. BPEL enables organizations to run business processes in an automated environment. BPEL also enables process choreography and orchestration. Business process choreography is the execution of independent business processes in an automated fashion using XML and web services, while orchestration is the arrangement and synchronization of those automated processes. For example, in an end-to-end "procure to pay" service, there are multiple processes within procurement and through to accounts payable. Choreography is the arrangement of those processes. Orchestration weaves those processes together into a cohesive flow so one process feeds and triggers the next series of process activities. All

of this begins by classifying an organization's functions and services using a standard taxonomy and then aligning organization specific processes to that taxonomy structure.

B.4 BRM Taxonomy

A narrative description of the Business Reference Model's Functional Taxonomy and a visual representation of each Mission Sector and their related functions and services are provided in Appendix H.

Appendix C: Data Reference Model (DRM)

DRM Executive Summary

The Data Reference Model (DRM) provides a foundation for describing, discovering, managing, sharing and reusing information within agencies and across the federal government. It describes best practices and artifacts that can be generated from the data architectures and data management practices of federal government agencies. The scope of the DRM is intended to be wide-ranging, as it may be applied within a single agency, Community of Interest (COI), or across various COIs and/or agencies.

Interoperability and information sharing challenges are key drivers for today's DRM priorities highlighted in several Federal guidance initiatives, such as the Federal Chief Information Officer's (CIO) *25-point Implementation Plan to Reform Federal Information Technology Management*. In particular, reducing information technology (IT) costs, improving data security and privacy controls, and delivering mission-aligned IT capabilities in weeks and months instead of years are critical to meeting the current goals of the Federal CIO and CIO Council.

This document supports the DRM, one of six reference models of the Federal Enterprise Architecture Framework (FEAF) v2. It is guided by the principle of managing government data as national assets. The DRM is the Federal Enterprise Architecture (FEA) mechanism for identifying what data the Federal government has and how to share that data in response to business/mission requirements.

C.1 Introduction

The DRM is a flexible and standards-based framework to enable information sharing and reuse across the federal government via the standard description and discovery of common data and the promotion of uniform data management practices. The DRM provides a standard means by which data may be described, categorized, and shared.

As a reference model, the DRM is presented as an abstract framework from which concrete implementations may be derived. The DRM's abstract nature will enable agencies to use multiple implementation approaches, methodologies and technologies while remaining consistent with the foundational principles of the DRM.

C.1.1 FEA DRM Focus

The key goals of the DRM are:

- Improving discovery, access, and sharing;
- Using Federal data to meet mission needs;
- Supporting shared services;
- Aiding cross-agency collaboration; and
- Positioning agencies to operate in a global information environment

As a catalyst, the DRM multiplies the value of existing data holdings hidden in "silos" through better discovery, understanding, and access of the data by categorizing Data Assets at a high level within the Federal DRM taxonomy in order to provide discovery capabilities for future data investments. This is achieved by:

- Leveraging data and information sharing in the context of business and community interests across organizational boundaries;
- Developing shared vocabularies to facilitate reuse of data across communities;
- Providing governance and performance measures to ensure the trust, accountability, and security of data being shared or exchanged; and
- Moving toward data consolidation based on authoritative data sources and best of breed solutions.

C.1.2 DRM as Federal Guidance

The DRM provides guidance for describing an agency's data architecture and associated artifacts in alignment with the FEAF v2. This guidance includes a description of best practice methods and notations to develop the artifacts necessary to:

- Enable decision-support;
- Guide solution and service architecture requirements; and
- Achieve compliance with Federal reform requirements

C.1.3 What the DRM Is and Is Not

The DRM provides guidance for agencies to leverage existing Data Assets across the government. The DRM increases the Federal government's agility in drawing out the value of information as a strategic asset. This reference-able, conceptual approach facilitates information sharing and reuse across the Federal government.

The DRM is:	• A consistent means to categorize agency data • A reference for consistently describing agency data architectures and associated artifacts • A reference for supporting planning activities for shared services • A reference supporting Office of Management and Budget (OMB) reporting activities, such as Enterprise Architecture (EA) maturity and use • A means to compare data among agencies in order to exchange, reuse, and integrate data
The DRM is not:	• Fixed and unchanging, rather it is flexible and scalable so that new Subjects and Topics can be added as the business model for the Federal government changes • A data management "how to" manual for building and maintaining data architectures • A government-wide all inclusive conceptual data model or fully attributed logical data model • An all-encompassing set of XML schemas • A replacement of existing data structures within the agencies

Table C.2 What the DRM Is and Is Not

C.1.4 The DRM and Knowledge Management

The DRM taxonomy can be used as a tool in Knowledge Management. "Knowledge Management is the collection of processes that govern the creation, dissemination, and utilization of knowledge. In one form or another, knowledge management has been around for a very long time. Practitioners have included philosophers, priests, teachers, politicians, scribes, Liberians, etc." from the introduction to *An Open Discussion of Knowledge Management*, Brian (Bo) Newman, 1991.

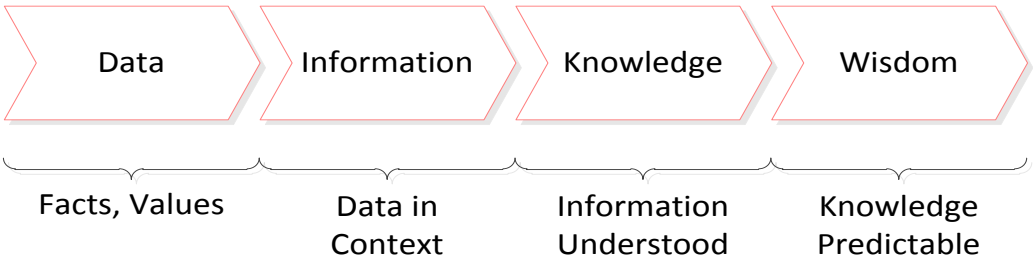


Figure C.7 Data, Information, Knowledge, Wisdom Continuum

Knowledge is also defined using taxonomy, with levels describing data, information, knowledge and wisdom. Briefly, data is defined as a fact. Information is a fact with some context. Knowledge is an understanding gained from a pattern that exists with related information. Wisdom combines an understanding of all of the above with some additional exploration to derive a cause and effect relationship.

A fact, such as the number 100, is data. We can intuitively discern that another fact such as 101 may be greater in value but without some further context we cannot be sure what the data represents. Stating that the number 100 is a dollar value adds some additional meaning, and adding that the dollar value is an account balance further extends the perspective of 100. The amount of background needed to transform data into information is subjective.

For the purposes of the FEA, we adopt the convention that the DRM, used alone, categorizes data, but the DRM used in concert with any of the other Reference Models categorizes information. For example, stating that a given Data Asset contains data in a specific Topic in the DRM Taxonomy isn't sufficient, by our convention, to qualify as information. If that same Data Asset is further stated to be used by a particular Service in the Business Reference Model (BRM), the combination of the DRM and BRM associations with the Data Asset qualifies as information.

Application of an algorithm or heuristic to relevant information, resulting in insights and experience, can produce knowledge – an understanding of the patterns or trends in information. Wisdom combines knowledge with cultural norms, ethical analysis or underlying principles to further explain why the patterns or trends identified as knowledge occur.

Though the DRM taxonomy is useful for the data and information layers of knowledge management taxonomy, a record of knowledge and wisdom can also be related to one or more topics in the DRM taxonomy. When necessary to classify knowledge or wisdom, the DRM should be supplemented with taxonomies from the field of library and information sciences, such as the Dewey Decimal System, to provide additional value.

In summary, as context is added to data, it enables data to become more useful and robust, and data becomes information. The DRM taxonomy provides a descriptive structure that makes the data contents more discoverable. When data can be discovered, it can be shared.

C.1.5 FEA DRM Meta-Model

The FEA DRM meta-model provides a structure and vocabulary for agencies to form a consensus as to how, at a Federal level, to categorize, describe, and share data. It is not intended to change an agency's method or notation used to develop data architecture artifacts; it is simply a means to provide a core standard set of terminology that can be used consistently across agencies to categorize data. The FEA DRM meta-model is represented in Figure C.2, using Unified Modeling Language Class Diagram notation.

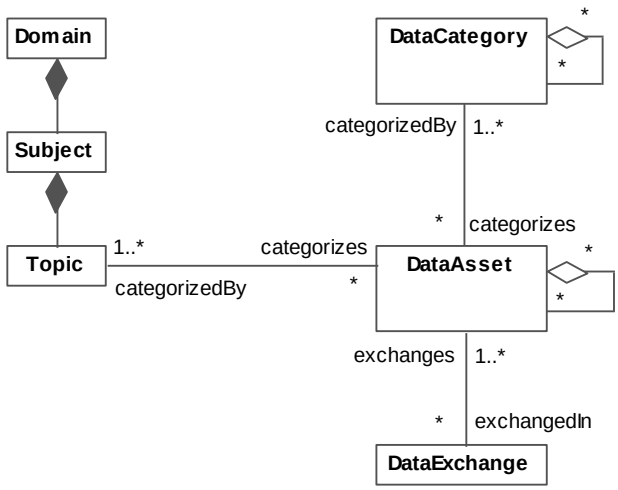


Figure C.2 DRM Meta-Model

The FEA DRM meta-model elements are defined in Table C.2 documented below.

Meta-model element definitions	
Element	**Definition**
Domain	The broadest data category, grouping data by general characteristics.
Subject	A sub-category of a Domain with more specific characteristics of the types of data that fit within it. A Subject may still be general enough to span the types of data used in many disparate business functions.
Topic	A sub-category of a Subject that further decomposes the Domain categorization into highly cohesive sets of data entities that support business processes and services.
Data Asset	A collection of data elements that make sense to group together. Each community of interest identifies the Data Assets specific to supporting the needs of their respective mission or business functions.
Data Exchange	A collection of data elements exchanged between an Information Provider and Consumer.
Data Concept	An alternative category, developed by a community of interest, used to organize Data Assets and Data Exchanges.

Table C.3 DRM meta-model definitions

The Domain, Subject and Topic classes illustrated in the meta-model and defined in the table above comprise the schema for the Data Reference Model taxonomy. DRM Domains are composed of DRM Subjects which are in turn compiled of DRM Topics.

The Data Asset concept above is not part of the DRM taxonomy but rather represent elements that can be categorized by the DRM taxonomy. The Data Assets are defined by a particular COI, an Agency, a

program office or even an international working group, to suit its needs. The DRM taxonomy provides a common language for categorizing the Data Assets, supporting analysis across organizational boundaries.

Notably, a Data Asset is a deliberately abstract concept. A given Data Asset may represent an entire database consisting of multiple distinct entity classes, or may represent a single entity class. As illustrated in the FEA DRM meta-model (Figure C.2), a Topic may categorize any number of Data Assets. (In other words, in any given organization's environment, a particular Topic may not apply to any Data Assets or it may apply to multiple Data Assets.) A Data Asset, however, must be categorized by at least one Topic and may be categorized by multiple Topics.

Ideally, the decomposition from Domain to Subject to Topic would simply extend to the Data Assets, so that each Data Asset was categorized by one and only one Topic. Such a strict mechanism for defining Data Assets would never satisfy the needs of every COI (i.e., there is no "one size fits all" way to categorize data) so the DRM meta-model reflects the reality that a Data Asset may be categorized by one or more Topics.

The FEA DRM meta-model also illustrates the relationship between Data Assets and Data Exchanges. As modeled, each Data Exchange exchanges the data in one or more Data Assets. Conversely, a Data Asset is not necessarily used in a Data Exchange but may be used in any number of Data Exchanges. As a side effect of the relationship between Data Assets and Data Exchanges, the set of Topics that categorize a Data Exchange is the union of the Topics that categorize the Data Assets used in the Data Exchange.

The Data Concept element in the DRM meta-model is also not a part of the DRM taxonomy. Recognizing that communities of interest may have already developed their own categorization schemes for their Data Assets, the DRM meta-model includes the Data Category for representing those alternative categorization schemes. These other data categorization schemes do not necessarily have any correlation to the DRM taxonomy beyond the fact that they can be used to categorize the same Data Assets.

C.1.6 DRM Fundamental Methods

The DRM describes data and information needed to perform Federal business and mission functions by use of collective methods. As depicted in the figure below, there are three fundamental method areas associated with the DRM to help agencies consistently categorize, describe, and share their data.

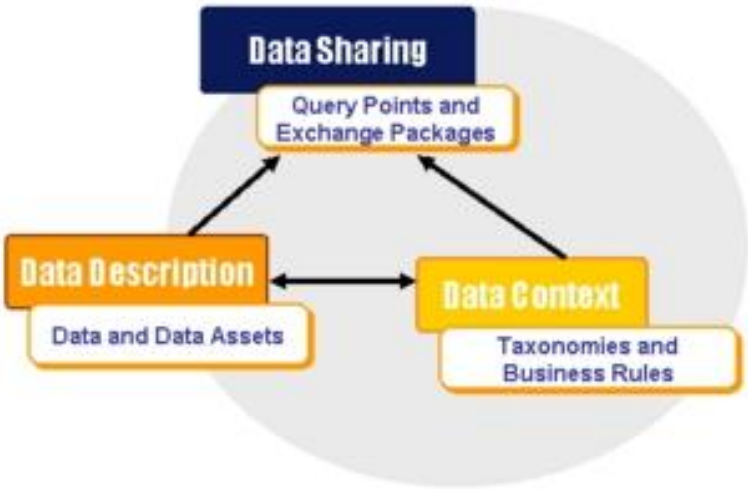


Figure C.3 FEA DRM Method Areas

- **Data Description**: Provides a means to uniformly describe data, thereby supporting its discovery and sharing
- **Data Context**: Facilitates discovery of data through an approach to the categorization of data according to taxonomies. Additionally, enables the definition of authoritative data assets within a COI
- **Data Sharing**: Supports the access and exchange of data where access consists of additional requests (such as a query of a data asset), and exchange consists of fixed, reoccurring transactions between parties. Enabled by capabilities provided by both the Data Context and Data Description standardization areas

The DRM provides a starting point and organizing mechanism for establishing collaboration around data to meet mission needs.

C.1.7 DRM Overview

The subsequent sections of this document provide a detailed description of each DRM component as follows:

Section C.2 - Associated Methods and Standards Overview: This section provides detailed information about methods and techniques to use in concert with the DRM to develop a data architecture and information exchanges. Where applicable, standards for the associated methods are identified.

Section C.3 – DRM Examples of Use: Provides implementation examples through the use of use cases to describe integration points with other FEA Reference Models and select agency DRM implementation examples.

Section C.4 – Measuring for Success: Provides recommended approaches and performances measures to establish and monitor DRM implementation results.

Section C.5 – Summary: Summarizes the overview of the DRM framework and its purpose.

Appendix C.i: Glossary of Selected Terms.

The contents of the DRM taxonomy are defined in **Appendix I**. Each Domain is documented in a separate subsection.

C.2 Associated Methods and Data Standards

The purpose of the Associated Methods and Data Standards Section is to further describe each DRM framework component and provide best practice methods. Each subsection describes the relevance of the framework components to an agency's overall data strategy, best practice methods to develop the component, and how the agency can use the three components to further data interoperability and sharing initiatives.

C.2.1 Data Description

Data Description extends the structure and depth of the FEA DRM Core Topics specific to an agency or community's mission needs, often by categorizing and harmonizing existing data assets. Similar to Data Context, the Data Description process is iteratively developed and decomposed to include detailed information about the Entities, Attributes and Exchange Packages. Part of the process includes transforming the conceptual data architectures into physical schema. Various views of data description include:

- ***Enterprise or Business View***: Used to communicate consistent definition of the meanings and descriptions of the data. This view is focused on the semantics (i.e., meaning) of the information stored as objects of interest and is independent of how that data is stored or accessed.
- ***Information Consumer View***: The external perspective of the information typically provided in information exchange specifications, end user interfaces, and reports.
- ***Physical View***: The information view focused on the physical structure needed to support the access, storage, and retrieval needs of an operational system.

C.2.1.1 Overview of Metadata

Traditionally, data description was solely focused on organizing structured data and describing this data within the structure of object, property, and representation. With unstructured data as the largest focus of agencies' data management challenges, the DRM Description component has been revised to focus on the larger topic of metadata, which includes both traditional structured data and unstructured data description. Examples of different types of metadata include:

- Semantic: conveys the meaning of data;
- Resource: provides bibliographic information;
- Discovery: enables search and discover (e.g., "tagging" and "metacard");

- Structural: defines physical implementation (e.g., database and exchange schemas, file formats);
- Technical: defines technical process execution, completion, success or failure.

Metadata is found in documents, messages, images, sound streams, data sets, Web sites, and videos. Metadata is important because it:

- Promotes clearer understanding;
- Helps users find information;
- Promotes more efficient use and reuse of information;
- Promotes better data management, particularly in environments of "Big Data"; and
- Uses DRM Data Description Best Practice Methods.

Metadata definitions are traditionally governed by the business community and enforced by technology managers therefore types of metadata such as business or technical have become focused on the community usage. Business metadata tends to be focused on the concepts that need to be executed or shared while technical metadata is more physical and focused on the technology. Business intelligence is an excellent example of a technology that incorporates both business and technical metadata to deliver the necessary content.

C.2.1.2 Data Description Methods

The *Common Approach to Federal EA* lists common agency data architecture artifacts to describe the components of the DRM framework based on lines of business, COIs and specific business services. These artifacts include:

Abbreviation	Artifact Name
DRM	Data Reference Model
D-1	Logical Data Model (Entity or Object)
D-2	Knowledge Management Plan
D-3	Data Quality Plan
D-4	Data Flow Diagram
D-5	Physical Data Model
D-6	Create, Retrieve, Update, Delete Matrix
D-7	Entity/Object State-Transition Diagram
D-8	Entity/Object Event Sequence Diagram
D-9	Data Dictionary / Taxonomy
D-10	Object Library

Table C.3 Data Description Artifacts

The methods listed in the table below explain best practice examples used to describe the common data architecture artifacts aligned with the FEA DRM Core Data Categorization. This guidance is meant to inform and enhance an agency's data description processes and to align agency data practices with the FEA DRM Metamodel.

Method	Description	Authoritative Reference
Integration Definition for Function Modeling **(IDEF)**	IDEF is a family of modeling languages developed by the U.S. Air Force and widely adopted by the Department of Defense (DoD). Most relevant to the DRM is the IDEF1X models. IDEF1X is used to define a logical data model when the target deployment is known to be a relational database.	The IDEF1X standard was published by the National Institute of Standards and Technology (NIST) in Federal Information Processing Standards (FIPS) Publication 184, but withdrawn on September 8, 2002. Though the IDEF1X notation and conventions are still in use and implemented by many data modeling tools, the standard is no longer maintained as a FIPS.
The Open Government Group Architecture Framework **(TOGAF)**	TOGAF® is an architecture implementation and governance framework that traces its lineage to the Technical Architecture Framework for Information Management (TAFIM) developed by DoD. TOGAF® defines an Architecture Development Method (ADM) that uses the four business, application, data, and technical architecture domains. Most relevant to the DRM is the data architecture domain that uses data architecture catalogs, matrices, and diagrams.	TOGAF® is managed by The Open Group, a vendor neutral consortium. http://www.opengroup.org/togaf
Unified Modeling Language™ **(UML)**	UML is a mature and widely adopted technology-independent modeling language that supports the application development life cycle. The UML specification is maintained by the Object Management Group, a not-for-profit computer industry consortium and is an ISO standard. UML notation can describe class, sequence, package, use case, component, and other diagrams.	http://www.omg.org/spec/UML/
Department of Defense Architecture Framework v2.02 **(DoDAF v2.02)**	The DoDAF v2.02 provides detailed guidance for “fit-for-purpose” architecture development. The principles and goals of DoDAF are to promote interoperability, intra- and inter-agency information sharing, and improved business processes through the development and implementation of Architectural Descriptions. The DIV-1 (Conceptual Data Model), DIV-2 (Logical Data Model) and DIV-3 (Physical Data Model) provide guidance to develop data artifacts at each layer of the Architectural Description.	http://dodcio.defense.gov/sites/dodaf20/

Method	Description	Authoritative Reference
ISO/IEC 11179	An international standard that specifies the kind and quality of metadata needed to describe data and that specifies how to manage metadata in a metadata registry.	http://www.iso.org/iso/home.htm
Dublin Core	A core metadata vocabulary intended to facilitate discovery and management of resources.	http://dublincore.org/

Table C.4 Data Description Best Practices

In summary, the Data Description component of the DRM framework enables the development of data architecture or structure at the conceptual, logical, and physical level. Specific activities and outcomes include, but are not limited to, the following:

- Data Inventories
- Data Discovery
- Definitions and Semantics
- Structure and Schemas
- Syntax
- Pedigree and Lineage
- Authoritative Data Sources
- Security and Protection
- Data Transfer Standards

C.2.2 Data Context

Context often takes the form of a set of terms (i.e., words or phrases) that are, themselves, organized in lists, hierarchies, or trees. These terms may be referred to as “context items”. The Data Context method can also be called “categorization” or “classification”.

Agencies and organizations participating in COIs are called upon to categorize their data. Once shared in data registries, these categorizations become vehicles for discovering data that offer value for data sharing. For an agency, the DRM taxonomy can be used to categorize core data sources (e.g., data bases, data warehouses, files) that support a particular business function. Its use provides context and enables discovery of information to support business mission requirements. The agency can define and make context metadata visible and accessible to potential users for either sharing information or developing services. Further, data consumers can subscribe to topics published within data registries, thus enhancing data discovery.

The DRM taxonomy is not meant to be fixed and unchanging. Rather, it is flexible and scalable so that new Subjects and Topics can be added as the business model for the Federal government changes. The core categorization provided by the DRM not only includes Domains, Subjects and Topics, but also allows agencies to decompose Topics further into Agency-specific entities, as needed, for their respective business processes.

C.2.2.1 Role of Data Context in Governance

Many classification schemes are formally created and administered by organizations or consortiums using a set of rules that describe how concepts are named and designated as terms, related artifacts designed, and how they can be used.

The DRM taxonomy enables data governance for Federal shared services and COIs. For agency or COI information sharing initiatives, the categorization helps to establish governance and/or stewardship for the data sources within the associated Subject and Topics. At a minimum, data context will enable data governance for a COI by identifying:

- What data (Subject Areas or Entity Groups) the COI needs;
- Which individual(s) are responsible for being the data steward(s);
- What organization(s) is (are) responsible for maintaining the data;
- What system(s) and service(s) are responsible for maintaining the data;
- What is the linkage to the FEA BRM; and
- What services are available to access or exchange the data.

C.2.2.2 Data Categorization Methods

The BRM and the DRM can be associated by mapping the Subjects and Topics that are input to or created by a Business Function. This mapping combined with the data asset to the FEA DRM Core Data Categories will enable identification of business functions that the data asset supports.

The methods listed in the table below explain best practice examples used to describe the common data architecture artifacts aligned with the FEA DRM Core Data Categorization. This guidance is meant to inform and enhance an agency's data description processes and to align agency data practices with the FEA DRM Metamodel.

Method	Description	Authoritative Reference
Data Asset Catalog	A data asset catalog reduces time and cost to implement change by reducing the time to locate needed data, identifies redundant data assets for decommissioning, and identifies opportunities to reuse or extend a data asset rather than creating a new data asset. Using the Data Taxonomy, agencies should inventory their data assets, associate or map the data assets to the Data Taxonomy and create a data catalog consisting of the Taxonomy Subject, Taxonomy Topic, Entity Name (table, class, file name) , Attribute Name (column, attribute, field, tag), and Data Asset Population (a rule to limit scope of an association). The data asset catalog is populated through a 'bottom up' process that associates the data contents of a data asset documented in the data asset's data model to the Data Taxonomy.	Data Management Book of Knowledge (DMBOK) DAMA April 2009 DoD 8320.02-G Guidance for Implementing Net-Centric Data Sharing April 2006 An agency can create a data catalog with the following steps: 1) Inventory data assets and collect the data model or structure for each asset, 2) Map the asset characteristics to the Data Taxonomy, 3) Present the results in a data catalog. The data asset catalog provides the foundation of an enterprise data inventory, which lists and describes all agency data sets used in the agency's information systems and is required by OMB's Policy on *Managing Government Information as an Asset*.

Method	Description	Authoritative Reference
Information Discovery and Search	This capability will allow Information Sharing Environment (ISE) users to discover the information they need without having to know in advance that the particular information exists or having to know its location. This capability will be designed to support the needs of a diverse user base with varied computer skills to search and discover information across the ISE. The discovery capability requires data sources to be categorized into agency or federal level taxonomies.	ISE Implementation Plan PM-ISE, November 2006 An agency can support the discovery layer of the Information Sharing Environment through the combination of the data asset catalog and a data categorization taxonomy with each data asset mapped to the agency's data categories. The discovery and search capability uses the data categorization taxonomy to identify the data assets that satisfy the search criteria of the user.

Table C.5 Data Categorization Methods

In summary, the Data Context component of the DRM framework enables Data Governance and sets the foundation for detailed Data Description. Specific activities and outcomes include, but are not limited to, the following:

- Governance oversight (i.e., Data Stewardship) including issue resolution;
- Data Management policies and procedures;
- Data Architecture development best practices and processes;
- Performance goals and measures for COIs' data management and information sharing initiatives; and
- Focused education and training for a COI's governance roles, data management policies, data architecture development processes, and associated core data category descriptions and potential data assets.

At the FEA level, Data Context sets the foundation for the DRM Core Data Categories. These categories provide the high level foundation for an agency's data architecture artifacts, including data catalogs, registries, metadata, and data models.

C.2.2.3 Usage Context

Data are managed and stored in various ways to optimize their use. The Data Pattern Quadrants figure below shows typical optimization patterns used by data repositories.

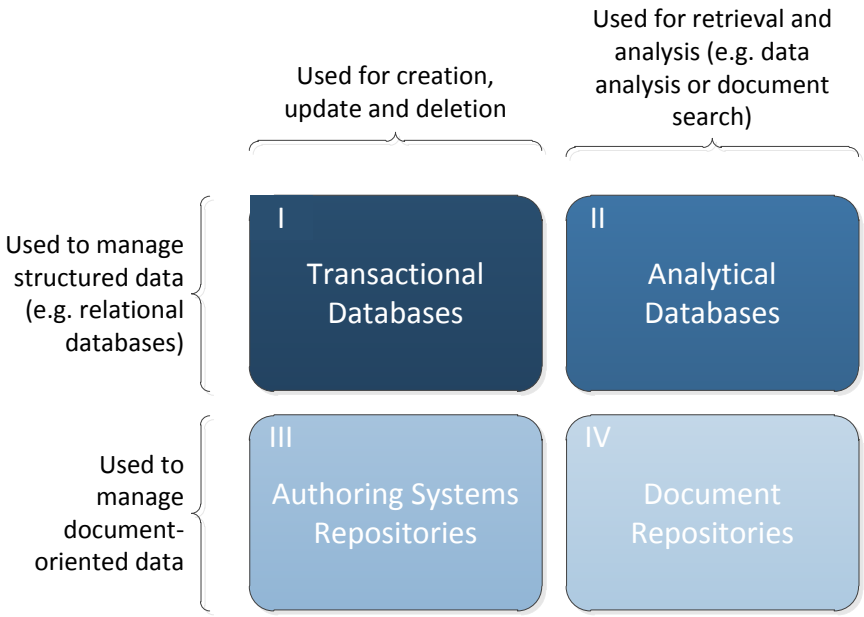


Figure C.4 Data Pattern Four Quadrants

Quadrant I - Transactional Databases: Databases in this usage context contain structured data objects that support business processes and workflow. These structured databases, when well designed, tend to be highly normalized and optimized for transactional performance. Quadrant I repositories include the databases supporting On-Line Transaction Processing (OLTP) Systems, Enterprise Resource Management Systems (ERPs), and other "back-office" systems that implement core business processes and workflows. The data within these repositories may not to be directly accessible to create, read, update, and delete (CRUD) operations of a database management system due to the need to impose complex business logic and referential integrity. In these instances, operations on the data are usually controlled through an Application Programming Interface (APIs).

Quadrant II – Analytical Databases: These databases contain structured data objects that support query and analysis. These structured databases tend to contain historical data and to be purposefully de-normalized, organized in a star schema, and optimized for query ease and performance. The data in these repositories are typically obtained from one or more Quadrant I databases and structured to support answering specific questions of business and/or mission interest. Quadrant II repositories include On-Line Analytical Processing (OLAP) systems, data warehouses, and data marts. Quadrant II also includes directories [e.g., repositories that support the Light Weight Directory Access Protocol (LDAP) or X.500)]. Data in these repositories tend to be directly accessible for query and read. Create, update, and delete operations are typically performed more indirectly than in transactional databases through an extract, transform, and load (ETL) process.

Quadrant III – Authoring Systems Repositories: The term "document" within the DRM context is broadly defined to encompass a wide range of data objects. These objects may be in any of a variety of formats, i.e., multimedia, text documents with embedded graphics, XML Schema, HTML web pages or DTD instances. Generically, in this context, the term "authoring system" is equally broad in scope. At one extreme, an "authoring system" may be a digital camera; at the other, an authoring system may

implement a complex workflow used for the production of a formal publication. In either extreme, the products of an authoring system are documents. The underlying repositories used by authoring systems may also be of any variety of constructs to store data objects - file systems and relational databases being the most common. Generally, as in Quadrant I repositories, data access is controlled through a software interface to preserve business logic and data integrity (e.g., version control of documents).

Quadrant IV – Document Repositories: Like Quadrant II repositories, document repositories store data objects so as to optimize discovery, search, and retrieval. These repositories include the file systems used by Web sites, relational databases underlying content management systems, and XML registries. The documents are typically made accessible using a document index that contains keywords, authoring date and document location. Generally, as in Quadrant II repositories, data tend to be directly accessible to query and read. Create, update and delete operations are not generally available to end users, but are provided through a publication function performed through an authoring system.

C.2.3 Data Sharing

Data Sharing is focused on architectural patterns for sharing and exchanging data. To guide architects in its use, a Data Provider-To-Consumer Matrix is provided for planning the services required for data access and exchange within and between COIs to support their business/mission needs. These COIs may include international, Federal, state, local, and tribal governments, as well as other public and private non-governmental institutions. This section describes two types of services that enable information:

- **Data Exchange Services:** Focus on the exchange of data between two data sources. The information exchange will vary in structure, based on the data objects being exchanged.
- **Data Access Services:** Make data accessible to other services, to the applications that use them, and ultimately, to the consumer of the data.

The FEA DRM Data Sharing Component focuses on the following:

- What flows of information are required within and between service areas in order to make them successful;
- How these flows of information can be harmonized, standardized, and protected to promote sharing that is efficient, accurate, and secure;
- How the data underlying the information flows will be formatted, generated, shared, and stored; and
- What the workforce, standards, and security issues are in this domain.

C.2.3.1 Sharing Data through Data Exchange Services

The Provider-to-Consumer Matrix provides a means to describe data exchange services for interchanges between repositories (data assets, database to database information sharing). These information exchanges vary in their structure and service category based upon the types of data assets being exchanged.

Entity Group	Information Provider	Provider Source Types*	Information Consumer	Consumer Source Type*	Information Service

* Structured or unstructured depending on service category

Table C.6 Provider-to-Consumer Matrix

Based upon this analysis, the architect may specify several types of services to support the sharing of information between databases within a collection used by a COI. These services address the data exchange element of the DRM Meta-model and fall within the following categories:

<table>
<tr><th>Service Category</th><th>Description</th></tr>
<tr><td>Publication (Structured data or documents to aggregate documents)</td><td>Publication is the process of assembling a document from its component pieces, putting into a desired format, and disseminating it to target databases. The payload of this type of service is a document.

This service applies to exchanges between:
<table>
<tr><th>Provider</th><th>Consumer</th></tr>
<tr><td>Transactional (I)</td><td>Document Repository (IV)</td></tr>
<tr><td>Analytical (II)</td><td>Document Repository (IV)</td></tr>
<tr><td>Authoring (III)</td><td>Authoring (III)</td></tr>
<tr><td>Authoring (III)</td><td>Document Repository (IV)</td></tr>
</table></td></tr>
<tr><td>Entity/Relationship Extraction (Unstructured documents to structured documents or structured data objects)</td><td>Entity/Relationship Extraction is the process of identifying and pulling out specified facts from documents. Entities are nouns that designate a specific person, place, or thing. Relationships are the association or affiliation of one entity to another. Typically, the Entities identified during an entity/relationship extraction process may be incorporated into the source document as metadata, inserted into a separated document (such as a metadata record used to support discovery), or incorporated into a structured database. The payloads for all of these exchanges are structured data.

This service applies to exchanges between:
<table>
<tr><th>Provider</th><th>Consumer</th></tr>
<tr><td>Document Repository (IV)</td><td>Transactional (I)</td></tr>
<tr><td>Document Repository (IV)</td><td>Analytical (II)</td></tr>
</table></td></tr>
<tr><td>Document Translation (Document to document)</td><td>Document translation is the process of transforming a document from its original format to a format required to support a target application. The transformations may be structural (e.g., transforming MS Word to PDF format), language-oriented (e.g., changing English to French), or special purpose (e.g., the development of abstracts from longer documents.) The payload of this type of service is a document.

This service applies to exchanges between:
<table>
<tr><th>Provider</th><th>Consumer</th></tr>
<tr><td>Document Repository (IV)</td><td>Authoring (II)</td></tr>
<tr><td>Document Repository (IV)</td><td>Document Repository (IV)</td></tr>
</table></td></tr>
</table>

Table C.7 Data Exchange Service Categories

C.2.3.2 Data Sharing through Data Access Services

The discussion above focuses on the transfer of data between repositories. Additional services are required to make data accessible to other services, to the applications that use them, and ultimately to the consumers of the data. The DRM Team performed a similar analysis to determine the services required to implement data access. The architect should ascertain the services that are required to support the COI in the use of its collection. These services address the data exchange element of the DRM Meta-model.

The services that the architect may be required to provision to support a COI's information sharing requirements are described below.

Service Category	Description
Context Awareness Services	A context awareness service allows the users of a collection to rapidly identify the context (as defined above) of the data assets managed by the COI. Context information may be captured in formalized data architecture, a metadata registry, or a separate database. The architect should plan for this service for all quadrants.
Structural Awareness Services	A structural awareness service allows data architects and database administrators to rapidly identify the structure of data within a data asset (i.e., a structural awareness service makes the Data Description as defined within the DRM available for use). Data Description information may be captured in a formalized data architecture, a metadata registry, or a separate database. Also, a number of commercial products are available to analyze and report data structures. The architect should plan for this service for all quadrants.
Transactional Services	A transactional service enables a transactional create, update or delete operation to an underlying data store while maintaining business and referential integrity rules. These services allow external services or end users to execute data related functions as a part of a workflow or business process. Most commercial products provide application programming interfaces that implement this type of service. The architect should plan to provision these services for the transactional and document authoring quadrants.
Data Query Services	A data query service enables a user, service, or application to directly query a repository within a collection. The architect should plan to provision these services for the transactional and analytical quadrants.
Content Search and Discovery Services	A search and discovery service enables free text search or search of metadata contained within the documents in a repository. The searchable metadata should include the Data Context as defined within the DRM Metamodel. The architect should plan to provision these services for the authoring and document repository quadrants.

Service Category	Description
Retrieval Services	A retrieval service enables an application to request return of a specific document from a repository based upon a unique identifier, such as a URL. The architect should plan to provision these services for the authoring and document repository quadrants.
Subscription Services	A subscription service enables another service or an end user to self-nominate to automatically receive new documents added to a repository in accordance with a predetermined policy or profile. The architect should plan to provision these services for the authoring and document repository quadrants.
Notification Services	A notification service automatically alerts another service or an end user of changes of the content of a repository in accordance with a predetermined policy or profile. The architect should plan to provision these services for the transactional, authoring, and document repository quadrants.

Table C.8 Data Access Service Categories

C.2.3.3 Information Sharing

The methods listed in the table below describe the best practices used for information sharing. This guidance is meant to inform and enhance effective agency information sharing processes.

Method	Description	Authoritative Reference
National Information Exchange Model (NIEM)	In 2005, the Department of Justice (DOJ) and the Department of Homeland Security (DHS) partnered with the Global Justice Information Sharing Initiative (Global) to partner to build and deliver the NIEM. It provides an information exchange and framework consistent with the FEA DRM with the mission to solve the cross-boundary problems through the use of a standardized exchange. NIEM is a federated model which enables interoperability across multiple mission areas or "domains", with each domain managing its data models and content standards separately, while benefiting from central investment in tools, training, model management, and governance. Domains are collections of data representing the key concepts across a specific mission area and are usually identifiable via recognizable governance or authoritative bodies.	NIEM was developed through a partnership between DHS and DOJ established in 2005 as an outgrowth of the Global Justice XML Data Model (GJXDM). www.NIEM.gov

Method	Description	Authoritative Reference
Data.gov	The purpose of Data.gov is to increase public access to high value, machine-readable datasets generated by the Executive Branch of the Federal Government. Data.gov increases the ability of the public to easily find, download, and use datasets that are generated and held by the Federal Government. It provides descriptions of the Federal datasets (metadata), information about how to access the datasets, and tools that leverage government datasets. Data.gov includes searchable catalogs that provide access to "raw" datasets and various tools. In the "raw" data catalog, you may access data in XML, Text/CSV, KML/KMZ, Feeds, XLS, or ESRI Shapefile formats.	www.data.gov
Linked Data, or Linked Open Data (LOD)	The Web enables us to link related documents. Similarly, it enables us to link related data. The term Linked Data, or Linked Open Data (LOD) refers to a set of best practices for publishing and connecting structured data on the Web. Key technologies that support Linked Data are URIs (a generic means to identify entities or concepts in the world), HTTP (a simple yet universal mechanism for retrieving resources, or descriptions of resources), and RDF (a generic graph-based data model with which to structure and link data that describes things in the world). *(Contributor: Tom Heath, including excerpts from Bizer, Heath and Berners-Lee (2009)*	http://linkeddata.org/home
Information Sharing Environment Building Blocks	The Information Sharing Environment Building Blocks guidance helps organizations promote responsible information sharing.	http://ise.gov/building-blocks

Table C.9 Information Sharing Methods

In summary, the Data Sharing component of the DRM framework enables information sharing and exchange services. Specific activities and outcomes include, but are not limited to, the following:

- Communities of Interest
- Search
- Data Registries
- Data Catalogs
- Shared Spaces
- Access Services
- Brokering
- Mediation

C.3 DRM Examples of Use

C.3.1 Use Case Example One: Comparing Data Sources across Federal Agencies

Goal: Improve the quality and depth of information available for mission performance.

Method: Compare data sources containing similar data, though possibly used for a different purpose.

Challenges:

- Finding data sources that are worth comparing
- Identifying what information is common between data sources, and thus usable, for correlation

How the DRM Helps: The DRM taxonomy identifies data categories, regardless of usage context. Used in concert with the BRM taxonomy, it allows us to classify what data is managed in a given data source and in what mission or business context that data is used. Classifying a set of data sources by the DRM and BRM taxonomies produces a data set that can be searched to determine, as an example, which data sources contain a common data class but use it for different business contexts. For a large set of data sources, that search capability saves considerable time over manually examining each data source to see if it contains what is required.

Brief Example: Compare a data source containing taxpayer records against another data source containing passport holder records. The quality of both data sources can be improved by identifying and correcting minor discrepancies in the records such as errors in name spelling. The depth of information available to users of both data sources is also increased.

Background: Federal Agencies often find the need to compare or merge information in a data source they manage with a data source managed by a different Federal Agency. This data source comparison requirement was prevalent enough to inspire Federal Law (Public Law 100-503, the Computer Matching and Privacy Protection Act (CMPPA)). If the data source comparison involves information about individuals, the CMPPA requires that a formal Computer Matching Agreement, describing what information is shared, from what sources, and how it is protected, be signed by officials at the Agencies involved in the data source comparison.

Though the CMPPA prescribes documenting the details of certain data source comparisons conducted by Federal Agencies, it does not offer any help in finding data sources worth comparing. Federal Agencies have had to rely on their understanding of the mission of other Agencies and inquiries to the personnel at those other Agencies to find data sources worth comparing. As noted, such data source comparisons have occurred frequently in the past. Thus, the Reference Model taxonomies are not enabling some new capability in this example, but the DRM and BRM taxonomies can simplify and improve the process of finding compatible data sources.

C.3.2 Use Case Example Two: Standardized Information Exchange for Suspicious Activity Reporting

Goal: Create a functional standard, using a standardized set of data elements, to facilitate the dissemination of Suspicious Activity Reports (SARs) across the homeland security and law enforcement

communities throughout the Federal, state, local, and tribal domains. Additionally, facilitate a standardized information exchange across a COI.

Method: Model the exchange and build exchange schemas using data standards available in the NIEM.

Challenges:

- Harmonizing the different data elements, definitions, and formats for participating organizations.
- Wide range of platforms and data structure types used in source and target systems.

How the DRM Helps: 1. *DRM Data Context* is applied by determining the business context data requirements for an exchange. 2. DRM Data Description is used to create a data model for the exchange, with agreed-upon definitions. Uniform definition of the exchange schema uses existing data standards where possible. 3. DRM Information Sharing leverages the method NIEM for exchanging data. As additional partners adopt the use of the standard exchange across the community of interest, they need only write one time the transformation from the NIEM-conformant schema to their own data structure. Existing exchange partners can use the new participant's data without having to write any interface or transformation.

Brief Example: The Nationwide Suspicious Activity Report (SAR) Initiative (NSI) and Program Manager for the Information Sharing Environment (PM-ISE or ISE) are improving the ability of law enforcement and other agencies to gather information regarding behaviors and incidents associated with crime and establish a process whereby SAR information can be shared to help detect and prevent terrorism-related criminal activity. NIEM and the Universal Core (UCore) specification were chosen as existing data standards with wide adoption across the Law Enforcement COI.

The ISE followed the NIEM Information Exchange Package Document (IEPD) development process. The process is described at a high level here. The detailed process and guidance can be found at www.niem.gov.

Background: Federal, state, local, and tribal organizations typically use different data definitions and structures in the storage and exchange of like data across a community of interest. As data is exchanged between organizations within or across these domains, transformations or interfaces must be created for each new data source. Creating a standardized information exchange with agreed-upon data descriptions enables each participating organization to create the necessary interface to receive or provide data only once. It improves the quality of information exchange by ensuring that the source and target mapping is accurate, through the exchange model and standardized data definitions.

C.4 Measurement Success Factors

The key goal of the DRM is to improve discovery, access, sharing, and use of Federal data to meet mission needs and to position agencies to operate in a global information environment.

The success of the DRM to support shared services and other key initiatives can be defined and tracked through performance measures defined in an agency's PRM. A DRM performance plan may be used to

set priorities, collect metrics, and measure progress toward defined outcomes. Performance results can only be achieved if the DRM is linked with the other FEA reference models at all levels of detail and effectively managed as part of an Agency's integrated governance (e.g., capital planning, project and portfolio management).

Data sharing performance metrics are based on the extent to which data can be:

- **Discovered** - Content made consistently findable or present;
- **Identified** - Content that is semantically consistent and reasonable;
- **Standardized** - Content that has syntactic and structural integrity;
- **Reused** - Content that can be leveraged within and across domains to minimize redundancy;
- **Trusted** - Content that is 'reliable';
- **Good Quality** - Content that embodies and shares conformance, integrity, and timeliness among many business processes; and
- **Protected** - Content that can be shared, free of inappropriate disclosure or compromise.

Other suggested measures include, but are not limited to, the following:

- Increase in the number of inter-agency data sharing interfaces;
- Increase in the number of approved data standards used by two or more agencies;
- Increase in the number of publicly-available web services providing data in machine-readable form;
- Decrease in the amount of redundant data collected from citizens;
- Decrease in the number of redundant data sources (i.e., data sources duplicating data already provided by other agencies);
- Decrease in the average processing time for inter-agency data transactions;
- Increase in the number of unique visitors to cross-agency data exchanges/information sharing platforms (e.g., FirstGov.gov, Business.gov, Forms.gov, Export.gov, etc.);
- Increase agency score for the data architecture of the OMB EA Assessment Framework
- Increase in the percentage of data elements for which standards and definitions exist in an enterprise data dictionary (i.e., increase data standardization);
- Extent to which data or information is current (as measured in days since last update);
- Increase in the number of hardcopy records digitized, indexed, and catalogued; and
- Percentage of standard and ad-hoc reports produced accurately and on time for internal and external stakeholders.

C.5 Summary

The DRM's primary purpose is to promote the common identification, use, and appropriate sharing of data and information across the federal government. Adoption of the DRM taxonomies to consistently and collectively categorize data will enable both business and technical outcomes that:

- Provide clear data ownership and stewardship to facilitate open standards based on interoperability
- Categorize and integrate data along functional lines of the business to establish common data vocabulary and data standardization to build integration adaptors and systems
- Facilitate global identification of security and privacy issues and solutions to provide consistent means to categorize and classify data and information
- Support electronic exchange of information to facilitate electronic registries and repositories for data components

The DRM process can be tracked using defined measures, and such measure can be included in existing performance plans. OMB will continue to assess the FEA common architecture for appropriate updates and further releases of the DRM and like data tools and resources.

Appendix C.i: List of Acronyms

ADM	Architecture Development Method
ADS	Authoritative Data Sources
AF	Architecture Framework
APIs	Application Program Interfaces
ARM	Application Reference Model
BRM	Business Reference Manual
CIO	Chief Information Officer
CMPPA	Computer Matching and Privacy Protection Act
CMS	Centers for Medicare and Medicaid Services
COI	Community of Interest
CRUD	Create, Read, Update, and Delete
DDMS	Discovery Metadata Specification
DHS	Department of Homeland Security
DoD	Department of Defense
DOJ	Department of Justice
DRM	Data Reference Model
DTD	Document Type Definition
EA	Enterprise Architecture
ERPs	Enterprise Resource Management Systems
ETL	Extract, Transform, and Load
FEA	Federal Enterprise Architecture
FEAFv2	Federal Enterprise Architecture Framework
FIPS	Federal Information Processing Standards
GJXDM	Global Justice XML Data Model
HHS	Health and Human Services
IDEF	Integration Definition for Function Modeling
IRM	Infrastructure Reference Model
LDAP or X.500	Light Weight Directory Access Protocol

NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
OLAP	On-Line Analytical Processing
OLTP	On-Line Transaction Processing Systems
OMB	Office of Management and Budget
PRM	Performance Reference Model
SRM	Security Reference Model
TAFIM	Technical Architecture Framework for Information Management
TOGAF	The Open Government Group Architecture Framework
UML	Unified Modeling Language

Appendix D: Application Reference Model (ARM)

D.1 Introduction to the Application Reference Model (ARM)

The Application Reference Model (ARM) is the framework for categorizing Federal IT systems and application components to help identify opportunities for sharing, reuse, and consolidation or renegotiation of licenses. This information will often be used in conjunction with the other Reference Models to identify these opportunities.

For the purposes of the CRM, **Application** is defined as: Software components (including websites, databases, email, and other supporting software) resting on Infrastructure that, when aggregated and managed, may be used to create, use, share, and store data and information to enable support of a business function.

The ARM is a categorization of different types of software, components and interfaces. It includes software that supports or may be customized to support business. It does not include operating systems or software that is used to operate hardware (e.g. firmware) because these are contained in the IRM. It also does not contain mission-oriented software (obtained from mappings to the BRM). See Figure D.8.

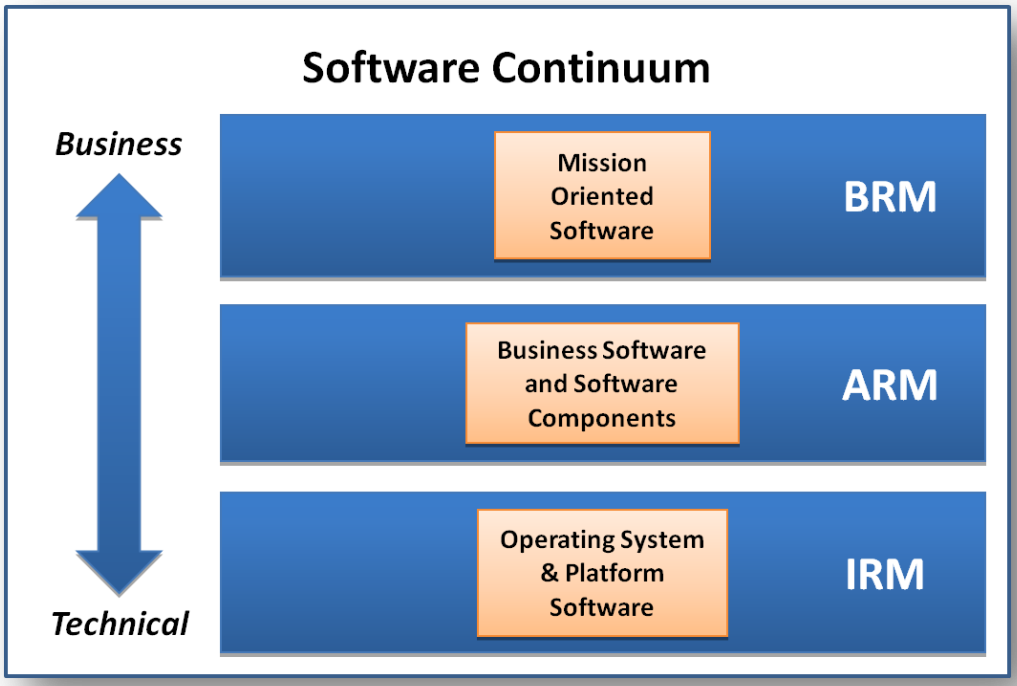


Figure D.8 - The Software Continuum and the Application Reference Model (ARM)

As shown in Figure , the ARM consists of three levels: Systems, Application Components, and Interfaces.

- **Systems** are discrete sets of information technology, data, and related resources, organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information in support of a specific business process. The ARM Systems category includes only the commodity IT (cross-domain or utility) variety and does not include mission-specific ones.
- **Application Components** are self-contained software, which can be aggregated or configured to support, or contribute to achieving, many different business objectives. For example, workflow management, document management, records management and many other types of components can support multiple IT Systems and business processes.
- **Interfaces** are protocols used to transfer information from system to system.

This ARM document presents the taxonomy for categorizing Applications, describes two Use Cases that indicate how the ARM can be used to support commonality analysis, and offers Methods and Best Practices that can be employed to exploit the information contained in the ARM and the mappings of agency assets to it.

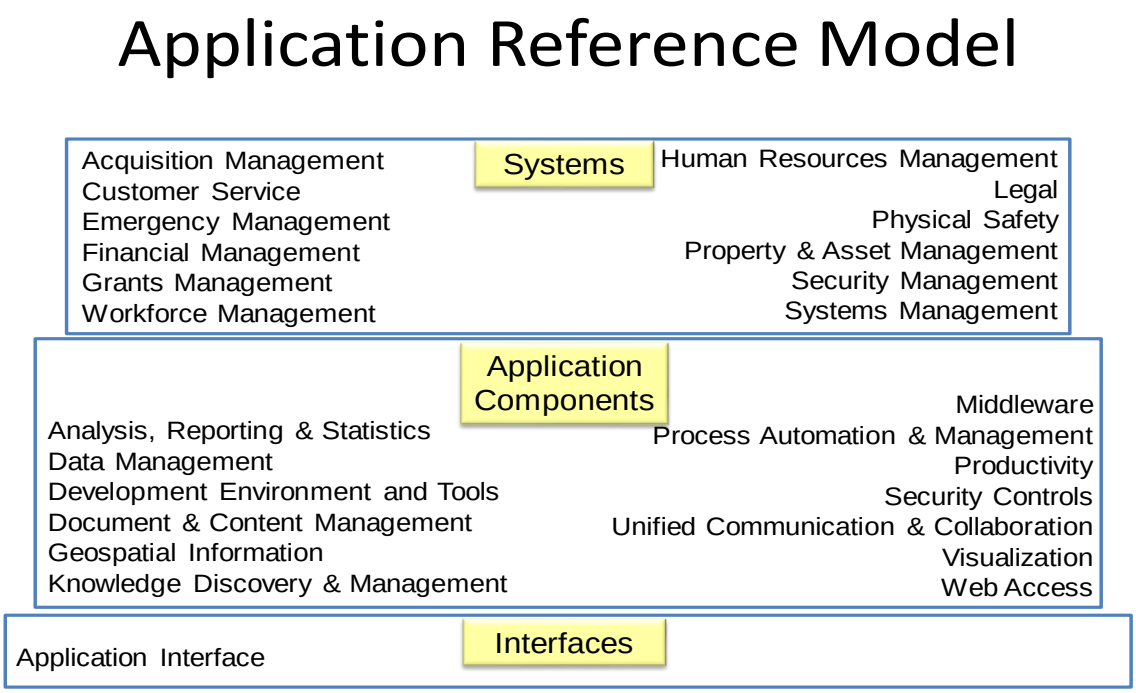


Figure D.9 - Application Reference Model (ARM) Hierarchy

D.1.1 Purpose

The purpose of the ARM is to provide the basis for categorizing applications and their components. As agencies map their current and planned Information Systems to the ARM categories, a base of information will emerge that will aid significantly in identifying opportunities for sharing and reuse, as well as illuminating redundancies and opportunities for consolidation.

The ARM implementation enables:

- Sharing and reuse of application components to reduce total lifecycle costs and exploit economies of scale (e.g., government-wide enterprise licenses).
- Identification and promotion of industry standard ways of accomplishing tasks to increase interoperability across the government and its partners.
- Identification of practical design-patterns as groups of application component building blocks (or combinations of them) that work well together (e.g., within a Product Line approach) to support efficient acquisition and deployment.
- Contribution to the delivery of consolidated and measurable (Enterprise Architecture Maturity Model Framework (EAMMF)) application services and service levels for efficient control and sustainment of IT assets and resources.
- Provision of the ability to consolidate licenses if there are multiple users of the same software.
- Provision of practical use cases and methods consistent with IT capabilities to enable business initiatives and greater access to information across enterprises.

D.1.1.1 ARM Guiding Principles

The ARM guiding principles were derived from the general principles of the *Common Approach to Federal EA* and were further refined by the purpose and desired outcomes of the Application Reference Model.

- ARM should be based on an adaptive structure that enables integration of new methods of providing IT capabilities (i.e., Separation of Concerns).
- ARM should be defined in terms of application services offered within a Service Oriented Architecture (SOA) and should facilitate shared services and interoperability.
- ARM should be defined as a hierarchy of IT application components (Loosely Coupled)
- ARM should be designed to promote ease of use, accessibility and reporting.
- The ARM should be standards-based (International and national, consensus driven standards organizations), with/for various levels of abstraction (to avoid vendor lock-in where possible).
- ARM should be supportive of the Business Reference Model (BRM) and the Data Reference Model (DRM), through identified relationships (touch points).

D.2 Associated Methods / Best Practices

This section presents three emerging approaches that can be used in conjunction with each other and exploit the information in the implemented ARM (i.e., the ARM structure plus the agency mapping of applications and investments to it), as well as the other Reference Models. These methods are: Capability Modeling and Analysis; Service Oriented Architecture; and Portfolio Management. The sharing and reuse objectives of the FEA Reference Models are facilitated by using these methods to

solve enterprise problems. In addition, the three methods enable modularization and improve the flexibility of applications and the IT acquisition process.

D.2.1 Capability Modeling and Analysis

Capability Modeling and Analysis is a Requirements Analysis technique that facilitates the translation of business/mission and technical requirements into discrete capabilities that lend themselves to sharing and reuse analysis (Shared-First). By casting requirements as capabilities at various levels of abstraction (meaning they may be decomposed into more detailed capabilities) and with capability dependencies modeled, the commonality across requirements is more obvious than with standard requirements analysis or business process analysis techniques. Within the context of the FEA Reference Models, capability requirements can be associated with elements and categories of the BRM for functional capabilities, the ARM for back-office and software support capabilities, and the IRM for infrastructure capabilities.

Capability Modeling and Analysis also has the advantage of modularizing the requirements so that capabilities can be combined in new ways to meet new business/mission and technical objectives. This method is a natural outgrowth of the Service Oriented Architecture (SOA) direction of OMB, the Federal CIO Council, and many Agencies. The method provides a direct analogy to the services that can be provided to meet the capability requirements – as discussed in the next section.

D.2.2 Service Oriented Architecture

Service Oriented Architecture (SOA) is an architectural style in which IT solutions are assembled from a collection of interacting services. This method not only provides more application flexibility because services can be more easily modified or replaced, but also reduces the cost of developing and maintaining applications (TCO) because the solution design is better understood and the impact of changes is isolated. The key to success with SOA is the development of an architecture of services – a layered diagram that depicts the services and their dependencies. This is critical in the consumption/reuse of services because it establishes the boundaries between services and indicates the relationships among them.

Services can be mapped to the appropriate FEA Reference Models to assist in identifying candidate services for use in particular applications. For example, if a solution requires a document management service, the ARM will identify other applications that have this capability or services that can satisfy this requirement. Services contained in registries or repositories should be mapped to the ARM and other reference models to facilitate the discovery process.

D.2.3 Portfolio Management

In the Federal Government, portfolio management is widely applied to IT investments and programs. This method has significant benefits when applied to all IT assets – in particular services and applications. To promote reuse or sharing of services, portfolio management techniques should be used to assess assets for viability into the future and to develop a service lifecycle plan for each asset. For example, to continue the use of the document management application component, each existing

(legacy or COTS) document management component should be mapped to the ARM so that the reuse potential can be evaluated by potential consumers. However, if the legacy document management service is to be deprecated in the near future, this information should be associated with the service. In this way, potential consumers of the service will be informed of the lifecycle plans for the service.

Portfolio Management techniques can also be used to support application functionality consolidation by analyzing the mappings to the ARM with the associated lifecycle information. In addition, this method may facilitate the analysis for shifting application components from legacy hosting to the Cloud Computing environment (Cloud-First) as well as the analysis for moving to open-source software.

Finally, Portfolio Management is an integral part of the entire lifecycle of IT assets, including budgeting and acquisition (OMB)[2], and is critical in the goal to improve acquisitions outcomes (GAO)[3].

D.3 Using the Application Reference Model

D.3.1 Use Case: IT Cost Reduction through IT / Application Portfolio Management

D.3.1.1 Synopsis

A Government Agency is looking for opportunities to reduce the cost of IT. The agency is comprised of multiple sub-agencies with both legacy and modern information systems. Each sub-agency has its own portfolio of information systems. The general consensus has been that duplicates of information systems exist, but are difficult to identify.

As required by federal enterprise architecture policies, all Applications in each agency and sub-agency map to the Application Reference Model in their reports to OMB.

D.3.1.2 Challenge

The IT and stakeholder culture is to continue with existing systems at the sub-agency level. The Federal Government is facing budget cuts, while at the same time facing higher expectations of delivery. The CIO believes it is a perfect opportunity to look for commonality to consolidate and cut down on duplication, and find commonalities which present opportunities for sharing, reuse, consolidation or renegotiation of licenses. The CIO is aware that changes to the IT environment will change information

[2] OMB budget guidance includes the following: "Integrate planning for information systems with plans for resource allocation and use, including budgeting, acquisition, and use of information technology." OMB, Transmittal Memorandum No. 4, "Memorandum for Heads of Executive Departments and Agencies", Circular No. A-130 Revised, Section 8.a.(e), available at http://www.whitehouse.gov/omb/circulars_a130_a130trans4, accessed 2012-10-19.

[3] GAO Report, "Coast Guard: Portfolio Management Approach Needed to Improve Major Acquisition Outcomes", GAO-12-918, 2012-09-20, available at http://www.gao.gov/products/GAO-12-918, accessed 2012-10-19.

systems with which business stakeholders are very comfortable, so he/she must deal with the change-management problem.

D.3.1.3 Solution

1. Review and map any missing systems to the ARM to report to OMB
2. Look for redundancy to find opportunities for sharing and reuse.
3. Look for opportunities to consolidate information systems where the business processes are similar and there is a way to ensure support of mission-critical processes.
4. Look for redundancies to find opportunities to consolidate licenses or negotiate for reduced costs.
5. Prioritize initiatives and identify the number of iterations that can be concurrently executed
6. Look for opportunities for sharing and reuse that span agencies if the mappings from across the Federal Government are available.

D.3.1.4 Possible Results

1. The potential to consolidate instances of the same application is found where duplication exists. This could not only save costs but might provide consistency, which would make it easier for the users.
2. Documentation shows that multiple sub-agencies use the same application for a particular function. Rather than consolidate the instances, it is determined that it would be best to consolidate licenses once they are up for renewal into a agency-wide license, and a reduced cost can be negotiated.
3. Across the parent agency multiple different systems for a commodity function (e.g. Call Center / Help Desk Management) are found. Because the sub-organizations are downstream recipients of the calls and need to work with the central Help Desk, they all work together to select one solution that can be hosted in the cloud. This not only provides a more complete solution but also reduces data center usage.
4. It is found that there are multiple Time and Attendance systems. The business needs are analyzed with the intent of consolidating to one system. It is found that there are employees with non-standard work hours to support the mission of one of the sub-organizations who are not accommodated in the system selected. Alternatives are analyzed to change the rules to support these employees, develop a system specifically for these employees, or develop a way to call a service from the central system that accommodates them.

D.3.2 Use Case: Using the ARM with the entire Consolidated Reference Model (CRM)

The following use case demonstrates how the ARM can be used in concert with the other reference models that make up the Consolidated Reference Model (CRM) to enable reuse of existing assets.

D.3.2.1 Synopsis

In this scenario, an agency (*Agency XYZ*) initiates a project to change from paper-based contract proposal management to electronic. *Agency XYZ* performs excellent background work, analyzing and documenting the efficiencies and cost savings to be achieved, and fully understanding and documenting

the business processes and the data required. Now *Agency XYZ* needs to determine the correct technologies. Components of the solution will include:

- Workflow to manage receipt and review of contract proposals;
- Document management to store contract proposals and provide records management;
- Integration with the existing financial system; and
- Validation of the proposers in the System for Award Management (SAM).

D.3.2.2 Challenge

In order to support the OMB Shared First approach, *Agency XYZ* needs an easy way to identify and analyze opportunities for re-using existing solutions, business services, technical services, platforms, or other components. *Agency XYZ* operates many existing solutions that might be potential candidates, so being able to quickly and easily navigate such information is critical. In addition, opportunities are likely to exist outside *Agency XYZ* in other agencies or in external providers, where their identification may be far more difficult.

D.3.2.3 Solution

Organizations create and maintain enterprise reference data for their existing environments, using the FEA CRM.

Each contiguous enterprise organization in the Federal Government (Department or Agency or Bureau, etc.) maps their program inventories, business services, data, systems, and infrastructure components to the Consolidated Reference Model (CRM), storing that information locally in an Enterprise Architecture Repository (EAR) for enterprise reporting purposes. The organization also provides the information to OMB, which makes it available to the entire Federal Government.

Architects map project elements to the FEA CRM.

The architects supporting *Agency XYZ's* efforts work with the solution team to:

- Map the project to the Performance Reference Model to document performance improvements desired;
- Map intended services to the Business Reference Model to document the area(s) that must be supported;
- Map intended data types to the Data Reference Model to document what types of Domains, Subjects, and Topics are contained within the proposed solution;
- Map proposed technical alternatives to the Application Reference Model to document any COTS business systems or components that might be assembled or reused;
- Map proposed technical alternatives to the Infrastructure Reference Module to document any technologies in the Platform, Network, and Facility categories that might be assembled or reused;
- Map program policies, controls, etc. to the Security Reference Model to place the ensure program compliance with the organizational security posture and identify any sensitive data or privacy concerns.

Architects search enterprise reference data, based on project mapping.
Using this mapping, the architects use the repository of organizational and governmental CRM mappings to find:

- Systems, services, and solutions that support the performance improvements desired;
- Systems, services, and solutions that support receipt of contract proposals;
- Systems, services, and solutions that use any COTS product to support the same needs;
- Common application components, such as a workflow tool or document management system, that can be shared or reused to support the needs;
- Alternative platforms available to support the needs such as hosting or cloud services;
- Security components that will be required.

D.3.2.4 Results

Architects find potential reuse candidates in reference data.
Agency XYZ's architects find that…

- *Agency A* uses a custom, internally-hosted solution that can accommodate *Agency XYZ*, and that can integrate with *Agency* XYZ's existing financial system.
- *Agency B* uses a COTS product that *Agency B* can host for *Agency XYZ*, and which integrates with *Agency XYZ's* existing financial system.
- *Agency C* uses a COTS product that is hosted in the cloud, that can be reused by *Agency XYZ*, and which integrates with *Agency XYZ's* existing financial system.
- Internally, *Agency XYZ* uses a workflow tool and document management system that can accommodate this need and will integrate with the existing financial system.

The project team analyzes the options.
The architects work with the solution team to acquire additional details regarding each option found in the repository search. The solution team uses these details to work with business owners to evaluate each option for:

- Degree of support for the desired performance characteristics and metrics;
- Degree of support for the detailed functions required;
- Degree of overlap with the required data types;
- Degree of overlap between application components and enterprise environment / standards;
- Degree of overlap between infrastructure components and enterprise environment / standards;
- Degree of compliance with organizational security posture, and applicability to degree of data sensitivity or privacy concerns for the project.

The solution team, including the business owners, uses industry standard methods to perform an objective, data-driven analysis, as is appropriate to the situation. They determine whether an existing solution is a sufficiently good fit for the environment and purpose, and if so, which one.

The project team selects an option.

Agency XYZ could decide to reuse any of the solutions or none, based on the results of the objective, data-driven analysis, for a wide variety of reasons with some examples including:

- *Agency A's* solution…
- Might not be selected because it is a custom solution; or
- Might be selected because the costs are perceived to be low.
- *Agency B's* solution:
- Might not be selected because it is hosted internally; or
- Might be selected because it uses a reliable product.
- *Agency C's* solution:
- Might not be selected because *Agency C* has difficulty with the vendor; or
- Might be selected because the volume of use might result in a favorable hosting/licensing fee.
- The *Agency XYZ*-internal solution:
- Might not be selected because it is not set up for additional volume; or
- Might be selected because the integration will be able to match the desired timeframe.
- A custom solution:
- Might not be selected because a sufficient number of COTS, cloud, and existing options make development redundant and unnecessary; or
- Might be selected because of some truly unique requirements in the given situation that are not addressed in other typical solutions.

Appendix E: Infrastructure Reference Model (IRM)

E.1 Introduction to the IRM

The Infrastructure Reference Model (IRM) is the framework and taxonomy-based reference model for categorizing IT infrastructure and the facilities that host and contain the IT infrastructure.

For the purposes of IRM, Infrastructure is defined as "The generic (underlying) platform consisting of HW, SW, and delivery platform upon which specific/customized capabilities (solutions, applications) can be deployed."

This IRM document presents the Taxonomy for classifying IT infrastructure, Methods for implementing the IRM taxonomy, and a set of Use Cases that showcase the practical usage of the IRM.

E.1.1 Purpose

The purpose of the IRM is to provide the foundation for classifying the technology infrastructure and the physical infrastructure that is needed to support it. The IRM supports definition of infrastructure technology items and best practice guidance to promote positive outcomes across technology implementations.

The IRM implementation enables:

- Sharing and reuse of infrastructure technologies to reduce total lifecycle costs (e.g., cloud computing) and exploit economies of scale (e.g., government-wide enterprise licenses).
- Identification and promotion of proven industry standards and associated platforms and products to increase interoperability across the government and its partners.
- Identification of practical design-patterns as groups of technology "packets" (or combinations of technologies) that work well together (best practices) to support efficient acquisition and deployment.
- Contribution to the delivery of consolidated and measurable (Enterprise Architecture Management Maturity Framework (EAMMF)) infrastructure services and service levels for efficient control and sustainment of IT assets/resources.
- Provision of practical Use Cases and Methods consistent with IT capabilities to enable business initiatives and greater access to information across enterprises.

E.1.1.1 Guiding Principles

The IRM guiding principles were derived from the general principles of the *Common Approach to Federal EA* and were further enhanced by the purpose and outcomes of the Infrastructure Reference Model. The IRM guiding principles are identified below:

- The IRM should be a readily adaptive taxonomy and approach to meet future needs (Future Ready) and accommodate new technologies.

- The IRM should be defined in terms of technology infrastructure services offered.
- The IRM should be defined as a hierarchy of IT infrastructure elements (Loosely Coupled).
- The IRM should be designed to promote ease of use, accessibility and reporting.
- The IRM should facilitate shared services and interoperability.
- The IRM should be standards-based (international and national, consensus driven standards organizations), with/for various levels of abstraction (to avoid vendor lock-in, where possible).
- The IRM should be supportive of the Application Reference Model (ARM) and Data Reference Model (DRM) through identified relationships (Touch Points).

E.1.1.2 IRM Outcomes

Four (4) primary outcomes, enabled by the *Common Approach to Federal EA*, and supported by the IRM are:

Service Delivery

The IRM provides a framework that will enable agencies to view their IT infrastructure assets in a consistent and coherent way. Success in supporting an agency's Mission and its Service Delivery capability in an era of resource-constrained operating environments requires a consistent understanding of IT assets, including all technology infrastructure assets. When adopted as part of the agency EA, the IRM will enable a coherent and consistent understanding of agency technology and physical infrastructure assets by classifying and contextualizing the technological resources.

Functional Integration

Interoperability is the foundational design principle in the *Common Approach to Federal EA*. The IRM provides the meta-context for integration between technology infrastructure implementations. Agencies will be able to understand technology infrastructure implementations across the Federal Government with relative ease and successfully partner with each other in new shared-infrastructure service models.

Authoritative Reference

Agency adoption and implementation of the IRM becomes the authoritative reference of technology infrastructure assets and the physical infrastructure that hosts them. Asset Management, Configuration Management, Security and Privacy controls of infrastructure assets will be enhanced by the IRM-based authoritative reference.

Resource Optimization

An IRM-based authoritative reference of agency infrastructure assets becomes a tool to understand the impact of introducing new technologies and paradigms that promote resource optimization, such as Cloud Computing, Virtualization, etc. In combination with the other FEA reference models, the IRM enables enterprise-wide impact analysis, which in turn enables informed IT Investment Portfolio planning and decision-making.

E.1.1.3 Stakeholder Usage

The IRM adaptive and loosely coupled approach supports multiple levels of executive management, capital planning and the analytical needs of architecture stakeholders.

Table E.1 captures some of the questions that an implementation of the IRM can answer. The Use Cases that detail how the IRM can be used are described in Section E.2.

Stakeholder	Performance Areas	Sample Questions/Concerns
Executive	Strategic Initiatives, Operational Effectiveness	Is the IT infrastructure ready to meet the next "big programs"?
Chief Technology Officer	Agility, Innovation	What is the direction for IT infrastructure?
Chief Enterprise Architect	Improved Architecture, Alignment and Governance	What are the technical standards? What are the approved IT products? Where are reuse and shared service opportunities?
Program Manager (Business Owner)	Business Case	Does this IT infrastructure meet the current SLAs and OLAs?
Project Manager (Implementation)	Cost, Schedule, Scope	Can the IT Infrastructure meet the performance needs? Is there a performance projection?
Business Architect	Business Impacts (Process Improvements)	Are there any IT infrastructure performance concerns that need to be addressed?
Business Analyst (Functional)	Business Process	What are the IT infrastructure requirements to enable business processes?
CPIC Analyst	Investment Alignment	Where are the potential savings from IT infrastructure optimization?
Solution Architect	Effective and Efficient Technical Solutions	What are the interoperability and IT infrastructure constraints and dilemmas?
Security Architect	Secure and Scalable Solutions	Which elements in the IT infrastructure are affected by identified security vulnerabilities?

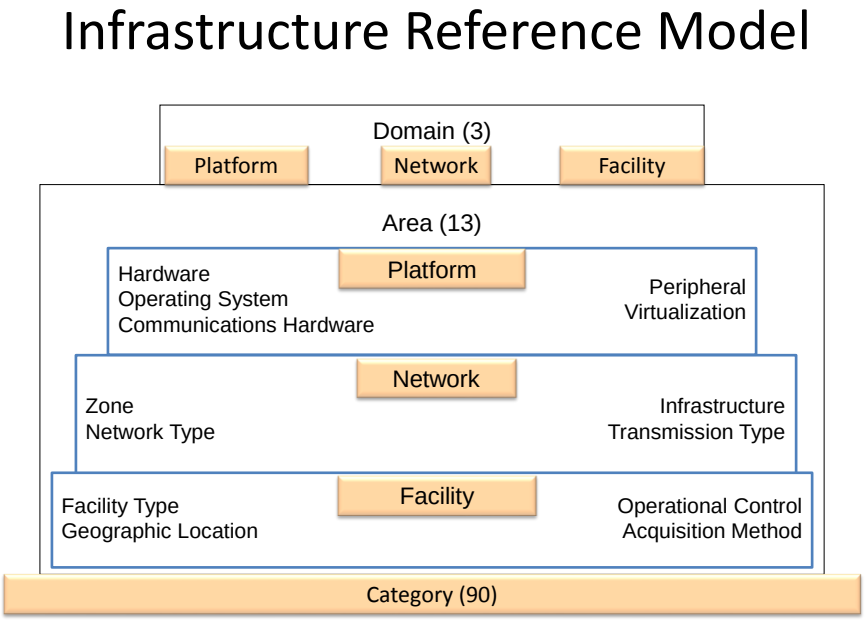
Table E.1 - Questions that an implementation of the IRM can answer

E.1.2 IRM Structure

The IRM taxonomy is intended to provide a categorization scheme for physical IT assets, the operating systems / firmware that run them and the locations/facilities that host the physical IT assets. The scope for the IRM encompasses all IT infrastructure-related assets (hardware, platforms and networks) and the facilities that host the infrastructure.

E.1.2.1 IRM Taxonomy

The IRM is divided into three levels as shown in



. Level 1 of the hierarchy, called “Domain”, consists of three entities:

- Platform
- Network
- Facility

Level 2 of the hierarchy, called “Area”, consists of 13 total Areas (for example, “Hardware”) linked to the three Domains in Level 1. Level 3 of the hierarchy, called “Category”, consists of 90 total Categories (for example, “Personal Computer – Laptop”) linked to the 13 Areas in Level 2.

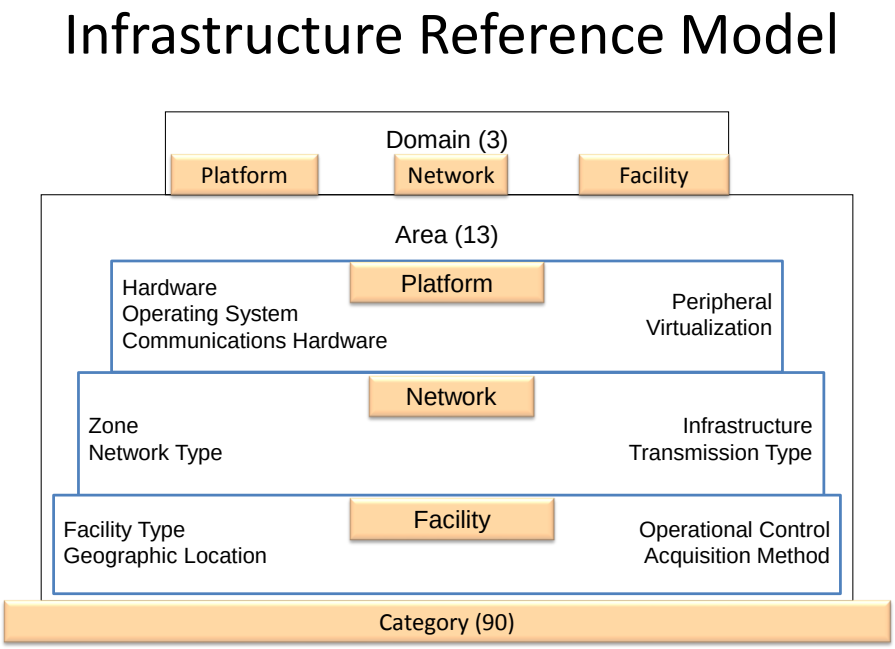


Figure E.10 - Infrastructure Reference Model (IRM) Hierarchy

E.1.2.2 IRM Relationships

The three Domains of the IRM, the Platform, Network and Facility, are linked and related to each other to enable analysis of IT assets across the three dimensions.

Figure E.11 shows the relationships between the three Domains.

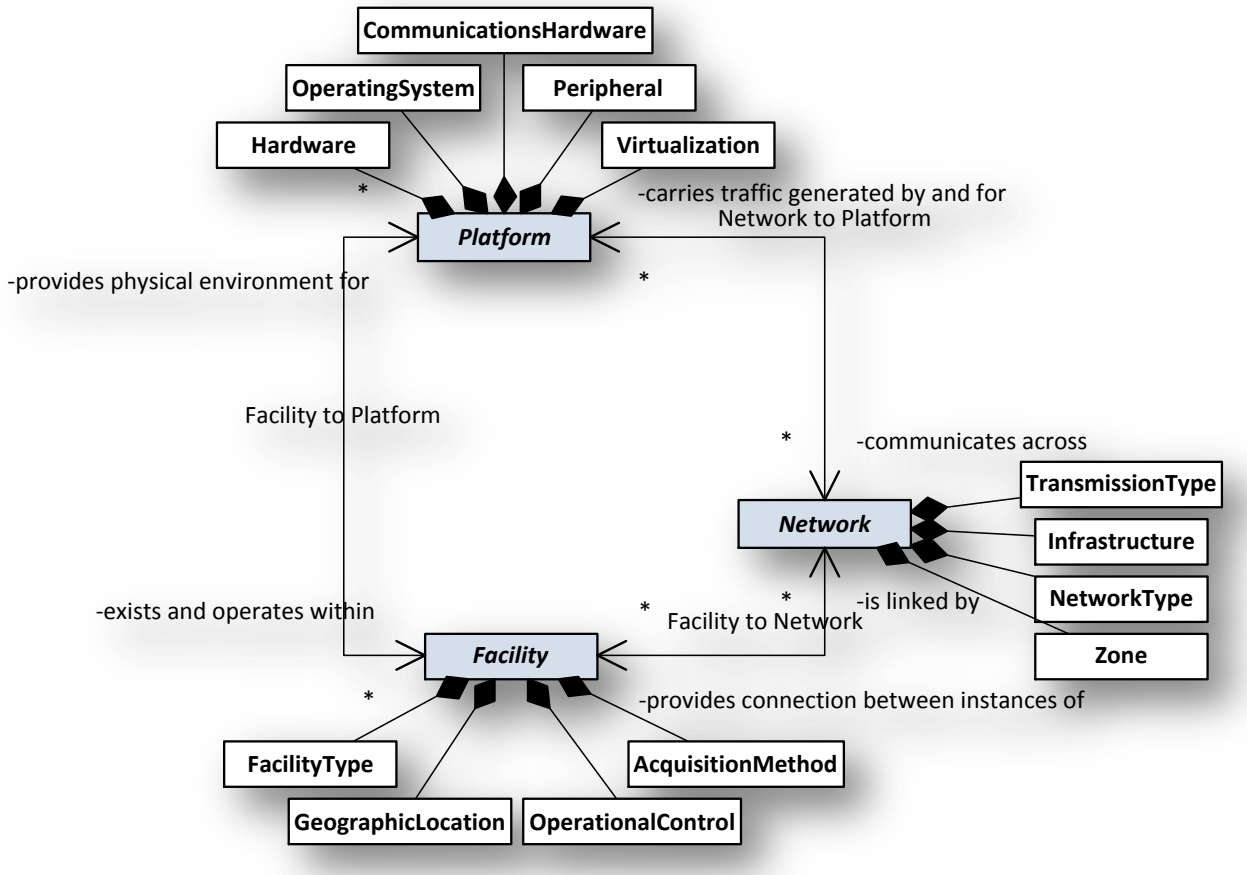


Figure E.11 - IRM Domain Relationship Model

In addition to providing a categorization scheme for IT infrastructure assets, the IRM implementations enable analysis of IT infrastructure assets at a Department/Agency level as well as at a Federal Government level.

Figure E.12 on the following page presents the IRM Usage Context for at these different levels.

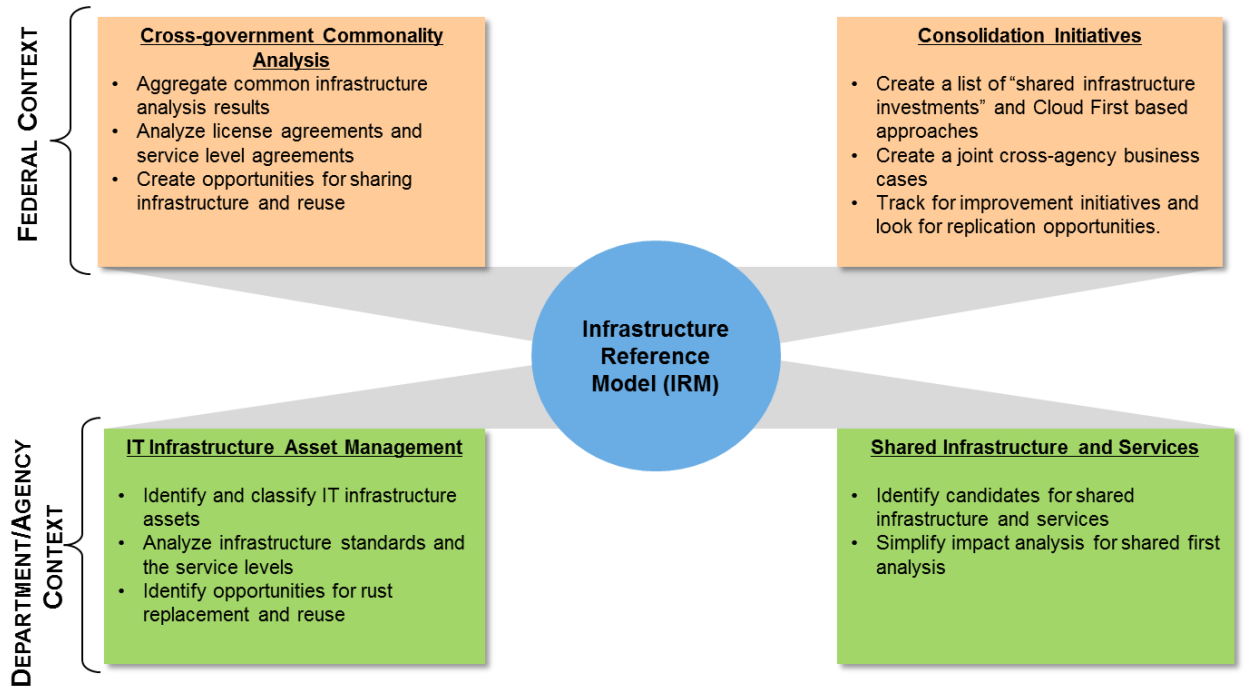


Figure E.12 - IRM Usage Context

The IRM is adopted and used in a Federal context to conduct Government-wide analysis of IT infrastructure assets and to identify consolidation initiatives. In the Department/Agency context, the IRM is used to drive good IT infrastructure asset management practices such as identifying end-of-life assets before they can affect the mission of an organization and to identify opportunities for sharing and consolidating infrastructure.

E.2 Using the IRM Taxonomy

The Use Cases described within this section present examples of how the IRM can be used to solve enterprise problems. Fundamental to an implementation of the IRM and using the IRM as a decision making tool, is an IT infrastructure asset inventory that is categorized using the IRM.

These Use Cases provide approaches for applying the taxonomy and accompanying reference model materials to: (1) complete an IT asset management inventory; and (2) evaluate whether to consolidate infrastructure to the cloud, using the IT infrastructure asset inventory.

The process diagram (Figure E.13) illustrates the linkage and collaboration between the Infrastructure Reference Model (IRM) and the Application Reference Model (ARM) to identify areas of reuse and consolidation. Using the IRM and ARM taxonomies as an input to the IT Asset Management (ITAM) process, especially for asset inventories, helps to discover highly useful information pertinent to the evaluation of where and how to share services. Understanding this process, the relationships between the IRM and ARM, and how to apply each is crucial to successful asset management and the sharing of services.

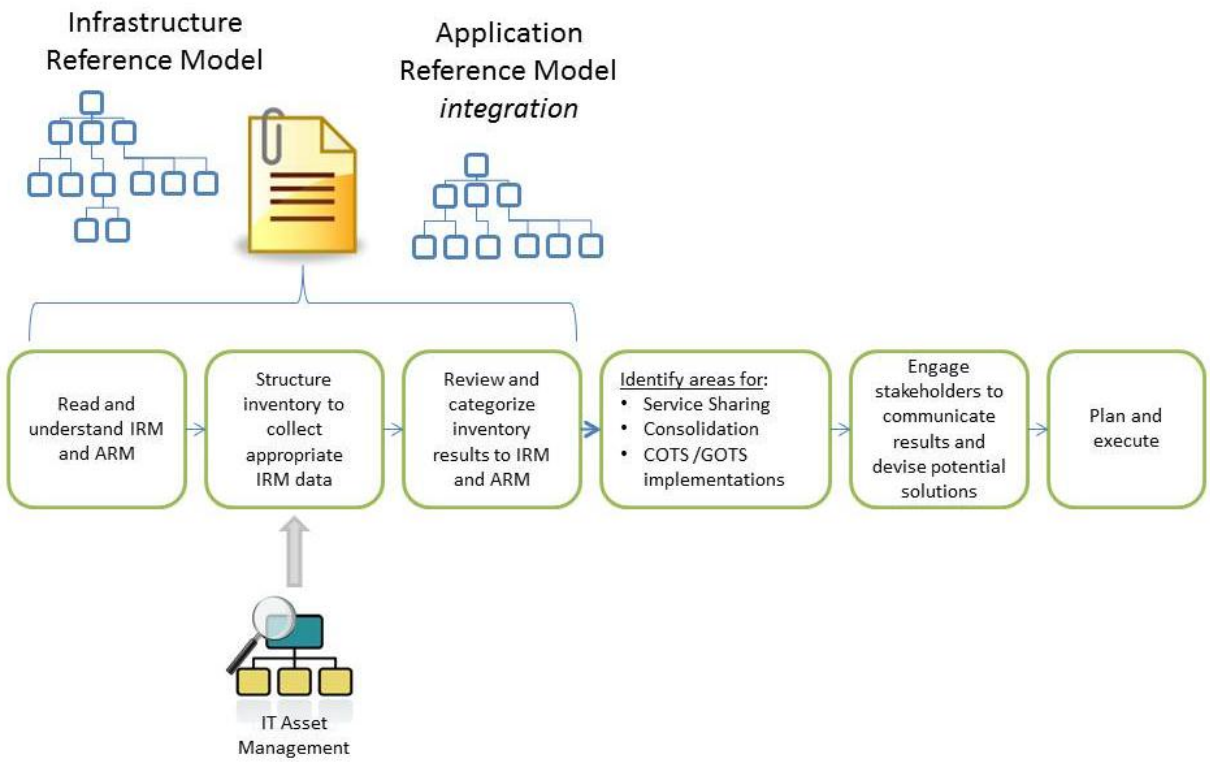


Figure E.13 - IRM and ARM Collaboration Process

E.2.1 Use Case: IT Asset Management (ITAM)

Many information technology (IT) organizations, especially within the federal, state and local sectors, are faced with the on-going challenges of providing and managing IT services that are responsive to the ever-changing demands and needs of diverse business customers. Couple this with the blinding pace of the technology evolution, seemingly infinite numbers of security vulnerabilities, and this age of constricting budgets, and these organizations are faced with a formidable challenge. To effectively and efficiently deliver these IT services, IT assets need to be inventoried, managed and refreshed over their entire asset lifecycle (acquisition to disposal). To this end, an IT Asset Management (ITAM) strategy is fundamental to managing the IT infrastructure that supports the delivery of IT services to the business and is concerned with all of the physical, financial and contractual aspects of IT assets throughout their life cycle.

E.2.1.1 Goal

Overall, ITAM goals should embody best practices to: (1) acquire appropriate IT assets with minimum costs and maximum benefits; (2) optimize the use of each IT asset during its service life; (3) dispose of IT assets when they no longer provide a benefit compared to the cost to maintain them; (4) support IT asset compliance; and (5) provide the information needed for internal and external requirements. Using this approach facilitates strong accountability of IT assets but also enables planning, configuration and

change management processes to be more agile to existing and emerging technology demands while improving the alignment of IT resources in support of business needs.

The architectural principles of the Enterprise Architecture (EA) process require definition and maintenance of the architectural layers between the current and desired states. Mapping an organization's IT assets to the Infrastructure Reference Model (IRM) and Application Reference Model (ARM) provides a robust technical definition, categorized by a common taxonomy, which is searchable by the services provided by each asset.

ITAM provides the foundation for the infrastructure architecture consisting of computing devices, peripherals, systems, applications and IT capital investments, interwoven with the other EA architectural layers, to render a "line of sight" that equates to measurable value chains (e.g., Return on Investment (ROI) and Total Cost of Ownership (TCO)) incorporating all associated costs. The outcome is improved IT resource decision-making delivering cost efficiencies, reducing duplication/redundancy and promoting information sharing across communities of interest. More importantly, the ITAM will facilitate improved alignment with mission and business functions, fiduciary responsibilities and compliance with legal and regulatory requirements. ITAM is the "glue" that ties it all together allowing organizations the opportunity to promote, enforce and verify IT industry policies, standards and best practices (e.g., security standards to avoid vulnerabilities and risk).

E.2.1.2 Challenges

- IT assets may not be effectively monitored throughout their asset life cycle - from planning through acquisition, management and retirement.
- The business may not know who owns or uses IT assets.
- The business may not know what cost IT assets contribute to overall program funding and service value-delivery (i.e., IT investment value).
- IT assets may not be efficiently managed within an organization's technology stack (i.e., approved standard/core configurations) with the least impact to end-user productivity.
- Collecting IT asset information with multiple IT management sensor/discovery tools (e.g., security vulnerability, network and system administration, and patch management) inhibits data analytics within a common view across domains.
- Redundant IT assets, performing similar business function(s) in multiple locations throughout an organization, contribute to increased acquisition, licensing, support and maintenance costs.
- Unlicensed or mismanaged software places organizations at risk, potentially facing large fines as a result of software audits (e.g., from the Business Software Alliance).

E.2.1.3 How the IRM Helps

Adopting the "data agnostic" taxonomy approach of the IRM and developing an IT asset inventory will help to harmonize the islands of IT asset information collected by proprietary IT management sensor/discovery tools. Additionally, adhering to universal standards and definitions that are consistent and acceptable across domains contributes to improved qualitative value of the information.

For example, the National Institute of Standards and Technology (NIST) provides standards for security automation tools and methods of describing and identifying IT assets and classes of applications, operating systems, and hardware devices present among an enterprise's computing assets. Additionally, considering an information exchange model (e.g., National Information Exchange Model (NIEM)) promotes the publishing, information sharing, and reporting capabilities desired by internal and external stakeholders.

Automated sensor/discovery tools strengthen the EA by providing timely and accurate data to the asset repository. The asset repository contains the details of each asset related to asset discovery, inventory, finance and contract management. The following are the benefits of using the IRM taxonomy to categorize the IT asset inventory.

- Improved organizational mission effectiveness, with better alignment of IT resources to business goal outcomes and objectives.
- Cost savings and avoidance; having quantifiable IT asset information enables IT to be more cost-effective, agile and responsive to ever-changing business needs.
- Improved IT resource utilization and project management of IT investments.
- Improved shared services capabilities.
- Improved identification and analysis of IT assets and their contribution (i.e., "line of sight" value chains) realized due to standardized data capture (asset repository).
- Improved and efficient IT infrastructure/roadmap planning by decreasing redundancies and reducing operational, training, maintenance and security (A&A) costs.
- Support for critical IT service management (ITSM) functions such as incident, problem, change (install, move, add, change (IMAC)), and service level management.
- Critical asset information to support ITIL v3 service asset and configuration management (SACM) full asset lifecycle support.

E.2.2 Use Case: Shared Services – Cloud First

Government agencies are facing slashed budgets, calls for optimization, pressure to use common sense approaches, and, most challenging of all, the directives to do more with less. To meet these challenges, it is of the utmost importance that shared services become a way of "thinking" in these agencies.

E.2.2.1 Goal

In this hypothetical use case, we discuss one agency that decided to use their IRM based infrastructure asset inventory and enterprise architecture data in delivering cost savings and efficiency to several components of their organization. The agency has a good cross section of characteristics including size, complexity of mission, geographic locations, and infrastructure maturity. Like many other peer agencies, they were experiencing massive IT costs due to traditional data center/server infrastructure, operations and maintenance costs.

E.2.2.2 Challenges

- Political hurdles when dealing with intra-agency and inter-agency requirements.

- Federal mandates to share services with ensuing budget reductions and funding challenges in determining how to allocate costs for shared services.
- Significant maintenance costs associated with legacy and antiquated systems.
- Development of highly customized services and platforms that do not lend themselves to information sharing across organizational boundaries.
- Lack of standards or lack of application of standards for sharing data and services.
- Acquisition issues.

E.2.2.3 How the IRM Helps

In the initial step, the agency used their IT Asset Management process coupled with the IRM taxonomy to arrive at their initial IRM view across their components.

Using the IT asset inventory and IRM categorization, the agency was able to quickly recognize patterns driving them to refine their categorization model to better identify common components and services repeated in various instances of the infrastructure. As depicted in Figure E.14, the outcome was a clear picture of duplicative infrastructure components and services in data centers that are owned and operated by the agency.

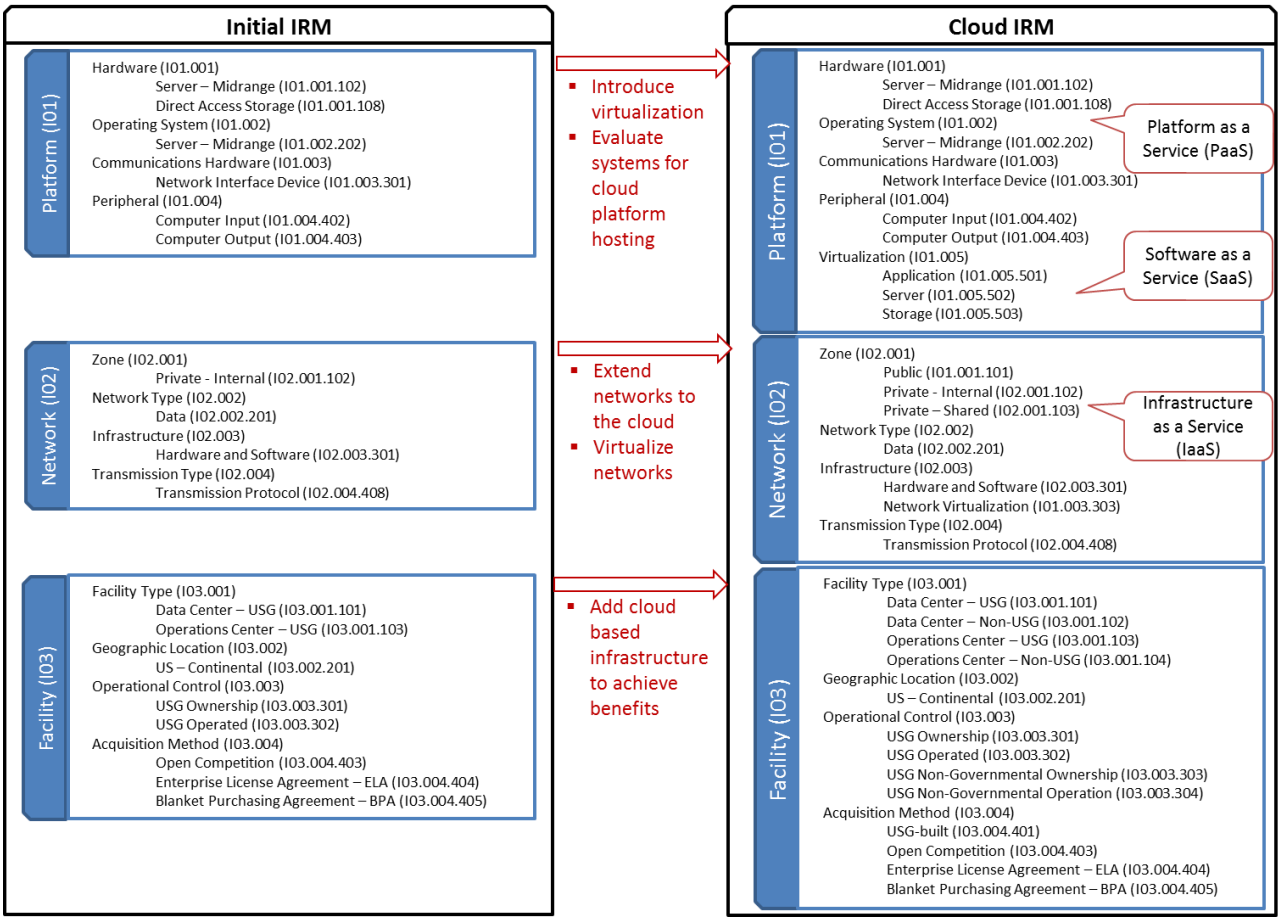


Figure E.14 - Applying IRM Cloud First Initiatives

The clear candidate components for shared services (i.e., Share First) were computer processing, memory, storage, load balancing, firewalls/security, and general networking.

Further analysis of the IT asset inventory, in conjunction with the ARM, revealed that systems with similar characteristics were deployed in enclaves that fit their situation. Addressing consolidation of the infrastructure that supports these systems improved reuse of IT infrastructure assets significantly. This is a simplistic and obvious example for identifying reuse and cost savings but it helps uncover the methods for applying the IRM to a real problem.

The agency then quickly identified multiple cloud based infrastructures as the logical solution for both existing and emerging service model needs, but also realized security requirements may drive other cloud-based solutions (e.g., public vs. private clouds or hybrid solutions).

The IRM and ARM Collaboration Process engaged

First, an inventory and categorization (I&C) process was conducted to map their commodity IT services (e.g., infrastructure and asset management, email and help desk) to the IRM taxonomy. The I&C process was repeated again for back-office IT services whose business functionality applied to multiple agencies (e.g., geospatial information systems, human resources management and financial management). They augmented this process by also relating the identified components to their application systems by cross-walking to the ARM taxonomy.

Next, the agency reviewed their results for candidate consolidation of intra-agency commodity IT services, while also reviewing established shared services suppliers of existing cross-agency Lines of Business (LoBs) and select E-Gov initiatives. Finally, not only did the agency identify component services for internal private cloud implementation, due to security and information sensitivity requirements, but they also identified public cloud solutions that sustained their existing re-hosting and O&M needs while enabling a migration towards their emerging technology and standards-based service model.

Additionally, by relating components to the ARM taxonomy, candidate applications were also considered in the “Share First & Future First” Strategy. The end outcome resulted in multiple efficiencies, cost savings/cost avoidance realized while providing improved service delivery through one or more shared services suppliers for use by multiple consumers.

The Solution

The primary benefit in this Use Case was not the technical solution delivered by the cloud computing alternatives, but rather the value delivered through the use of a reference model that could be cross-walked to the IRM & ARM taxonomies to more clearly identify shared services opportunities. The agency understood they were spending too much on infrastructure; they had too many instances of infrastructure services, and were facing several issues that compromised their ability to fund all infrastructure efforts fully. The architecture team introduced the technical team to the value of utilizing the IRM & ARM reference models. They collectively structured an IT asset inventory exercise to gather the required data about the architecture. The IT asset inventory results were then quantified,

categorized and cross-walked to the reference models' taxonomy of infrastructure services and back-office application systems.

The organization and categorization of this information contributed to:

- Improved management of the agency's IT Investment Portfolio (both infrastructure and back-office application systems).
- Improved sharing of systems and data, using universally accepted standards, which support the linkage between constituents, federal communities and suppliers.
- Reduced operational infrastructure and systems footprints (i.e., fewer systems and infrastructure resulting in fewer costs).
- Improved fee-for-service based models with better performance metrics improving engaged customer feedback as a result of predictable costs.
- Simplified the Assessment and Authorization (A&A) process through continuous monitoring (formerly C&A process).
- Improved performance of Capital Planning and Investment Control (CPIC) processes that eliminated redundant investments while enabling better justification for new IT investment business cases.

E.3 Associated Methods/Best Practices

The Methods section presents how to quickly apply the IRM to the Use Cases discussed in Section 2 to solve enterprise problems. Fundamental to an implementing and using the IRM as a decision-making tool is an IT infrastructure asset inventory that is categorized using the IRM.

E.3.1 Methods

The IRM provides a framework for categorization of IT assets which is helpful in developing IT infrastructure inventories and identifying opportunities for reuse, cost savings, and shared services. For an implementation of an IRM-based categorization of assets to be useful, additional data points including the manufacturer of the asset, cost, end-of-life/end-of-support dates, and a mapping to the Security Reference Model (SRM) should be captured.

Table E.2 offers an IT infrastructure asset inventory template to further assist with the method of implementing the IRM. This template identifies key types of data that should be captured for any/all IT infrastructure assets that are categorized by the IRM and are pertinent to identifying opportunities to share services, reduce redundancy, and promote consolidation. This template, based on the NIST SP 800-128 specification, is meant to be *extended* per the requirements of an agency's situation.

Data Element	Description	Example
Category	Categorization of the type of asset	IRM mapping to Platform, Network and Facility at appropriate level of detail
Manufacturer/Provider	Manufacturer or provider of the hardware/software	HP, IBM, Microsoft, Oracle
Model/Version	Model/version of the hardware or software	Version 1.0
Acquisition Date	Date the hardware/software was acquired	6/6/2012
Purchase Price	Cost of the software/hardware	$ value of acquisition
End-of-Life Date	Date at which the manufacturer determines the product will be obsolete for usage or designated by Federal Acquisition Regulations (FAR).	MM/DD/YYYY or computed based on Federal Supply Class (FSC) code and asset's useful life.
Location(s)	Location(s) of component	IRM Facility Mapping (US – Government Owned) and further elaboration if needed by physical address of the location
IP/Access Address	The IP address or other access mechanism to reach the asset	
Status	Status of this component	active, inactive, disposed
BRM Mapping	How does this component map/support the IT-related BRM functions	
ARM Mapping	How does this component map to the ARM	Enterprise service bus, Messaging
SRM Mapping	How does this component map to the SRM	
Owning Organization	Organization responsible for this item	Finance, HR, Accounting

Data Element	Description	Example
Benefitting Organizations	Organizations benefitting from this component	Finance, HR, Accounting
Services Provided	Services provided by this component	Interest rate calculation
Dependencies	Systems that are dependent upon this component	System XYZ
Contract Vehicle	The contract vehicle(s) that pay for this item	CIO-SP3
Management POC	Manager responsible for this component	Name and contact information of the POC
Technical POC	Technical person responsible for this component	Name and contact information of the POC
Security POC	Security person responsible for this component	Name and contact information of the POC
Remarks	Comments about this component	This is considered a GSS

Table E.2 - Sample IT Infrastructure Asset Inventory Template

E.3.2 Best Practices

Apart from the above basic IT infrastructure asset inventory template, the following are widely accepted best practices, guidance and standards in the public and private sector that can adopt the IRM categorization as part of their implementation.

- **Control Objectives for Information and related Technology (CobiT)** provides an end-to-end business view of the governance of enterprise IT that reflects the central role of information and technology in creating value for enterprises (i.e., CobiT helps to define what should be done). The principles, practices, analytical tools and models found in CobiT embody thought leadership and guidance from business, IT and governance experts around the world.
- **Information Technology Infrastructure Library (ITIL) v3** the most widely accepted approach to IT Service Management in the world. ITIL provides a cohesive set of best practices, drawn from the public and private sectors internationally (i.e., ITIL helps provide the how for service management aspects). ITIL is aligned with various international quality standards including international standard ISO/IEC 20000 (IT Service Management Code of Practice).
- **Object Management Group (OMG)** is an international, open membership, not-for-profit computer industry consortium with members worldwide, including government agencies, small and large IT users, vendors and research institutions. OMG is most known for their standards development work. Over time, OMG has evolved to meet the changing business needs of IT by

playing a strong role as a builder of practitioner-driven Communities of Practice focused on Green/Sustainability, Service Oriented Architecture, BPM, Cyber Security and Event Processing, while staying true to its standards development roots.

- **Federal IT Shared Services Strategy** provides Federal Agency Chief Information Officers and key stakeholders guidance on the implementation of shared IT services as a key part of their efforts to eliminate waste and duplication and reinvest in innovative mission systems. An *IT Shared Service* is "**An information technology function that is provided for consumption by multiple organizations within or between Federal Agencies**. " There are three **(3) general categories** of *IT shared services*: **commodity, support, and business**; these can be delivered through cloud-based or legacy infrastructures.
- NIST Cloud Computing Reference Architecture (CCRA) and Taxonomy (Tax), NIST SP 500-292 - communicates the components and offerings of cloud computing. Guiding principles for the creation of CCRA were that it had to be a vendor-neutral architecture that did not stifle innovation by defining a prescribed technical solution (i.e., "the How").
- Related NIST Standards and Specifications:
  - NIST Interagency or Internal Report (IR) 7693, *Specification for Asset Identification 1.1*, as amended.
  - NIST IR 7695, *Common Platform Enumeration*: Naming Specification Version 2.3, as amended.
  - NIST Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems.
  - NIST Special Publication (SP) 800-53 Rev. 4, Recommended Security Controls for Federal Information Systems, as amended.
  - NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems, as amended.
  - NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations, as amended.
  - NIST SP 800-70 Rev. 2, National Checklist Program for IT Products--Guidelines for Checklist Users and Developers, as amended.
  - NIST SP 800-117 Rev. 1, Guide to Adopting and Using the Security Content Automation Protocol (SCAP) Version 1.2, as amended.
  - NIST SP 800-126 Rev. 2, The Technical Specification for the Security Content Automation Protocol (SCAP) Version 1.2, as amended.

Appendix F: Security Reference Model (SRM)

F.1 Approach to Security Architecture

F.1.1 The Security Reference Model

Security is integral to all architectural domains and at all levels of an organization. As opposed to common practice, it is not a separate entity that can be programmed for, designed in, or applied, without integrating it as an aspect of the domain involved. Security is a global problem that permeates across all layers of an organization; impacts to security at any level have impacts on each successive layer both upward and downward. Enterprise Architecture Governance is the perfect place for security standards, policies, and norms to be developed and followed, since it is an enforcement point for Information Technology investments.

The Federal Security Reference Model (SRM) is a framework for developing a security architecture based on information security and privacy standards. The SRM creates a uniform security architecture through three areas: Purpose, Risk, and Controls. The three areas are then divided into six total subareas (see figure below). Each one of these subareas must be addressed at the enterprise, agency, and system level. The SRM uses the information from the purpose and risk of each level of the enterprise to find and classify the correct controls to secure the environment.

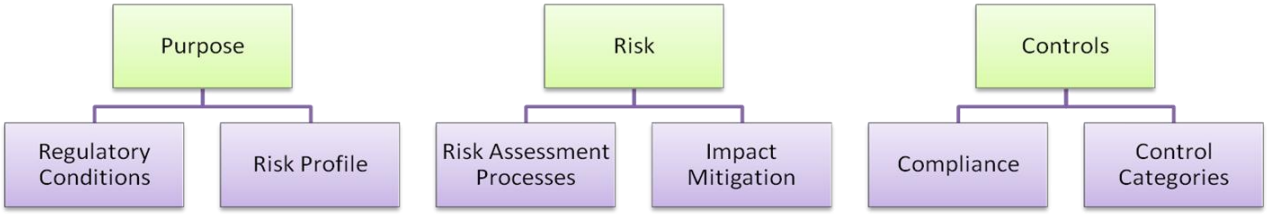


Figure F.15: High Level SRM Taxonomy

The Security Model also represents a microcosm of the overall EA Model. The Security Model is pervasive, weaving itself into all of the sub-architectures of the overarching EA across all the other reference models (Performance, Business, Data, Application and Infrastructure). This means that the view of the Security Model is a security-focused or security-aligned view of the EA Model. As a model, it provides a mechanism for communicating what the actual world looks like in terms of its framework. The model permits us to communicate between Enterprises, between other models, and up and down the different levels of the Enterprise those pieces of information that are relevant to making decisions affecting its domain.

Enterprise Architects must be aware of all technology, business, performance and security drivers in order to properly drive IT strategy in their agency. Similarly, solution architects must also be aware of these factors in order to architect Information Technology systems and make appropriate technology choices that map to their needs. Security is a primary non-functional requirement driver for IT solutions,

and a driver for enterprise IT strategy. A map of the security drivers present a clear picture of the landscape for the Enterprise Architect to identify where multiple segments, sub-agencies, and investments can share Security Control Implementations. The EA can recommend investments, standards and policies that will drive how controls will be applied across their organization.

Without modeling the appropriate drivers for the security requirements within the Enterprise, solution architects find themselves without singular sets of standards and guidance with respect to their solution. They must then collect and try to determine which regulatory guidance is appropriate and make individualized determinations that may conflict across the enterprise. Development of technical solutions are then only appropriate for the requirements gathered at that solution level, rather than with an appropriate distributed need in mind.

Goals of architecture include developing shared services that can appropriately provide for multiple segments and business areas, preventing duplicate investments in shareable technology, and the ability to ensure proper implementation and interpretation of higher level guidance. The SRM provides architects at all levels with a roadmap to understanding when those requirements can be consolidated toward those ends.

F.1.2 SRM Approach to Security

Security practices must balance both risk reduction and regulatory compliance. The SRM drives the Enterprise approach to security across multiple levels (International, National, Federal, State/Agency, Segment, down to System and Application). The SRM needs to incorporate both regulatory compliance from enterprise and cross-enterprise levels, and drive decisions for creating regulation for segment, system and application levels. To this end, the SRM identifies this general area as “Purpose”, which includes the drivers for making security choices.

It is important to note that risk reduction is the ultimate reason for the application of security controls. Regulatory compliance is not itself a reason, but a component of the process by which we choose risks and controls that apply to the situation at hand. Depending upon the level at which an Enterprise Architect is applying the SRM, the development of regulation itself may be the focus, rather than the development of technical controls. At the lowest levels (application architecture), the architect will be defining application requirements that directly drive technical control selection. At agency levels, however, the development of agency-wide controls may or may not be possible. In the example of user authentication, a Federal entity may decide to implement an agency-wide service to provide authentication technology, such as PIV-card authentication servers and associated hardware and software. However, it may be too difficult of a task

> Security for mobile technology may be governed by standards across the Federal enterprise, by policies within an agency, and by specific controls selected at the solution level.
>
> - Federal: All mobile devices must use encrypted channels.
> - Agency: All mobile devices must be cleared by CISO review prior to deployment.
> - Solution: Only approved managers may utilize iPads to access the system.

for that same agency to provide authorization services (such as role based access rules) at that same level. At higher levels still, such as Federal or State Governments, the enterprise may not be in a position to provide any security control services, due to disparity in requirements and the inability to form fit a single solution to multiple agencies.

In architecting based on the SRM, it is imperative that the Enterprise Architect is aware of these limitations and that expected outputs from the modeling is in line with the role and level of involvement desired. At the largest scales of EA, the outputs from these models will drive the architect to develop management controls in the form of standards, regulations or directives. At medium scales of EA involvement, the expectation is that these will be further refined as agency guidance. At smaller scales, where EA becomes solution architecture, these standards, policies and guidance are put into practice through appropriate selection of controls that will ultimately mitigate the identified risks. These decisions are driven by the architecture(s) above, and the directives and standards that have been pushed down upon the solution architect.

F.1.2.1 What is a Risk?

According to NIST SP 800-30[4], Risk is "A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems."

The Security Architect reduces risk through exercising control over the potential impact and/or likelihood of a vulnerability being exploited or through elimination of a threat source. Impact is the effect or impression of one thing on another. Types of impact include, but aren't limited to, the following examples:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss or agency liability
- Harm to agency programs or public interests
- Unauthorized release of sensitive information
- Personal safety
- Civil or criminal violations

Impacts can apply to many areas of the enterprise: Program acquisition (cost schedule performance), compliance and regulatory, financial, legal, operational (Mission/business), political, projects, reputational, safety, strategic planning, supply chain.

[4] NIST SP 800-30, Guide to Conducting Risk Assessments

Probability of occurrence and impact of an exploited vulnerability are themselves factors of the vulnerabilities, the threat source, and any controls implemented to prevent them from occurring. These concepts are discussed below.

According to NIST SP 800-30, a vulnerability is "a weakness that can be accidentally triggered or intentionally exploited". This is expanded in NIST SP 800-37 to "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source". As one of the three factors of risk, potential vulnerabilities are vulnerabilities that could be introduced to an Enterprise given the existing threats and existing security controls. As Enterprises build out technology capability, they are more reliant upon technological services and capabilities that are outside of their control. Choosing secure and trusted products alone is not enough to ensure there are no vulnerabilities to exploit; without controls in place to assure the hardware and software, the Enterprise will have a more difficult time keeping up with the vulnerabilities present from these technologies. Examples of these controls are requirements for certification for devices providing security functionality, certification of encryption algorithms to meet performance standards (e.g. FIPS 140-2 certification).

Threat sources are a second factor of risk. A threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.[5] A threat source is the intent and method targeted at the intentional exploitation of vulnerability or a situation and method that may accidentally trigger a vulnerability. The remaining controls in place reduce the exposure to threat sources (further definition below). For example, a basic firewall configuration will prevent traffic from entering a network unless it is destined for a known service.

The third and final factor of risk is existing controls. Existing controls are security controls that are already in place. From a security architect's stand point, these controls are usually implemented at the enterprise level (network firewalls can be used as an example). This factor is arguably the only risk factor that is under the complete control of the Enterprise Architect. Concentration on existing controls provides the greatest impact for dollar spent, and is the most executable for Information Technology investment. Each security control provides a reduction in risk associated with how it reduces either potential vulnerabilities or potential threat source exposure. Through the layering of existing controls and calculating the reduction provided by each control, an Enterprise can provide a probability reduction to vulnerability exposure. Managing risks are discussed in more detail in section F.3.1.

> Anti-virus software is deployed to identify and eliminate exploits against known vulnerabilities. However, it itself may introduce new vulnerabilities if the software provider has been compromised.

Methodologies for measuring risk are plentiful, with standard

[5] NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems

guidance for measuring and cataloguing risk for Federal agencies being given by NIST SP 800-30. It is not the purpose of the SRM to provide guidance on risk measurement, but rather to provide a framework for communicating the findings. Several existing lists of threat sources and vulnerabilities can be found in Appendix F.iv.

The phrase "security should be baked in, not bolted on" has been an adage used by security experts for years, but is not an easily defined concept. "Baked in security" requires a business process that links risk management with organizational requirements. The Enterprise Architect must consider what risks the organization faces. Risk must be defined, documented and managed. Risks in the Federal government are commonly categorized into Confidentiality, Integrity and Availability (aka C-I-A Triad). Confidentiality – Assurance that the data is protected and not released to persons that are not authorized to view. Integrity – Assurance the data is not altered from its original content during its storage or transmission. Availability – Assurance the data will be ready for use when required. The Architectural layers provide our context for consideration of risks to the government's information systems. Section 2 provides architects considerations when defining requirements.

F.2 Design Compliance for Architectural Layers

The SRM allows architects to classify or categorize security architecture at all levels of the Federal Architecture: International, National, Federal, Sector, Agency, Segment, System and Application. The highest levels transform federal laws, regulations, and publications into specific policies. The segment level transforms department specific policies into security controls and measurements. The system level transforms segment controls into system specific designs or requirements. Each level of the SRM is critical to the overall security posture and health of an organization and/or system.

F.2.1 International, National, Federal, Sector, Enterprise or Department -> Standards set Policy

At the enterprise level, the key tenet of the SRM is to use the standards in place across the federal or national IT security space to classify policy for a specific enterprise or agency. This is the broadest level of security architecture which creates a foundation for all segment and system security controls to exist. The standards and policies in place at this level can be used at the system level as well, removing duplicative security processes or requirements.

The SRM includes many policies and regulations from across the entire Federal IT space. While FISMA is a critical part of any security model, it is just a component of the Federal SRM and is intended to complement and enhance its end security goals. Therefore, the SRM includes policies such as FISMA, HIPAA, FISCAM, and other security and privacy laws and regulations enacted by the US Government to control information and IT infrastructure. The SRM can then identify overlap between standards and policies within an enterprise.

F.2.1.1 Architecture Guidance

The enterprise architect must define the risk profile and applicable policies for the enterprise based on standards. The Risk Profile informs the rest of the enterprise on what their minimums will be. Confidentiality, Integrity, Availability (C-I-A) considerations can become very prescriptive. The enterprise architect must balance policy with appropriate requirements that will not be so prescriptive that lower levels cannot achieve their business objectives.

Considerations at the Enterprise Level:

- What is the enterprise/department's primary business: to gather information, provide information, analyze information, manipulate information or store information?
- What aspect of Confidentiality, Integrity and Availability is most important to that information? There is no truly balanced C-I-A Triad.
- What would be the most embarrassing thing that could happen to this organization: loss of information, modified information, cannot retrieve information.
- What affect will a minimum policy statement have on subordinate agency business requirements? At the enterprise level all lower level architectures must be considered and layered into considerations.
- What process or technology can be made available to facilitate C-I-A across the Enterprise?
- If this process or technology is implemented at the enterprise level will it hinder lower level capabilities?
- Based on our primary business what other departments/agencies would it be logical to share services?
- What in the enterprise can create risk for other entities (inter or intra departmental connections)?

Appendix F.iii contains several mappings of the various reference documents regarding security in the Federal IT space as they relate to policy, legal and OMB requirements. It can be used for reference to gauge completeness of agency policies and guidance.

F.2.2 Agency or Segment -> Policy influences Controls

At the agency or segment level, the SRM uses the policies in place from the enterprise level to classify controls for a specific agency or segment. These controls are defined in the various sets of FISMA Special Publications from NIST, HIPAA regulations and requirements, FISCAM control sets from GAO, and additional security controls as required by statute or department need. The SRM allows the architect to choose controls based on the purpose of an agency or segment as well as by the risks faced by that particular agency. Again, these controls maintained or satisfied at the agency or segment level can then be inherited or used at lower system or application levels.

While the FISMA specific controls (such as those from NIST SP 800-53 and NIST SP 800-53a) are a crucial part of the SRM, they are not the only controls. Architects can look towards developing additional

controls based on specific needs of their environment. (Appendix F.ii includes these and controls from HIPAA, FISCAM, and the Privacy Act so many sources of Federal security and privacy requirements can be viewed at once.) This allows the SRM to encompass all of an agency's security architecture instead of FISMA system-level concerns. The SRM sets up a framework to inform systems where they may inherit policies and controls in place at the agency level, allowing the architect to concentrate on other critical security areas that are not covered.

F.2.2.1 Architecture Guidance

The risk profile of the agency must be defined within the minimums established by higher architectural levels, so it is important that the architect understand the business owner's goals and processes and articulate this understanding to the enterprise level. This will enable informed decisions at the enterprise level and proper implementation of appropriate controls at the agency level. (Note: independent agencies must perform both enterprise/department and agency/segment level functions.)

Considerations at the Agency Level:

- What is the agency's primary business: to gather information, provide information, analyze information, manipulate information or store information?
- What aspect of Confidentiality, Integrity and Availability is most important to that information?
- What types of information (e.g. health, personal, classified) are there, and is there regulatory guidance specific to that type of information?
- What controls are required based on the types of information?
- What controls affect (may limit) business processes?
- Does this create a risk to the business goal/objective?
- What is the genesis of this control (Law, Policy, Standards, Best Practice)?
- Is the risk to the goal/objective greater that the risk of not implementing the control? (Risk Assessment)

> The agency must provide segment level guidance to standardize control requirements. Specific systems could encrypt data at rest in a given server, but the encrypted data would still be at risk when moved from server to server, across a network, or even placed at the application level for an end-user. For example, the budget numbers considered sensitive by a procurement area may be viewed as public information by an e-Government portfolio manager. Even if system developers aren't aware of their duties to encrypt, the system owner is still liable for any breach.

F.2.3 System or Application -> Controls enforce Design

At the system or application level, the SRM uses the controls in place at the agency or segment level to facilitate the design and/or requirements of the specific system. While the FISMA controls in use across the federal government allow agencies and security personnel to audit or review a system, the SRM uses the controls selected by the agency or segment to actually

"bake" security into a system or application. It is critical for architects to be involved in the earliest stages of planning a system or application in order to minimize the impact sometimes involved if security is added or addressed at a later stage. The SRM will inform the design as to the controls used or prescribed at the agency or segment.

Another key issue for the architect is that all three levels must be satisfied in order to properly secure a system or application. For example, if there are no enterprise security policies for classifying data or agency controls for securing sensitive information, then it is not possible to check if a system is properly encrypting data. Notwithstanding, if a Federal law specifies certain action, the system level must comply whether or not an agency capability or policy has been developed to support that law. *Security flows down;* but if no agency or segment provides or defines the control, the system architect must put them in place whether or not it aligns with other system implementations. Consequently, it is critical for the architect to use the SRM to ensure that proper security controls are placed at each level.

This level is critical given today's IT environment. Shared services and cloud computing are hot topics both in federal and private sectors. Using the SRM will allow architects to map the overall security architecture of an entire infrastructure instead of just measure the security controls of a specific application. The SRM can use the different levels of architecture to map the standard and policies of an overall data center and then transform these into inheritable controls, reducing compliance time and efforts while improving security posture and audit reviews. The various layers of the architecture correspond well to cloud computing in cloud environment, cloud infrastructure, and specific system or service.

F.2.3.1 Architecture Guidance:

Business processes drive the risk management model. The system and application architects will follow the guidelines established from higher layers in the architecture. However, it is crucial that the architect understand the business goals and processes that are driving decisions. The architect should be asking what the major concerns are for this particular system or application in this particular organization. For example, an organization may be most concerned with availability of the data. This business driver would cause the organization to be more accepting of a risk to integrity and confidentiality and less accepting of a risk to availability. This would cause a different risk/security concern than an organization that was most concerned with integrity or confidentiality of the data.

Considerations at the System or Application Level:

- What function is this system or application providing: gathering information, providing information, analyzing information, manipulating information or storing information?
- What aspect of Confidentiality, Integrity and Availability is most important to that information?
- Is there law/regulation/policy guidance that sets a minimum standard on this type of system/application/information?
- Are there pre-defined controls required for this type of information?
- How do these controls affect (limit) business processes (business goals)?

- Does this create a risk to the business goal/objective?
- Are there risk concerns not covered by predefined controls?

F.3 Relationship to other Reference Models

The SRM is closely linked with the other five reference models of the Consolidated Reference Model Framework as security and privacy controls must be addressed within the business, data flows, information systems, applications, and infrastructure. Figure 2 depicts the reference models and demonstrates how the five models interrelate and support security planning.

Linking security and privacy to agency enterprise architecture, including agency performance objectives, business processes, data flows, applications and infrastructure technologies, ensures that each aspect of the business receives appropriate security and privacy considerations. Additionally, addressing security and privacy through enterprise architecture promotes interoperability and aids in the standardization and consolidation of security and privacy capabilities.

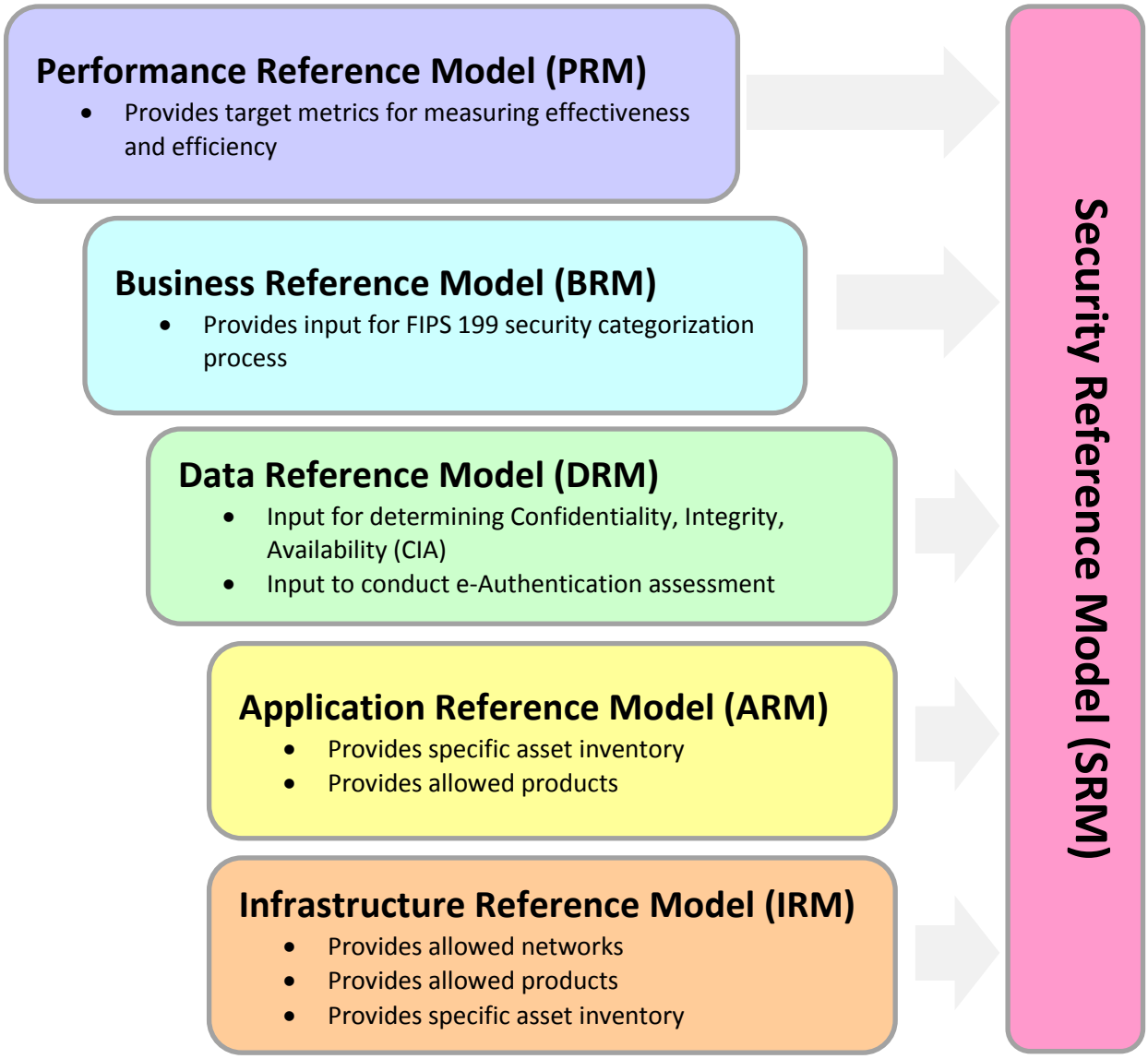


Figure F.2: Reference Model Tie-ins

At the high level, the SRM relationship and tie-in to the other reference models are:

- **Performance –** Provides a framework for monitoring and evaluating implementation of security controls and security investments
- **Business –** Provides assurance that the business focus is on priorities and mission-critical security issues
- **Data –** Addresses appropriate security requirements and security controls for data
- **Application –** Provides the standards for software providing functionality
- **Infrastructure –** Provides the standards for hardware providing functionality

In some instances, security features may be inherent for a particular asset, such as the security features built into a web server, or part of a particular requirement, such as PIV card enablement. In other instances, security may be the primary objective of a capability (e.g., an antivirus protection for an organizational network). Agency enterprise architectures must capture information about both types of capabilities/requirements and document security features across each model. This enables agencies to better understand and align security and privacy activities to the business and performance objectives of the organization. Additionally, effectively representing security in the enterprise architecture ensures that security is adequately included in the lifecycle processes of the agency.

The SRM enables early identification and understanding of essential security requirements to support well-informed risk-based decision-making. The SRM helps business owners with risk-based decision-making to achieve security objectives by understanding the purpose and impact of security controls on a business processes, or IT systems. Table F.1 includes some examples of security areas for consideration as they relate to the other reference models.

Identify purpose, functions, and capabilities and missions/business processes supported	
Business Reference Model (BRM)	Review applicable laws, directives, policies, regulations, or standards affecting the security
	Determine security categorization for information (FIPS 199)
	Determine parent or governing organization that manages, owns, and/or controls the data
	Identify users (including organizational affiliations, access rights, privileges, citizenship, if applicable)
Establish type and flow of information supported	
Data Reference Model (DRM)	Identify information flows and paths (including inputs and outputs)
	Determine types of information processed, stored, and transmitted
	Determine boundary of information flow
	Identify encryption techniques used for information processing, transmission, and storage
Determine software and hardware interfaces (internal and external)	
Application Reference Model (ARM)	Determine which systems and applications are needed to generate, share, and store the data and information
	Identify application software used
Infrastructure Reference Model (IRM)	Review types of voice, data, and video networks are required to host the IT systems/applications
	Determine location and environment in which the system will operate
	Identify hardware and firmware devices utilized
	Determine cross domain devices/requirements
	Define network connection rules for communicating with external information
	Determine cryptographic key management information (public key infrastructures, certificate authorities, etc.)
	Identify interconnected data sources

Table F.1: Security considerations as related to the other Reference Models

Security integration across layers is essential to ensure the protection of information and IT assets. Security must start at the business layer and work its way down to the application and infrastructure layers.

F.4 Optimal Risk Based Design

Government Agencies all strive for the best solutions to identify, assess, and manage risks to their systems, applications, and infrastructures. The National Institute of Standards and Technology (NIST) is at the forefront of risk guidance for the public sector. These methodologies will be outlined below.

NIST uses a three-tiered approach to risk management that addresses risk-related concerns at: (i) the *organization* level; (ii) the *mission and business process* level; and (iii) the *information system* level, as illustrated in the Figure below.

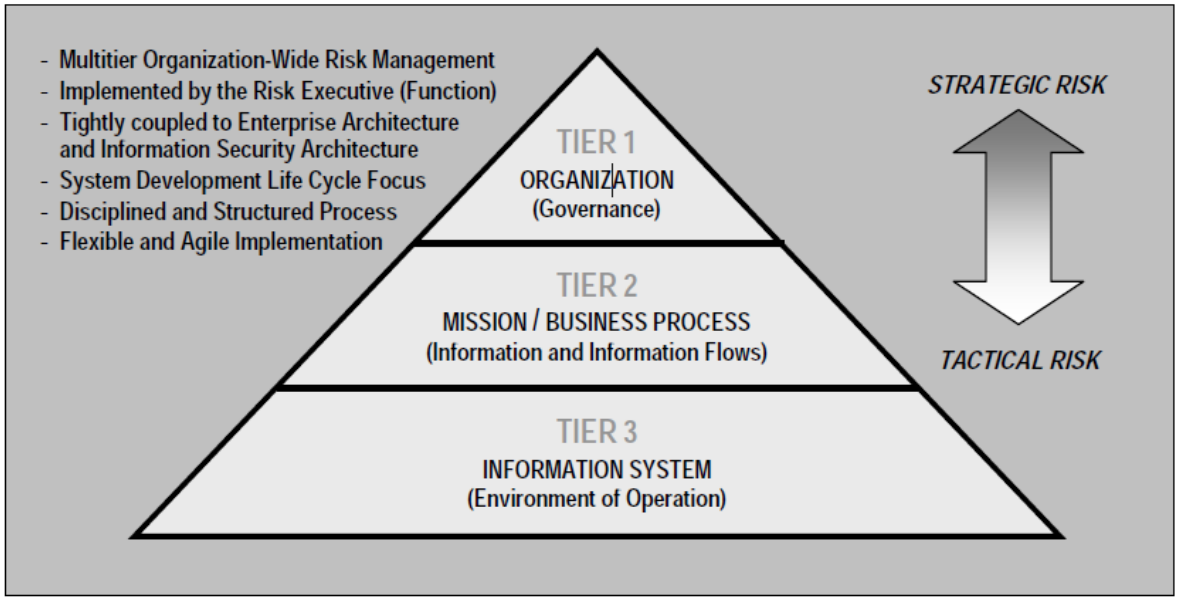


Figure F.3: Tiered Risk Management Approach (NIST Special Publication 800-37 Rev 1)

In this illustration, risk is identified at all three tiers, starting at the organization level and continuing to the information system level. Emphasis is still being placed mostly on the Information System Tier. Moving forward, more attention must be paid to risk management at the upper levels of the organization, as the business risk needs will drive the technology solutions and the controls applied to these solutions.

Tier 1: Organization. Tier 1 of the risk management approach is concerned with an organization's development of a comprehensive governance structure and organization-wide risk management strategy. The organization-wide risk management strategy includes components such as methods and procedures, risk mitigation measures, risk tolerance, risk monitoring, and oversight responsibilities of agency officials.

Tier 2: Mission /Business Process. Tier 2 of the risk management approach is concerned with examining core mission and business processes, identifying how these processes relate to the overall strategy of the organization or program, and providing an overarching Information Security framework. In this tier, Enterprise Architecture professionals work closely with the business units and Information Security professionals to ensure that risk is identified early at the upper layers of the organization before progressing to the system and application levels.

Tier 3: Information System. Tier 3 of the NIST tiered risk management approach addresses risk from an information system perspective and is guided by the risk decisions at Tiers 1 and 2. Risk decisions at Tiers 1 and 2 impact the ultimate selection and deployment of needed safeguards and countermeasures

(i.e., security controls) at the information system level. At the Tier 3 level, controls are assigned to information systems identified to assist the organization to perform its mission. This framework can be applied to all major systems, minor systems, and global support systems.

The Risk Management Framework (RMF), as described in NIST SP 800-30 rev 1 and illustrated in the Figure below, provides a process that integrates information security and risk management activities into the system development life cycle.

The RMF steps include system categorization, selection of security baseline controls, control implementation, control assessment, system authorization, and system monitoring.

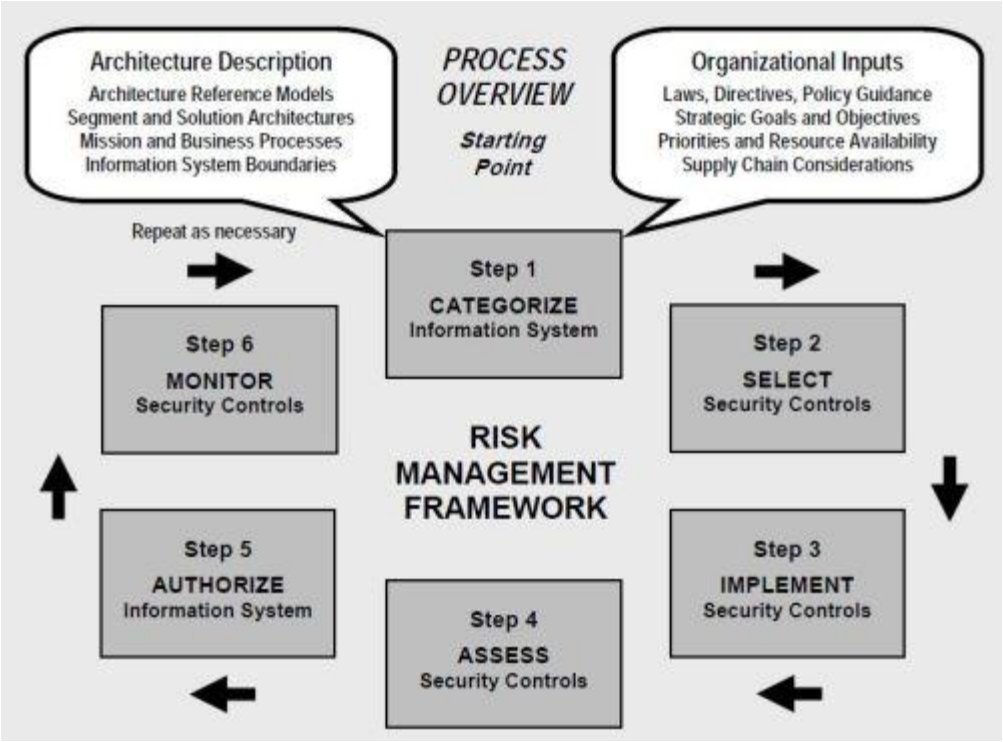


Figure F.16: Guide for Applying the Risk Management Framework to Federal Information Systems (NIST Special Publication 800-37 Rev 1)

Security controls, policy, and processes must be built into the systems development life cycle (SDLC) for the information security process to be implemented successfully and cost-effectively. Many programs fail to include security in the initiation and acquisition stages, creating cost and schedule impacts due to security requirements being added at the operations and maintenance stage of the SDLC.

Risk must be assessed, mitigated, and managed at every level of the Systems Development Life Cycle. Most agencies utilize the Federal Information Security Management Act (FISMA) reporting metrics for CIOs. The goal is to base Agency FISMA compliance on real-time understanding and risk management. The questions are not limited to checklist compliance. “The intent is to gather information on best

practices and agency implementation status beyond minimal requirements."[6] Each organization should have a mechanism by which risk and security concerns inform the design and implementation of systems and applications. The Table below depicts the required security activities which agencies should focus on by SDLC phase. The continuous assessment of risk and the effectiveness of controls is required throughout the entire lifecycle of the IT system.

SDLC Phase	**Key security activities for this phase include:**
Initiation	Initial delineation of business requirements in terms of confidentiality, integrity, and availability: • Determine information categorization and identification of known special handling requirements to transmit, store, or create information such as personally identifiable information • Determine any privacy requirements • Early planning and awareness will result in cost and timesaving through proper risk management planning. Security discussions should be performed as part of (not separately from) the development project to ensure solid understandings among project personnel of business decisions and their risk implications to the overall development project
Development / Acquisition	Conduct the risk assessment and use the results to supplement the baseline security controls: • Analyze security requirements • Perform functional and security testing • Prepare initial documents for system authorization and accreditation • Design security architecture
Implementation / Assessment	Integrate the information system into its environment: • Plan and conduct system certification activities in synchronization with testing of security controls • Complete system accreditation activities
Operations and Maintenance	Manage the configuration of the system: • Institute processes and procedures for assured operations and continuous monitoring of the information system's security controls • Perform reauthorization as required
Disposal	Build and Execute a Disposal/Transition Plan: • Archive critical information • Sanitize media • Dispose of hardware and software

Table F.2: Key Security Activities by SDLC Phase (NIST Special Publication 800-64 Rev 2)

[6] Chief Information Officer Federal Information Security Management Act Reporting Metrics paper

F.5 Security Controls and Metrics

Implementing controls is not the primary goal of security. Rather, it is an indispensable part of achieving the goal of reducing risk through layered security measures. Metrics should measure both the completeness and effectiveness of the selected controls (compliance) as well as how well they achieve the risk reduction (performance). Metrics can also capture the cost associated with various controls and security processes so decisions can be made about trade-offs regarding risk reduction and value.

There are some standard controls for the Federal Executive Branch flowing from various sources, including NIST SP 800-53, DoDI 8510, and public laws such as HIPAA and the Privacy Act. Appendix F.ii also lists commonly implemented controls.

F.5.1 Purpose of Controls

F.5.1.1 Managing Risk as Part of the Control Strategy

Risk management relies on the ability to identify risk and select an appropriate control set to reduce the information security risk of the organization to acceptable levels (as discussed above). The primary ways to deal with risk include:

- Mitigate Risk (such as by hardening software and closing back doors)
- Avoid Risk (such as by not implementing particular solutions with known vulnerabilities)
- Transfer Risk (such as by contractually obligating vendors to assume risk)
- Accept Risk (such as by deciding not to build reinforced bunkers to protect against meteor showers)

Of these options, NIST security controls are primarily directed towards risk mitigation. However, it is critical in the process of designing systems and solutions that security architects consider whether particular solutions can transfer or avoid risk altogether.

- Avoid: Architects can identify where certain configurations are unacceptable and use the Agency IRM and ARM to disallow particular standards, technologies and vendors from use.
- Transfer: Agency policy should mandate certain risk related assurances when leasing contracts to third parties. If no Agency policies exist, the architect should work with contracting officials to achieve a balance where the government is not unduly carrying risk. This is particularly important when implementing infrastructure and platform as a service, and for all cloud services.
- Acceptance: Most importantly, risk acceptance should be a driver in understanding which controls are best suited to the design of the system/solution. If a risk is unlikely or of low impact, cost/benefit can be applied to whether controls to mitigate the risk are needed at all.

Security controls implemented to mitigate risk refer to the procedural operational, technical and management mechanisms designed to:

- Eliminate or mitigate vulnerabilities that could be exploited
- Reduce the likelihood and impact of a security incident
- Reduce, eliminate or mitigate threat vectors
- Reduce the impact once a security breach occurs
- Provide a way to evaluate the effectiveness of implemented controls.

Controls can achieve these objectives in various ways. Controls implemented at the organization level help to guide processes and minimum standards for risk reduction. Controls at a system level may be more technical in nature. However, all controls work in concert to provide layered security such that if one control fails, it does not compromise the organization's ability to function. There is rarely a one-to-one match of a control to a specific performance outcome related to risk reduction.

The graphic below shows how controls are used to mitigate risk and protect assets within an overarching risk ecosystem. It shows how threat sources and vulnerabilities inter-relate, and how controls are used to influence one or more of the factors involved. Risk mitigation (reducing likelihood of risk) and incident management (once likelihood is 100%--after the incident has occurred) are both key areas of focus of controls.

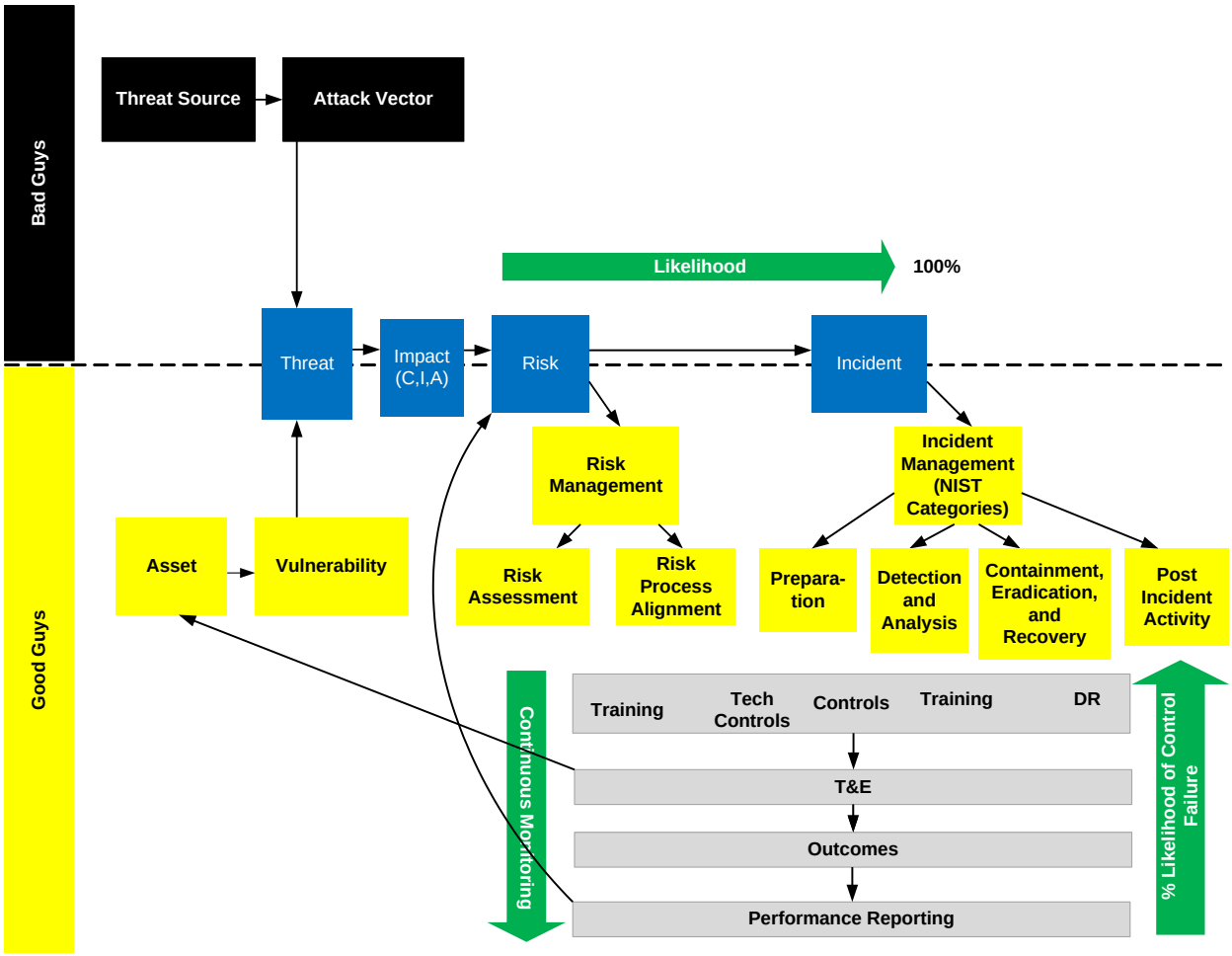


Figure F.5: Risk Ecosystem

F.5.1.2 Security Value Chain

To restate, controls are not the purpose of security; the measure of success is not implemented controls, but the outcome of reduced risk. In order to achieve the reduced risk profile, controls must be integrated across the organization vertically (lowest granularity to top level policies), as well as horizontally across system and solution deployments.

As controls are implemented across an organization and across the life of information systems, across all stages of the SDLC, controls are progressively layered, building upon previous control implementations. For example, encryption policy requirements are a required building block for encryption standards deployed on an organization's laptop assets. Without the policy in place, an organization will struggle to ensure consistency of the encryption standards deployed.

Figure F.6 depicts one possible example of the layering and relationship of controls across the organization. This example provides an approach for an organization to establish the correct building blocks (from left to right) so that the organization can focus its attention on measuring the business impact, or value proposition (from right to left). Assuming the desired outcome is being produced, there would be less emphasis on measuring foundational controls such as policies in a reoccurring or continuous manner. This approach is one of many possible strategies for monitoring the established risk tolerance within an organization.

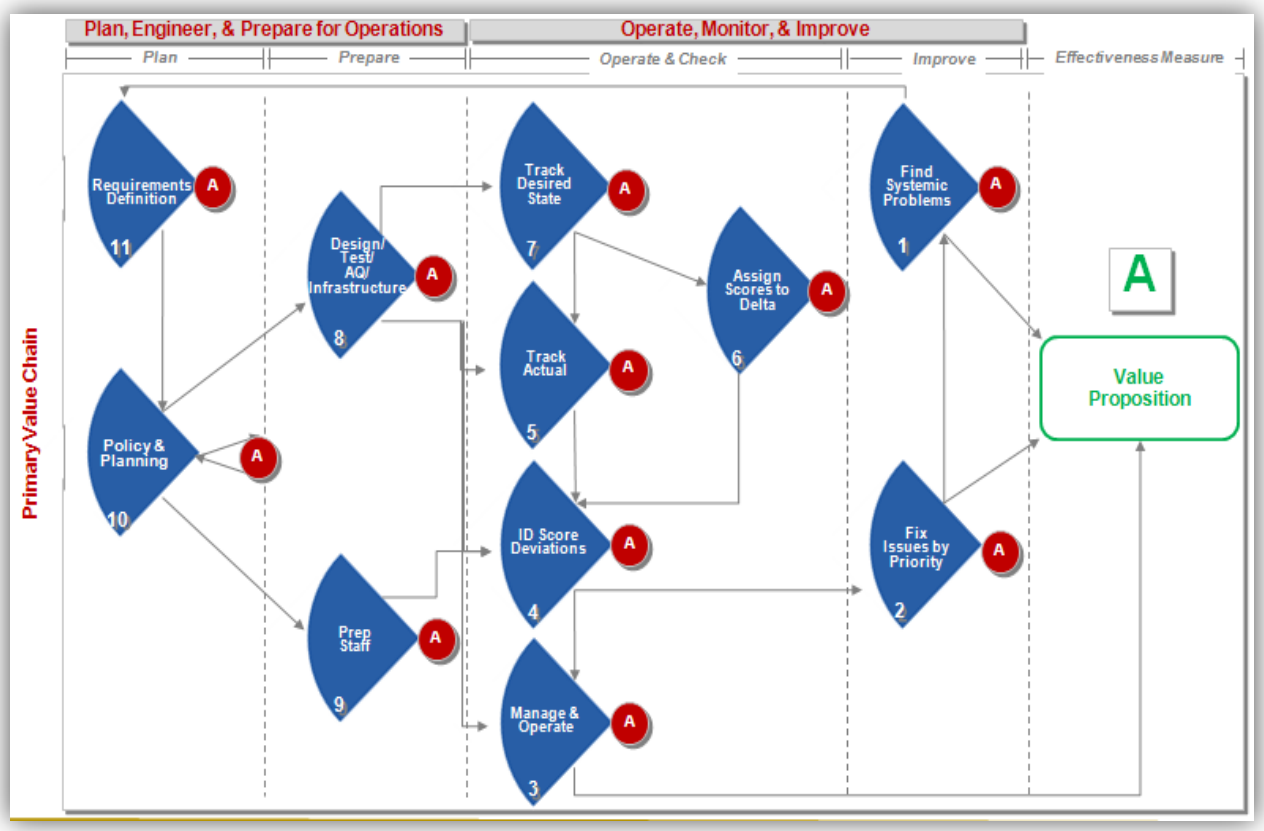


Figure F.6: State Department Primary Value Chain Framework

F.5.1.3 Control Selection

As mentioned above, the control set implemented within an organization should be tailored for that specific organization's needs. This tailoring process is defined in several security management processes, including FIPS 199, SP 800-53 for the NIST RMF, and mission assurance category (MAC) and confidentiality level (CL) for DIACAP (see Appendix F.ii). Design standards include concepts such as:

- Control types should match the technology and organization structure (e.g., no wireless controls if the system doesn't employ wireless technology)
- The scope of controls should match the importance of the mission (fewer controls for a low importance system)
- Control selection should take into account regulatory needs (HIPAA for medical systems)
- Controls should be aligned to performance requirements (if rapid response time if needed, controls that slow response time may not be appropriate)

Each control should be evaluated for usefulness to the overall goal of reducing risk to acceptable margins. A one-size-fits-all approach ultimately focuses too much on the controls and process of implementing controls rather than the desired outcomes. It is ultimately the Authorizing Official (AO), Designated Accrediting Authority (DAA), or similarly appointed authority who must determine and accept appropriate risk and associated controls. There is guidance available to understanding what level of risk to accept based on some foundational parameters, found in FIPS 200, SP 800-39, SP 800-30 and other documents (see Appendix F.i).

F.5.1.4 Defense in Depth

Within each specific implementation of controls within the context of an organization or system, the risk reduction strategy must follow a layered security approach. Layering multiple controls through different security domains improves the overall security posture of an organization, and is a critical area for security architects to manage. Key concepts include:

- No single point of failure; single control failure should expose a vulnerability
- Controls can be complementary, and layered onto more critical areas of a system
- Security improves exponentially

F.5.1.5 How to use Control Appendices

Appendix F.ii lists the controls that are either recommended or mandated for Federal IT systems and host organizations. They flow from the NIST, Privacy Act, HIPAA and other sources (see Appendix F.i). Within the SRM taxonomy, the controls map to one or more category under the Controls.

Appendix F.ii contains mappings that list controls, indicate when each control may be most appropriate, and under what circumstances. This includes considerations such as outsourcing infrastructure, storing PII designated for healthcare use, or rated as a high system through the FIPS 199 categorization process.

Additionally, they provide context as to whether the control maps to or has impact on another Reference Model (e.g. security training is also a BRM activity, encryption controls are important in data model design). Finally, they map controls to where in the organization the control is best suited to be placed, such as at an enterprise, segment, or system level. Use of the appendix is recommended for all types of actors in the design of security controls, including business and operations leads, security practitioners and architects.

F.5.2 Metrics

F.5.2.1 Performance and Compliance

Federal reporting of the measurement of information security has largely been focused on compliance reporting of implementation. While compliance reporting is important in measuring the adherence to federal mandates and adds value in driving organizations towards the desired outcomes, it does not measure the desired outcomes directly. The outcomes of security are more difficult to measure and vary depending on the organization's business. In general, metrics that measure performance outcomes (e.g., risk reduction) are preferred to those that measure inputs (controls). However, both are needed.

Metrics drive the outcomes we achieve. Selecting performance based metrics that are measurable can improve the way in which we apply controls and layer security. Focusing on metrics for compliance will achieve better compliance scores, but will not necessarily correlate to how much risk we've reduced as a result. Difficulty in standardizing and measuring performance outcomes for risk reduction remains a significant hurdle in shifting how we report. It also makes reporting on costs related to security practices more difficult, as outcomes are the result of many aspects of the organization or system design and controls.

Currently, there are two areas where security metrics are collected within the Federal Executive Branch:

- FISMA compliance by system: designed to measure compliance with implementation of security controls.
    - CyberScope is a system designed to handle manual and automated inputs of agency data for FISMA reporting.
- OMB Exhibit 53B cost metrics by investment: designed to focus on costs associated with some security topics to answer specific questions posed by Congress.

F.5.2.2 PRM

The Performance Reference Model has four top tier categories of performance, including customer service, efficiency, process and activities, and input. Security related work should be done within the context of measuring outcomes in appropriate PRM categories with specific focus on measuring the cost, effectiveness, and performance of security activities. When developing security related performance measures, using the PRM provides a way to:

- Align metrics at both the organization and system levels
- Measure and report different thing to different people (cost, compliance, etc.)

- Align depth of metrics and reporting to the organization needs

F.5.2.3 Metrics Maturity

Metrics are an indicator of an organization's growth. As shown in the graphic below, immature organizations have little ability to define or collect metrics, and have only defined broad security goals. From setting strategic goals, the organization then begins to implement in stages in which it can measure and collect implementation level data; representative of this stage is the collection of compliance metrics. Next level maturity brings the ability to measure the efficiency and/or effectiveness of implementations, which is the bridge between the compliance and performance metrics. Final maturity measures the business impact of those implementations—essentially the performance of security controls.

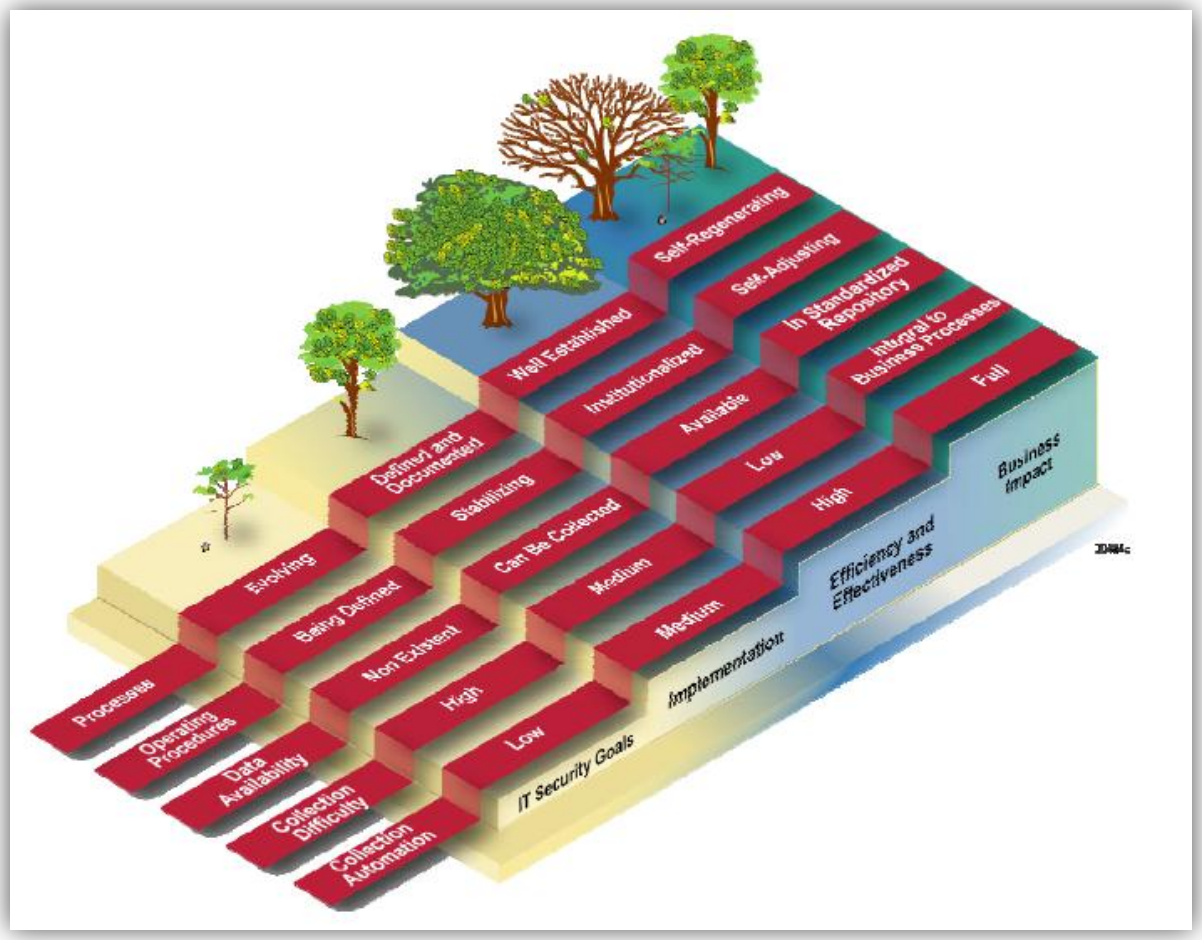


Figure F.7: NIST SP 800-55 Rev.1 – Information Security Program Maturity and Types of Measurement

F.5.2.4 How to use Performance Metrics

In current Federal practice, there aren't many performance-based security metrics commonly accepted or measured. Partly, this is due to the individual nature of what outcomes are best to drive towards for an organization. Partly, this is due to the difficulty of measuring security performance. As indicated

earlier, an organization must have a mature security practice before it can adequately measure its security performance. A common step to addressing this is institutionalizing continuous monitoring to make information more available. Another step is institutionalizing central network, system, hardware and application scans for configuration, logs, and other aspects. These steps along with other best security practices can make measuring security performance easier.

Mature security performance measures are those that are linked to outcomes. Appendix F.ii has a list of example performance metrics that can be used by systems, organizations and portfolios. The intent is to provide a variety of metrics that may be useful at each level of the architecture broken out by status, effectiveness, and cost. These target metrics can be used by security managers and architects as a starting place to select and design their security performance goals. Selecting several performance metrics to add to a system's Key Performance Indicators or to ongoing monitoring plans can help drive compliance level activities to more outcome based activities.

Appendix F.i: Ontology List of Methods

Public Law
Computer Security Act of 1987 (P.L. 100-35)
Paperwork Reduction Act of 1995 (P.L. 104-13)
Information Technology Management Reform Act of 1996 (i.e. Clinger-Cohen Act, P.L. 104-106, Division E)
Federal Information Security Act of 2002 (P.L. 107-347, Title III)
Gramm-Leach-Bliley Act (P.L. 106-102, 15 USC Chapter 94, §6801 et seq.)
Health Insurance Portability and Accountability Act of 1996, (P.L. 104-191, Title II, Subtitle F, Sec. 262, 42 USC 1320d et seq.)
Sarbanes-Oxley Act of 2002 (P.L.107-204, §404)
Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (P.L. 98-473, Title II, §2102(a), 18 USC 1030,
USA PATRIOT Act (P.L. 107-56, §506(a))
E-Government Act [includes FISMA] (P.L. 107-347)
Electronic Communications Privacy Act. (P.L. 99-508, USC Chapters 119,121,206)
Privacy Act of 1974 (P.L. 93-579)
Freedom of Information Act (FOIA), 5 U.S.C. § 552, As Amended By Public Law No.104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996.
The Atomic Energy Act of 1954 (P.L. 83-703), August 1954.
Homeland Security Act of 2002 (Public Law 107-296, 116 Stat. 2135)
Executive Orders
Executive Order 12958 - Classified National Security Information, April 1995
Executive Order 13292 - Further Amendment to Executive Order 12958, March 2003
Executive Order 13526 - Classified National Security Information, December 2009 (replaced EO 12958 and EO 13292)
Executive Order 13556, Controlled Unclassified Information, November 2010
Policies
Code of Federal Regulations, Title 5, Administrative Personnel, Section 731.106, Designation of Public Trust Positions and Investigative Requirements (5 C.F.R.731.106)
Code of Federal Regulations, Part 5 Administrative Personnel, Subpart C—Employees Responsible for the Management or Use of Federal Computer Systems, Section 930.301 through 930.305 (5 C.F.R 930.301-305)
Directives
Director of Central Intelligence Directive 6/9, Physical Security Standards For Sensitive Compartmented Information Facilities, November 2002
Federal Continuity Directive 1 (FCD 1), Federal Executive Branch National Continuity Program and

Requirements, February 2008
Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection, December 2003.
Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 2004
Intelligence Community Directive Number 704, Personnel Security Standards and Procedures Governing Eligibility For Access To Sensitive Compartmented Information And Other Controlled Access Program Information, October 2008
Memoranda
Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, Management of Federal Information Resources, November 2000
Office of Management and Budget, Federal Enterprise Architecture Program Management Office, FEA Consolidated Reference Model Document, Version 2.3, October 2007
Office of Management and Budget, Federal Segment Architecture Methodology (FSAM), January 2009
Office of Management and Budget Memorandum M-01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy, December 2000
Office of Management and Budget Memorandum M-02-01, Guidance for Preparing and Submitting Security Plans of Action and Milestones, October 2001
Office of Management and Budget Memorandum M-03-19, Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting, August 2003.
Office of Management and Budget Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 2003
Office of Management and Budget Memorandum M-04-04, E-Authentication Guidance for Federal Agencies, December 2003
Office of Management and Budget Memorandum M-04-26, Personal Use Policies and File Sharing Technology, September 2004
Office of Management and Budget Memorandum M-05-08, Designation of Senior Agency Officials for Privacy, February 2005
Office of Management and Budget Memorandum M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors, August 2005
Office of Management and Budget Memorandum M-06-15, Safeguarding Personally Identifiable Information, May 2006
Office of Management and Budget Memorandum M-06-16, Protection of Sensitive Information, June 2006
Office of Management and Budget Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, July 2006
Office of Management and Budget Memorandum, Recommendations for Identity Theft Related Data Breach Notification Guidance, September 2006
Office of Management and Budget Memorandum M-07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems, March 2007
Office of Management and Budget Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 2007

Office of Management and Budget Memorandum M-07-18, Ensuring New Acquisitions Include Common Security Configurations, June 2007
Office of Management and Budget Memorandum M-08-09, New FISMA Privacy Reporting Requirements for FY 2008, January 2008
Office of Management and Budget Memorandum M-08-21, FY08 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, July 2008
Office of Management and Budget Memorandum M-08-22, Guidance on the Federal Desktop Core Configuration (FDCC), August 2008
Office of Management and Budget Memorandum M-08-23, Securing the Federal Government's Domain Name System Infrastructure, August 2008
The White House, Office of the Press Secretary, Designation and Sharing of Controlled Unclassified Information (CUI), May 2008
The White House, Office of the Press Secretary, Classified Information and Controlled Unclassified Information, May 2009
Office of Management and Budget Memorandum 11-33, FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, September 2011
Office of Management and Budget Memorandum 12-20, FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, October 2012
Standards
International Organization for Standardization/International Electrotechnical Commission 27001, Information Security Management System Requirements, October 2005
International Organization for Standardization/International Electrotechnical Commission 15408-1, Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model, October 2005
International Organization for Standardization/International Electrotechnical Commission 15408-2, Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements, October 200
International Organization for Standardization/International Electrotechnical Commission 15408-3, Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements, October 2005
National Institute of Standards and Technology Federal Information Processing Standards Publication 140-2, Security Requirements for Cryptographic Modules, May 2001
National Institute of Standards and Technology Federal Information Processing Standards Publication 180-3, Secure Hash Standard (SHS), October 2008
National Institute of Standards and Technology Federal Information Processing Standards Publication 186-3, Digital Signature Standard (DSS), June 2009
National Institute of Standards and Technology Federal Information Processing Standards Publication 188, Standard Security Labels for Information Transfer, September 1994
National Institute of Standards and Technology Federal Information Processing Standards Publication 190, Guideline for the Use of Advanced Authentication Technology Alternatives, September 1994
National Institute of Standards and Technology Federal Information Processing Standards Publication 197, Advanced Encryption Standard (AES), November 2001
National Institute of Standards and Technology Federal Information Processing Standards Publication 198-1, The Keyed-Hash Message Authentication Code (HMAC), July 2008
National Institute of Standards and Technology Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February

2004
National Institute of Standards and Technology Federal Information Processing Standards Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
National Institute of Standards and Technology Federal Information Processing Standards Publication 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006
Committee for National Security Systems (CNSS) Instruction 4009, National Information Assurance Glossary, June 2006
National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003, Protective Distribution Systems (PDS), December 1996
Guidelines
NIST SP 800-39, Managing Information Security Risk, Organization, Mission, and Information System View (NIST, 2011)
NIST SP 800-37 Rev 1, Guide for Applying the Risk Management Framework to Federal Information Systems (NIST, 2010)
NIST SP 800-53 Rev 4, DRAFT Security and Privacy Controls for Federal Information Systems and Organizations
NIST SP 800-30 Rev 1, Guide for Conducting Risk Assessments (NIST, 2012)
NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (NIST, 2011)
NIST SP 800-55 Rev 1, Performance Measure Guide for Information Security (NIST 2008)
NIST SP 800-61 Rev 2, Computer Security Incident Handling Guide (NIST 2012)

Appendix F.ii: Controls and Metrics Mapping

Main Reporting Category	Sub-Category	Enterprise	Segment	System	Metrics/Reports on Costs	Metrics/Reports on Effectiveness	Metrics on Status (numbers, condition, etc.)
System Inventory and Categorization	Risk Management	X	X			Number of systems or services with a Security Assessment and ATO	Number of systems rated "high"
System Inventory and Categorization	PII and Special Cases (Healthcare, etc.)	X				Number of systems covered by a current PIA	Number of systems that require PIA
System Inventory and Categorization	SOA and Cloud Utilization	X			Costs for Enterprise Tools	Number of systems or services leveraging a public Cloud	
Asset Management	Appliance Count (Router, IDS, etc)		X		Cost for Security Authorization (C&A)		
Asset Management	Device Detection						
Asset Management	Network Scanning				Costs for SOC Support		Number of discrete networks
Asset Management	PO&Ams roll-up	X		X	Costs for Weakness Remediation	Number of PO&Ams closed per time period	Number of PO&Ams per agency

Main Reporting Category	Sub-Category	Enterprise	Segment	System	Metrics/Reports on Costs	Metrics/Reports on Effectiveness	Metrics on Status (numbers, condition, etc.)
Configuration Management	Application			X	Cost Impact of APT on resources	Percentage of approved and implemented configuration changes	
Configuration Management	Infrastructure						
Configuration Management	Enterprise Apps	X					Number of enterprise-wide applications
Vulnerability Management and Software Assurance	Patching			X	Costs for Anti-Malware Software	Number of high vulnerabilities mitigated within organizationally defined time period--System	Number of high vulnerabilities identified
Vulnerability Management and Software Assurance	Patching	X			Costs of mission impact at affected locations (i.e. POEs)	Number of high vulnerabilities mitigated within organizationally defined time period--Enterprise	Number of vulnerabilities identified through vulnerability scans
Vulnerability Management and Software Assurance	System Scanning			X	Costs for Anti-Virus Software Licensing	Number of vulnerabilities determined to be non-applicable	Number of vulnerabilities identified through vulnerability scans

Main Reporting Category	Sub-Category	Enterprise	Segment	System	Metrics/Reports on Costs	Metrics/Reports on Effectiveness	Metrics on Status (numbers, condition, etc.)
Identity and Asset Management	Application	X					Number of applications not using a PIV for access
Identity and Asset Management	Infrastructure/Network	X					Number of users accessing networks using a PIV
Identity and Asset Management	PIV implementation status	X					Number of users with a PIV
Identity and Asset Management	Privileged Use Access						Number of users with access to system
Identity and Asset Management	Separation of Duties Management						
Identity and Asset Management	Provisioning and Revocation						

Main Reporting Category	Sub-Category	Enterprise	Segment	System	Metrics/Reports on Costs	Metrics/Reports on Effectiveness	Metrics on Status (numbers, condition, etc.)
Data Protection	Mobile devices	X		X	Cost of securing mobile devices (includes infrastructure, antivirus software and training)	Number of mobile computers and devices employ FIPS140-2 validated encryption	Number of mobile computers and devices are in use
Data Protection	Local Encryption	X				Number of media passed sanitation testing for FIPS199 high-impact systems	
Data Protection	PKI						
Data Protection	Data Leakage	X			Costs for Data Leakage Protection	Mitigation methods	Number of Data leaks per quarter, etc.
Boundary Protection	Email Systems	X			Cost for Email Filtering Software		
Boundary Protection	TIC implementation	X			Cost for Web Filtering Software Licensing		

Main Reporting Category	Sub-Category	Enterprise	Segment	System	Metrics/Reports on Costs	Metrics/Reports on Effectiveness	Metrics on Status (numbers, condition, etc.)
Boundary Protection	TIC implementation	X		X	Cost of NGFW	# of Application Visibility, Application Control, and unauthorized apps incidents logged.	
Boundary Protection	Wireless Control						
Boundary Protection	Virtualization						
Boundary Protection	Other Media (AV/Fax/Phone)						
Incident Management	Pen Testing	X			Costs for Penetration Testing Activities		
Incident Management	Breach Reporting	X		X	Cost for Intrusion Detection Systems Licensing	Number of incidents involving PII were reported	Number of incidents reported
Training and Education	General Security	X			Costs for Security Awareness	Percentage of information systems security personnel received training	Number of information system security personnel received security training

Main Reporting Category	Sub-Category	Enterprise	Segment	System	Metrics/Reports on Costs	Metrics/Reports on Effectiveness	Metrics on Status (numbers, condition, etc.)
Training and Education	Specific Training	X			Costs for Security Training (Employees with significant security responsibilities)		
Remote Access	Access Points	X					Number of remote access points
Remote Access	Available Factors	X				Percentage of remote access point used to gain unauthorized access	
Network Security	DNS and IP availability						
Network Security	IPv6						
Software Assurance							
Software Assurance							
Continuous Monitoring				X	Cost for SIM/SIEM Tools		

Main Reporting Category	Sub-Category	Enterprise	Segment	System	Metrics/Reports on Costs	Metrics/Reports on Effectiveness	Metrics on Status (numbers, condition, etc.)
Continuous Monitoring				X	Costs for Annual FISMA Testing	Timeframe for reporting DHS Einstein critical incidents to all authorities	# of DHS critical incidents reported in Einstein 2.
Continuity	Disaster response						
Continuity	MEF Designation						
Continuity	Availability Factors						

			BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
Control ID	**Control Name or Requirement Text**	**Class**	**Establishing Policy and Procedures**	**Planning and Training**	**Monitoring, Response and Reporting**	**Securing Infrastructure and Networks (incl physical security)**	**Securing Platforms & Applications**	**Securing Data**		**FISCAM General Controls ***	**FISCAM Business Process Application Controls ***	**HIPAA Requirements**	**Safeguarding PII ****	**Outsourced Infrastructure / Services *****
AC-1	Access Control Policy And Procedures	Technical	X							X		X	X	
AC-2	Account Management	Technical					X			X		X		

Control ID	Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
			Establishing Policy and Procedures	Planning and Training	Monitoring, Response and Reporting	Securing Infrastructure and Networks (incl physical security)	Securing Platforms & Applications	Securing Data		FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
AC-3	Access Enforcement	Technical					X			X		X	X	
AC-4	Information Flow Enforcement	Technical				X				X		X	X	
AC-5	Separation Of Duties	Technical	X				X			X		X		
AC-6	Least Privilege	Technical	X				X			X		X	X	
AC-7	Unsuccessful Login Attempts	Technical					X			X				
AC-8	System Use Notification	Technical					X			X				
AC-9	Previous Logon [Access] Notification	Technical					X			X				
AC-10	Concurrent Session Control	Technical					X			X				
AC-11	Session Lock	Technical					X			X		X		
AC-12	Session Termination	Technical					X			X		X		
AC-13	Supervision And Review — Access Control	Technical			X					X		X	X	
AC-14	Permitted Actions Without Identification Or Authentication	Technical					X			X				
AC-15	Automated Marking	Technical					X			X		X		
AC-16	Security Attributes	Technical					X			X		X		
AC-17	Remote Access	Technical				X	X			X		X	X	

Control ID	Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
			Establishing Policy and Procedures	Planning and Training	Monitoring, Response and Reporting	Securing Infrastructure and Networks (incl physical security)	Securing Platforms & Applications	Securing Data		FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
AC-18	Wireless Access	Technical					X			X				
AC-19	Access Control For Mobile Devices	Technical					X			X		X		
AC-20	Use Of External Information Systems	Technical					X			X				
AC-21	User-Based Collaboration And Information Sharing	Technical						X						
AC-22	Publicly Accessible Content	Technical	X	X	X									
AT-1	Security Awareness And Training Policy And Procedures	Operational	X							X		X	X	
AT-2	Security Awareness	Operational		X						X		X		
AT-3	Security Training	Operational		X						X		X		
AT-4	Security Training Records	Operational		X						X		X		
AT-5	Contacts With Security Groups And Associations	Operational		X						X		X		
AU-1	Audit And Accountability Policy And Procedures	Technical	X							X		X	X	X
AU-2	Auditable Events	Technical			X					X		X	X	
AU-3	Content Of Audit Records	Technical			X					X		X		

Control ID	Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
			Establishing Policy and Procedures	Planning and Training	Monitoring, Response and Reporting	Securing Infrastructure and Networks (incl physical security)	Securing Platforms & Applications	Securing Data		FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
AU-4	Audit Storage Capacity	Technical			X					X		X		
AU-5	Response To Audit Processing Failures	Technical			X					X				
AU-6	Audit Review, Analysis, And Reporting	Technical			X					X		X	X	
AU-7	Audit Reduction And Report Generation	Technical			X					X		X		
AU-8	Time Stamps	Technical			X					X				
AU-9	Protection Of Audit Information	Technical			X					X				
AU-10	Non-Repudiation	Technical			X					X				
AU-11	Audit Record Retention	Technical			X					X				
AU-12	Audit Generation	Technical			X									
AU-13	Monitoring For Information Disclosure	Technical			X									
AU-14	Session Audit	Technical			X									
CA-1	Security Assessment And Authorization Policies And Procedures	Management	X							X		X		
CA-2	Security Assessments	Management	X							X		X		
CA-3	Information System Connections	Management	X							X		X		

Control ID	Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
			Establishing Policy and Procedures	Planning and Training	Monitoring, Response and Reporting	Securing Infrastructure and Networks (incl physical security)	Securing Platforms & Applications	Securing Data		FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
CA-4	Security Certification	Management	X							X		X		
CA-5	Plan Of Action And Milestones	Management	X							X				
CA-6	Security Authorization	Management	X							X		X		
CA-7	Continuous Monitoring	Management			X					X		X		
										X				
CM-1	Configuration Management Policy And Procedures	Operational	X							X				
CM-2	Baseline Configuration	Operational					X			X				
CM-3	Configuration Change Control	Operational					X			X				
CM-4	Security Impact Analysis	Operational			X					X				
CM-5	Access Restrictions For Change	Operational					X			X				
CM-6	Configuration Settings	Operational					X			X		X		
CM-7	Least Functionality	Operational					X			X				
CM-8	Information System Component Inventory	Operational					X			X				
CM-9	Configuration Management Plan	Operational					X							

Control ID	Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
			Establishing Policy and Procedures	Planning and Training	Monitoring, Response and Reporting	Securing Infrastructure and Networks (incl physical security)	Securing Platforms & Applications	Securing Data		FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
CP-1	Contingency Planning Policy And Procedures	Operational	X							X		X		X
CP-2	Contingency Plan	Operational		X						X		X		
CP-3	Contingency Training	Operational		X						X		X		
CP-4	Contingency Plan Testing And Exercises	Operational		X						X		X		
CP-5	Contingency Plan Update	Operational		X						X		X		
CP-6	Alternate Storage Site	Operational				X	X			X		X		
CP-7	Alternate Processing Site	Operational				X	X			X		X		
CP-8	Telecommunications Services	Operational				X	X			X		X		
CP-9	Information System Backup	Operational				X	X			X		X		
CP-10	Information System Recovery And Reconstitution	Operational				X	X			X		X		
IA-1	Identification And Authentication Policy And Procedures	Technical	X							X			X	
IA-2	Identification And Authentication [Organizational Users]	Technical				X	X			X		X		
IA-3	Device Identification And Authentication	Technical				X	X			X		X		
IA-4	Identifier Management	Technical				X	X			X		X		

Control ID	Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
			Establishing Policy and Procedures	Planning and Training	Monitoring, Response and Reporting	Securing Infrastructure and Networks (incl physical security)	Securing Platforms & Applications	Securing Data		FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
IA-5	Authenticator Management	Technical				X	X			X		X	X	
IA-6	Authenticator Feedback	Technical				X	X			X		X		
IA-7	Cryptographic Module Authentication	Technical				X	X			X		X		
IA-8	Identification And Authentication [Non-Organizational Users]	Technical				X	X							
IR-1	Incident Response Policy And Procedures	Operational	X							X		X		X
IR-2	Incident Response Training	Operational		X						X		X		
IR-3	Incident Response Testing And Exercises	Operational			X					X		X		
IR-4	Incident Handling	Operational			X					X		X		
IR-5	Incident Monitoring	Operational			X					X		X		
IR-6	Incident Reporting	Operational			X					X		X		
IR-7	Incident Response Assistance	Operational			X					X		X		
IR-8	Incident Response Plan	Operational			X									
MA-1	System Maintenance Policy And Procedures	Operational	X							X		X		

Control ID	Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
			Establishing Policy and Procedures	Planning and Training	Monitoring, Response and Reporting	Securing Infrastructure and Networks (incl physical security)	Securing Platforms & Applications	Securing Data		FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
MA-2	Controlled Maintenance	Operational					X			X		X		
MA-3	Maintenance Tools	Operational					X			X				
MA-4	Non-Local Maintenance	Operational					X			X				
MA-5	Maintenance Personnel	Operational					X			X		X		
MA-6	Timely Maintenance	Operational					X			X		X		
MP-1	Media Protection Policy And Procedures	Operational	X							x		X	X	
MP-2	Media Access	Operational				X				X		X		
MP-3	Media Marking	Operational				X				X		X		
MP-4	Media Storage	Operational				X				X		X		
MP-5	Media Transport	Operational				X				X		X	X	
MP-6	Media Sanitization	Operational				X				X		X		
												X		
PE-1	Physical And Environmental Protection Policy And Procedures	Operational	X							X		X		
PE-2	Physical Access Authorizations	Operational				X				X		X		

Control ID	Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
			Establishing Policy and Procedures	Planning and Training	Monitoring, Response and Reporting	Securing Infrastructure and Networks (incl physical security)	Securing Platforms & Applications	Securing Data		FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
PE-3	Physical Access Control	Operational				X				X		X		
PE-4	Access Control For Transmission Medium	Operational				X				X		X		
PE-5	Access Control For Output Devices	Operational				X				X		X		
PE-6	Monitoring Physical Access	Operational				X				X		X		
PE-7	Visitor Control	Operational				X				X		X		
PE-8	Access Records	Operational				X				X		X		
PE-9	Power Equipment And Power Cabling	Operational				X				X				
PE-10	Emergency Shutoff	Operational				X				X				
PE-11	Emergency Power	Operational				X				X				
PE-12	Emergency Lighting	Operational				X				X				
PE-13	Fire Protection	Operational				X				X				
PE-14	Temperature And Humidity Controls	Operational				X				X				
PE-15	Water Damage Protection	Operational				X				X				
PE-16	Delivery And Removal	Operational				X				X				
PE-17	Alternate Work Site	Operational	X							X		X		
PE-18	Location Of Information System Components	Operational				X				X		X		

Control ID	Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
			Establishing Policy and Procedures	Planning and Training	Monitoring, Response and Reporting	Securing Infrastructure and Networks (incl physical security)	Securing Platforms & Applications	Securing Data		FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
PE-19	Information Leakage	Operational			X					X				
PL-1	Security Planning Policy And Procedures	Management	X							X		X		
PL-2	System Security Plan	Management		X						X		X		
PL-3	System Security Plan Update	Management		X						X		X		
PL-4	Rules Of Behavior	Management		X						X			X	
PL-5	Privacy Impact Assessment	Management		X						X			X	X
PL-6	Security-Related Activity Planning	Management		X						X		X		
PM-1	Information Security Program Plan	Management	X							X				
PM-2	Senior Information Security Officer	Management	X							X				
PM-3	Information Security Resources	Management	X							X				
PM-4	Plan Of Action And Milestones Process	Management	X							X				
PM-5	Information System Inventory	Management	X							X				
PM-6	Information Security Measures Of Performance	Management	X							X				
PM-7	Enterprise Architecture	Management	X							X				

			BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
Control ID	**Control Name or Requirement Text**	**Class**	Establishing Policy and Procedures	Planning and Training	Monitoring, Response and Reporting	Securing Infrastructure and Networks (incl physical security)	Securing Platforms & Applications	Securing Data		FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
PM-8	Critical Infrastructure Plan	Management	X							X				
PM-9	Risk Management Strategy	Management	X							X				
PM-10	Security Authorization Process	Management	X							X				
PM-11	Mission/Business Process Definition	Management	X							X				
PS-1	Personnel Security Policy And Procedures	Operational	X							X		X		
PS-2	Position Categorization	Operational					X			X		X		
PS-3	Personnel Screening	Operational					X			X		X		
PS-4	Personnel Termination	Operational					X			X		X		
PS-5	Personnel Transfer	Operational					X			X		X		
PS-6	Access Agreements	Operational					X			X		X		X
PS-7	Third-Party Personnel Security	Operational					X			X		X		X
PS-8	Personnel Sanctions	Operational					X			X		X		
RA-1	Risk Assessment Policy And Procedures	Management	X							X		X		X
RA-2	Security Categorization	Management	X							X		X	X	

			BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
Control ID	**Control Name or Requirement Text**	**Class**	Establishing Policy and Procedures	Planning and Training	Monitoring, Response and Reporting	Securing Infrastructure and Networks (incl physical security)	Securing Platforms & Applications	Securing Data		FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
RA-3	Risk Assessment	Management			X					X		X		
RA-4	Risk Assessment Update	Management			X					X		X	X	
RA-5	Vulnerability Scanning	Management			X					X				
SA-1	System And Services Acquisition Policy And Procedures	Management	X							X				X
SA-2	Allocation Of Resources	Management	X							X				
SA-3	Life Cycle Support	Management	X							X				
SA-4	Acquisitions	Management	X							X		X		
SA-5	Information System Documentation	Management	X							X				
SA-6	Software Usage Restrictions	Management	X				X			X				
SA-7	User-Installed Software	Management					X			X				
SA-8	Security Engineering Principles	Management				X	X			X				
SA-9	External Information System Services	Management				X	X			X		X		X
SA-10	Developer Configuration Management	Management				X	X			X				
SA-11	Developer Security Testing	Management				X	X			X				

Control ID	Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
			Establishing Policy and Procedures	Planning and Training	Monitoring, Response and Reporting	Securing Infrastructure and Networks (incl physical security)	Securing Platforms & Applications	Securing Data		FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
SA-12	Supply Chain Protection	Management			X									
SA-13	Trustworthiness	Management			X									
SA-14	Critical Information System Components	Management			X									
SC-1	System And Communications Protection Policy And Procedures	Technical	X							X			X	
SC-2	Application Partitioning	Technical					X			X				
SC-3	Security Function Isolation	Technical				X	X			X				
SC-4	Information In Shared Resources	Technical				X	X	X		X			X	
SC-5	Denial Of Service Protection	Technical				X				X				
SC-6	Resource Priority	Technical				X				X				
SC-7	Boundary Protection	Technical				X				X				
SC-8	Transmission Integrity	Technical				X				X		X		
SC-9	Transmission Confidentiality	Technical				X				X		X		
SC-10	Network Disconnect	Technical				X				X				
SC-11	Trusted Path	Technical				X				X				

Control ID	Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
			Establishing Policy and Procedures	Planning and Training	Monitoring, Response and Reporting	Securing Infrastructure and Networks (incl physical security)	Securing Platforms & Applications	Securing Data		FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
SC-12	Cryptographic Key Establishment And Management	Technical				X	X	X		X		X		
SC-13	Use Of Cryptography	Technical				X	X			X		X	X	
SC-14	Public Access Protections	Technical				X	X			X				
SC-15	Collaborative Computing Devices	Technical				X	X			X				
SC-16	Transmission Of Security Attributes	Technical				X				X				
SC-17	Public Key Infrastructure Certificates	Technical				X				X				
SC-18	Mobile Code	Technical				X				X				
SC-19	Voice Over Internet Protocol	Technical				X				X				
SC-20	Secure Name / Address Resolution Service [Authoritative Source]	Technical				X				X				
SC-21	Secure Name / Address Resolution Service [Recursive Or Caching Resolver]	Technical				X				X				
SC-22	Architecture And Provisioning For Name / Address Resolution Service	Technical				X				X				
SC-23	Session Authenticity	Technical				X				X				
SC-24	Fail In Known State	Technical				X	X							

Control ID	Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
			Establishing Policy and Procedures	Planning and Training	Monitoring, Response and Reporting	Securing Infrastructure and Networks (incl physical security)	Securing Platforms & Applications	Securing Data		FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
SC-25	Thin Nodes	Technical				X								
SC-26	Honeypots	Technical				X	X	X						
SC-27	Operating System-Independent Applications	Technical					X							
SC-28	Protection Of Information At Rest	Technical				X								
SC-29	Heterogeneity	Technical				X	X							
SC-30	Virtualization Techniques	Technical				X								
SC-31	Covert Channel Analysis	Technical				X								
SC-32	Information System Partitioning	Technical				X		X						
SC-33	Transmission Preparation Integrity	Technical				X	X							
SC-34	Non-Modifiable Executable Programs	Technical					X							
SI-1	System And Information Integrity Policy And Procedures	Operational	X							X				
SI-2	Flaw Remediation	Operational					X			X				
SI-3	Malicious Code Protection	Operational					X			X		X		
SI-4	Information System Monitoring	Operational					X			X		X		

Control ID	Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
			Establishing Policy and Procedures	Planning and Training	Monitoring, Response and Reporting	Securing Infrastructure and Networks (incl physical security)	Securing Platforms & Applications	Securing Data		FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
SI-5	Security Alerts, Advisories, And Directives	Operational			X					X		X		
SI-6	Security Functionality Verification	Operational			X					X				
SI-7	Software And Information Integrity	Operational			X					X		X		
SI-8	Spam Protection	Operational			X	X	X			X		X		
SI-9	Information Input Restrictions	Operational					X	X			X			
SI-10	Information Input Validation	Operational					X				X			
SI-11	Error Handling	Operational					X				X			
SI-12	Information Output Handling And Retention	Operational		X			X			X	X			
SI-13	Predictable Failure Prevention	Operational					X							
164.308(a)(1)(i)	Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.	Standard	X									X		
164.308(a)(1)(ii)(A)	Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.	Required			X	X	X	X				X		

Control ID	Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
			Establishing Policy and Procedures	Planning and Training	Monitoring, Response and Reporting	Securing Infrastructure and Networks (incl physical security)	Securing Platforms & Applications	Securing Data		FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
164.308(a)(1)(ii)(B)	Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).	Required										X		
164.308(a)(1)(ii)(D)	Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Required	X		X	X	X					X		
164.308(a)(2)	Standard: Assigned security responsibility. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.	Standard		X								X		
164.308(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	N/A	X	X		X	X	X				X		

Control ID	Control Name or Requirement Text	Class	BRM Establishing Policy and Procedures	BRM Planning and Training	BRM Monitoring, Response and Reporting	IRM Securing Infrastructure and Networks (incl physical security)	ARM Securing Platforms & Applications	DRM Securing Data		Cross-Mapping FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
164.308(a)(3)(ii)(A)	Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	Addressable	X		X	X	X	X				X		
164.308(a)(3)(ii)(B)	Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	Addressable	X		X							X		
164.308(a)(3)(ii)(C)	Termination procedures (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	Addressable	X	X	X	X	X	X				X		
164.308(a)(4)(i)	Standard: Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.	Standard	X			X	X	X				X		

Control ID	Control Name or Requirement Text	Class	BRM Establishing Policy and Procedures	BRM Planning and Training	BRM Monitoring, Response and Reporting	IRM Securing Infrastructure and Networks (incl physical security)	ARM Securing Platforms & Applications	DRM Securing Data	Cross-Mapping FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
164.308(a)(4)(ii)(A)	Isolating health care clearinghouse functions (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	Required	X	X		X		X			X		
164.308(a)(4)(ii)(B)	Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	Addressable	X			X	X				X		
164.308(a)(4)(ii)(C)	Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	Addressable	X		X	X	X				X		
164.308(a)(5)(i)	Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).	Standard		X							X		
164.308(a)(5)(ii)(A)	Security reminders (Addressable). Periodic security updates.	Addressable			X						X		

Control ID	Control Name or Requirement Text	Class	BRM Establishing Policy and Procedures	BRM Planning and Training	BRM Monitoring, Response and Reporting	IRM Securing Infrastructure and Networks (incl physical security)	ARM Securing Platforms & Applications	DRM Securing Data	Cross-Mapping FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
164.308(a)(5)(ii)(B)	Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.	Addressable			X						X		
164.308(a)(5)(ii)(C)	Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.	Addressable	X		X						X		
164.308(a)(5)(ii)(D)	Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.	Addressable	X								X		
164.308(a)(6)(i)	Standard: Security incident procedures. Implement policies and procedures to address security incidents.	Standard	X		X						X		
164.308(a)(6)(ii)	Implementation specification: Response and Reporting (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.	Required			X						X		
164.308(a)(7)(i)	Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health	Standard	X	X							X		

Control ID	Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
			Establishing Policy and Procedures	Planning and Training	Monitoring, Response and Reporting	Securing Infrastructure and Networks (incl physical security)	Securing Platforms & Applications	Securing Data		FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
	information.													
164.308(a)(7)(ii)(A)	Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	Required	X	X				X				X		
164.308(a)(7)(ii)(B)	Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.	Required	X	X				X				X		
164.308(a)(7)(ii)(C)	Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	Required	X		X							X		
164.308(a)(7)(ii)(D)	Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.	Addressable	X		X							X		
164.308(a)(7)(ii)(E)	Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.	Addressable		X								X		

Control ID	Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
			Establishing Policy and Procedures	Planning and Training	Monitoring, Response and Reporting	Securing Infrastructure and Networks (incl physical security)	Securing Platforms & Applications	Securing Data		FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
164.308(a)(8)	Standard: Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.	Standard			X							X		
164.308(b)(1)	Standard: Business associate contracts and other arrangements. A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information.	Standard	X									X		X
164.308(b)(4)	Implementation specifications: Written contract or other arrangement (Required). Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).	Required	X									X		X

Control ID	Control Name or Requirement Text	Class	BRM Establishing Policy and Procedures	BRM Planning and Training	BRM Monitoring, Response and Reporting	IRM Securing Infrastructure and Networks (incl physical security)	ARM Securing Platforms & Applications	DRM Securing Data	Cross-Mapping FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
164.310(a)(1)	Standard: Facility access controls. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	Standard	X			X					X		
164.310(a)(2)(i)	Contingency operations (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	Addressable	X	X	X	X					X		
164.310(a)(2)(ii)	Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	Addressable	X			X					X		
164.310(a)(2)(iii)	Access control and validation procedures (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	Addressable	X			X					X		
164.310(a)(2)(iv)	Maintenance records (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example,	Addressable	X		X	X					X		

Control ID	Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
			Establishing Policy and Procedures	Planning and Training	Monitoring, Response and Reporting	Securing Infrastructure and Networks (incl physical security)	Securing Platforms & Applications	Securing Data		FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
	hardware, walls, doors, and locks).													
164.310(b)	Standard: Workstation use. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	Standard	X			X						X		
164.310(c)	Standard: Workstation security. Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	Standard				X						X		
164.310(d)(1)	Standard: Device and media controls. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.	Standard				X						X		
164.310(d)(2)(i)	Disposal (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.	Required				X		X				X		

Control ID	Control Name or Requirement Text	Class	BRM Establishing Policy and Procedures	BRM Planning and Training	BRM Monitoring, Response and Reporting	IRM Securing Infrastructure and Networks (incl physical security)	ARM Securing Platforms & Applications	DRM Securing Data	Cross-Mapping FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
164.310(d)(2)(ii)	Media reuse (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for reuse.	Required						X			X		
164.310(d)(2)(iii)	Accountability (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	Addressable			X	X		X			X		
164.310(d)(2)(iv)	Data backup and storage (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	Addressable				X		X			X		
164.312(a)(1)	Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	Standard	X	X			X	X			X		
164.312(a)(2)(i)	Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.	Required			X						X		
164.312(a)(2)(ii)	Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected	Required	X	X							X		

Control ID	Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
			Establishing Policy and Procedures	Planning and Training	Monitoring, Response and Reporting	Securing Infrastructure and Networks (incl physical security)	Securing Platforms & Applications	Securing Data		FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
	health information during an emergency.													
164.312(a)(2)(iii)	Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Addressable				X	X					X		
164.312(a)(2)(iv)	Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.	Addressable						X				X		
164.312(b)	Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Standard			X	X	X					X		
164.312(c)(1)	Standard: Integrity. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	Standard	X					X				X		
164.312(c)(2)	Mechanism to authenticate electronic protected health information (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	Addressable						X				X		

Control ID	Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
			Establishing Policy and Procedures	Planning and Training	Monitoring, Response and Reporting	Securing Infrastructure and Networks (incl physical security)	Securing Platforms & Applications	Securing Data		FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
164.312(d)	Standard: Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	Standard	X			X	X					X		
164.312(e)(1)	Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	Standard				X		X				X		
164.312(e)(2)(i)	Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	Addressable			X	X		X				X		
164.312(e)(2)(ii)	Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	Addressable						X				X		

Control ID	Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
			Establishing Policy and Procedures	Planning and Training	Monitoring, Response and Reporting	Securing Infrastructure and Networks (incl physical security)	Securing Platforms & Applications	Securing Data		FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
164.314(a)(1)	Standard: Business associate contracts or other arrangements. (i) The contract or other arrangement between the covered entity and its business associate required by § 164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable. (ii) A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful— (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary.	Standard			X							X		X

Control ID	Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
			Establishing Policy and Procedures	Planning and Training	Monitoring, Response and Reporting	Securing Infrastructure and Networks (incl physical security)	Securing Platforms & Applications	Securing Data		FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
164.314(a)(2)(i)	Business associate contracts. The contract between a covered entity and a business associate must provide that the business associate will— (A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart; (B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; (C) Report to the covered entity any security incident of which it becomes aware; (D) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.	N/A	X	X								X		X
164.314(a)(2)(ii)	Other arrangements. (A) When a covered entity and its business associate are both governmental entities, the covered entity is in compliance with paragraph (a)(1) of this section, if— (1) It enters into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (a)(2)(i) of this section; or (2) Other law (including regulations adopted by the covered entity or its	N/A	X	X								X		

Control ID	Control Name or Requirement Text	Class	BRM Establishing Policy and Procedures	BRM Planning and Training	BRM Monitoring, Response and Reporting	IRM Securing Infrastructure and Networks (incl physical security)	ARM Securing Platforms & Applications	DRM Securing Data	Cross-Mapping FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
	business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (a)(2)(i) of this section.												
164.314(b)(1)	Requirements for group health plans. Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to § 164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.	N/A	X	X							X		
164.314(b)(2)(i)	Group Health Plan Implementation specifications (Required). The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to— (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health	N/A	X	X							X		

Control ID	Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
			Establishing Policy and Procedures	Planning and Training	Monitoring, Response and Reporting	Securing Infrastructure and Networks (incl physical security)	Securing Platforms & Applications	Securing Data		FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
	information that it creates, receives, maintains, or transmits on behalf of the group health plan;													
164.314(b)(2)(ii)	Group Health Plan Implementation specifications (Required). Ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;	Required	X	X								X		
164.314(b)(2)(ii)	§ 164.504(f)(2)(iii) Reads: "(iii) Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must: (A) Describe those employees or classes of employees or other persons under the control of the plan sponsor to be given access to the protected health information to be disclosed, provided that any employee or person who receives protected health information relating to payment under, health care operations of, or other matters pertaining to the group health plan in the ordinary course of business must be included in such description;	Required	X	X								X		

Control ID	Control Name or Requirement Text	Class	BRM Establishing Policy and Procedures	BRM Planning and Training	BRM Monitoring, Response and Reporting	IRM Securing Infrastructure and Networks (incl physical security)	ARM Securing Platforms & Applications	DRM Securing Data	Cross-Mapping FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
164.314(b)(2)(ii)	§ 164.504(f)(2)(iii) Reads: "(iii) Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must: (B) Restrict the access to and use by such employees and other persons described in paragraph (f)(2)(iii)(A) of this section to the plan administration functions that the plan sponsor performs for the group health plan; and	Required	X	X							X		
164.314(b)(2)(ii)	§ 164.504(f)(2)(iii) Reads: "(iii) Provide for adequate separation between the group health plan and the plan sponsor. The plan documents must: (C) Provide an effective mechanism for resolving any issues of noncompliance by persons described in paragraph (f)(2)(iii)(A) of this section with the plan document provisions required by this paragraph."	Required	X	X							X		
164.314(b)(2)(iii)	Group Health Plan Implementation specifications (Required). Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information;	Required	X	X							X		X
164.314(b)(2)(iv)	Group Health Plan Implementation specifications (Required). (iv) Report to the group health plan any security incident of which it becomes aware.	Required			X						X		

Control ID	Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
			Establishing Policy and Procedures	Planning and Training	Monitoring, Response and Reporting	Securing Infrastructure and Networks (incl physical security)	Securing Platforms & Applications	Securing Data		FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
164.316(a)	Standard: Policies and procedures. Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.	Standard	X									X		
164.316(b)(1)	Standard: Documentation. (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.	Standard	X									X		
164.316(b)(2)(i)	Time limit (Required). Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.	Required		X								X		

Control ID	Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		Cross-Mapping				
			Establishing Policy and Procedures	Planning and Training	Monitoring, Response and Reporting	Securing Infrastructure and Networks (incl physical security)	Securing Platforms & Applications	Securing Data		FISCAM General Controls *	FISCAM Business Process Application Controls *	HIPAA Requirements	Safeguarding PII **	Outsourced Infrastructure / Services ***
164.316(b)(2)(ii)	Availability (Required). Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	Required		X								X		
164.316(b)(2)(iii)	Updates (Required). Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.	Required		X								X		
164.306(a)	General requirements. Covered entities must do the following: (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part. (4) Ensure compliance with this subpart by its workforce.	Reference	N/A	N/A	N/A	N/A	N/A	N/A				X		

*FISCAM references FISMA controls and does not put forth independent requirements.

** PII requirements are those areas specifically aligned to protecting the personal information of the public held in Federal systems.

*** Outsourced infrastructure (SOA, Cloud, etc.) requires security plans and implementation on the part of the vendor, but also additional focus on contracting and expected service levels on the part of the government.

Appendix F.iii: Security Reference Document Mappings

This table provides a mapping of Security Reference Documents to Legal Security Requirements.

	Legal Security Requirements					
Reference Security Documents	E-Government Act	HSPD-7	HSPD-12	HIPAA	OMB Circular A-11	OMB Circular A-130, App. III
	Public Law 107-347	Critical Infrastructure Identification, Prioritization, and Protection	Common Identification Standard For Federal Employees and Contractors	Health Insurance Portability and Accountability Act	Preparation, Submission, and Execution Of The Budget	Management Of Federal Information Resources, Appendix III: Security Of Federal Automated Information Resources
NIST FIPS 199 Standards for Security Categorization of Federal Information and Information Systems	x	x				x
NIST FIPS 200 Minimum Security Requirements for Federal Information and Information Systems	x	x				x
NIST FIPS 201-1 Personal Identity Verification for Federal Employees and Contractors			x			
NIST IR 7284 Personal Identity Verification Card Management Report			x			
NIST IR 7316 Assessment of Access Control Systems						x
NIST IR 7337 Personal Identity Verification Demonstration Summary			x			
NIST IR 7497 DRAFT Security Architecture Design Process for Health Information Exchanges (HIEs)				x		
NIST IR 7511 Rev. 1 DRAFT Security Content Automation Protocol (SCAP) Version 1.0 Validation Program Test Requirements						x
NIST ITL 1999-04 Guide for Developing Security Plans for Information Technology Systems		x				

	Legal Security Requirements					
Reference Security Documents	E-Government Act	HSPD-7	HSPD-12	HIPAA	OMB Circular A-11	OMB Circular A-130, App. III
NIST ITL 2006-03 Minimum Security Requirements For Federal Information And Information Systems: Federal Information Processing Standard (FIPS) 200 Approved By The Secretary Of Commerce		x				x
NIST ITL 2006-04 Protecting Sensitive Information Transmitted in Public Networks		x				
NIST ITL 2006-08 Protecting Sensitive Information Processed And Stored In Information Technology (IT) Systems		x				
NIST ITL 2006-10 Log Management: Using Computer And Network Records To Improve Information Security				x		
NIST ITL 2006-11 Guide To Securing Computers Using Windows XP Home Edition		x				
NIST ITL 2006-12 Maintaining Effective Information Technology (IT) Security Through Test, Training, And Exercise Programs		x				
NIST ITL 2007-01 Security Controls For Information Systems: Revised Guidelines Issued By NIST		x				
NIST ITL 2007-02 Intrusion Detection And Prevention Systems		x			x	
NIST ITL 2007-04 Securing Wireless Networks		x				
NIST ITL 2007-05 Securing Radio Frequency Identification (RFID) Systems		x				
NIST ITL 2007-07 Border Gateway Protocol Security		x				
NIST ITL 2008-10 Keeping Information Technology (IT) System Servers Secure: A General Guide To Good Practices						x
NIST SB 2005-03 Personal Identity Verification (PIV) Of Federal Employees and Contractors: Federal Information Processing Standard (FIPS) 201			x			

	Legal Security Requirements					
Reference Security Documents	E-Government Act	HSPD-7	HSPD-12	HIPAA	OMB Circular A-11	OMB Circular A-130, App. III
NIST SB 2005-08 Implementation Of FIPS 201, Personal Identity Verification (PIV) Of Federal Employees and Contractors			x			
NIST SB 2006-01 Testing and Validation Of Personal Identity Verification (PIV) Components and Subsystems For Conformance To Federal Information Processing Standard 201			x			
NIST SP 800-100 Information Security Handbook: A Guide for Managers						x
NIST SP 800-101 Guidelines on Cell Phone Forensics						x
NIST SP 800-101 Guidelines on Cell Phone Forensics		x				x
NIST SP 800-103 DRAFT An Ontology of Identity Credentials, Part I: Background and Formulation						x
NIST SP 800-104 A Scheme for PIV Visual Card Topography						x
NIST SP 800-106 Randomized Hashing for Digital Signatures						x
NIST SP 800-107 Recommendation for Applications Using Approved Hash Algorithms						x
NIST SP 800-111 Guide to Storage Encryption Technologies for End User Devices				x		x
NIST SP 800-113 Guide to SSL VPNs						x
NIST SP 800-117 DRAFT Guide to Adopting and Using the Security Content Automation Protocol (SCAP)						x
NIST SP 800-118 DRAFT Guide to Enterprise Password Management						x
NIST SP 800-12 An Introduction to Computer Security: The NIST Handbook						x
NIST SP 800-122 DRAFT Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)						x
NIST SP 800-123 Guide to General Server Security						x

	Legal Security Requirements					
Reference Security Documents	E-Government Act	HSPD-7	HSPD-12	HIPAA	OMB Circular A-11	OMB Circular A-130, App. III
NIST SP 800-124 Guidelines on Cell Phone and PDA Security						x
NIST SP 800-126 DRAFT The Technical Specification for the Security Content Automation Protocol (SCAP)						x
NIST SP 800-127 DRAFT Guide to Security for Worldwide Interoperability for Microwave Access (WiMAX) Technologies						x
NIST SP 800-16 Information Technology Security Training Requirements: A Role- and Performance-Based Model						x
NIST SP 800-16 Rev. 1 DRAFT Information Security Training Requirements: A Role- and Performance-Based Model						x
NIST SP 800-18 Guide for Developing Security Plans for Information Technology Systems		x				
NIST SP 800-18 Rev.1 Guide for Developing Security Plans for Federal Information Systems		x				x
NIST SP 800-30 Risk Management Guide for Information Technology Systems		x				
NIST SP 800-34 Contingency Planning Guide for Information Technology Systems						x
NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems		x				x
NIST SP 800-37 Rev. 1 DRAFT Guide for Security Authorization of Federal Information Systems: A Security Lifecycle Approach		x				x
NIST SP 800-41 Rev. 1 Guidelines on Firewalls and Firewall Policy		x				
NIST SP 800-44 Version 2 Guidelines on Securing Public Web Servers						x
NIST SP 800-46 Security for Telecommuting and Broadband Communications						x

	Legal Security Requirements					
Reference Security Documents	E-Government Act	HSPD-7	HSPD-12	HIPAA	OMB Circular A-11	OMB Circular A-130, App. III
NIST SP 800-46 Rev. 1 Guide to Enterprise Telework and Remote Access Security						x
NIST SP 800-48 Rev. 1 Guide to Securing Legacy IEEE 802.11 Wireless Networks		x				x
NIST SP 800-50 Building an Information Technology Security Awareness and Training Program						x
NIST SP 800-53 Recommended Security Controls for Federal Information Systems		x				
NIST SP 800-53 Rev. 1 Recommended Security Controls for Federal Information Systems		x			x	x
NIST SP 800-53 Rev. 2 Recommended Security Controls for Federal Information Systems		x			x	x
NIST SP 800-53 Rev. 3 Recommended Security Controls for Federal Information Systems and Organizations		x			x	x
NIST SP 800-54 Border Gateway Protocol Security		x				x
NIST SP 800-55 Rev. 1 Performance Measurement Guide for Information Security					x	
NIST SP 800-59 Guideline for Identifying an Information System as a National Security System		x				
NIST SP 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories		x				
NIST SP 800-63 Version 1.0.2 Electronic Authentication Guideline						x
NIST SP 800-64 Rev. 1 Security Considerations in the Information System Development Life Cycle						x
NIST SP 800-64 Rev. 2 Security Considerations in the System Development Life Cycle						x
NIST SP 800-65 Integrating IT Security into the Capital Planning and Investment Control Process					x	

	Legal Security Requirements					
Reference Security Documents	E-Government Act	HSPD-7	HSPD-12	HIPAA	OMB Circular A-11	OMB Circular A-130, App. III
NIST SP 800-65 Rev. 1 DRAFT Recommendations for Integrating Information Security into the Capital Planning and Investment Control Process (CPIC)					x	
NIST SP 800-66 An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act Security Rule				x		
NIST SP 800-66 Rev 1 An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule				x		
NIST SP 800-68 Rev. 1 Guide to Securing Microsoft Windows XP Systems for IT Professionals						x
NIST SP 800-70 Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developer						x
NIST SP 800-70 Rev. 1 National Checklist Program for IT Products--Guidelines for Checklist Users and Developers						x
NIST SP 800-73 Rev 1 Integrated Circuit Card for Personal Identification Verification			x			
NIST SP 800-76 Biometric Data Specification for Personal Identity Verification			x			
NIST SP 800-78 Cryptographic Algorithms and Key Sizes for Personal Identity Verification			x			
NIST SP 800-78-1 Cryptographic Algorithms and Key Sizes for Personal Identity Verification						x
NIST SP 800-79-1 Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations			x			
NIST SP 800-82 DRAFT Guide to Industrial Control Systems (ICS) Security		x				
NIST SP 800-85A PIV Card Application and Middleware Interface Test Guidelines (SP 800-73 compliance)			x			

	Legal Security Requirements					
Reference Security Documents	E-Government Act	HSPD-7	HSPD-12	HIPAA	OMB Circular A-11	OMB Circular A-130, App. III
NIST SP 800-85B PIV Data Model Test Guidelines			x			
NIST SP 800-88 Guidelines for Media Sanitization						x
NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS)						x
NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS)		x				x
NIST SP 800-98 Guidelines for Securing Radio Frequency Identification (RFID) Systems		x		x		x

Appendix F.iv: Links to Lists of Threat Sources and Vulnerabilities

Type of Threat Source	Description	Characteristics

ADVERSARIAL
- Individual
  - Outsider
  - Insider
  - Trusted Insider
  - Privileged Insider
- Group
  - Ad hoc
  - Established
  - Organization
  - Nation-State
	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).	Capability, Intent, Targeting

ACCIDENTAL -Ordinary User -Privileged User/Administrator	Erroneous actions taken by individuals in the course of executing their everyday responsibilities.	Range of effects

STRUCTURAL
- IT Equipment
  - Storage
  - Processing
  - Communications
  - Display
  - Sensor
  - Controller
- Environmental Controls
  - Temperature/Humidity Controls
  - Power Supply
- Software
  - Operating System
  - Networking
  - General-Purpose Application
  - Mission-Specific Application
	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.	Range of effects

Type of Threat Source	Description	Characteristics
ENVIRONMENTAL - Natural or man-made disaster - Fire - Flood/Tsunami - Windstorm/Tornado - Hurricane - Earthquake - Bombing - Overrun - Unusual Natural Event (e.g., sunspots) - Infrastructure Failure/Outage - Telecommunications - Electrical Power	Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization. Note: Natural and man-made disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities housing mission-critical systems, making those systems unavailable for three weeks).	Range of effects

Table 4: Taxonomy of Threat Sources (NIST Special Publication 800-30 rev 1)

Vulnerability Information:

US-CERT Resources: http://www.us-cert.gov/related-resources/

National Vulnerability Database (NVD): http://web.nvd.nist.gov/view/vuln/search

Common Vulnerabilities and Exposures List (CVE): http://cve.mitre.org/about/

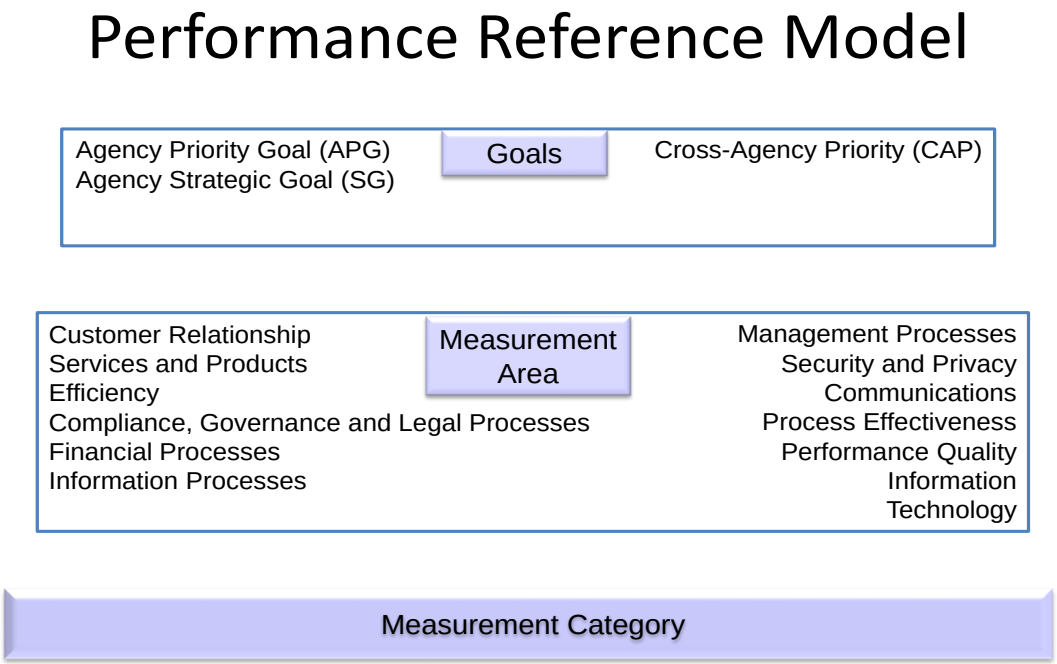
US-CERT list of vulnerabilities for specific CVEs: http://www.kb.cert.org/vuls/

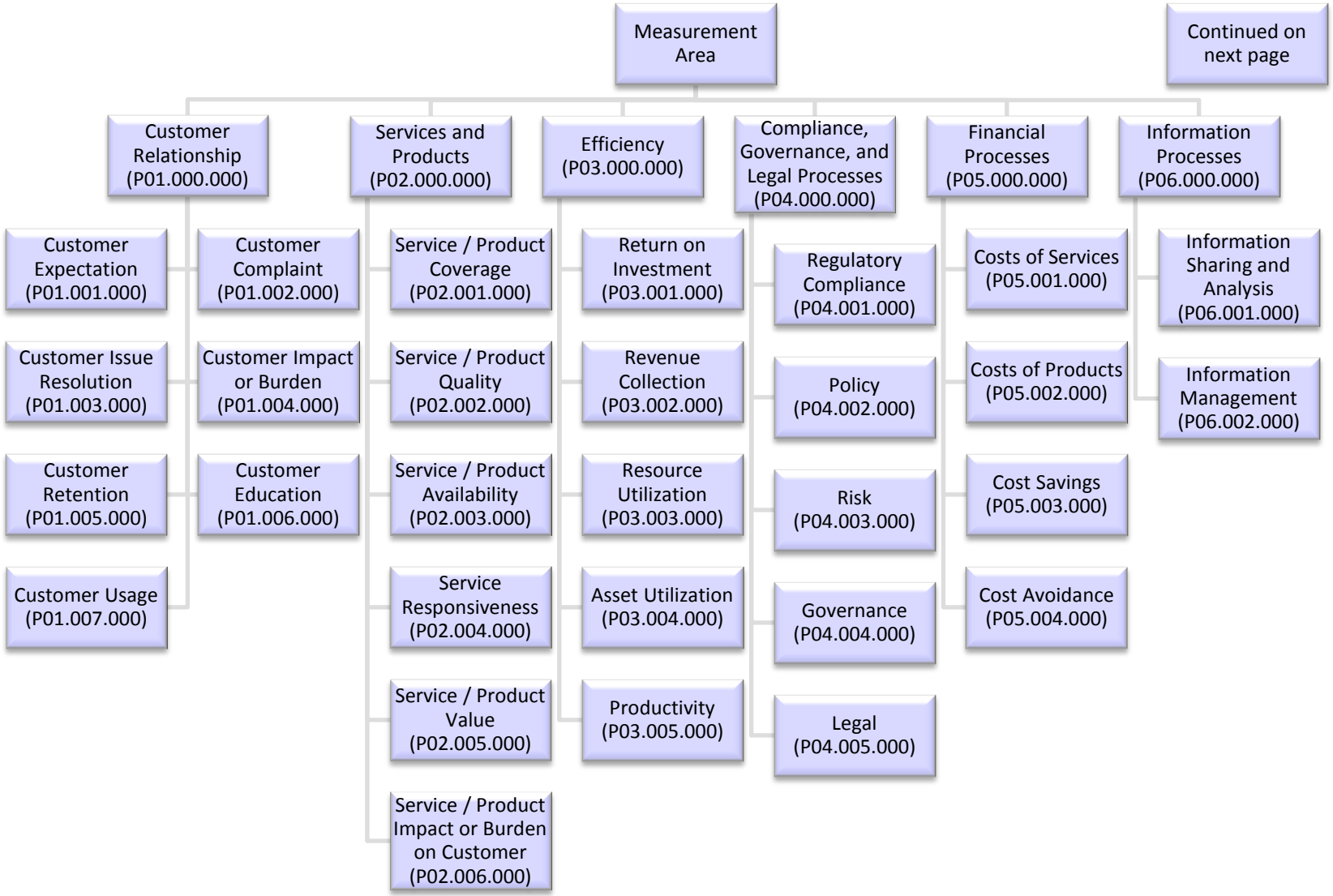
Open Vulnerability Assessment Language (OVAL): http://oval.mitre.org/

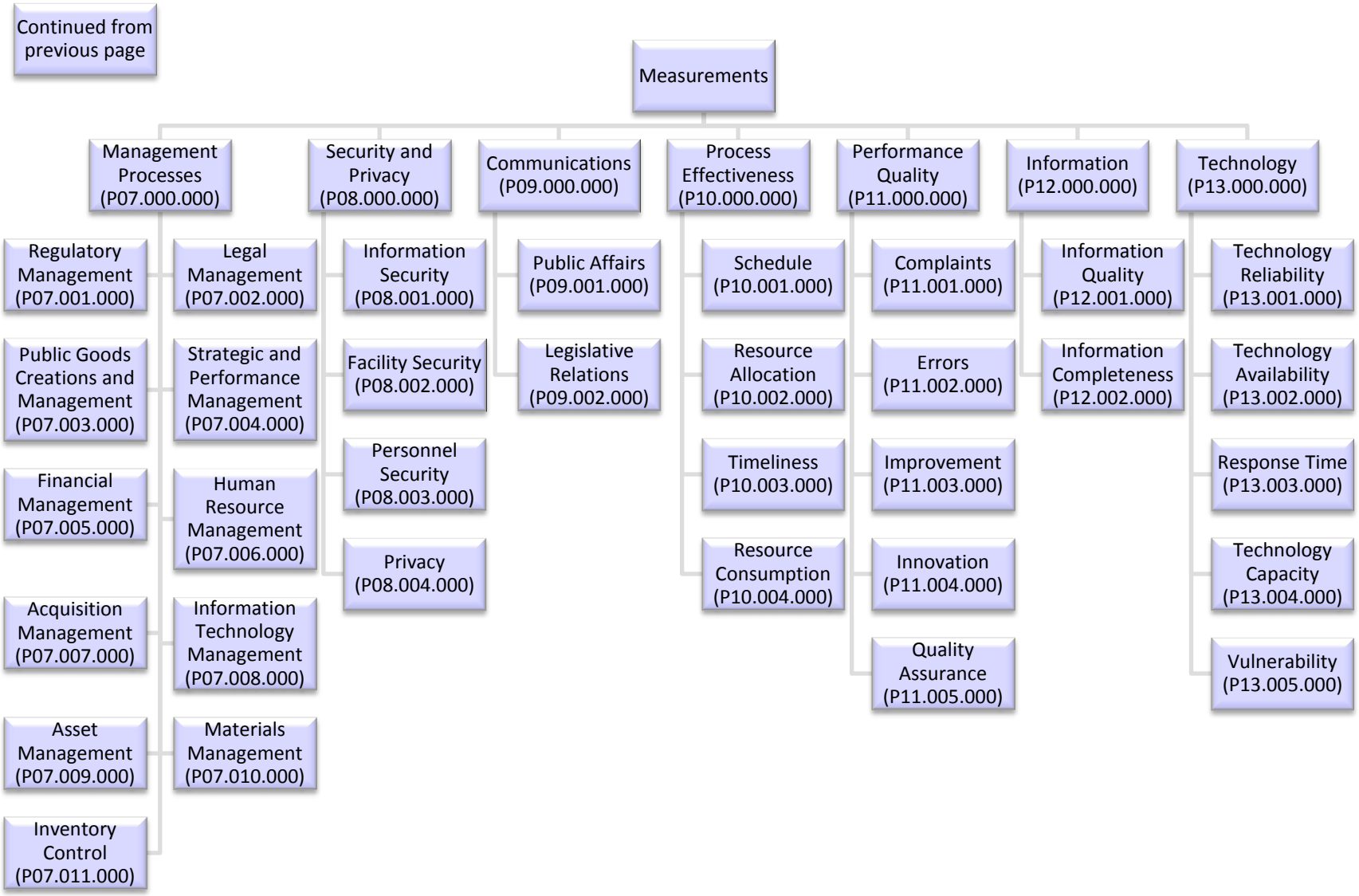
National Infrastructure Advisory Council's Vulnerability Disclosure Framework: http://www.dhs.gov/xlibrary/assets/vdwgreport.pdf

Appendix G: Performance Reference Model Taxonomy with Definitions

There are three areas to the Performance Reference Model. The first is the Goal. This enables grouping of investments and activities through a common and authoritative framework established by agencies in compliance with OMB direction and the GPRA Modernization Act. The second area of the Performance Reference Model is Measurement Area. This describes the manner in which the investment or activity supports the achievement of the supported performance element identified by the Agency Goal. The third area, Measurement Category, refines Measurement Area. Any Measurement Category may be applied to any Goal.




Measurement Area
Continued on next page
Customer Relationship (P01.000.000)
Services and Products (P02.000.000)
Efficiency (P03.000.000)
Compliance, Governance, and Legal Processes (P04.000.000)
Financial Processes (P05.000.000)
Information Processes (P06.000.000)
Customer Expectation (P01.001.000)
Customer Complaint (P01.002.000)
Customer Issue Resolution (P01.003.000)
Customer Impact or Burden (P01.004.000)
Customer Retention (P01.005.000)
Customer Education (P01.006.000)
Customer Usage (P01.007.000)
Service / Product Coverage (P02.001.000)
Service / Product Quality (P02.002.000)
Service / Product Availability (P02.003.000)
Service Responsiveness (P02.004.000)
Service / Product Value (P02.005.000)
Service / Product Impact or Burden on Customer (P02.006.000)
Return on Investment (P03.001.000)
Revenue Collection (P03.002.000)
Resource Utilization (P03.003.000)
Asset Utilization (P03.004.000)
Productivity (P03.005.000)
Regulatory Compliance (P04.001.000)
Policy (P04.002.000)
Risk (P04.003.000)
Governance (P04.004.000)
Legal (P04.005.000)
Costs of Services (P05.001.000)
Costs of Products (P05.002.000)
Cost Savings (P05.003.000)
Cost Avoidance (P05.004.000)
Information Sharing and Analysis (P06.001.000)
Information Management (P06.002.000)


Continued from previous page
Measurements
Management Processes (P07.000.000)
Security and Privacy (P08.000.000)
Communications (P09.000.000)
Process Effectiveness (P10.000.000)
Performance Quality (P11.000.000)
Information (P12.000.000)
Technology (P13.000.000)
Regulatory Management (P07.001.000)
Public Goods Creations and Management (P07.003.000)
Financial Management (P07.005.000)
Acquisition Management (P07.007.000)
Asset Management (P07.009.000)
Inventory Control (P07.011.000)
Legal Management (P07.002.000)
Strategic and Performance Management (P07.004.000)
Human Resource Management (P07.006.000)
Information Technology Management (P07.008.000)
Materials Management (P07.010.000)
Information Security (P08.001.000)
Facility Security (P08.002.000)
Personnel Security (P08.003.000)
Privacy (P08.004.000)
Public Affairs (P09.001.000)
Legislative Relations (P09.002.000)
Schedule (P10.001.000)
Resource Allocation (P10.002.000)
Timeliness (P10.003.000)
Resource Consumption (P10.004.000)
Complaints (P11.001.000)
Errors (P11.002.000)
Improvement (P11.003.000)
Innovation (P11.004.000)
Quality Assurance (P11.005.000)
Information Quality (P12.001.000)
Information Completeness (P12.002.000)
Technology Reliability (P13.001.000)
Technology Availability (P13.002.000)
Response Time (P13.003.000)
Technology Capacity (P13.004.000)
Vulnerability (P13.005.000)

Measurements

Code	Measurement Area	Measurement Category	Definition
P01.000.000	Customer Relationship		The Customer Relationship Measurement Area includes those Measurement Groupings used to categorize Measurement Indicators related to an agency's performance in handling relationships with its customers.
P01.001.000	Customer Relationship	Customer Expectation	Metrics regarding customer beliefs about a product or service prior to its initial use and that serve as standards or reference points against which the product or service is judged.
P01.002.000	Customer Relationship	Customer Complaint	Metrics that express dissatisfaction with a product or service, either orally or in writing, from an internal or external customer.
P01.003.000	Customer Relationship	Customer Issue Resolution	Metrics regarding actions or course of actions taken to address a customer complaint.
P01.004.000	Customer Relationship	Customer Impact or Burden	Metrics associated with difficulties encountered by a customer when accessing customer support services, including direct customer support and customer self-management.
P01.005.000	Customer Relationship	Customer Retention	Metrics related to the "lifetime" over which customers continue to use or purchase products and services offered. An example method of calculation for such a Performance Indicator is [(TotalNumberOfCustomers – NumberOfRepeatCustomers) / TotalNumberOfCustomers].
P01.006.000	Customer Relationship	Customer Education	Metrics related to purposeful, sustained and organized learning activities designed to impart attitudes, knowledge, or skills to customers or potential customers.
P01.007.000	Customer Relationship	Customer Usage	Metrics that express the degree to which a product or service is purchased or used by members of the total population of potential customers, including the frequency with which individual customers do so.
P02.000.000	Services and Products		The Customer Services and Products Measurement Category includes those Measurement Groupings used to categorize Measurement Indicators related to an agency's performance related to the extent to which intended customer populations are being provided desired services and products.

P02.001.000	Services and Products	Service / Product Coverage	Metrics regarding the extent to which a specific service or product is provided to its target customers. This may be expressed in terms of geographic areas or locations, populations (groups) or number of individuals to which provided.
P02.002.000	Services and Products	Service / Product Quality	Metrics expressing the degree to which a service or product provides the claimed or formally agreed level of service to the customer, e.g., is fit for intended purpose.
P02.003.000	Services and Products	Service / Product Availability	Metrics related to a service's or product's ability to provide its agreed function when required by its customer. Such metrics may include ones related to Reliability, Maintainability, Serviceability, Performance, Security, and Accessibility (e.g., Section 508 requirements).
P02.004.000	Services and Products	Service Responsiveness	Metrics related to the time that elapses from the invocation of a service until the service delivers the response sought by the customer.
P02.005.000	Services and Products	Service / Product Value	Metrics that express the perceived benefit (utility) of a service or product relative to its cost (real or perceived) as seen from the customer's point of view.
P02.006.000	Services and Products	Service / Product Impact or Burden on Customer	Metrics regarding demands placed on the customer of the service or product and having the effect of encumbering or impeding its use or placing undue demands on the customer, e.g., cognitive load, physical or perceptual challenge.
P03.000.000	Efficiency		The Efficiency Measurement Area of the PRM provides the highest-level organization of metric categories that express how well an agency is utilizing its resources.
P03.001.000	Efficiency	Return on Investment	Metrics that express the benefit derived from capital expended (investment), e.g., as the ratio of benefit to expenditure. These metrics may include ones based on different perspectives of investment such as return on assets.
P03.002.000	Efficiency	Revenue Collection	Metrics that express the efficiency of revenue collection, e.g., the ratio of revenue collected to some measure of the cost of collection. Cost measures may be expressed in financial terms or other measure of resource consumption.
P03.003.000	Efficiency	Resource Utilization	Metrics that express the benefit or value derived from the expenditure of resources such as capital and materiel.
P03.004.000	Efficiency	Asset Utilization	Metrics that express the benefit or value derived from the expenditure of fixed assets such as land, facilities, and equipment.
P03.005.000	Efficiency	Productivity	Metrics that express the benefit or value derived from the expenditure of personnel resources.
P04.000.000	Compliance, Governance, and Legal Processes		The Compliance, Governance, and Legal Measurement Category includes those Measurement Groupings used to categorize Measurement Indicators that express to how well an agency performs processes and activities related to these specific areas of concern.

P04.001.000	Compliance, Governance, and Legal Processes	Regulatory Compliance	Metrics expressing the effectiveness of agency processes or activities related to maintaining compliance with international, federal, state, local or tribal regulations. Does not include compliance with state or federal laws (see 3.1.5, Legal).
P04.002.000	Compliance, Governance, and Legal Processes	Policy	Metrics expressing the effectiveness of agency processes or activities related to conformance with international, federal, or agency policies.
P04.003.000	Compliance, Governance, and Legal Processes	Risk	Metrics expressing the effectiveness of agency processes or activities related to analyzing and mitigating risk.
P04.004.000	Compliance, Governance, and Legal Processes	Governance	Metrics expressing the effectiveness of agency processes or activities related to controls imposed on processes or activities.
P04.005.000	Compliance, Governance, and Legal Processes	Legal	Metrics expressing the effectiveness of agency processes or activities related to compliance with international, federal, or state law.
P05.000.000	Financial Processes		The Financial Processes Measurement Category includes those Measurement Groupings used to categorize Measurement Indicators related to the performance of agency financial processes and activities.
P05.001.000	Financial Processes	Costs of Services	Metrics expressing the effectiveness of agency processes or activities related to controlling direct and/or indirect total or per unit cost of services provided.
P05.002.000	Financial Processes	Costs of Products	Metrics expressing the effectiveness of agency processes or activities related to controlling direct and/or indirect total or per unit cost of the products provided.
P05.003.000	Financial Processes	Cost Savings	Metrics expressing the effectiveness of agency processes or activities related to reduction in direct and/or indirect total or per unit costs, used when actual year-over-year cost savings can be realized.
P05.004.000	Financial Processes	Cost Avoidance	Metrics expressing the effectiveness of agency processes or activities related to reduction in **additional** direct and/or indirect total or per unit costs, used when actual year-over-year cost savings cannot be realized because, for example, unit production rises while per unit costs fall.
P06.000.000	Information Processes		The Information Processes Measurement Category includes those Measurement Groupings used to categorize Measurement Indicators that address the performance of the agency's information-related processes and activities.

P06.001.000	Information Processes	Information Sharing and Analysis	Metrics that relate the degree to which processes and activities have improved the reuse of information produced by the agency.
P06.002.000	Information Processes	Information Management	Metrics expressing the effectiveness of management control processes and activities on the information produced by the agency.
P07.000.000	Management Processes		The Management Processes Measurement Category includes those Measurement Groupings used to categorize Measurement Indicators related to the performance of agency management processes and activities.
P07.001.000	Management Processes	Regulatory Management	Metrics expressing the effectiveness of processes or activities related to regulatory management.
P07.002.000	Management Processes	Legal Management	Metrics expressing the effectiveness of processes or activities related to legal management.
P07.003.000	Management Processes	Public Goods Creations and Management	Metrics expressing the effectiveness of processes or activities related to public goods creation and management.
P07.004.000	Management Processes	Strategic and Performance Management	Metrics expressing the effectiveness of processes or activities related to strategic and performance management.
P07.005.000	Management Processes	Financial Management	Metrics expressing the effectiveness of processes or activities related to financial management.
P07.006.000	Management Processes	Human Resource Management	Metrics expressing the effectiveness of processes or activities related to human resource management.
P07.007.000	Management Processes	Acquisition Management	Metrics expressing the effectiveness of processes or activities related to acquisition management.
P07.008.000	Management Processes	Information Technology Management	Metrics expressing of the effectiveness of processes or activities related to information technology management.
P07.009.000	Management Processes	Asset Management	Metrics expressing of the effectiveness of processes or activities related to asset management.
P07.010.000	Management Processes	Materials Management	Metrics expressing the effectiveness of processes or activities related to materials management, i.e., the management of the provisioning of physical components that are required inputs to processes and activities.
P07.011.000	Management Processes	Inventory Control	Metrics expressing the effectiveness of processes or activities related to the control of inventory.

P08.000.000	Security and Privacy		The Security and Privacy Measurement Category includes those Measurement Groupings used to categorize Measurement Indicators related to how well an agency performs processes and activities related to these areas of concern.
P08.001.000	Security and Privacy	Information Security	Metrics that express the effectiveness of processes and activities related to information security controls or compliance with federal information security requirements.
P08.002.000	Security and Privacy	Facility Security	Metrics that express the effectiveness of processes and activities related to facility security controls or compliance with federal facility security requirements.
P08.003.000	Security and Privacy	Personnel Security	Metrics that express the effectiveness of processes and activities related to personnel security controls or compliance with federal personnel security requirements.
P08.004.000	Security and Privacy	Privacy	Metrics that express the effectiveness of processes and activities related to information privacy controls or compliance with federal privacy requirements.
P09.000.000	Communications		The Communications Measurement Category includes those Measurement Groupings that express how well an agency performs processes and activities related to communications with stakeholders.
P09.001.000	Communications	Public Affairs	Metrics expressing the effectiveness of processes and activities related to communications with taxpayers and other stakeholders.
P09.002.000	Communications	Legislative Relations	Metrics expressing the effectiveness of processes and activities related to communications with Congress.
P10.000.000	Process Effectiveness		The Process Effectiveness Measurement Area includes those Measurement Groupings used to categorize Measurement Indicators related to effective execution of processes, activities, or tasks.
P10.001.000	Process Effectiveness	Schedule	Metrics related to the definition of, and adherence to, schedules.
P10.002.000	Process Effectiveness	Resource Allocation	Metrics related to the effectiveness with which resource use is optimized.
P10.003.000	Process Effectiveness	Timeliness	Metrics related to the time required to start a process, activity, or task after it is authorized to commence, and the time required to complete it.
P10.004.000	Process Effectiveness	Resource Consumption	Metrics related to the expenditure of personnel, materiel, or other resources during execution of a process, activity, or task.
P11.000.000	Performance Quality		The Performance Quality Measurement Area includes those Measurement Groupings used to categorize Measurement Indicators related to how well an agency satisfies general stakeholder and constituent needs.

P11.001.000	Performance Quality	Complaints	Metrics that express dissatisfaction with the agency, not specifically related to the delivery of services or products it provides customers.
P11.002.000	Performance Quality	Errors	Metrics related to agency deviations from accuracy or correctness.
P11.003.000	Performance Quality	Improvement	Metrics related to agency actions taken to better its capabilities.
P11.004.000	Performance Quality	Innovation	Metrics related to agency actions taken to promote innovation or exploit innovations.
P11.005.000	Performance Quality	Quality Assurance	Metrics related to systematic monitoring and evaluation of agency capabilities to maximize the probability that defined standards of quality are achieved.
P12.000.000	Information		The Information Measurement Category includes those Measurement Groupings used to categorize Measurement Indicators related to the fitness for purpose of information.
P12.001.000	Information	Information Quality	Metrics expressing the degree to which information set content is considered reliable for user's needs.
P12.002.000	Information	Information Completeness	Metrics expressing the degree to which information sets include the elements necessary to support user needs with sufficient confidence.
P13.000.000	Technology		The Technology Measurement Area includes those Measurement Groupings used to categorize Measurement Indicators related to the effectiveness of technology being employed by an agency.
P13.001.000	Technology	Technology Reliability	Metrics used to express the ability of a technology-based system, subsystem, assembly, or component to operate under defined conditions for a specified period of time.
P13.002.000	Technology	Technology Availability	Metrics used to express the proportion of time a technology-based system, subsystem, assembly, or component is in an operational state.
P13.003.000	Technology	Response Time	Metrics used to express the elapsed time from stimulus to response of technology-based systems, subsystems, assemblies, or components.
P13.004.000	Technology	Technology Capacity	Metrics used to express the ability of technology-based systems, subsystems, assemblies, or components, to operate under various load conditions, e.g., peak demand, sustained.
P13.005.000	Technology	Vulnerability	Metrics used to express the susceptibility of technology-based systems, subsystems, assemblies, or components, to external events that degrade, compromise, damage, or allow their unauthorized exploitation.

Goals (P00)				
Code	**GOAL TYPE**	**Goal Number**	**Agency Name**	**Goal Title**
P00.000.001	APG	001	Department of Agriculture	Further improve the high payment accuracy of the Supplemental Nutrition Assistance Program (SNAP). By September 30, 2013, USDA will improve the Supplemental Nutrition Assistance Program (SNAP) payment accuracy rate, which is at an all-time high of 96.2 percent.
P00.000.002	APG	002	Department of Agriculture	Assist rural communities to build and maintain prosperity through increased agricultural exports. By September 30, 2013, the U.S. Department of Agriculture (USDA) will expand U.S. agricultural exports to at least $150 billion to assist rural communities to build and maintain prosperity through increased agricultural exports.
P00.000.003	APG	003	Department of Agriculture	Accelerate the protection of clean, abundant water resources by implementing high impact targeted (HIT) practices through USDA's Forest Service, Natural Resource Conservation Service, and Farm Service Agency programs on 4 million acres within critical and/or impaired watersheds. By September 30, 2013, quantify improvements in water quality by developing and implementing an interagency outcome metric within 2-4 pilot watersheds.
P00.000.004	APG	004	Department of Commerce	Expand Broadband Service to Communities. By September 30, 2013, the Department will increase the nation's broadband infrastructure developed through the Broadband Technology Opportunities Program (BTOP) from 29,200 miles at the end of FY 2011 to 75,000 miles.
P00.000.005	APG	005	Department of Commerce	Advance Commercialization of New Technologies by Reducing Patent Application Pendency and Backlog. By September 30, 2013, the Department will reduce patent pendency for first action and for final actions from the end of FY 2011 levels of 28.0 and 33.7 months to 16.9 months and 30.1 months, as well as the patent backlog of 670,000 applications to 529,000 applications.
P00.000.006	APG	006	Department of Commerce	Expand Markets for U.S. Exporters. By September 30, 2013, the Department will increase the annual number of new markets that current U.S. exporters enter with U.S. and Foreign Commercial Service assistance by 7 percent, from 5,700 at the end of FY 2011 to 6,100.

P00.000.007	APG	007	Department of Commerce	Weather Ready Nation: Improve local weather warnings and lead times; By September 30, 2013, the Department will implement technology to improve local severe weather warnings, including improving flash flood warning lead time from 38 minutes at the end of FY 2011 to 45 minutes;
P00.000.008	APG	008	Department of the Interior	Identify vulnerable resources and implement coordinated adaptation strategies to mitigate risks of changing climate; By September 30, 2013, for 50 percent of the Nation, the Department of the Interior will identify resources that are particularly vulnerable to climate change and implement coordinated adaptation response actions.
P00.000.009	APG	009	Department of the Interior	Build the next generation of conservation and community leaders by supporting youth employment at the Department of the Interior. By September 30, 2013, the Department of Interior will maintain the increased level of employment of individuals between the ages of 15 to 25 that was achieved in FY2010 (35% increase in total youth employment over FY2009) to support the Department's mission of natural and cultural resource management.
P00.000.010	APG	010	Department of the Interior	Enable capability to increase the available water supply in the western states through conservation related programs to ensure adequate and safe water supplies. By September 30, 2013, the Department of the Interior will further enable the capability to increase the available water supply for agricultural, municipal, industrial, and environmental uses in the western United States through Reclamation water conservation programs to 730,000 acre-feet, cumulatively since 2009.
P00.000.011	APG	011	Department of the Interior	Improved production accountability, safety, and environmental protection of oil and gas operations through increased inspection of high-risk oil and gas production cases. By September 30, 2013 the Bureau of Land Management (BLM) will increase the completion of inspections of federal and Indian high risk oil and gas cases by 9 percent over FY 2011 levels, which is equivalent to covering as much as 95 percent of the potential high risk cases.
P00.000.012	APG	012	Department of the Interior	Reduce violent crime in Indian communities; By September 30, 2013, in addition to continued efforts at four targeted tribal reservations that have achieved reductions of at least 5% in violent criminal offenses, achieve significant reduction in violent criminal offenses of at least 5% within 24 months on two additional targeted tribal reservations by implementing a comprehensive strategy involving community policing, tactical deployment, and critical interagency and intergovernmental partnerships.

P00.000.013	APG	013	Department of the Interior	Increase the approved capacity for production of energy from domestic renewable resources to support a growing economy and protect our national interests while reducing our dependence on foreign oil and climate-changing greenhouse gas emissions; By September 30, 2013, increase approved capacity authorized for renewable (solar, wind, and geothermal) energy resources affecting Department of the Interior managed lands, while ensuring full environmental review, by at least 11,000 Megawatts.
P00.000.014	APG	014	Department of Justice	Better inform the Intelligence Community, thereby increasing the ability to protect Americans from terrorism and other threats to national security - both at home and abroad. By September 30, 2013, the FBI will increase by 6% the number of counterterrorism intelligence products shared with the U.S. Intelligence Community, state and local Law Enforcement Community partners, and foreign government agencies.
P00.000.015	APG	015	Department of Justice	Reduce Gang Violence. By September 30, 2013, in conjunction with state and local law enforcement agencies, reduce the number of violent crimes attributed to gangs by achieving 5% increases on 3 key indicators: youths who exhibited a change in targeted behaviors as a result of participation in DOJ gang prevention program; coordination on gang investigations among Federal, State, and local law enforcement, resulting in gang arrests; intelligence products produced in support of Federal, State, and local investigations that are focused on gangs posing a significant threat to communities.
P00.000.016	APG	016	Department of Justice	Protect those most in need of help - with special emphasis on child exploitation and civil rights. By September 30, 2013, working with state and local law enforcement agencies, protect potential victims from abuse and exploitation by achieving a 5% increase for 3 sets of key indicators: open investigations concerning non-compliant sex offenders, sexual exploitation of children, and human trafficking; matters/investigations resolved concerning sexual exploitation of children and human trafficking; number of children depicted in child pornography that are identified by the FBI.

P00.000.017	APG	017	Department of Justice	Protect the American people from financial and healthcare fraud. In order to efficiently and effectively address financial fraud and healthcare fraud, by the end of FY 2013, increase by 5 percent over FY 2011 levels, the number of investigations completed per Department of Justice attorney working on financial fraud and healthcare fraud cases; additionally, institute a system for tracking compliance by corporate defendants with the terms of judgments, consent decrees, settlements, deferred prosecution agreements, and non-prosecution agreements.
P00.000.018	APG	018	Department of Labor	Reduce worker fatalities. By September 30, 2013, reduce worker fatalities resulting from common causes by two percent in Occupational Safety and Health Administration-covered workplaces, and worker fatality rates in mining by five percent per year based on a rolling five-year average.
P00.000.019	APG	019	Department of Labor	Reduce time lost to injury or illness for federal workers. By September 30th, 2013 create a model return-to-work program to reduce lost production day rates by one percent per year and reduce total and lost time injury and illness rates by at least four percent per year.
P00.000.020	APG	020	Department of Labor	Improve opportunities for America's workers to succeed in a knowledge-based economy through industry-recognized credentials. By September 30, 2013, increase the percent of training program exiters who earn industry-recognized credentials by 10 percent;
P00.000.021	APG	021	Department of Labor	Improve the Transition Assistance Program (TAP) to better support veterans. By the end of FY 2013, the Transition Assistance Program (TAP), with redesigned and improved curriculum, will be fully implemented at all 188 domestic and 50 international sites.
P00.000.022	APG	022	Department of State and USAID	With mutual accountability, assistance from the United States and the international community will continue to help improve the Government of the Islamic Republic of Afghanistan's (GIRoA) capacity to meet its goals and maintain stability. Bonn Conference commitments call on GIRoA to transition to a sustainable economy, namely improve revenue collection, increase the pace of economic reform, and instill a greater sense of accountability and transparency in all government operations; Strengthen Afghanistan's ability to maintain stability and development gains through transition. By September 30, 2013, U.S. Government assistance delivered will help the Afghan government increase domestic revenue level from sources such as customs and electrical tariffs from 10% to 12% of GDP.

P00.000.023	APG	023	Department of State and USAID	Through our more than 200 diplomatic missions overseas, the Department of State will promote U.S. exports in order to help create opportunities for U.S. businesses. By September 30, 2013, our diplomatic missions overseas will increase the number of market-oriented economic and commercial policy activities and accomplishments by 15 percent.
P00.000.024	APG	024	Department of State and USAID	Strengthen local civil society and private sector capacity to improve aid effectiveness and sustainability, by working closely with our implementing partners on capacity building and local grant and contract allocations. By September 30, 2013, USAID will expand local development partners from 746 to 1200.
P00.000.025	APG	025	Department of State and USAID	Strengthen diplomacy and development by leading through civilian power. By September 30, 2013, the State Department and USAID will reduce vacancies in high priority positions overseas to 0% and 10 % respectively and will reduce instances of employees not meeting language standards to 24% and 10% respectively.
P00.000.026	APG	026	Department of State and USAID	Advance progress toward sustained and consolidated democratic transitions in Egypt, Jordan, Lebanon, Morocco, Tunisia, Libya, Bahrain, Yemen, Iran, Syria, and West Bank/Gaza. By September 30, 2013, support continued progress toward or lay the foundations for transitions to accountable electoral democracies in 11 countries in the Middle East and North Africa (MENA) that respect civil and political liberties and human rights.
P00.000.027	APG	027	Department of State and USAID	Advance low emissions climate resilient development. Lay the groundwork for climate-resilient development, increased private sector investment in a low carbon economy, and meaningful reductions in national emissions trajectories through 2020 and the longer term. By the end of 2013, U.S. assistance to support the development and implementation of Low Emission Development Strategies (LEDS) will reach 20 countries (from a baseline of 0 in 2010). This assistance will be strategically targeted and will result in strengthened capacity for and measureable progress on developing and implementing LEDS by the end of the following year.
P00.000.028	APG	028	Department of State and USAID	Increase food security in Feed the Future initiative countries in order to reduce prevalence of poverty and malnutrition. By the end of the FY 2013, agricultural profitability will improve, on average, by 15% among FTF beneficiary farmers, and one million children under age 2 will experience improved nutrition due to increased access to and utilization of nutritious foods (prevalence of receiving a minimum acceptable diet).

P00.000.029	APG	029	Department of State and USAID	By September 30, 2013, the Global Health Initiative (GHI) will support the creation of an AIDS-free generation, save the lives of mothers and children, and protect communities from infectious diseases by: a) decreasing incident HIV infections in the President's Emergency Plan for AIDS Relief (PEPFAR)-supported Sub-Saharan African countries by more than 20%; b) reducing the all-cause mortality rate for children under five by 4.8 deaths/1,000 live births in USAID priority countries; c) increasing the percent of births attended by a skilled doctor, nurse, or midwife by 2.1 % in USAID priority countries; and d) increasing the number of people no longer at risk for lymphatic filariasis (in the target population) from 7.7 million to 63.7 million in USAID-assisted countries;
P00.000.030	APG	030	Department of the Treasury	Increase Electronic Transactions with the Public to Improve Service, Prevent Fraud, and Reduce Costs. By September 30, 2013, Treasury will: increase the percentage of electronic benefit payments from 84 percent in FY 2011 to 93 percent in FY 2013; increase the percentage of electronic collections from 86 percent in FY 2011 to 93 percent in FY 2013; increase the individual e-File rate from 76.9 percent in FY 2011 to 80 percent in FY 2013; and decrease the volume of paper savings bond sale transactions by 99 percent.
P00.000.031	APG	031	Department of the Treasury	Increase voluntary tax compliance. By September 30, 2013, Treasury will increase voluntary tax compliance from 83.1 to 86 percent;
P00.000.032	APG	032	Office of Personnel Management	Ensure high quality Federal employees. By September 30, 2013, increase Federal manager satisfaction with applicant quality (as an indicator of hiring quality) from 7.7 to 8.3 on a scale of 1 to 10, while continually improving timeliness, applicant satisfaction, and other hiring process efficiency and quality measures.
P00.000.033	APG	033	Office of Personnel Management	Maintain speed of national security background investigations. Through September 30, 2013, maintain a 40 day or less average completion time for the fastest 90% of initial national security investigations.
P00.000.034	APG	034	Office of Personnel Management	Reduce Federal retirement processing time. By July 31, 2013, Retirement Services will have eliminated its case backlog so that 90 percent of all claims will be adjudicated within 60 days.

P00.000.035	APG	035	Office of Personnel Management	Improve performance culture in the five GEAR pilot agencies to inform the development of government-wide policies. By September 30, 2013, employee responses to the annual Employee Viewpoint Survey in each of 5 agencies participating in a performance culture pilot project will increase by 5 percent or greater on the results-oriented culture index and the conditions for employee engagement index, using 2011 survey results as the baseline.
P00.000.036	APG	036	Office of Personnel Management	Increase health insurance choices for Americans. By October 1, 2013 expand competition within health insurance markets by ensuring participation of at least 2 multi-state health plans in State Affordable Insurance Exchanges.
P00.000.037	APG	037	Social Security Administration	Faster hearing decisions; By the end of FY 2013, we will reduce the average time for a hearing decision from 345 days at the end of FY 2011 to 270 days.
P00.000.038	APG	038	Social Security Administration	Reduce Supplemental Security Income (SSI) overpayments; By the end of FY 2013*, we will increase our SSI overpayment accuracy rate from 93.3 percent at the end of FY 2010 to 95 percent. * FY 2013 data will not be available until April 2014.
P00.000.039	APG	039	Social Security Administration	Increase use of our online services; By the end of FY 2013, we will increase our online filing rates from 36 percent at the end of FY 2011 to 48 percent.
P00.000.040	APG	040	Department of Veterans Affairs	Improve accuracy and reduce the amount of time it takes to process Veterans' disability benefit claims. By September 30, 2013, reduce the Veterans' disability claims backlog to 40 percent from 60.2 percent while achieving 90 percent rating accuracy up from 83.8 percent, in pursuit of eliminating the Veterans' disability claims backlog (defined as claims pending more than 125 days) and improving rating accuracy to 98 percent by 2015.
P00.000.041	APG	041	Department of Veterans Affairs	House 24,400 additional homeless Veterans and reduce the number of homeless Veterans to 35,000; By September 2013, working in conjunction with the Interagency Council on Homelessness (ICH), HUD and VA will also assist homeless Veterans in obtaining employment, accessing VA services, and securing permanent supportive housing, with a long-range goal of eliminating homelessness among Veterans by 2015.
P00.000.042	APG	042	Department of Veterans Affairs	Improve awareness of VA services and benefits by increasing the timeliness and relevance of on-line information available to Veterans, Service members and eligible beneficiaries. By September 30, 2013, increase the number of registered eBenefits users from 1.0 million to 2.5 million.
P00.000.043	APG	043	National Science Foundation	Develop a diverse and highly qualified science and technology workforce. By September 30, 2013, 80% of institutions funded through NSF undergraduate programs document the extent of use of proven instructional practices.

P00.000.044	APG	044	National Science Foundation	Increase the number of entrepreneurs emerging from university laboratories. By September 30, 2013, 80 percent of teams participating in the Innovation Corps program will have tested the commercial viability of their product or service.
P00.000.045	APG	045	National Science Foundation	Increase opportunities for research and education through public access to high value digital products of NSF funded research. By September 30, 2013, NSF will have established policies for public access to high value data and software in at least two data intensive scientific domains.
P00.000.046	APG	046	Environmental Protection Agency	Improve public health protection for persons served by small drinking water systems by strengthening the technical, managerial, and financial capacity of those systems. By September 30, 2013, EPA will engage with twenty states to improve small drinking water system capability through two EPA programs, the Optimization Program and/or the Capacity Development Program.
P00.000.047	APG	047	Environmental Protection Agency	Increase transparency and reduce burden through E-reporting; By September 30, 2013, develop a plan to convert existing paper reports into electronic reporting, establish electronic reporting in at least four key programs, and adopt a policy for including electronic reporting in new rules.
P00.000.048	APG	048	Environmental Protection Agency	Clean up contaminated sites and make them ready for use. By September 30, 2013, an additional 22,100 sites will be ready for anticipated use.
P00.000.049	APG	049	Environmental Protection Agency	Reduce greenhouse gas emissions from cars and trucks. Through September 30, 2013, EPA in coordination with DOT's fuel economy standards program will be implementing vehicle and truck greenhouse gas standards that are projected to reduce GHG emissions by 1.2 billion metric tons and reduce oil consumption by about 98 billion gallons over the lifetime of the affected vehicles and trucks.
P00.000.050	APG	050	Environmental Protection Agency	Improve, restore, or maintain water quality by enhancing nonpoint source program accountability, incentives, and effectiveness. By September 30, 2013, 50% of the states will revise their nonpoint source program according to new Section 319 grant guidelines that EPA will release in November 2012;
P00.000.051	APG	051	Department of Transportation	Reduce risk of aviation accidents. By September 30, 2013, reduce aviation fatalities by addressing risk factors both on the ground and in the air. Commercial aviation (i.e. airlines): Reduce fatalities to no more than 7.4 per 100 million people on board; General aviation (i.e. private planes): Reduce fatal accident rate per 100,000 flight hours to no more than 1.06.

P00.000.052	APG	052	Department of Transportation	Improve the Nation's intercity passenger rail service. By September 30, 2013, initiate construction on all 7 high speed rail corridors and 36 individual high speed rail projects.
P00.000.053	APG	053	Department of Transportation	Reduce roadway fatalities. By September 30, 2013, reduce the rate of roadway fatalities per miles traveled from 1.25 per 100 million miles in 2008 to 1.03 per 100 million miles in 2013.
P00.000.054	APG	054	Department of Transportation	Air traffic control systems can improve the efficiency of airspace. By September 30, 2013, replace a 40-year old computer system serving 20 air traffic control centers with a modern, automated system that tracks and displays information on high altitude planes.
P00.000.055	APG	055	Department of Homeland Security	Improve the efficiency of the process to detain and remove criminal aliens from the United States; By September 30, 2013, reduce the average length of stay in immigration detention of all convicted criminal aliens prior to their removal from the country by 5%.
P00.000.056	APG	056	Department of Homeland Security	Ensure resilience to disasters by strengthening disaster preparedness and response capabilities; By September 30, 2013, every state will have a current, DHS-certified threat, hazard, identification and risk assessment (THIRA).
P00.000.057	APG	057	Department of Homeland Security	Strengthen aviation security counterterrorism capabilities by using intelligence driven information and risk-based decisions. By September 30, 2013, TSA will expand the use of risk-based security initiatives to double the number of passengers going through expedited screening at airports, thereby enhancing the passenger experience.
P00.000.058	APG	058	Small Business Administration	Process Disaster Assistance applications efficiently; By September 30, 2013, increase the use of the Disaster Assistance electronic loan application (ELA) by 50%.
P00.000.059	APG	059	Small Business Administration	Expand access to long term capital; From FY 2012 through September 30, 2013, commit at least $4.3 billion of capital via the Small Business Investment Company program in order to facilitate access to capital for high growth companies and enhance job creation and retention by these companies.
P00.000.060	APG	060	Small Business Administration	Process business loans as efficiently as possible; By September 30, 2013, increase the use of paperless processing in the 7(a) program from 72% to 90% and in the 504 program from 55% to 75% to improve the efficiency, effectiveness, and level of service in its business loan programs.

P00.000.061	APG	061	Small Business Administration	Increase small business participation in government contracting. By September 30, 2013, SBA will increase small business participation in federal government contracting to meet the government wide goal that 23 percent of all prime contracting dollars go to small businesses, and continue to ensure that the benefits of SBA's small business contracting programs flow to the intended recipients;
P00.000.062	APG	062	Department of Health and Human Services	Improve the quality of early childhood education; By September 30, 2013,improve the quality of early childhood programs for low-income children through implementation of the Quality Rating and Improvement Systems (QRIS) in the Child Care and Development Fund (CCDF), and through implementation of the Classroom Assessment Scoring System (CLASS: Pre-K) in Head Start.
P00.000.063	APG	063	Department of Health and Human Services	Improve patient safety; By September 30, 2013,reduce the national rate of healthcare-associated infections (HAIs) by demonstrating significant, quantitative and measurable reductions in hospital-acquired central line-associated bloodstream infections (CLABSI) and catheter-associated urinary tract infections (CAUTI).
P00.000.064	APG	064	Department of Health and Human Services	Increase the number of health centers certified as Patient Centered Medical Homes (PCMH). By September 30, 2013, the quality of care provided by health centers will be improved by increasing the proportion of health centers that are nationally recognized as Patient Centered Medical Homes (PCMH) from 1% to 25%.
P00.000.065	APG	065	Department of Health and Human Services	Reduce cigarette smoking. By December 31, 2013, reduce annual adults' cigarette consumption in the United States from 1,281 cigarettes per capita to 1,062 cigarettes per capita, which represents a 17.1% decrease from the 2010 baseline.
P00.000.066	APG	066	Department of Health and Human Services	Reduce foodborne illness in the population. By December 31, 2013, decrease the rate of Salmonella Enteritidis (SE) illness in the population from 2.6 cases per 100,000 (2007-2009 baseline) to 2.1 cases per 100,000.
P00.000.067	APG	067	Department of Health and Human Services	Improve health care through meaningful use of health information technology. By September 30, 2013, increase the number of eligible providers who receive an incentive payment from the CMS Medicare and Medicaid EHR Incentive Programs for the successful adoption or meaningful use of certified EHR technology to 140,000.
P00.000.068	APG	068	National Aeronautics and Space Administration	Use the Mars Science Laboratory Curiosity Rover to explore and quantitatively assess a local region on the surface of Mars as a potential habitat for life, past or present. By September 30, 2013, NASA will assess the biological potential of at least one target environment on Mars by obtaining chemical and/or mineralogical analysis of multiple samples of its surface.

P00.000.069	APG	069	National Aeronautics and Space Administration	Develop the Nation's next generation Human Space Flight (HSF) system to allow for travel beyond low Earth orbit (LEO). By September 30, 2013, NASA will finalize cross-program requirements and system definition to ensure that the first test flight of the Space Launch System (SLS) and Multi-Purpose Crew Vehicle (MPCV) programs is successfully achieved at the end of 2017 in an efficient and cost effective way.
P00.000.070	APG	070	National Aeronautics and Space Administration	Sustain operations and full utilization of the International Space Station (ISS). By the end of FY 2013, NASA will complete at least three flights delivering research and logistics hardware to the ISS by U.S.-developed cargo delivery systems.
P00.000.071	APG	071	National Aeronautics and Space Administration	Enable bold new missions and make new technologies available to Government agencies and U.S. industry. By September 30, 2013, document the maturation of new technologies by completing 4,065 technology-related products, including patents, licenses, and mission use agreements.
P00.000.072	APG	072	Department of Housing and Urban Development	Prevent foreclosures. By September 30, 2013, assist 700,000 homeowners who are at risk of losing their homes due to foreclosure.
P00.000.073	APG	073	Department of Housing and Urban Development	Reducing homelessness. By September 30 2013, in partnership with the VA, reduce the number of homeless Veterans to 35,000 by serving 35,500 additional homeless veterans. HUD is also committed to making progress towards reducing family and chronic homelessness and is working towards milestones to allow for tracking of these populations.
P00.000.074	APG	074	Department of Housing and Urban Development	Improve program effectiveness by awarding funds fairly and quickly. By September 30, 2013, HUD will improve internal processes to ensure that we can obligate 90 percent of NOFA programs within 180 calendar days from budget ensuring that America's neediest families have the shelter and services they need, when they need them to enable the timely obligation and subsequent disbursement of funds will positively impact the agency's ability to achieve all of our priority goals.
P00.000.075	APG	075	Department of Housing and Urban Development	Reduce vacancy rates. By September 30, 2013, reduce average residential vacancy rate in 70% of the communities hardest hit by the foreclosure crisis relative to comparable areas.

P00.000.076	APG	076	Department of Housing and Urban Development	Increase the energy efficiency and health of the nation's housing stock; By September 30, 2013, HUD will enable a total of 159,000 cost effective energy efficient or healthy housing units, as a part of a joint HUD-DOE goal of 520,000in 2012-2013 and a total goal of 1.2 million units from 2010 through 2013.
P00.000.077	APG	077	Department of Housing and Urban Development	Preserve affordable rental housing. By September 30, 2013, preserve affordable rental housing by continuing to serve 5.4M families and serve an additional 84,500 families through HUD's affordable rental housing programs.
P00.000.078	APG	078	Department of Energy	Make solar energy as cheap as traditional sources of electricity. By the end of the decade, drive the cost of solar electricity down to: $1/W at utility scale; $1.25/W at commercial scale; and $1.50/W at residential scale. By December 2013, demonstrate a prototype thin film or film silicon module with an efficiency of greater than 21% and a balance-of-system with a 50% reduction in the permitting and installation costs to $1.50/W.
P00.000.079	APG	079	Department of Energy	Reduce consumer energy use and costs for household appliances. By December 31, 2013, issue at least 9 new energy conservation standards to deliver net consumer savings of hundreds of billions of dollars over 30 years and require efficient products across domestic and international manufacturers.
P00.000.080	APG	080	Department of Energy	Save low-income families money and energy through weatherization retrofits. From FY2010 through FY2013, in collaboration with HUD, enable the cost-effective energy retrofits of a total of 1.2 million housing units, of which more than 75% are low income.
P00.000.081	APG	081	Department of Energy	Maintain the U.S. nuclear weapons stockpile and dismantle excess nuclear weapons to meet national nuclear security requirements as assigned by the President through the Nuclear Posture Review. Each year through 2013 and into the future, maintain 100% of warheads in the stockpile that are safe, secure, reliable, and available to the President for deployment.
P00.000.082	APG	082	Department of Energy	Make significant progress toward securing the most vulnerable nuclear materials worldwide within four years. By December 31, 2013, remove or dispose of a cumulative total of4,353 kg of vulnerable nuclear material (highly enriched uranium and plutonium), and complete material protection, control and accounting (MPC& A) upgrades on a cumulative total of229 buildings containing weapons usable material;
P00.000.083	APG	083	Department of Energy	Reduce the Department's Cold War legacy environmental footprint. By September 30, 2013, achieve a 71% reduction in DOE's cold war environmental footprint.

P00.000.084	APG	084	Department of Energy	Reduce the cost of batteries for electric drive vehicles to help increase the market for Plug-In Hybrids and All Electric Vehicles and thereby reduce petroleum use and greenhouse gas emissions. By October 2013, demonstrate a prototype Plug-In Hybrid battery technology that is capable of achieving a cost of $400/kWhr (useable energy) during high volume manufacturing (100,000 packs per year) compared to a 2008 baseline of $1000/kWhr.
P00.000.085	APG	085	Department of Energy	Prioritization of scientific facilities to ensure optimal benefit from Federal investments. By September 30, 2013, formulate a 10-year prioritization of scientific facilities across the Office of Science based on (1) the ability of the facility to contribute to world-leading science, (2) the readiness of the facility for construction, and (3) an estimated construction and operations cost of the facility.
P00.000.086	APG	086	Department of Education	Improve learning by ensuring that more students have an effective teacher. By September 30, 2013, at least 500 school districts will have comprehensive teacher and principal evaluation and support systems and the majority of states will have statewide requirements for comprehensive teacher and principal evaluation and support systems.
P00.000.087	APG	087	Department of Education	Demonstrate progress in turning around the nation's lowest-performing schools. By September 30, 2013, 500 of the nation's persistently lowest-achieving schools will have demonstrated significant improvement and will have served as potential models for future turnaround efforts.
P00.000.088	APG	088	Department of Education	Prepare all students for college and career. By September 30, 2013, all states will adopt internationally-benchmarked college-and career-ready standards.
P00.000.089	APG	089	Department of Education	Make informed decisions and improve instruction through the use of data. By September 30, 2013, all states and territories will implement comprehensive statewide longitudinal data systems.
P00.000.090	APG	090	Department of Education	Improve outcomes for all children from birth through third grade. By September 30, 2013, at least nine states will implement a high-quality plan to collect and report disaggregated data on the status of children at kindergarten entry.
P00.000.091	APG	091	Department of Education	Improve students' ability to afford and complete college. By September 30, 2013, the Department will develop a college scorecard designed to improve consumer decision-making and transparency about affordability for students and borrowers by streamlining information on all degree-granting institutions into a single, comparable, and simplified format, while also helping all states and institutions develop college completion plans.

P00.000.092	APG	092	Department of Defense	Improve the care and transition of Wounded, Ill, and Injured (WII) Warriors; By September 30, 2013, DOD will: 1) increase the use of Recovery Care Coordinators and ensure WII Service members have active recovery plans; 2) improve effectiveness of behavioral health programs and ensure all Service members complete quality post-deployment health screenings; and 3) accelerate the transition of WII Service members into veteran status by reducing the processing time required for disability evaluation boards;
P00.000.093	APG	093	Department of Defense	Improve energy performance. By September 30, 2013, DOD will: 1) improve its facility energy performance by reducing average building energy intensity by 24 percent from the 2003 baseline of 116,134 BTUs per gross square foot, and producing or procuring renewable energy equal to 13 percent of its annual electric energy usage; and 2) improve its operational energy performance by establishing an operational energy baseline with all available data on fuel use; developing a plan for remediating data gaps; funding and implementing a comprehensive data plan; establishing and executing operational energy performance targets based on this comprehensive data for each Military Service and relevant agency.
P00.000.094	APG	094	Department of Defense	Improve cybersecurity compliance. By September 30, 2013, DoD will attain a passing score on a comprehensive cybersecurity inspection that assesses compliance with technical, operational, and physical security standards, on an overwhelming majority of inspected military cyberspace organizations resulting in improved hardening and cyber defense.
P00.000.095	APG	095	Department of Defense	Reform the DOD acquisition process; By September 30, 2013, DoD will improve its acquisition process by ensuring that: 100 percent of Acquisition Category (ACAT) 1 programs going through Milestone A decision reviews will present an affordability analysis; 100 percent of ACAT 1 programs going through milestone decision reviews will present a competitive strategy; The average cycle time for Major Defense Acquisition Programs (MDAPs) will not increase by more than 5% from the Acquisition Program Baseline; The annual number of MDAP breaches - significant or critical cost overruns for reasons other than approved changes in quantity - will be zero; and DOD will increase the amount of contract obligations that are competitively awarded to 60 percent in FY 2012 and 61 percent in FY 2013.
P00.000.096	APG	096	Department of Defense	Improve audit readiness. By September 30, 2013, DoD will improve its audit readiness on the Statement of Budgetary Resources for Appropriations Received from 80 to 100 percent.

P00.000.097	APG	097	General Services Administration	Manage customer agency real estate portfolio needs in a cost-effective and environmentally sustainable manner. By September 30, 2013, GSA will complete and begin implementation of Customer Portfolio Plans (CPPs) with six agencies to identify opportunities and develop action plans to optimize their real estate portfolios' through reducing space, improving utilization and leveraging market opportunities to reduce costs. The three portfolio plans completed in FY11 identified future real estate opportunities which will result in millions of dollars in savings;
P00.000.098	APG	098	General Services Administration	GSA will increase the sustainability of the Federal supply chain by increasing the sale of green product and service offerings to 5 percent of total business volume; By September 30, 2013 GSA will increase the availability of green product and service offerings by 10 percent relative to its total inventory.
P00.000.099	APG	099	General Services Administration	Drive greater transparency and openness in government. By September 30, 2013, GSA will develop at least 10 new innovative, cost effective information technology solutions that increase government openness, including solutions to serve businesses with one-stop access to federal services, provide the public information about federal performance, engage the public in providing expertise on specific problems to Federal agencies, provide effective registration and management of government web sites, and streamline and leverage security assessments of innovative cloud computing products and solutions.
P00.000.100	APG	100	Army Corps of Engineers - Civil Works	Reduce the Nation's risk of flooding that places individuals at risk of injury or loss of life and damages property. By 30 September 2013, reduce at least 10 Dam Safety classification ratings, conduct at least 600 levee risk screenings, and improve the condition rating for at least 15 high consequence projects that have failed or have inadequate condition ratings.
P00.000.101	APG	101	Army Corps of Engineers - Civil Works	Aquatic Ecosystem Restoration. By 30 September 2013, the Corps will: Show progress through completion of identified study, design, and construction activities that will contribute to a long-term goal of improved ecological conditions in the Great Lakes Basin, the Everglades, and Columbia River basin, consistent with the Federal restoration strategies developed for each unique ecosystem.
P00.000.102	APG	102	Army Corps of Engineers - Civil Works	Improve the current operating performance and asset reliability of Hydropower plants in support of Executive Order 13514. By 30 September 2013, the Corps, Department of Energy Power Marketing Administrations (PMA), and PMA preference customers will implement sub-agreements which will provide funds to accomplish major maintenance and/or major rehabilitation on existing power plants.

P00.000.103	APG	103	Army Corps of Engineers - Civil Works	Help facilitate commercial navigation by providing safe, reliable, highly cost-effective, and environmentally-sustainable waterborne transportation systems. Through 30 September 2013, limit annual lock closures due to mechanical failures of main lock chambers on high and moderate use waterways to no more than 46 for closures lasting more than 1 day and no more than 26 for closures lasting more than one week.
P00.000.201	CAP	001		Real Property
P00.000.202	CAP	002		Energy Efficiency
P00.000.203	CAP	003		Improper Payments
P00.000.204	CAP	004		Data Center Consolidation
P00.000.205	CAP	005		Closing Skills Gaps
P00.000.206	CAP	006		Cybersecurity
P00.000.207	CAP	007		Exports
P00.000.208	CAP	008		Science, Technology, Engineering, and Math (STEM) Education
P00.000.209	CAP	009		Broadband
P00.000.210	CAP	010		Entrepreneurship and Small Business
P00.000.211	CAP	011		Veteran Career Readiness
P00.000.212	CAP	012		Strategic Sourcing
P00.000.213	CAP	013		Job Training
P00.000.214	CAP	014		Sustainability
P00.000.401	SG	001	Environmental Protection Agency	Cleaning Up Communities and Advancing Sustainable Development
P00.000.402	SG	002	Environmental Protection Agency	Taking Action on Climate Change and Improving Air Quality
P00.000.403	SG	003	Environmental Protection Agency	Protecting America's Waters
P00.000.404	SG	004	Environmental Protection Agency	Ensuring the Safety of Chemicals and Preventing Pollution

P00.000.405	SG	005	Environmental Protection Agency	Enforcing Environmental Laws
P00.000.407	SG	007	Department of Education	Postsecondary Education, Career-Technical Education, and Adult Education. Increase college access, quality, and completion by improving higher education and lifelong learning opportunities for youth and adults.
P00.000.408	SG	008	Department of Education	Elementary and Secondary. Prepare all students for college and career by improving the Elementary and Secondary education system's ability to consistently deliver excellent classroom instruction and supportive services.
P00.000.409	SG	009	Department of Education	Early Learning. Improve the health, social-emotional, and cognitive outcomes for all children from birth through third grade, so that all children, particularly those with high needs, are on track for graduating from high school, college and career-ready
P00.000.418	SG	018	Department of State and USAID	Effectively manage transitions in the frontline states.
P00.000.419	SG	019	Department of Homeland Security	Enforcing and Administering our Immigration Laws
P00.000.420	SG	020	Department of State and USAID	Expand and sustain the ranks of prosperous, stable and democratic states by promoting effective, accountable, democratic governance; respect for human rights; sustainable, broad-based economic growth; and well-being.
P00.000.422	SG	022	Department of State and USAID	Support American prosperity through economic diplomacy.
P00.000.424	SG	024	Department of State and USAID	Build a 21st Century workforce; and achieve U.S. Government operational and consular efficiency and effectiveness, transparency and accountability; and a secure U.S. government presence internationally.
P00.000.427	SG	027	Department of Homeland Security	Preventing Terrorism and Enhancing Security
P00.000.433	SG	033	Department of Energy	The Science and Engineering Enterprise: Maintain a vibrant U.S. effort in science and engineering as a cornerstone of our economic prosperity with clear leadership in strategic areas.
P00.000.436	SG	036	National Science Foundation	Innovate for Society

P00.000.443	SG	043	Department of the Interior	Building a 21st Century Department of the Interior
P00.000.448	SG	048	General Services Administration	Be an innovation engine for the government
P00.000.449	SG	049	General Services Administration	Seek an intimate understanding of and resonance with customers in order to serve with integrity, creativity, and responsibility
P00.000.450	SG	050	General Services Administration	Strive to achieve performance excellence, continuous improvement, and the elimination of waste in all operations
P00.000.451	SG	051	Department of Housing and Urban Development	Strengthen the Nation's Housing Market to Bolster the Economy and Protect Consumers
P00.000.452	SG	052	Department of Housing and Urban Development	Meet the Need for Quality Affordable Rental Homes
P00.000.453	SG	053	Department of Housing and Urban Development	Utilize Housing as a Platform for Improving Quality of Life
P00.000.454	SG	054	Department of Housing and Urban Development	Build Inclusive and Sustainable Communities Free from Discrimination
P00.000.455	SG	055	Department of Housing and Urban Development	Transform the Way HUD Does Business
P00.000.466	SG	066	Department of Homeland Security	Ensuring Resilience to Disasters
P00.000.471	SG	071	Department of Veterans Affairs	Improve the quality and accessibility of health care, benefits, and memorial services while optimizing value.

P00.000.476	SG	076	Army Corps of Engineers - Civil Works	Implement Effective, Reliable, and Adaptive Life-Cycle Performance Management of Infrastructure
P00.000.496	SG	096	Department of Veterans Affairs	Increase Veteran client satisfaction with health, education, training, counseling, financial, and burial benefits and services.

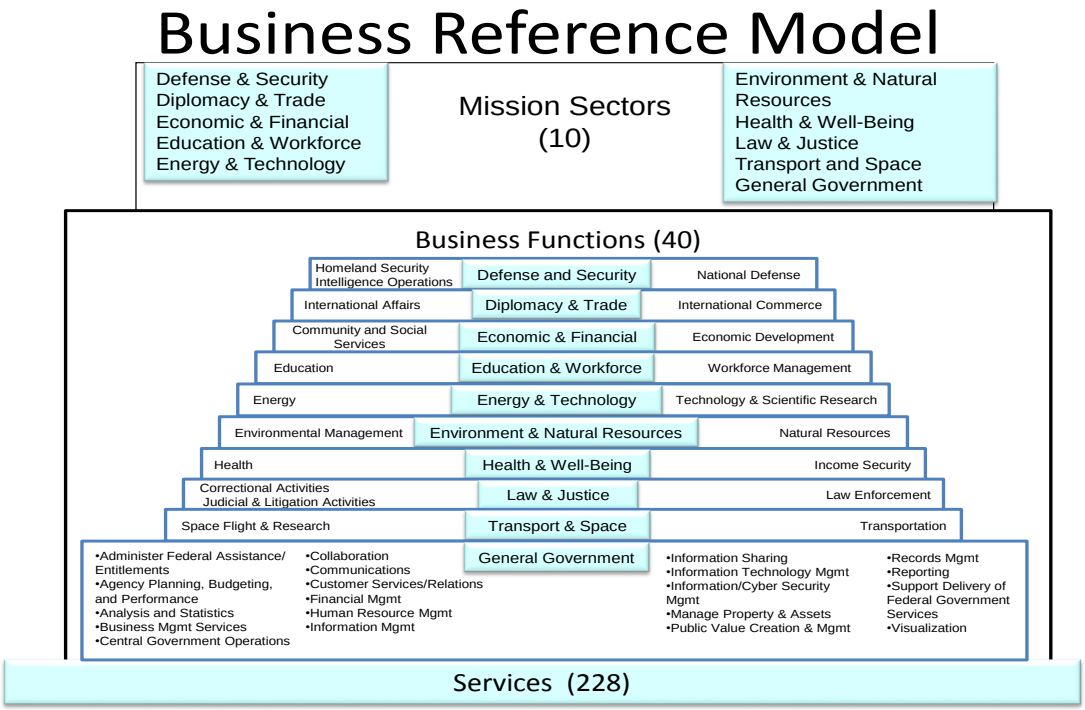
Appendix H: Business Reference Model Taxonomy with Definitions

The BRM taxonomy is structured as a three-layer hierarchy representing Executive Branch Mission Sectors, Business Functions and Services.

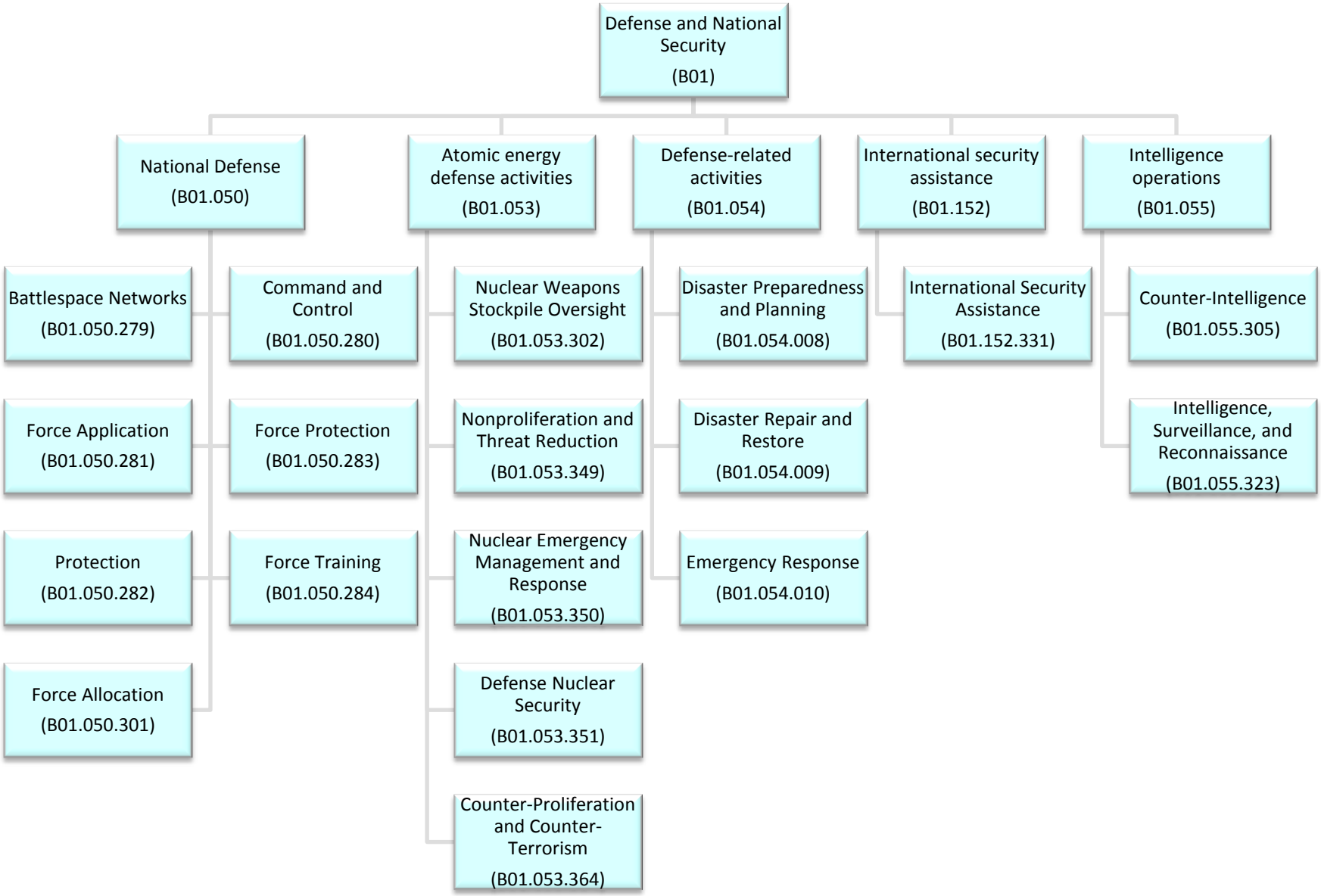
Mission Sector – Identifies the ten business areas of the Federal Government in the *Common Approach to EA*

Business Function – Describes what the Federal government does at an aggregated level, using the budget function classification codes provided in OMB Circular A-11

Service – Further describes what the Federal government does at a secondary or component level



In the sections below, each BRM Domain is shown as a tree diagram, followed by definitions of the taxonomy elements in the corresponding tree.

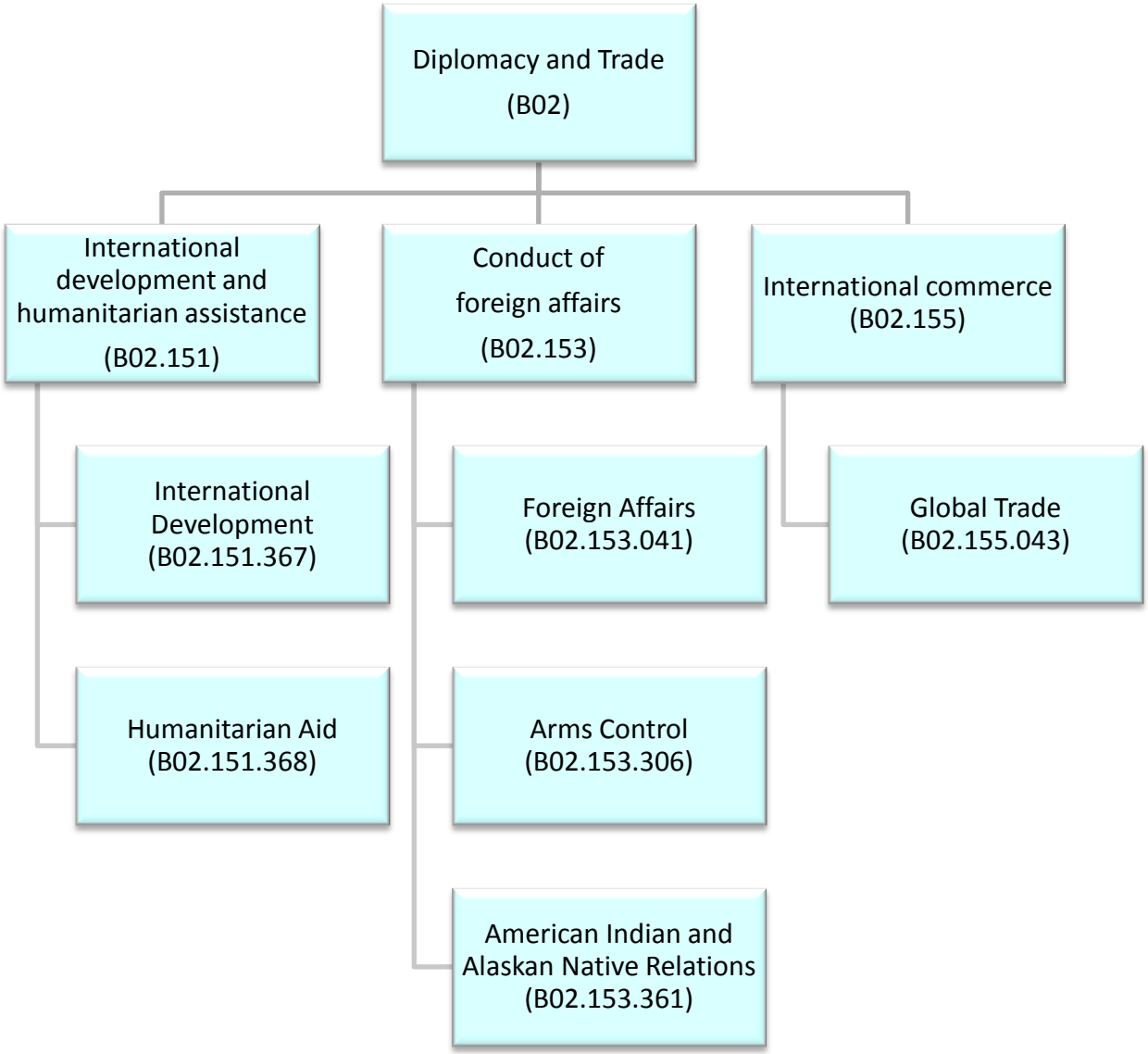

Defense and National Security (B01)
National Defense (B01.050)
Atomic energy defense activities (B01.053)
Defense-related activities (B01.054)
International security assistance (B01.152)
Intelligence operations (B01.055)
Battlespace Networks (B01.050.279)
Command and Control (B01.050.280)
Force Application (B01.050.281)
Force Protection (B01.050.283)
Protection (B01.050.282)
Force Training (B01.050.284)
Force Allocation (B01.050.301)
Nuclear Weapons Stockpile Oversight (B01.053.302)
Nonproliferation and Threat Reduction (B01.053.349)
Nuclear Emergency Management and Response (B01.053.350)
Defense Nuclear Security (B01.053.351)
Counter-Proliferation and Counter-Terrorism (B01.053.364)
Disaster Preparedness and Planning (B01.054.008)
Disaster Repair and Restore (B01.054.009)
Emergency Response (B01.054.010)
International Security Assistance (B01.152.331)
Counter-Intelligence (B01.055.305)
Intelligence, Surveillance, and Reconnaissance (B01.055.323)

Defense and National Security (B01)				
Code	**Mission Sector**	**Business Function**	**Service**	**Definition**
B01.050	Defense and National Security	National Defense		Common defense and security of the United States. It encompasses the raising, equipping, and maintaining of armed forces (including civilian support activities), development and utilization of weapons systems (including nuclear weapons), and related programs; direct compensation and benefits paid to active military and civilian personnel and contributions to their retirement, health, and life insurance funds; defense research, development, testing, and evaluation; and procurement, construction, stockpiling, and other activities undertaken to directly foster national security.
B01.050.279	Defense and National Security	National Defense	Battlespace Networks	Battlespace Networks includes activities that extend “commercial like” IT Infrastructure to meet the connectivity and interoperability needs of deployed and mobile warfighting capabilities. This function focuses on information transport; and computing and enterprise services capabilities for the tactical edge users. It includes tactical edge networks and gateways to enable end-to-end connectivity between battlespace networks and IT infrastructure capabilities.
B01.050.280	Defense and National Security	National Defense	Command and Control	Command and Control includes activities that facilitate the exercise of authority and direction by a properly designated commander or decision maker over assigned and attached forces and resources in the accomplishment of the mission. It includes activities to align or synchronize interdependent and disparate entities to achieve unity of effort, understand information about the environment and situation to aid in decision making, establish a framework and select a course of action to employ resources to achieve a desired outcome/effect; and observe and assess events/effects of a decision.

B01.050.281	Defense and National Security	National Defense	Force Application	Force Application includes activities to integrate the use of maneuver and engagement in all environments, to create the effects necessary for achieving DoD mission objectives. Maneuver is the ability to move to a position of advantage in all environments in order to generate or enable the generation of effects in all domain and the information environment. Engagement is the ability to use kinetic and non-kinetic means in all environments to generate the desired lethal and/or non-lethal effects from all domains and the information environment.
B01.050.283	Defense and National Security	National Defense	Force Protection	Refers to activities to prevent and/or mitigate adverse effects of attacks on personnel (combatant or non-combatant) and physical assets of the United States, its allies and friends. This encompasses, but is not limited to: air and missile defense operations, strategic nuclear deterrent and prevention of non-kinetic attacks; mitigation of chemical, biological, radiological, nuclear, electromagnetic pulse and other lethal/non-lethal effects; and military support to civil defense activities.
B01.050.282	Defense and National Security	National Defense	Protection	Protection involves Citizen Protection, Leadership Protection and Property Protection; it involves all activities performed to protect the general population of the United States, president, vice-president, their families, foreign leaders and dignitaries, and other high-level government officials from criminal activity and entails all activities performed to ensure the security of civilian and government property as well as foreign diplomatic missions.
B01.050.284	Defense and National Security	National Defense	Force Training	Force Training includes activities to develop, enhance, adapt and sustain the capacity to perform specific functions and tasks, during and in preparation for wartime and conflicts, in order to improve the individual or collective performance of personnel, units, forces, and staffs. These activities include, but are not limited to, unit force training; and training in operating weapon systems. This does not include general professional development or training.
B01.050.301	Defense and National Security	National Defense	Force Allocation	Force Allocation includes Application and Management; activities to integrate the use of maneuver and engagement in all environments, to create the effects necessary for achieving mission objectives and activities to integrate new and existing human and technical assets from across the Total Force and its mission partners, during and in preparation for wartime and conflicts, to make the right capabilities available at the right time/place to support national security.

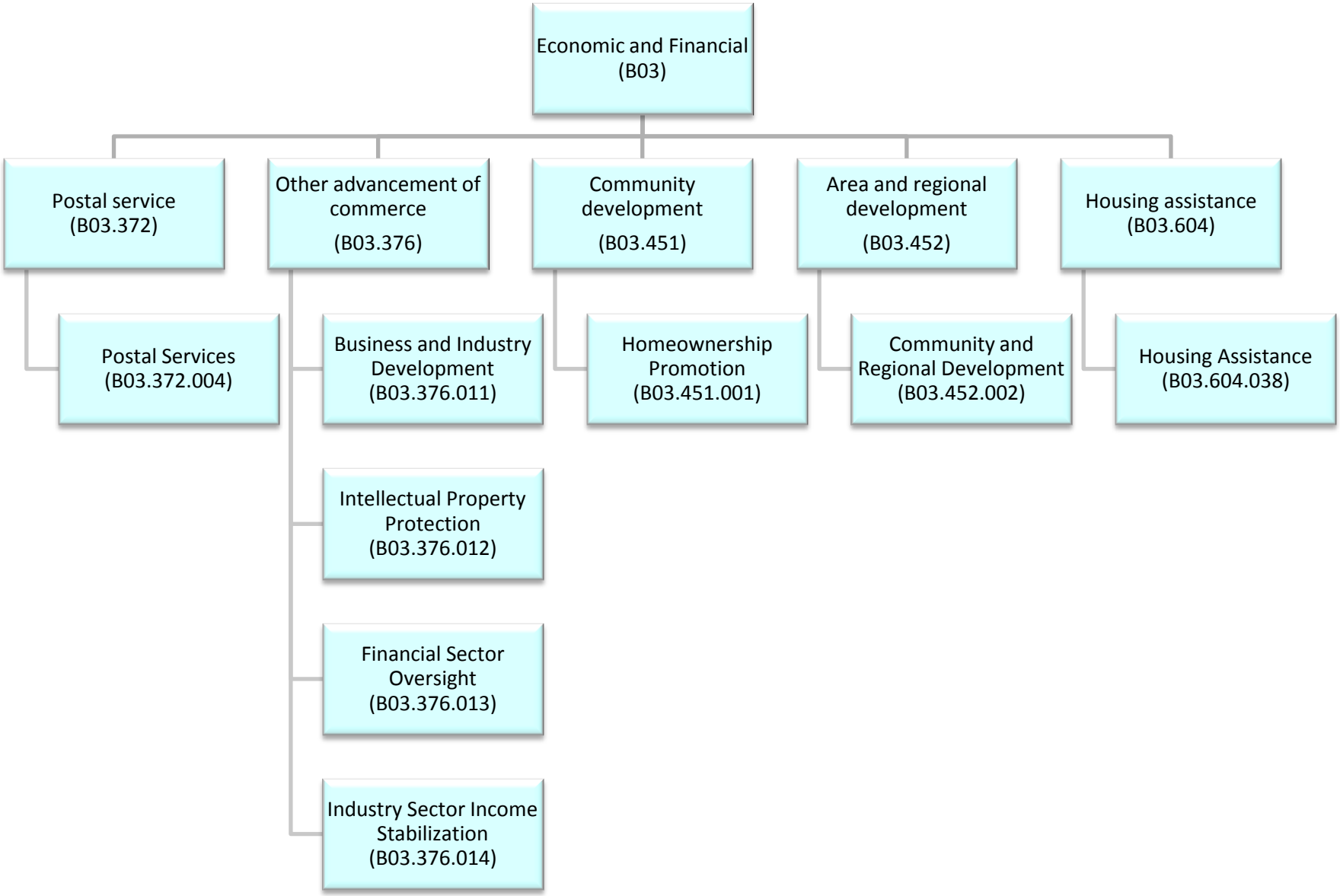
B01.053	Defense and National Security	Atomic energy defense activities		Programs devoted to national defense, such as naval ship reactors and nuclear weapons.
B01.053.302	Defense and National Security	Atomic energy defense activities	Nuclear Weapons Stockpile Oversight	Nuclear Weapons Stockpile and Oversight includes all processes around the counting, tracking, transferring, securing, and decommissioning of various weapons that contain nuclear materials.
B01.053.349	Defense and National Security	Atomic energy defense activities	Nonproliferation and Threat Reduction	Nonproliferation and Threat Reduction encompasses the activities necessary to limit or prevent the spread of materials, technology, or expertise relating to weapons of mass destruction; advance the technologies to detect the proliferation of weapons of mass destruction worldwide; and eliminate or secure inventories of surplus fissile materials and infrastructure usable for nuclear weapons, while working closely with its federal, international, and regional partners.
B01.053.350	Defense and National Security	Atomic energy defense activities	Nuclear Emergency Management and Response	Nuclear Emergency Management and Response encompasses the Services associated with the planning, management and response to facility emergencies, and nuclear or radiological incidents within the United States or abroad, as well as operational planning and training to counter domestic and international nuclear terrorism.
B01.053.351	Defense and National Security	Atomic energy defense activities	Defense Nuclear Security	Defense Nuclear Security encompasses the services associated with providing engineering, technical, operational, and administrative security support and oversight to assure effective security, to include the physical, personnel, materials control and accounting, classified and sensitive information protection, and technical security for defense nuclear weapon programs.
B01.053.364	Defense and National Security	Atomic energy defense activities	Counter-Proliferation and Counter-Terrorism	Encompasses counter-proliferation, counter-terrorism, and nuclear threat response, domestically and internationally, including nuclear threat identification, nuclear forensics, and the neutralization of improvised nuclear and radiological devices.
B01.054	Defense and National Security	Defense-related activities		Miscellaneous defense activities, such as the expenses connected with selective services and with defense stockpiles outside of the Departments of Defense and Energy.

B01.054.008	Defense and National Security	Defense-related activities	Disaster Preparedness and Planning	Disaster Preparedness and Planning involves the development of response programs to be used in case of a disaster as well as pre-disaster mitigation efforts to minimize the potential for loss of life and property. This involves the development of emergency management programs and activities as well as staffing and equipping regional response centers, and mitigation focused construction and preparation.
B01.054.009	Defense and National Security	Defense-related activities	Disaster Repair and Restore	Disaster Repair and Restore involves the immediate actions taken to respond to a disaster and the cleanup and restoration activities that take place after a disaster. These actions include, but are not limited to, providing mobile telecommunications, operational support, power generation, search and rescue, and medical life-saving actions. It also involves the cleanup and rebuilding of homes, buildings, roads, environmental resources, or infrastructure that may be damaged due to a disaster.
B01.054.010	Defense and National Security	Defense-related activities	Emergency Response	Emergency Response involves the immediate actions taken to respond to a disaster. These actions include, but are not limited to, providing mobile telecommunications, operational support, energy emergency preparedness, power generation, search and rescue, and medical life-saving actions.
B01.152.331	Defense and National Security	International security assistance	International Security Assistance	International Security Assistance involves activities taken abroad to protect and advance U.S. interests and, if deterrence fails, decisively defeat threats to those interests.
B01.055.305	Defense and National Security	Intelligence operations	Counter-Intelligence	Counter-Intelligence includes: All planning, collection, processing, analysis, production and dissemination of contrary intelligence
B01.055.323	Defense and National Security	Intelligence operations	Intelligence, Surveillance, and Reconnaissance	Intelligence, Surveillance, and Reconnaissance (ISR) refers to the ability to understand dispositions and intentions as well as the characteristics and conditions of the operational environment that bear on national and military decision-making. ISR also defines the ability to conduct activities to meet the intelligence needs of national and military decision-makers. It includes ISR planning/direction, collection, processing/exploitation, analysis & production and ISR dissemination.


Diplomacy and Trade
(B02)
International development and humanitarian assistance
(B02.151)
Conduct of foreign affairs
(B02.153)
International commerce
(B02.155)
International Development
(B02.151.367)
Humanitarian Aid
(B02.151.368)
Foreign Affairs
(B02.153.041)
Arms Control
(B02.153.306)
American Indian and Alaskan Native Relations
(B02.153.361)
Global Trade
(B02.155.043)

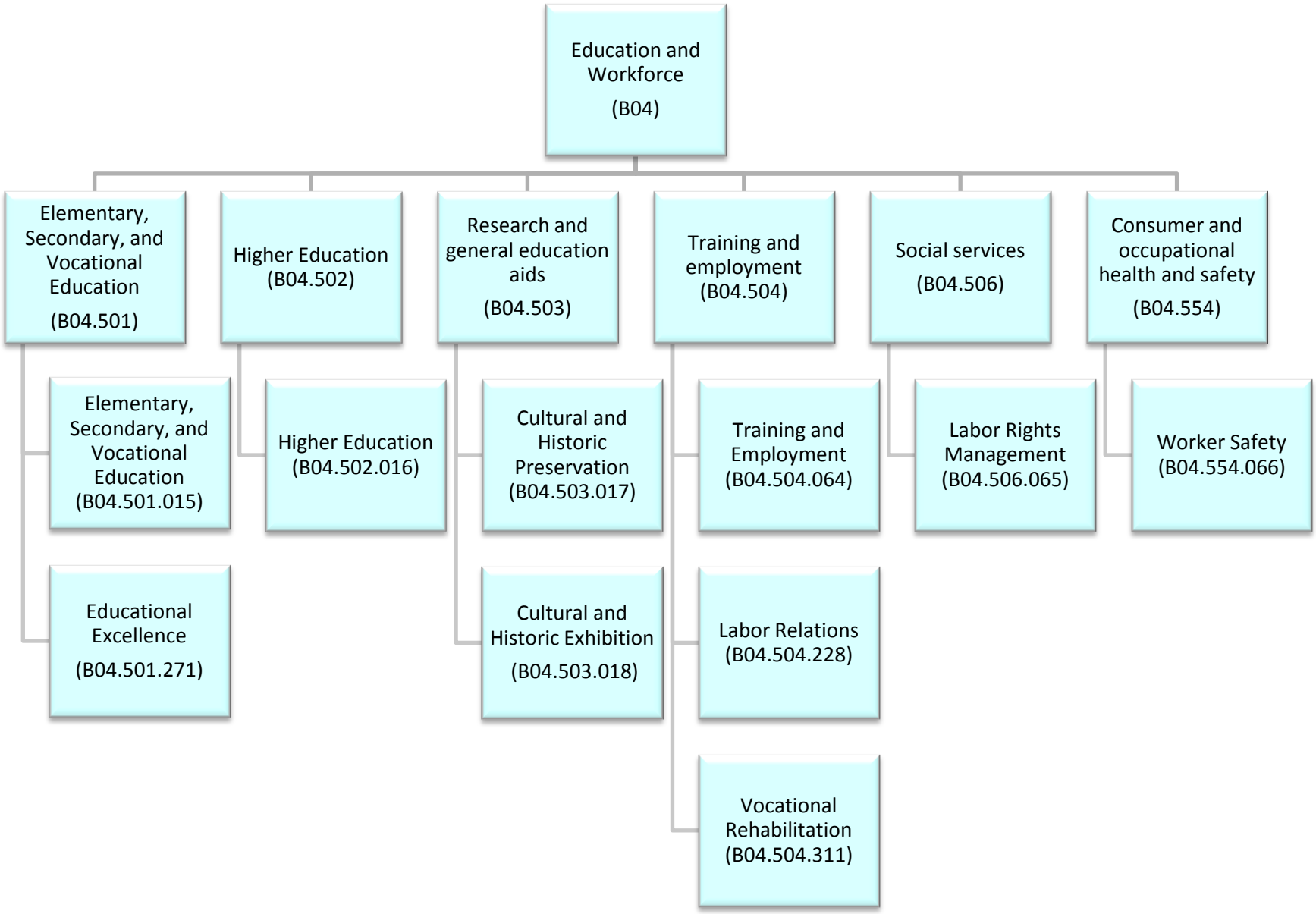
Diplomacy and Trade (B02)				
Code	**Mission Sector**	**Business Function**	**Service**	**Definition**
B02.151	Diplomacy and Trade	International development and humanitarian assistance		Humanitarian assistance, development assistance, security support assistance, grants to and investments in international financial and development institutions, and the budgetary costs associated with concessionary agricultural exports.
B02.151.367	Diplomacy and Trade	International development and humanitarian assistance	International Development	International Development refers to those activities related to the implementation of development assistance programs to developing and transitioning countries throughout the world. Development-may include technical assistance (the transfer of knowledge and expertise), and the delivery of equipment, commodities.
B02.151.368	Diplomacy and Trade	International development and humanitarian assistance	Humanitarian Aid	Humanitarian Aid refers to those activities related to the implementation of humanitarian assistance programs to developing and transitioning countries throughout the world. Aid may include technical assistance (the transfer of knowledge and expertise), and the delivery of equipment, commodities and urgent humanitarian assistance including food aid.
B02.153	Diplomacy and Trade	Conduct of foreign affairs		Diplomatic and consular operations of the Department of State, assessed contributions to international organizations, and closely related activities in other agencies (such as the Arms Control and Disarmament Agency).
B02.153.041	Diplomacy and Trade	Conduct of foreign affairs	Foreign Affairs	Foreign Affairs refers to those activities associated with the implementation of foreign policy and diplomatic relations, including the operation of embassies, consulates, and other posts; ongoing membership in international organizations; the development of cooperative frameworks to improve relations with other nations; and the development of treaties and agreements.
B02.153.306	Diplomacy and Trade	Conduct of foreign affairs	Arms Control	Arms Control includes all activities for managing both legal and illegal weapons in accordance with State, Federal and international law.

B02.153.361	Diplomacy and Trade	Conduct of foreign affairs	American Indian and Alaskan Native Relations	American Indian and Alaskan Native Relations involves all activities related to working with tribal governments, in tribal trust relationships or supporting tribal nations through treaties and/or other legal agreements.
B02.155.043	Diplomacy and Trade	International commerce	Global Trade	Global Trade refers to those activities the federal government undertakes to advance worldwide economic prosperity by increasing trade through the opening of overseas markets and freeing the flow of goods, services, and capital.


Economic and Financial (B03)
Postal service (B03.372)
Other advancement of commerce (B03.376)
Community development (B03.451)
Area and regional development (B03.452)
Housing assistance (B03.604)
Postal Services (B03.372.004)
Business and Industry Development (B03.376.011)
Homeownership Promotion (B03.451.001)
Community and Regional Development (B03.452.002)
Housing Assistance (B03.604.038)
Intellectual Property Protection (B03.376.012)
Financial Sector Oversight (B03.376.013)
Industry Sector Income Stabilization (B03.376.014)

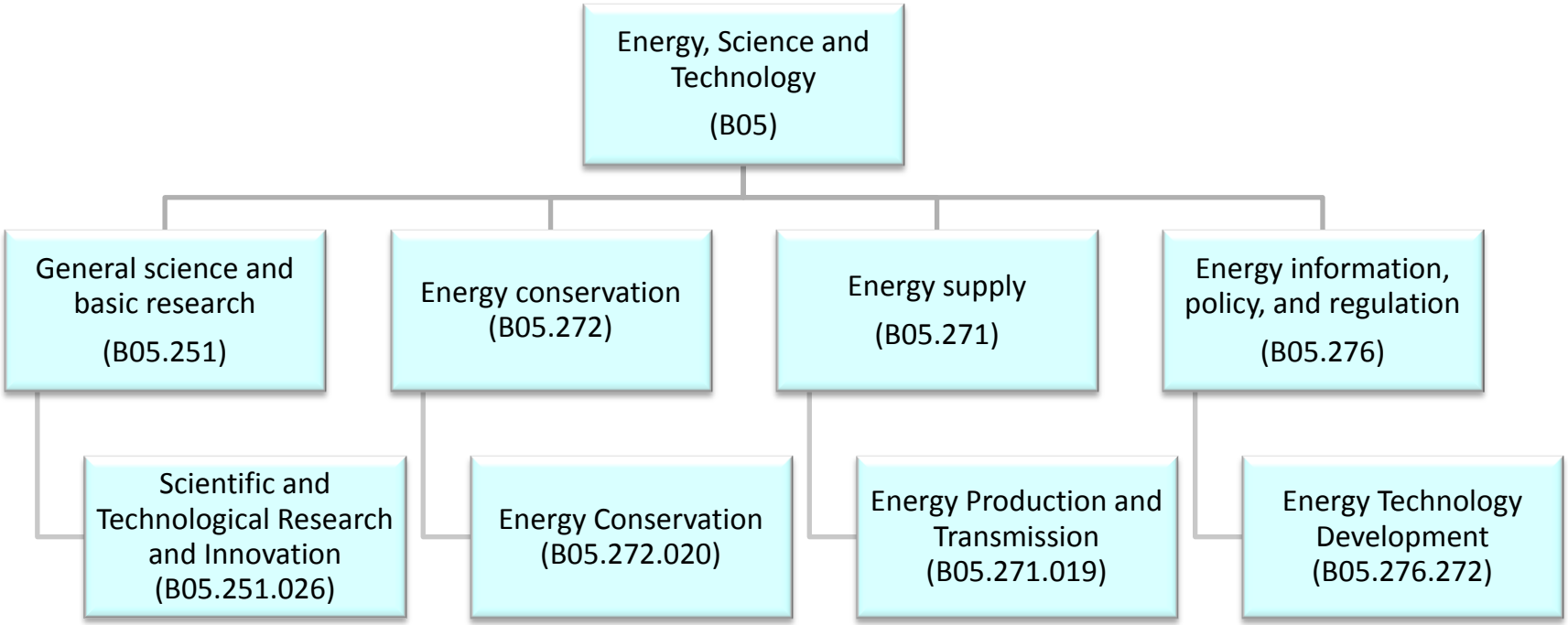
Economic and Financial (B03)				
Code	**Mission Sector**	**Business Function**	**Service**	**Definition**
B03.372.004	Economic and Financial	Postal service	Postal Services	Postal Services provide for the timely and consistent exchange and delivery of mail and packages between businesses, organizations, and residents of the United States or between businesses, organizations, and residents of the United States and the rest of the world. It also includes the nationwide retail infrastructure required to make Postal Services easily accessible to customers.
B03.376	Economic and Financial	Other advancement of commerce		Loan programs to aid specialized forms of business (such as small business) that are not included elsewhere in the functional structure. For such transactions undertaken prior to credit reform, includes the total cash flows. For activities under credit reform, includes the credit subsidy cost of the loans or guarantees. Also includes collecting and disseminating economic and demographic statistics (such as census data) and regulating business.
B03.376.011	Economic and Financial	Other advancement of commerce	Business and Industry Development	Business and Industry Development supports activities related to the creation of economic and business opportunities and stimulus, and the promotion of financial and economic stability for corporations and citizens involved in different types of business.
B03.376.012	Economic and Financial	Other advancement of commerce	Intellectual Property Protection	Intellectual Property Protection involves all activities to protect and promote the ownership of ideas and control over the tangible or virtual representation of those ideas, including inventions and discoveries; literary and artistic works; and symbols, names, images, and designs used in commerce.
B03.376.013	Economic and Financial	Other advancement of commerce	Financial Sector Oversight	Financial Sector Oversight involves the regulation of private sector firms and markets (stock exchanges, corporations, etc.) to protect investors from fraud, monopolies, and illegal behavior. This also includes deposit protection.
B03.376.014	Economic and Financial	Other advancement of commerce	Industry Sector Income Stabilization	Industry Sector Income Stabilization involves all programs and activities devoted to assisting adversely impacted industrial sectors (farming, commercial transportation, etc.) to ensure the continued availability of their services for the American public and the long-term economic stability of these sectors.
B03.451.001	Economic and Financial	Community development	Homeownership Promotion	Homeownership Promotion includes activities devoted to assisting citizens interested in buying homes and educating the public as to the benefits of homeownership.

B03.452.002	Economic and Financial	Area and regional development	Community and Regional Development	Community and Regional Development involves activities designed to assist communities in preventing and eliminating blight and deterioration, assist economically distressed communities, and encourage and foster economic development through improved public facilities and resources.
B03.604.038	Economic and Financial	Housing assistance	Housing Assistance	Housing Assistance involves the development and management programs that provide housing to those who are unable to provide housing for themselves including the rental of single-family or multifamily properties, and the management and operation of federally supported housing properties.

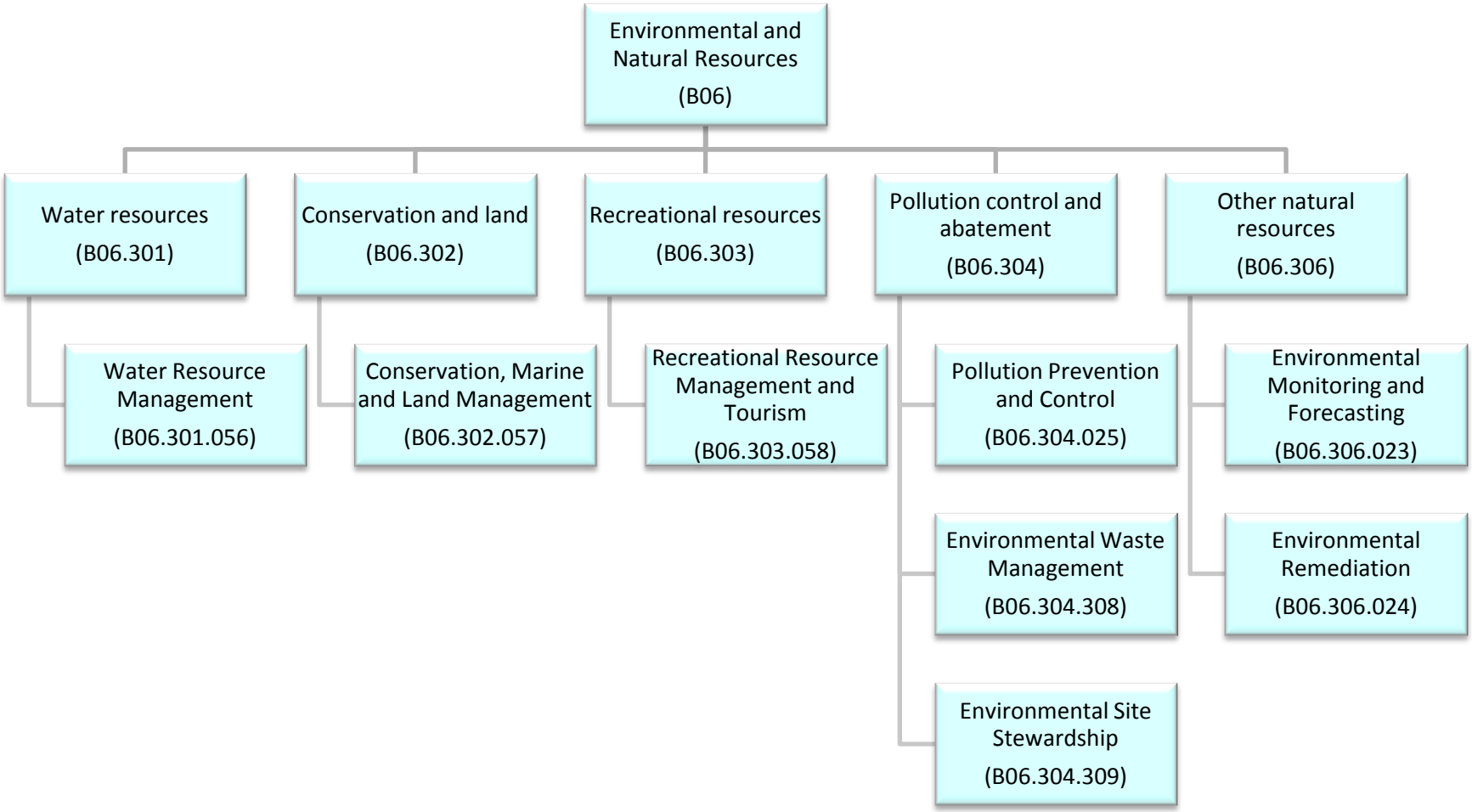

Education and Workforce (B04)
Elementary, Secondary, and Vocational Education (B04.501)
Higher Education (B04.502)
Research and general education aids (B04.503)
Training and employment (B04.504)
Social services (B04.506)
Consumer and occupational health and safety (B04.554)
Elementary, Secondary, and Vocational Education (B04.501.015)
Educational Excellence (B04.501.271)
Higher Education (B04.502.016)
Cultural and Historic Preservation (B04.503.017)
Cultural and Historic Exhibition (B04.503.018)
Training and Employment (B04.504.064)
Labor Relations (B04.504.228)
Vocational Rehabilitation (B04.504.311)
Labor Rights Management (B04.506.065)
Worker Safety (B04.554.066)

Education and Workforce (B04)				
Code	**Mission Sector**	**Business Function**	**Service**	**Definition**
B04.501	Education and Workforce	Elementary, Secondary, and Vocational Education		Preschool, elementary, secondary, and vocational education programs.
B04.501.015	Education and Workforce	Elementary, Secondary, and Vocational Education	Elementary, Secondary, and Vocational Education	Elementary, Secondary, and Vocational Education refers to the provision of education in elementary subjects (reading and writing and arithmetic); education provided by a high school or college preparatory school; and vocational and technical education and training.
B04.501.271	Education and Workforce	Elementary, Secondary, and Vocational Education	Educational Excellence	Educational Excellence refers to activities undertaken by the US Government to evaluate educational programs, collect data on America's schools, and disseminate information and research
B04.502.016	Education and Workforce	Higher Education	Higher Education	Higher Education refers to education beyond the secondary level; specifically, education provided by a college or university.
B04.503	Education and Workforce	Research and general education aids		Education research and assistance for the arts, the humanities, educational radio and television, public libraries, and museums.
B04.503.017	Education and Workforce	Research and general education aids	Cultural and Historic Preservation	Cultural and Historic Preservation involves all activities performed by the federal government to collect and preserve information and artifacts important to the culture and history of the United States and its citizenry and the education of U.S. citizens and the world.
B04.503.018	Education and Workforce	Research and general education aids	Cultural and Historic Exhibition	Cultural and Historic Exhibition includes all activities undertaken by the U.S. government to promote education through the exhibition of cultural, historical, and other information, archives, art, etc.
B04.504	Education and Workforce	Training and employment		Job or skill training, employment services and placement, and payments to employers to subsidize employment.

B04.504.064	Education and Workforce	Training and employment	Training and Employment	Training and Employment includes programs of job or skill training, employment services and placement, and programs for non-federal employees to promote the hiring of marginal, unemployed, or low-income workers.
B04.504.228	Education and Workforce	Training and employment	Labor Relations	Labor Relations manages the relationship between the agency and its unions and bargaining units. This includes negotiating and administering labor contracts and collective bargaining agreements; managing negotiated grievances; and participating in negotiated third party proceedings.
B04.504.311	Education and Workforce	Training and employment	Vocational Rehabilitation	Vocational Rehabilitation includes all activities devoted to providing educational resources and life skills necessary to rejoin society as responsible and contributing members.
B04.506.065	Education and Workforce	Social services	Labor Rights Management	Labor Rights Management refers to those activities undertaken to ensure that employees and employers are aware of and comply with all statutes and regulations concerning labor rights, including those pertaining to wages, benefits, safety and health, whistleblower, and non-discrimination policies for non-federal employees.
B04.554.066	Education and Workforce	Consumer and occupational health and safety	Worker Safety	Worker Safety refers to those activities undertaken to save lives, prevent injuries, and protect the health of America's workers.

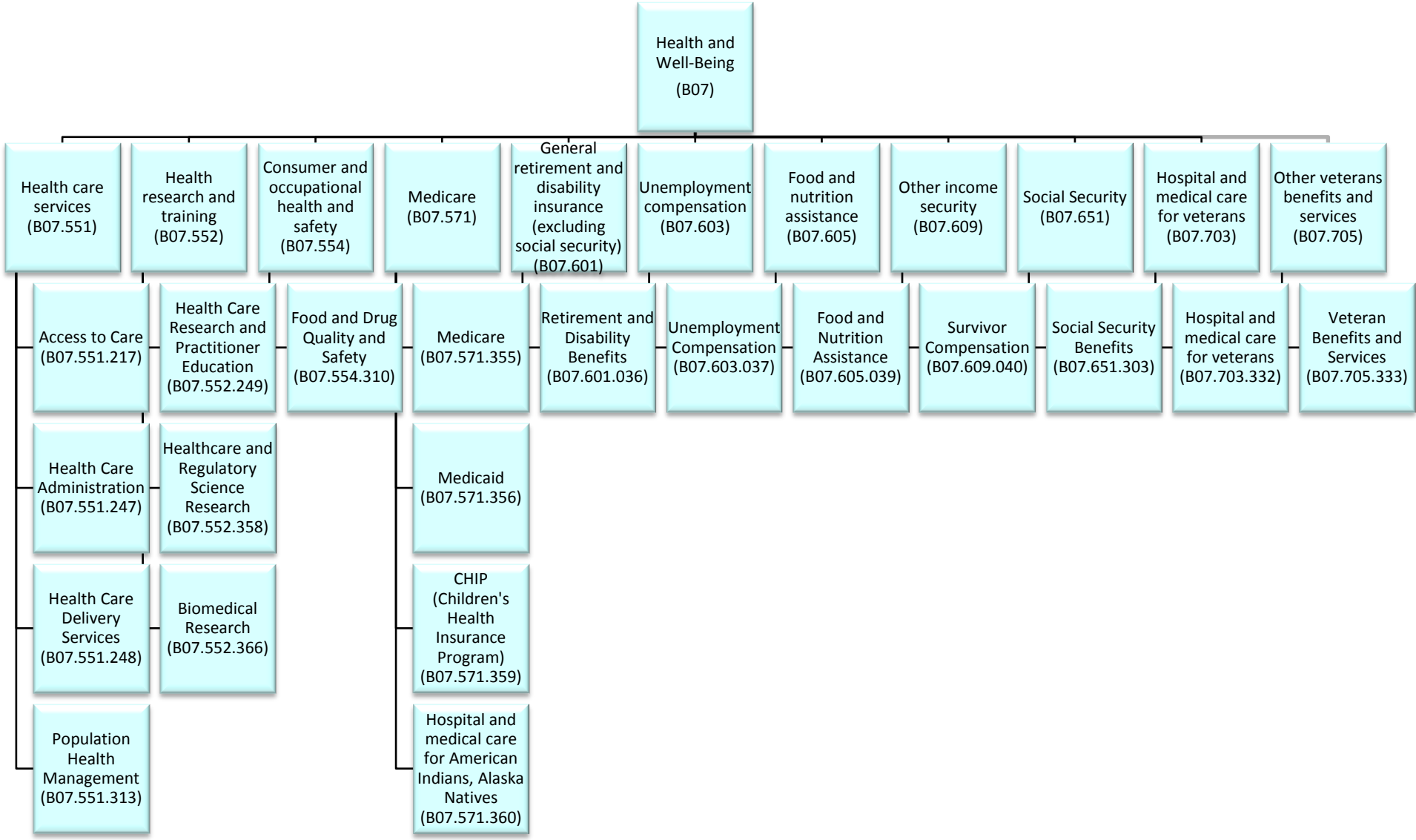

Energy, Science and Technology
(B05)
General science and basic research
(B05.251)
Energy conservation
(B05.272)
Energy supply
(B05.271)
Energy information, policy, and regulation
(B05.276)
Scientific and Technological Research and Innovation
(B05.251.026)
Energy Conservation
(B05.272.020)
Energy Production and Transmission
(B05.271.019)
Energy Technology Development
(B05.276.272)

Energy, Science and Technology (B05)				
Code	**Mission Sector**	**Business Function**	**Service**	**Definition**
B05.251.026	Energy, Science and Technology	General science and basic research	Scientific and Technological Research and Innovation	Scientific and Technological Research and Innovation includes all federal activities whose goal is the creation of new scientific and/or technological knowledge as a goal in itself, without a specific link to the other LoBs or Services of the BRM.
B05.272.020	Energy, Science and Technology	Energy conservation	Energy Conservation	Energy Conservation and Preparedness involves protection of energy resources from over consumption to ensure the continued availability of fuel resources and to promote environmental protection.
B05.271.019	Energy, Science and Technology	Energy supply	Energy Production and Transmission	Energy Production involves the transformation of raw energy resources into useable, deliverable energy. all activities devoted to ensuring the availability of an adequate supply of energy for the United States and its citizens. It involves the management and oversight of energy producing resources including facilities, dams, land, offshore resources and the private sector and includes all types of mass-produced energy (e.g., hydroelectric, nuclear, wind, solar, or fossil fuels).
B05.276.272	Energy, Science and Technology	Energy information, policy, and regulation	Energy Technology Development	Energy Technology Development encompasses the activities that apply the results of scientific research to design, develop, and test new technologies, components, and processes. This service focuses on the development of prototypes and pilots for wide-scale technologies and components that can be mass produced by private-sector partners. The fabrication of one-time components used in very specific research techniques is an activity within the General Sciences and Innovation LOB.


Environmental and Natural Resources (B06)
Water resources (B06.301)
Conservation and land (B06.302)
Recreational resources (B06.303)
Pollution control and abatement (B06.304)
Other natural resources (B06.306)
Water Resource Management (B06.301.056)
Conservation, Marine and Land Management (B06.302.057)
Recreational Resource Management and Tourism (B06.303.058)
Pollution Prevention and Control (B06.304.025)
Environmental Monitoring and Forecasting (B06.306.023)
Environmental Waste Management (B06.304.308)
Environmental Remediation (B06.306.024)
Environmental Site Stewardship (B06.304.309)

Environmental and Natural Resources (B06)				
Code	**Mission Sector**	**Business Function**	**Service**	**Definition**
B06.301.056	Environmental and Natural Resources	Water resources	Water Resource Management	Water Resource Management includes all activities that promote the effective use, protection and management of the nation's water resources.
B06.302.057	Environmental and Natural Resources	Conservation and land management	Conservation, Marine and Land Management	Conservation, Marine and Land Management involves the responsibilities of surveying, maintaining, and operating public lands and monuments, as well as activities devoted to ensuring the preservation of land, water, wildlife, and natural resources, both domestically and internationally. It also includes the sustainable stewardship of natural resources on federally owned/controlled lands for commercial use (mineral mining, grazing, forestry, fishing, etc.).
B06.303.058	Environmental and Natural Resources	Recreational resources	Recreational Resource Management and Tourism	Recreational Resource Management and Tourism involves the management of national parks, monuments, and tourist attractions as well as visitor centers, campsites, and park service facilities.
B06.304	Environmental and Natural Resources	Pollution control and abatement		Controlling and reducing air, water, and land pollution, or enhancing the environment. Excludes water resources programs, water treatment plants, and similar programs that are not funded as part of an environmental enhancement activity.
B06.304.025	Environmental and Natural Resources	Pollution control and abatement	Pollution Prevention and Control	Pollution Prevention and Control includes activities associated with identifying appropriate pollution standards and controlling levels of harmful substances emitted into the soil, water and atmosphere from manmade sources. Environmental mitigation projects are also included in this business line.
B06.304.308	Environmental and Natural Resources	Pollution control and abatement	Environmental Waste Management	Environmental Waste Management includes activities associated with identifying appropriate pollution standards and controlling levels of harmful substances emitted into the soil, water and atmosphere from manmade sources. Environmental mitigation projects are also included.

B06.304.309	Environmental and Natural Resources	Pollution control and abatement	Environmental Site Stewardship	Environmental Site Stewardship supports the immediate and long-term activities associated with the correcting and offsetting of environmental deficiencies or imbalances, including restoration activities at facilities under the stewardship of the Federal Government.
B06.306	Environmental and Natural Resources	Other natural resources		Miscellaneous natural resources programs, not classified under other subfunctions, such as marine-, earth-, and atmosphere-related research and geological surveys and mapping.
B06.306.023	Environmental and Natural Resources	Other natural resources	Environmental Monitoring and Forecasting	Environmental Monitoring and Forecasting involves the observation and prediction of environmental conditions. This includes but is not limited to the monitoring and forecasting of water quality, water levels, ice sheets, air quality, regulated and non-regulated emissions, as well as the observation and prediction of weather patterns and conditions.
B06.306.024	Environmental and Natural Resources	Other natural resources	Environmental Remediation	Environmental Remediation supports the immediate and long-term activities associated with the correcting and offsetting of environmental deficiencies or imbalances, including restoration activities.

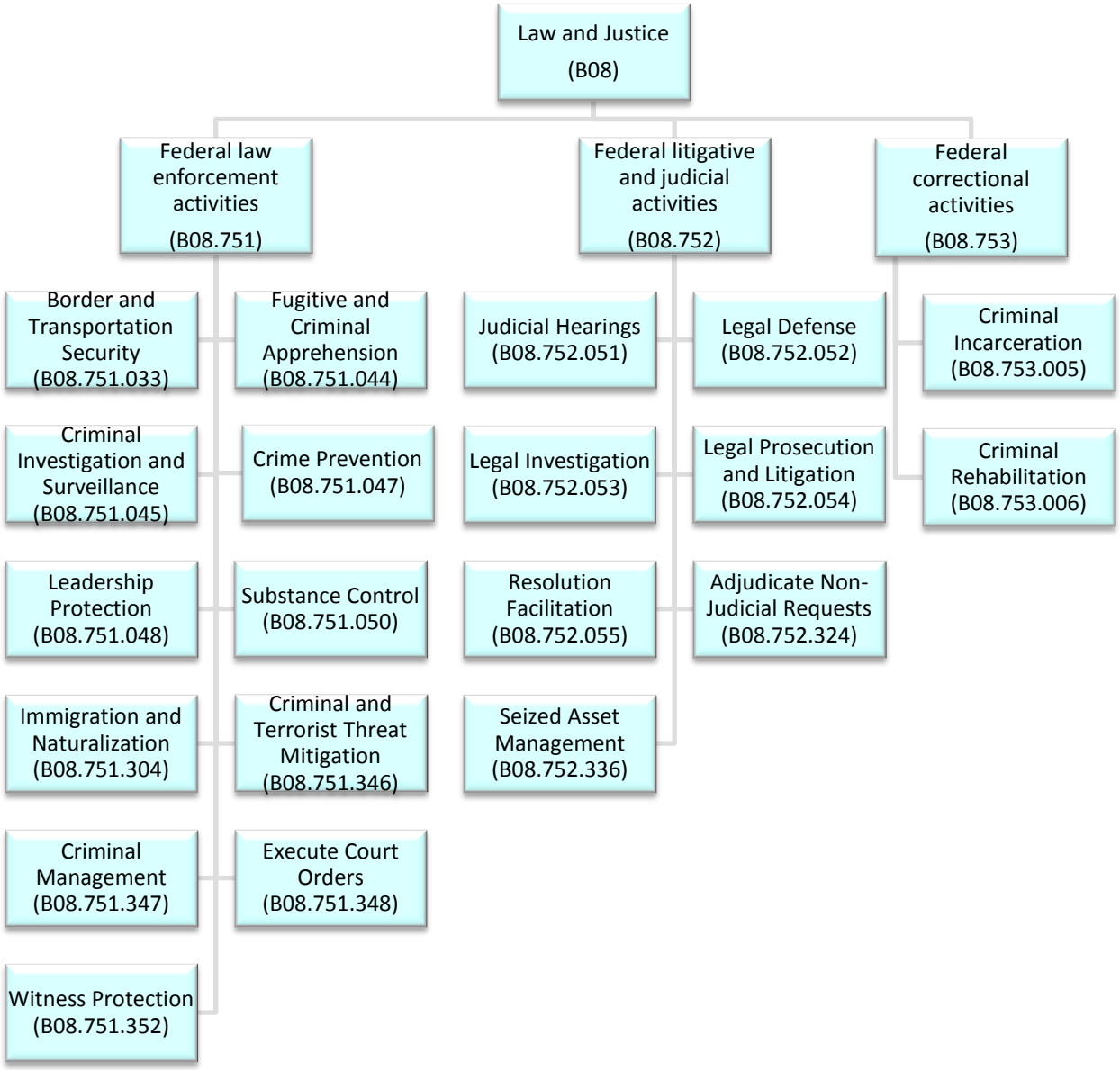

Health and Well-Being (B07)
Health care services (B07.551)
Health research and training (B07.552)
Consumer and occupational health and safety (B07.554)
Medicare (B07.571)
General retirement and disability insurance (excluding social security) (B07.601)
Unemployment compensation (B07.603)
Food and nutrition assistance (B07.605)
Other income security (B07.609)
Social Security (B07.651)
Hospital and medical care for veterans (B07.703)
Other veterans benefits and services (B07.705)
Access to Care (B07.551.217)
Health Care Research and Practitioner Education (B07.552.249)
Food and Drug Quality and Safety (B07.554.310)
Medicare (B07.571.355)
Retirement and Disability Benefits (B07.601.036)
Unemployment Compensation (B07.603.037)
Food and Nutrition Assistance (B07.605.039)
Survivor Compensation (B07.609.040)
Social Security Benefits (B07.651.303)
Hospital and medical care for veterans (B07.703.332)
Veteran Benefits and Services (B07.705.333)
Health Care Administration (B07.551.247)
Healthcare and Regulatory Science Research (B07.552.358)
Medicaid (B07.571.356)
Health Care Delivery Services (B07.551.248)
Biomedical Research (B07.552.366)
CHIP (Children's Health Insurance Program) (B07.571.359)
Population Health Management (B07.551.313)
Hospital and medical care for American Indians, Alaska Natives (B07.571.360)

Health and Well-Being (B07)				
Code	**Mission Sector**	**Business Function**	**Service**	**Definition**
B07.551	Health and Well-Being	Health care services		Medical services to individuals and families, whether such services are provided directly by the federal government or financed through grants, contracts, insurance, or reimbursements.
B07.551.217	Health and Well-Being	Health care services	Access to Care	Access to Care focuses on the access to appropriate care. This includes streamlining efforts to receive care; ensuring care is appropriate in terms of type, care, intensity, location and availability; providing seamless access to health knowledge, enrolling providers; performing eligibility determination, and managing patient movement. It can include aid to family with children, immunization programs, and child support enforcement.
B07.551.247	Health and Well-Being	Health care services	Health Care Administration	Health Care Administration assures that federal health care resources are expended effectively to ensure quality, safety, and efficiency. This includes managing health care quality, cost, workload, utilization, and fraud/abuse efforts.
B07.551.248	Health and Well-Being	Health care services	Health Care Delivery Services	Health Care Delivery Services provides and supports the delivery of health care to its beneficiaries. This includes assessing health status; planning health services; ensuring quality of services and continuity of care; and managing clinical information and documentation. It can include aid to family with children, immunization programs, and child support enforcement.
B07.551.313	Health and Well-Being	Health care services	Population Health Management	Population Health Management assesses health indicators as a means to protect and promote the health of the general population. This includes monitoring of health, health planning, and health management of humans, animals, animal products, and plants, as well as tracking the spread of diseases and pests. Also includes evaluation of consumer products, drug, and foods to assess the potential risks and dangers; education of the consumer and the general population; and facilitation of health promotion and disease and injury prevention.

B07.552	Health and Well-Being	Health research and training		All research programs—whether basic or applied—that are financed specifically as health or medical research. Excludes research that is an integral part of other functions (such as biomedical research in the space program).
B07.552.249	Health and Well-Being	Health research and training	Health Care Research and Practitioner Education	Health Care Research and Practitioner Education fosters advancement in health discovery and knowledge. This includes developing new strategies to handle diseases; promoting health knowledge advancement; identifying new means for delivery of services, methods, decision models and practices; making strides in quality improvement; managing clinical trials and research quality; and providing for practitioner education.
B07.552.358	Health and Well-Being	Health research and training	Healthcare and Regulatory Science Research	The application of advanced technology and science-based standards in a regulatory framework to support pre-market and post-market evaluation and approval of new technologies, products, services, and manufacturing practices.
B07.552.366	Health and Well-Being	Health research and training	Biomedical Research	Basic, clinical, and translational research concerned with the application of biological, physiological, sociological principles to clinical medicine to improve human health.
B07.554.310	Health and Well-Being	Consumer and occupational health and safety	Food and Drug Quality and Safety	Food and Drug Quality and Safety assesses quality indicators and safety metrics as a means to protect and promote the health of the general population. This includes monitoring of humans, animals, animal products, and plants, as well as tracking the spread of diseases and pests. Also includes evaluation of food and drug related incidents to assess the potential risks and dangers; education of the consumer and the general population; and facilitation of health promotion and disease and injury prevention.
B07.571	Health and Well-Being	Medicare		Federal hospital insurance and federal supplementary medical insurance, along with general fund subsidies of these funds and associated offsetting receipts.
B07.571.355	Health and Well-Being	Medicare	Medicare	Medicare involves all activities related to the disbursement of Medicare funds from the federal government directly to beneficiaries (individuals or organizations) who satisfy federal eligibility requirements.
B07.571.356	Health and Well-Being	Medicare	Medicaid	Medicaid involves all activities related to the disbursement of Medicaid funds from the federal government directly to beneficiaries (individuals or organizations) who satisfy federal eligibility requirements.

B07.571.359	Health and Well-Being	Medicare	CHIP (Children's Health Insurance Program)	CHIP (Children's Health Insurance Program) involves all activities related to the disbursement of CHIP funds from the federal government directly to beneficiaries (individuals or organizations) who satisfy federal eligibility requirements.
B07.571.360	Health and Well-Being	Medicare	Hospital and medical care for American Indians, Alaska Natives	Hospital and medical care for American Indians and Alaska Natives assures that federal health care resources for tribes and tribal members are expended effectively to ensure quality, safety, and efficiency and provides and supports the delivery of health care to American Indians and Alaska Natives.
B07.601.036	Health and Well-Being	General retirement and disability insurance (excluding social security)	Retirement and Disability Benefits	Retirement and Disability Benefits involves the development of policies and management of retirement benefits, pension benefits, and income security for those who are retired or disabled (excluding Veteran Benefits).
B07.603.037	Health and Well-Being	Unemployment compensation	Unemployment Compensation	Unemployment Compensation provides income security to those who are no longer employed, while they seek new employment.
B07.605.039	Health and Well-Being	Food and nutrition assistance	Food and Nutrition Assistance	Food and Nutrition Assistance involves the development and management of programs that provide food and nutrition assistance to those members of the public who are unable to provide for these needs themselves.
B07.609.040	Health and Well-Being	Other income security	Survivor Compensation	Survivor Compensation provides compensation to the survivors of individuals currently receiving or eligible to receive benefits from the federal government. This includes, but is not limited to, survivors such as spouses or children of veterans or wage earners eligible for social security payments.
B07.651.303	Health and Well-Being	Social Security	Social Security Benefits	Social Security Benefits includes all direct transfers to Individuals and involves the disbursement of funds from the federal government directly to beneficiaries who satisfy federal eligibility requirements with no restrictions imposed on the recipient as to how the money is spent. Purposes include Retirement, Survivors, and Old Age/ Supplemental Security Income (needs-based).

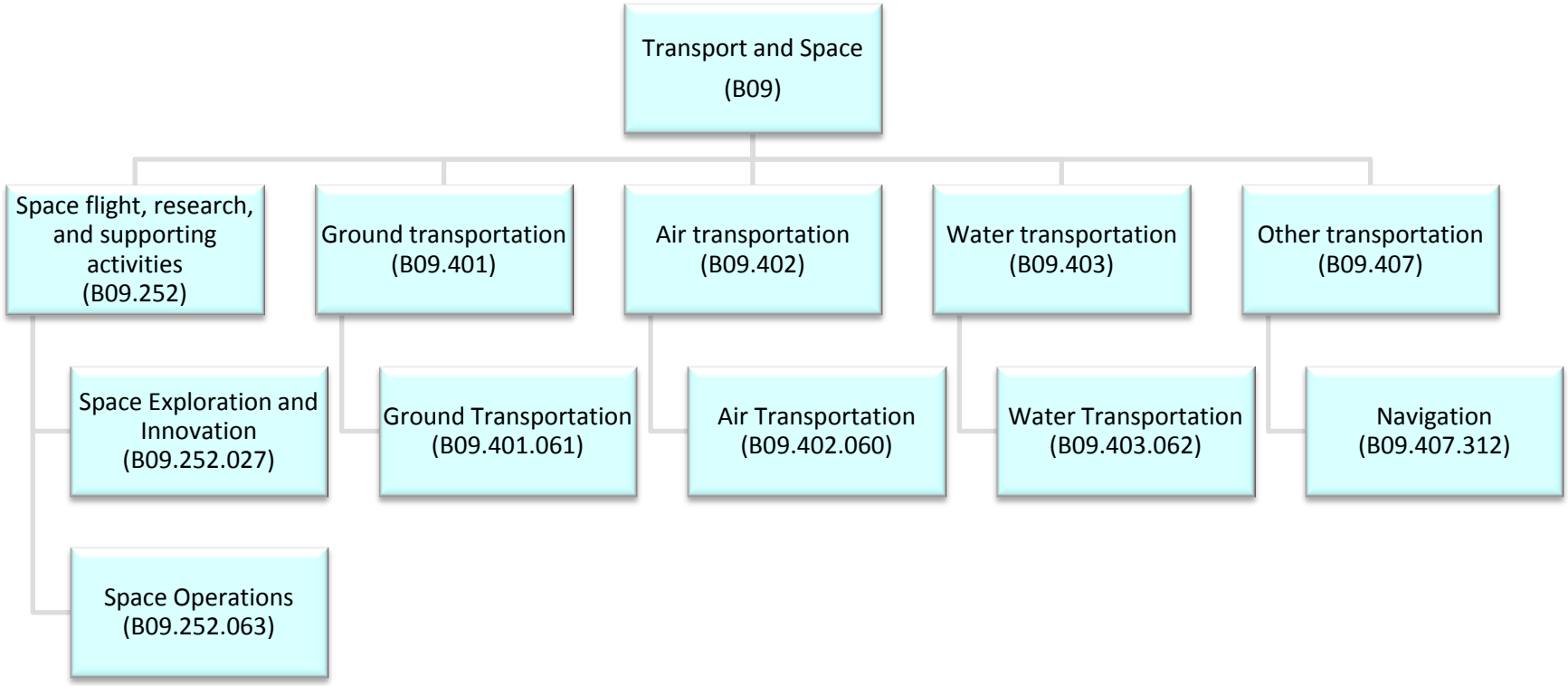
B07.703.332	Health and Well-Being	Hospital and medical care for veterans	Hospital and medical care for veterans	Hospital and medical care for veterans assures that federal health care resources for Veterans are expended effectively to ensure quality, safety, and efficiency and provides and supports the delivery of health care to Veterans.
B07.705.333	Health and Well-Being	Other veterans benefits and services	Veteran Benefits and Services	The Veteran Benefits and Services service involves the development and management of retirement benefits, pension benefits, and income security for Veterans.


Law and Justice
(B08)
Federal law enforcement activities
(B08.751)
Federal litigative and judicial activities
(B08.752)
Federal correctional activities
(B08.753)
Border and Transportation Security
(B08.751.033)
Fugitive and Criminal Apprehension
(B08.751.044)
Criminal Investigation and Surveillance
(B08.751.045)
Crime Prevention
(B08.751.047)
Leadership Protection
(B08.751.048)
Substance Control
(B08.751.050)
Immigration and Naturalization
(B08.751.304)
Criminal and Terrorist Threat Mitigation
(B08.751.346)
Criminal Management
(B08.751.347)
Execute Court Orders
(B08.751.348)
Witness Protection
(B08.751.352)
Judicial Hearings
(B08.752.051)
Legal Defense
(B08.752.052)
Legal Investigation
(B08.752.053)
Legal Prosecution and Litigation
(B08.752.054)
Resolution Facilitation
(B08.752.055)
Adjudicate Non-Judicial Requests
(B08.752.324)
Seized Asset Management
(B08.752.336)
Criminal Incarceration
(B08.753.005)
Criminal Rehabilitation
(B08.753.006)

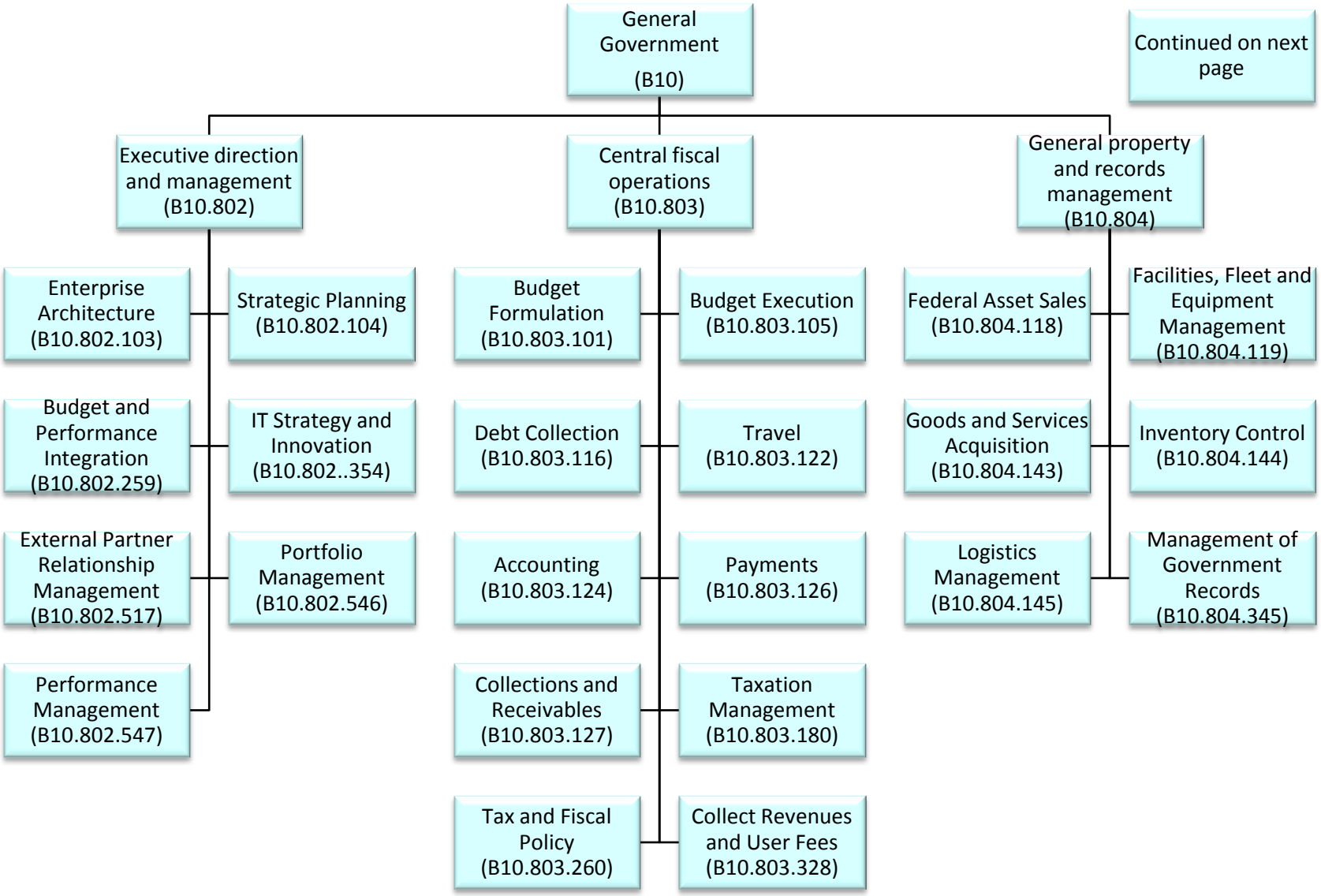
Law and Justice (B08)				
Code	**Mission Sector**	**Business Function**	**Service**	**Definition**
B08.751	Law and Justice	Federal law enforcement activities		The costs of operating the Federal Bureau of Investigation, Customs and Border Protection, Immigration and Customs Enforcement, the Drug Enforcement Administration, and police and crime prevention activities in other programs. Also includes the readily identifiable enforcement cost of civil rights activities.
B08.751.033	Law and Justice	Federal law enforcement activities	Border and Transportation Security	Border and Transportation Security includes appropriately facilitating or deterring entry and exit of people, goods, and conveyances at and between U.S. ports of entry, as well as ensuring the security of transportation and infrastructure networks, facilities, vehicles, and personnel within the United States.
B08.751.044	Law and Justice	Federal law enforcement activities	Fugitive and Criminal Apprehension	Criminal Apprehension involves activities associated with the tracking, arrest, detention, and transportation of groups or individuals responsible and believed to be responsible for committing federal crimes.
B08.751.045	Law and Justice	Federal law enforcement activities	Criminal Investigation and Surveillance	Criminal Investigation and Surveillance includes collecting evidence required to determine responsibility for a crime and monitoring and questioning affected parties.
B08.751.047	Law and Justice	Federal law enforcement activities	Crime Prevention	Crime Prevention entails all efforts designed to create safer communities through the control and reduction of crime by addressing the causes of crime and reducing opportunities for crimes to occur.
B08.751.048	Law and Justice	Federal law enforcement activities	Leadership Protection	Leadership Protection involves all activities performed to protect the health and well-being of the president, vice-president, their families, foreign leaders and dignitaries, federal judges, and other high-level government officials.

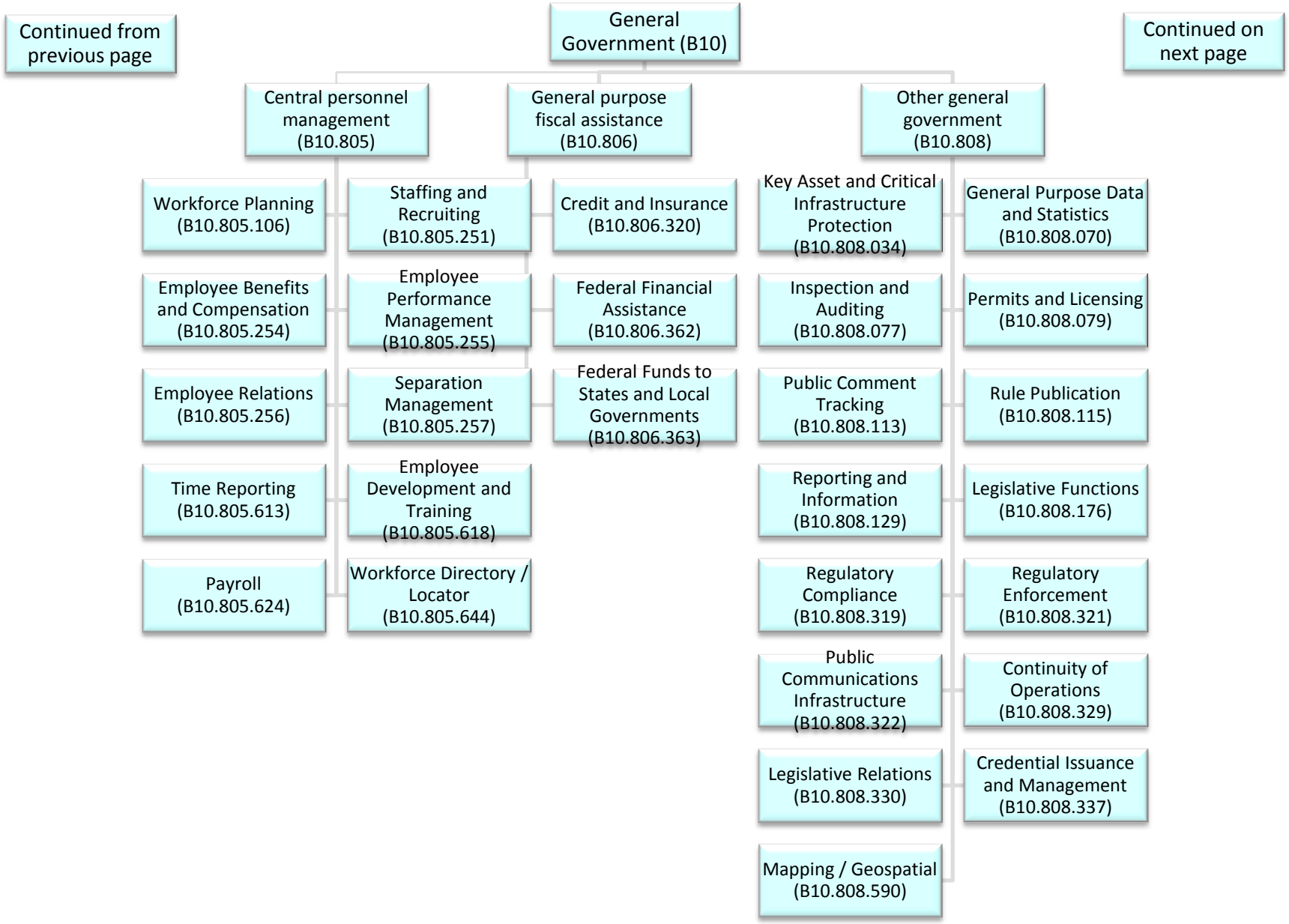
B08.751.050	Law and Justice	Federal law enforcement activities	Substance Control	Substance Control supports activities associated with the enforcement of laws regarding legal substances (i.e., alcohol and tobacco) and illegal narcotics including trafficking, possession, sale, distribution, and other related activities.
B08.751.304	Law and Justice	Federal law enforcement activities	Immigration and Naturalization	Immigration and Naturalization includes all activities for tracking and granting of official status on all non-native non-US citizens, including: refugees, naturalized citizens, legal and illegal immigrants.
B08.751.346	Law and Justice	Federal law enforcement activities	Criminal and Terrorist Threat Mitigation	Criminal and Terrorist Threat Mitigation involves counter activities to prevent, disrupt, weaken, eliminate, and bring to justice threats from organized crime groups, terror networks, gangs, and drug-cartels.
B08.751.347	Law and Justice	Federal law enforcement activities	Criminal Management	Criminal Management includes various functions associated with administering sentences of imprisonment, such as sentence computations, transportation of criminals, and interaction with the public.
B08.751.348	Law and Justice	Federal law enforcement activities	Execute Court Orders	Execute Court Orders involves executing civil, criminal, and foreign orders as directed by the court.
B08.751.352	Law and Justice	Federal law enforcement activities	Witness Protection	Witness Protection involves securing, relocating, and giving Federal witnesses (and their families) new identities.
B08.752	Law and Justice	Federal litigative and judicial activities		The cost of the judiciary, the cost of prosecution, and federal expenses connected with financing legal defense activities.
B08.752.051	Law and Justice	Federal litigative and judicial activities	Judicial Hearings	Judicial Hearings includes activities associated with proceedings (usually by a court of law) where evidence is taken for the purpose of determining an issue of fact and reaching a decision based on that evidence.
B08.752.052	Law and Justice	Federal litigative and judicial activities	Legal Defense	Legal Defense includes those activities associated with the representation of a defendant in a criminal or civil proceeding.

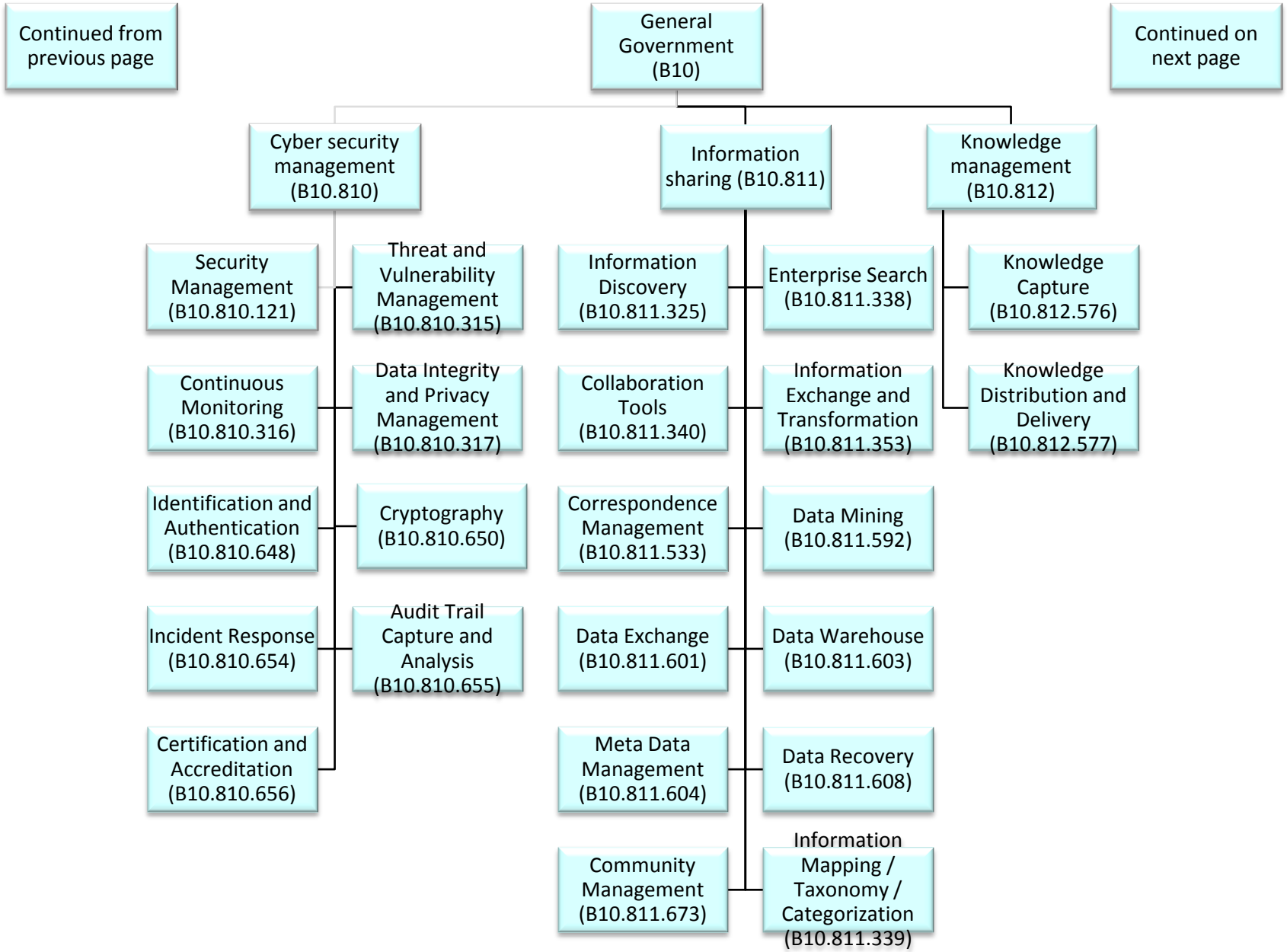
B08.752.053	Law and Justice	Federal litigative and judicial activities	Legal Investigation	Legal Investigation includes activities associated with gathering information about a given party (government agency, citizen or corporation) that would be admissible in a court of law in an attempt to determine a legal question or matter.
B08.752.054	Law and Justice	Federal litigative and judicial activities	Legal Prosecution and Litigation	Legal Prosecution and Litigation includes all activities involved with presenting a case in a legal proceeding both in a criminal or civil court of law in an attempt to prove guilt/responsibility.
B08.752.055	Law and Justice	Federal litigative and judicial activities	Resolution Facilitation	Resolution Facilitation refers to those activities outside a court of law, such as mediation and arbitration, which may be used in an attempt to settle a dispute between two or more parties (government agency, citizen, or corporation).
B08.752.324	Law and Justice	Federal litigative and judicial activities	Adjudicate Non-Judicial Requests	Determining the applicability of relevant statute, regulation, standard or policy to a specific individual or organizations actions or requests. Also, adjudicate Non-Judicial Requests includes those activities outside a court of law, such as mediation and arbitration, which may be used in an attempt to settle a dispute between two or more parties (government agency, citizen, or corporation).
B08.752.336	Law and Justice	Federal litigative and judicial activities	Seized Asset Management	Seized Asset Management involves the seizure, storage, administrative tracking and management of property seized from individuals responsible or believed to be responsible for committing federal crimes.
B08.753	Law and Justice	Federal correctional activities		Covers the costs of incarceration, supervision, parole, and rehabilitation of federal prisoners.
B08.753.005	Law and Justice	Federal correctional activities	Criminal Incarceration	Criminal Incarceration includes activities associated with the housing, custody and general care of criminals serving time in penitentiaries. This includes self-improvement opportunities provided as part of Criminal Incarceration.
B08.753.006	Law and Justice	Federal correctional activities	Criminal Rehabilitation	Criminal Rehabilitation includes all government activities devoted to providing convicted criminals with the educational resources and life skills necessary to rejoin society as responsible and contributing members. This includes work and treatment opportunities provided as part of Criminal Rehabilitation.

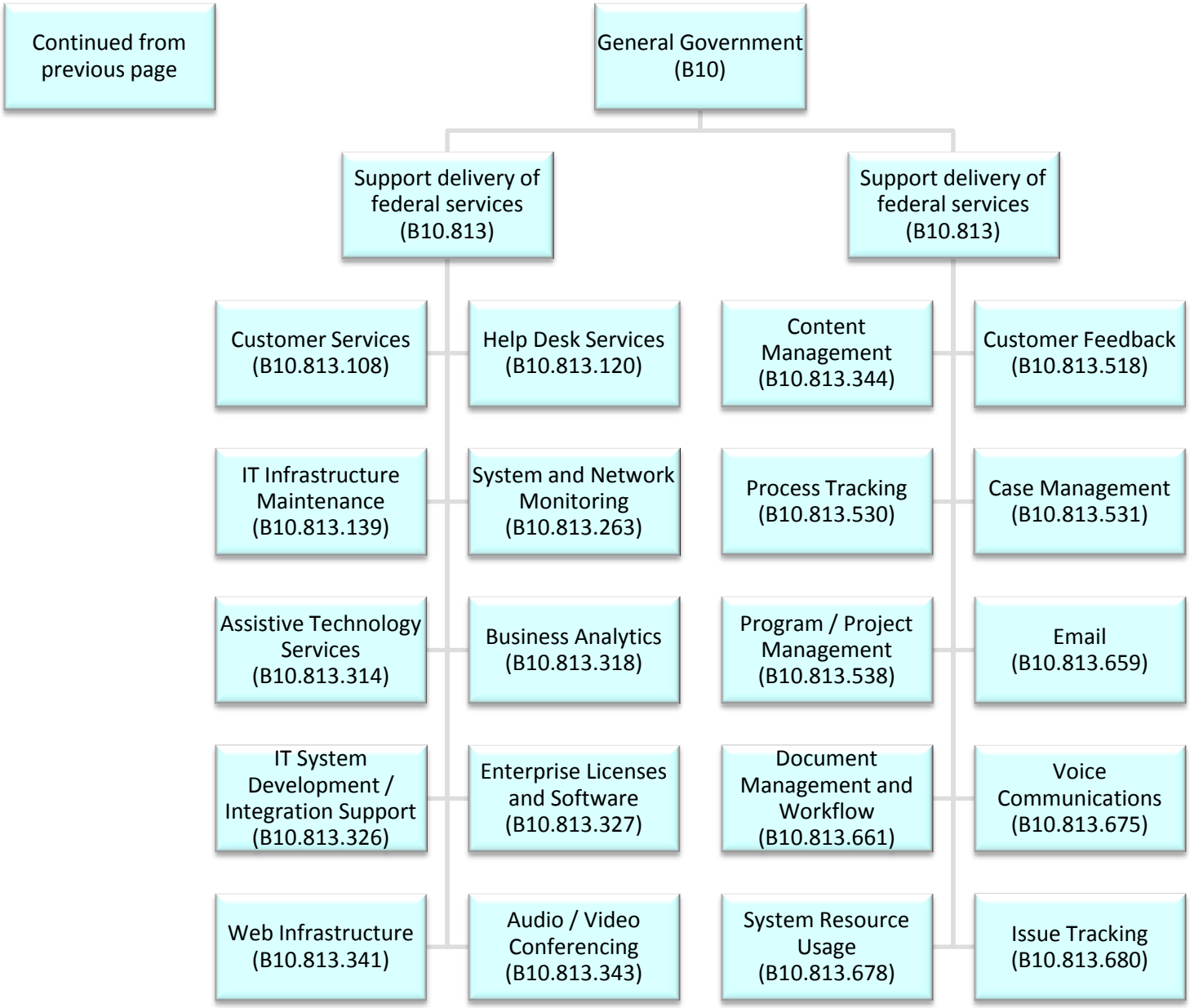

Transport and Space
(B09)
Space flight, research, and supporting activities
(B09.252)
Ground transportation
(B09.401)
Air transportation
(B09.402)
Water transportation
(B09.403)
Other transportation
(B09.407)
Space Exploration and Innovation
(B09.252.027)
Ground Transportation
(B09.401.061)
Air Transportation
(B09.402.060)
Water Transportation
(B09.403.062)
Navigation
(B09.407.312)
Space Operations
(B09.252.063)

Transport and Space (B09)				
Code	**Mission Sector**	**Business Function**	**Service**	**Definition**
B09.252	Transport and Space	Space flight, research, and supporting activities		Development and operation of space transportation systems, basic scientific research connected with outer space, research and demonstrations designed to promote terrestrial applications of technology developed through space research, and development of new space technologies for future flight missions. Also includes costs of tracking and data relay support for the National Aeronautics and Space Administration space science and applications for flight missions.
B09.252.027	Transport and Space	Space flight, research, and supporting activities	Space Exploration and Innovation	Space Exploration and Innovation includes all activities devoted to innovations directed at human and robotic space flight and the development and operation of space launch and transportation systems, and the general research and exploration of outer space
B09.252.063	Transport and Space	Space flight, research, and supporting activities	Space Operations	Space Operations involves the activities related to the safe launches/missions of passengers or goods into aerospace and includes commercial, scientific, and military operations.
B09.401.061	Transport and Space	Ground transportation	Ground Transportation	Ground Transportation involves the activities related to ensuring the availability of transit and the safe passage of passengers and goods over land.
B09.402.060	Transport and Space	Air transportation	Air Transportation	Air Transportation involves the activities related to the safe passage of passengers or goods through the air. It also includes command and control activities related to the safe movement of aircraft through all phases of flight for commercial and military operations.
B09.403.062	Transport and Space	Water transportation	Water Transportation	Water Transportation involves the activities related to ensuring the availability of transit and the safe passage of passengers and goods over sea and water.
B09.407.312	Transport and Space	Other transportation	Navigation	Navigation includes all means for the representation of position information through the use of attributes such as elevation, latitude, and longitude coordinates. This includes land-based and space-based geo-positioning technologies and services.


General Government (B10)
Continued on next page
Executive direction and management (B10.802)
Central fiscal operations (B10.803)
General property and records management (B10.804)
Enterprise Architecture (B10.802.103)
Strategic Planning (B10.802.104)
Budget and Performance Integration (B10.802.259)
IT Strategy and Innovation (B10.802..354)
External Partner Relationship Management (B10.802.517)
Portfolio Management (B10.802.546)
Performance Management (B10.802.547)
Budget Formulation (B10.803.101)
Budget Execution (B10.803.105)
Debt Collection (B10.803.116)
Travel (B10.803.122)
Accounting (B10.803.124)
Payments (B10.803.126)
Collections and Receivables (B10.803.127)
Taxation Management (B10.803.180)
Tax and Fiscal Policy (B10.803.260)
Collect Revenues and User Fees (B10.803.328)
Federal Asset Sales (B10.804.118)
Facilities, Fleet and Equipment Management (B10.804.119)
Goods and Services Acquisition (B10.804.143)
Inventory Control (B10.804.144)
Logistics Management (B10.804.145)
Management of Government Records (B10.804.345)


Continued from previous page
General Government (B10)
Continued on next page
Central personnel management (B10.805)
General purpose fiscal assistance (B10.806)
Other general government (B10.808)
Workforce Planning (B10.805.106)
Staffing and Recruiting (B10.805.251)
Credit and Insurance (B10.806.320)
Key Asset and Critical Infrastructure Protection (B10.808.034)
General Purpose Data and Statistics (B10.808.070)
Employee Benefits and Compensation (B10.805.254)
Employee Performance Management (B10.805.255)
Federal Financial Assistance (B10.806.362)
Inspection and Auditing (B10.808.077)
Permits and Licensing (B10.808.079)
Employee Relations (B10.805.256)
Separation Management (B10.805.257)
Federal Funds to States and Local Governments (B10.806.363)
Public Comment Tracking (B10.808.113)
Rule Publication (B10.808.115)
Time Reporting (B10.805.613)
Employee Development and Training (B10.805.618)
Reporting and Information (B10.808.129)
Legislative Functions (B10.808.176)
Payroll (B10.805.624)
Workforce Directory / Locator (B10.805.644)
Regulatory Compliance (B10.808.319)
Regulatory Enforcement (B10.808.321)
Public Communications Infrastructure (B10.808.322)
Continuity of Operations (B10.808.329)
Legislative Relations (B10.808.330)
Credential Issuance and Management (B10.808.337)
Mapping / Geospatial (B10.808.590)


Continued from previous page
General Government (B10)
Continued on next page
Cyber security management (B10.810)
Information sharing (B10.811)
Knowledge management (B10.812)
Security Management (B10.810.121)
Threat and Vulnerability Management (B10.810.315)
Continuous Monitoring (B10.810.316)
Data Integrity and Privacy Management (B10.810.317)
Identification and Authentication (B10.810.648)
Cryptography (B10.810.650)
Incident Response (B10.810.654)
Audit Trail Capture and Analysis (B10.810.655)
Certification and Accreditation (B10.810.656)
Information Discovery (B10.811.325)
Enterprise Search (B10.811.338)
Collaboration Tools (B10.811.340)
Information Exchange and Transformation (B10.811.353)
Correspondence Management (B10.811.533)
Data Mining (B10.811.592)
Data Exchange (B10.811.601)
Data Warehouse (B10.811.603)
Meta Data Management (B10.811.604)
Data Recovery (B10.811.608)
Community Management (B10.811.673)
Information Mapping / Taxonomy / Categorization (B10.811.339)
Knowledge Capture (B10.812.576)
Knowledge Distribution and Delivery (B10.812.577)


Continued from previous page
General Government (B10)
Support delivery of federal services (B10.813)
Support delivery of federal services (B10.813)
Customer Services (B10.813.108)
Help Desk Services (B10.813.120)
Content Management (B10.813.344)
Customer Feedback (B10.813.518)
IT Infrastructure Maintenance (B10.813.139)
System and Network Monitoring (B10.813.263)
Process Tracking (B10.813.530)
Case Management (B10.813.531)
Assistive Technology Services (B10.813.314)
Business Analytics (B10.813.318)
Program / Project Management (B10.813.538)
Email (B10.813.659)
IT System Development / Integration Support (B10.813.326)
Enterprise Licenses and Software (B10.813.327)
Document Management and Workflow (B10.813.661)
Voice Communications (B10.813.675)
Web Infrastructure (B10.813.341)
Audio / Video Conferencing (B10.813.343)
System Resource Usage (B10.813.678)
Issue Tracking (B10.813.680)

General Government (B10)				
Code	**Mission Sector**	**Business Function**	**Service**	**Definition**
B10.802.103	General Government	Executive direction and management	Enterprise Architecture	Enterprise Architecture is an established process for describing the current state and defining the target state and transition strategy for an organization's people, processes, and technology.
B10.802.104	General Government	Executive direction and management	Strategic Planning	Strategic Planning entails the determination of annual and long-term goals and the identification of the best approach for achieving those goals.
B10.802.259	General Government	Executive direction and management	Budget and Performance Integration	Budget and Performance Integration involves activities that align Federal resources allocated through budget formulation, execution, and management actions with examinations of program objectives, performance, and demonstrated results such as Program Performance Assessments, Government Performance Results Act (GPRA) plans and reports, performance-based agency budget submissions, and Financial Management Cost Accounting and Performance Measurement data.
B10.802.354	General Government	Executive direction and management	IT Strategy and Innovation	IT Strategy and Innovation includes all activities outside of normal Strategic Planning that focus on trying new approaches, new systems and thinking about/ planning IT investments in different ways.
B10.802.517	General Government	Executive direction and management	External Partner Relationship Management	Provides a framework to promote the effective collaboration between an organization and its business partners, particularly members of the distribution chain (e.g., channel and alliance partners, resellers, agents, brokers, and dealers) and other third parties that support operations and service delivery to an organization's customers; includes performance evaluation of partners, if necessary
B10.802.546	General Government	Executive direction and management	Portfolio Management	Defines the set of capabilities to support the administration of a group of investments held by an organization
B10.802.547	General Government	Executive direction and management	Performance Management	Defines the set of capabilities to measure the effectiveness of an organization's financial assets and capital. This can include Corrective Action, Program Evaluation, and Program Monitoring.

B10.803.101	General Government	Central fiscal operations	Budget Formulation	Budget Formulation involves all activities undertaken to determine priorities for future spending and to develop an itemized forecast of future funding and expenditures during a targeted period of time. This includes the collection and use of performance information to assess the effectiveness of programs and develop budget priorities.
B10.803.105	General Government	Central fiscal operations	Budget Execution	Budget Execution involves the legal (apportionment) and managerial (allotment and sub-allotment) distribution of budget authority to achieve results consistent with the formulated budget.
B10.803.116	General Government	Central fiscal operations	Debt Collection	Debt Collection supports activities associated with the collection of money owed to the U.S. government from both foreign and domestic sources.
B10.803.122	General Government	Central fiscal operations	Travel	Travel involves the activities associated with planning, preparing, and monitoring of business related travel for an organization's employees.
B10.803.124	General Government	Central fiscal operations	Accounting	Accounting entails accounting for assets, liabilities, fund balances, revenues and expenses associated with the maintenance of federal funds and expenditure of federal appropriations (Salaries and Expenses, Operation and Maintenance, Procurement, Working Capital, Trust Funds, etc.), in accordance with applicable federal standards (FASAB, Treasury, OMB, GAO, etc.).
B10.803.126	General Government	Central fiscal operations	Payments	Payments includes disbursements of federal funds, via a variety of mechanisms, to federal and private individuals, federal agencies, state, local and international governments, and the private sector, to effect payment for goods and services, or distribute entitlements, benefits, grants, subsidies, loans, or claims.
B10.803.127	General Government	Central fiscal operations	Collections and Receivables	The Collections and Receivables service includes deposits, fund transfers, and receipts for sales or service.
B10.803.180	General Government	Central fiscal operations	Taxation Management	Taxation Management includes activities associated with the implementation of the Internal Revenue Code and the collection of taxes in the United States and abroad.

B10.803.260	General Government	Central fiscal operations	Tax and Fiscal Policy	Tax and Fiscal Policy encompasses analysis of the implications for economic growth and stability in the United States and the world of Federal tax and spending policies. This includes assessing the sustainability of current programs and policies, the best means for raising revenues, the distribution of tax liabilities, and the appropriate limits on debt.
B10.803.328	General Government	Central fiscal operations	Collect Revenues and User Fees	Collect Revenues and User Fees supports activities associated with the collection of money owed to the U.S. government from both foreign and domestic sources. It also involves the collection of fees assessed on individuals or organizations for the provision of Government services and for the use of Government goods or resources.
B10.804.118	General Government	General property and records management	Federal Asset Sales	Federal Asset Sales encompasses the activities associated with the acquisition, oversight, tracking, and sale of non-internal assets managed by the federal government with a commercial value and sold to the private sector.
B10.804.119	General Government	General property and records management	Facilities, Fleet and Equipment Management	Facilities, Fleet, and Equipment Management involves the maintenance, administration, certification, and operation of office buildings, fleets, machinery, and other capital assets that are the responsibility of the federal government.
B10.804.143	General Government	General property and records management	Goods and Services Acquisition	Goods and Services Acquisition involves the procurement of physical goods, products, and capital assets to be used by the federal government and the oversight and/or management of contractors and service providers from the private sector.
B10.804.144	General Government	General property and records management	Inventory Control	Inventory Control refers to the tracking of information related to procured assets and resources with regard to quantity, quality, and location.
B10.804.145	General Government	General property and records management	Logistics Management	Logistics Management involves the planning and tracking of personnel and their resources in relation to their availability and location.

B10.804.345	General Government	General property and records management	Management of Government Records	Management of Government Records involves the management and stewardship of a type of information by the federal government in order to facilitate communication and information archival. This classification and taxonomic processes that links logical data and information sets.
B10.805.106	General Government	Central personnel management	Workforce Planning	Workforce Planning involves the processes for identifying the workforce competencies required to meet the agency's strategic goals and for developing the strategies to meet these requirements.
B10.805.251	General Government	Central personnel management	Staffing and Recruiting	Staffing and Recruiting establishes procedures for attracting and selecting high-quality, productive employees with the right skills and competencies, in accordance with merit system principles. This includes: establishing an applicant evaluation approach (which may include drug and alcohol testing); announcing the vacancy, sourcing and evaluating candidates against the competency requirements for the position; initiating pre-employment activities; and hiring employees.
B10.805.254	General Government	Central personnel management	Employee Benefits and Compensation	Employee Benefits and Compensation designs, develops, and implements benefits and compensation programs that attract, retain and fairly compensate agency employees. This Service includes: establishing and communicating benefits programs; processing benefits actions; and interacting as necessary with third party benefits providers. It also includes: developing and implementing compensation programs; administering bonus and monetary awards programs; administering pay changes; managing time, attendance, leave and pay; and managing payroll. In addition, designs, develops, and implements pay for performance compensation programs to recognize and reward high performance, with both base pay increases and performance bonus payments.

B10.805.255	General Government	Central personnel management	Employee Performance Management	Employee Performance Management designs, develops, and implements a comprehensive performance management approach to ensure agency employees are demonstrating competencies required of their work assignments. Design, develop and implement a comprehensive performance management strategy that enables managers to make distinctions in performance and links individual performance to agency goal and mission accomplishment. This Service also includes managing employee performance at the individual level and evaluating the overall effectiveness of the agency's employee development approach.
B10.805.256	General Government	Central personnel management	Employee Relations	Employee Relations designs, develops, and implements programs that strive to maintain an effective employer-employee relationship that balance the agency's needs against its employees' rights. This Service includes: addressing employee misconduct; addressing employee performance problems; managing administrative grievances; providing employee accommodation; administering employees assistance programs; participating in administrative third party proceedings; and determining candidate and applicant suitability.
B10.805.257	General Government	Central personnel management	Separation Management	Separation Management conducts efficient and effective employee separation programs that assist employees in transitioning to non-Federal employment; facilitates the removal of unproductive, non-performing employees; and assists employees in transitioning to retirement.
B10.805.613	General Government	Central personnel management	Time Reporting	Defines the set of capabilities to support the submission, approval and adjustment of an employee's hours
B10.805.618	General Government	Central personnel management	Employee Development and Training	Employee Development and Training designs, develops, and implements a comprehensive employee development and training approach to ensure that agency employees have the right competencies and skills for current and future work assignments. This includes conducting employee development needs assessments; designing employee development programs; administering and delivering employee development and training programs; and evaluating the overall effectiveness of the agency's employee development approach.

B10.805.624	General Government	Central personnel management	Payroll	Defines the set of capabilities to involve the administration of employees compensation
B10.805.644	General Government	Central personnel management	Workforce Directory / Locator	Defines the set of capabilities to support the listing of employees and their whereabouts
B10.806	General Government	General purpose fiscal assistance		Federal aid to state, local, and territorial governments that is available for general fiscal support. The transactions of the now discontinued general revenue-sharing program are included in the historical data for this subfunction. Also includes grants for more restricted purposes when the stipulated purposes cross two or more major budgetary functions and the distribution among those functions is at the discretion of the recipient jurisdiction rather than the federal government. Includes payments in lieu of taxes, broad-purpose shared revenues, and the federal payment to the District of Columbia. Excludes payments specifically for community development or social services programs.
B10.806.320	General Government	General purpose fiscal assistance	Credit and Insurance	Credit and Insurance includes providing protection to individuals or entities against specified risks (The specified protection generally involves risks that private sector entities are unable or unwilling to assume or subsidize and where the provision of insurance is necessary to achieve social objectives), Loan Guarantees and Direct Loans.
B10.806.362	General Government	General purpose fiscal assistance	Federal Financial Assistance	Federal Financial Assistance refers to the transfer of money, property, services, or anything of value, the principal purpose of which is to accomplish a public purpose of support or stimulation authorized by Federal statute. Assistance includes, but is not limited to grants, loans, loan guarantees, scholarships, mortgage loans, insurance, and other types of financial assistance, including cooperative agreements; property, technical assistance, counseling, statistical, and other expert information; and service activities of regulatory agencies.

B10.806.363	General Government	General purpose fiscal assistance	Federal Funds to States and Local Governments	Federal Funds to States and Local Governments includes Formula Grants, Project/Competitive Grants (Project/Competitive grants can include fellowships, scholarships, research grants, training grants, traineeships, experimental and demonstration grants, evaluation grants, planning grants, technical assistance grants, survey grants, and construction grants), State Loans, and other direct payment to State or Local jurisdictions by the Federal Government.
B10.808	General Government	Other general government		Miscellaneous other costs, such as federal costs of territorial governments.
B10.808.034	General Government	Other general government	Key Asset and Critical Infrastructure Protection	Key Asset and Critical Infrastructure Protection involves assessing key asset (e.g. bridge, power grid, dam, subways) and critical infrastructure vulnerabilities and taking direct action to mitigate vulnerabilities, enhance security, and ensure continuity and necessary redundancy in government operations and personnel.
B10.808.070	General Government	Other general government	General Purpose Data and Statistics	General Purpose Data and Statistics includes activities performed in providing empirical, numerical, and related data and information pertaining to the current state of the nation in areas such as the economy, labor, weather, international trade, etc.
B10.808.077	General Government	Other general government	Inspection and Auditing	Inspections and Auditing involves the methodical examination and review of regulated activities to ensure compliance with standards for regulated activity. This can include (but does not have to include) Firearms, Explosives, and Controlled Substances inspections and auditing.
B10.808.079	General Government	Other general government	Permits and Licensing	Permits and Licensing involves activities associated with granting, revoking, and the overall management of the documented authority necessary to perform a regulated task or function.
B10.808.113	General Government	Other general government	Public Comment Tracking	Public Comment Tracking involves the activities of soliciting, maintaining, and responding to public comments regarding proposed regulations.
B10.808.115	General Government	Other general government	Rule Publication	Rule Publication includes all activities associated with the publication of a proposed or final rule in the Federal Register and Code of Federal Regulations.
B10.808.129	General Government	Other general government	Reporting and Information	Reporting and Information includes providing financial information, reporting and analysis of financial transactions.

B10.808.176	General Government	Other general government	Legislative Functions	Legislative Functions is defined by the Executive branch processes associated with working with the Legislative Branch (i.e. Congress) except for the Tax Court, the Library of Congress, and the Government Printing Office revolving fund.
B10.808.319	General Government	Other general government	Regulatory Compliance	Activities associated with the direct monitoring and oversight of a specific industry or mission sector participating in a regulated activity including sector specific standard setting/reporting guideline development. Includes activities associated with developing sector specific regulations, policies, and guidance to implement laws to include public comment and tracking, regulatory creation, and rule publication.
B10.808.321	General Government	Other general government	Regulatory Enforcement	Activities associated with the direct enforcement of a specific industry or mission sector participating in a regulated activity using inspections and auditing. Includes activities associated with developing sector specific regulations, policies, and guidance to implement laws to include public comment and tracking, regulatory creation, and rule publication.
B10.808.322	General Government	Other general government	Public Communications Infrastructure	Public Communications Infrastructure includes the management and stewardship of a type of information by the federal government and/or the creation of physical communication infrastructures on behalf of the public in order to facilitate communication. This includes management of the nation's spectrum assets.
B10.808.329	General Government	Other general government	Continuity of Operations	Continuity of Operations involves the activities associated with the identification of critical systems and processes, and the planning and preparation required to ensure that these systems and processes will be available in the event of a catastrophic event and involves the internal actions necessary to develop a plan for resuming operations after a catastrophic event occurs. This can include Contingency Planning, Continuity of Operations and Service Recovery work.
B10.808.330	General Government	Other general government	Legislative Relations	Legislative Relations involves activities aimed at the development, tracking, and amendment of public laws through the legislative branch of the federal government. It includes tracking, testimony, proposal development and congressional liaison operations.

B10.808.337	General Government	Other general government	Credential Issuance and Management	Credential Issuance and Management: the researching, tracking and providing of user access credentials (logical and physicals) and associated security features for the protection of federal information and information systems from unauthorized access, use, disclosure, disruptions, modification, or destruction, as well as the creation and implementation of related security policies, procedures and controls. This includes background checks and related personnel security management services.
B10.808.590	General Government	Other general government	Mapping / Geospatial	Provide for the representation of mapping and geospatial information through the use of attributes such as zip code, country code, elevation, natural features and other spatial measures.
B10.810.121	General Government	Cyber security management	Security Management	Security Management involves the physical protection of an organization's personnel, assets, and facilities (including security clearance management). Note: Activities related to securing data and information systems are addressed under additional Services in the "810-Cyber security management" Function.
B10.810.315	General Government	Cyber security management	Threat and Vulnerability Management	Threat and Vulnerability Management involves all functions pertaining to the protection of federal information and information systems from unauthorized access, use, disclosure, disruptions, modification, or destruction, as well as the creation and implementation of security policies, procedures and controls. It includes all risk and controls tracking for IT systems.
B10.810.316	General Government	Cyber security management	Continuous Monitoring	Continuous Monitoring includes all activities related to the real-time monitoring of security controls employed within or inherited by a system. (see Appendix G of NIST Special Publication 800-37)
B10.810.317	General Government	Cyber security management	Data Integrity and Privacy Management	Data Integrity and Privacy Management involves the coordination of data collection, storage, dissemination, and destruction as well as managing the policies, guidelines, and standards regarding data management, so that data quality is maintained and information is shared or available in accordance with the law and best practices
B10.810.648	General Government	Cyber security management	Identification and Authentication	Defines the set of capabilities to support the management of permissions for logging onto a computer, application, service, or network; includes user management and role/privilege management. This includes Identification and Authentication for digital signatures

B10.810.650	General Government	Cyber security management	Cryptography	Defines the set of capabilities to support the use and management of ciphers, including encryption and decryption processes, to ensure confidentiality and integrity of data
B10.810.654	General Government	Cyber security management	Incident Response	Defines the set of capabilities to provide active response and remediation to a security incident that has allowed unauthorized access to a government information system
B10.810.655	General Government	Cyber security management	Audit Trail Capture and Analysis	Defines the set of capabilities to support the identification and monitoring of activities within an application, system, or network
B10.810.656	General Government	Cyber security management	Certification and Accreditation	Defines the set of capabilities to support the certification and accreditation (C&A) of federal information systems, as described in NIST SP800-37.
B10.811.325	General Government	Information sharing	Information Discovery	Information Discovery consists of all activities used to obtain information that is not readily obtainable.
B10.811.338	General Government	Information sharing	Enterprise Search	Enterprise Search includes Query capabilities, Precision / Recall Ranking, Classification and Pattern Matching.
B10.811.340	General Government	Information sharing	Collaboration Tools	The Tools or systems that allow multiple parties to interact and share documents or data through a shared work space or environment. Multiple parties contribute or update the shared environment and view, update, edit, & share files. This includes systems such as SharePoint, MAX, Web Conferencing, Cisco TelePresence, etc.)
B10.811.353	General Government	Information sharing	Information Exchange and Transformation	Information Exchange and Transformation – The tools and systems used to search, link, analyze, share and transport information such as reports or critical mission data. Transformation includes the set of capabilities to support the removal of incorrect or unnecessary characters and data from a data source
B10.811.533	General Government	Information sharing	Correspondence Management	Correspondence Management is the set of capabilities used to manage externally initiated and internally initiated communication between an organization and its stakeholders.
B10.811.592	General Government	Information sharing	Data Mining	Defines the set of capabilities to provide for the efficient discovery of non-obvious, valuable patterns and relationships within a large collection of data

B10.811.601	General Government	Information sharing	Data Exchange	Supports the interchange of information between multiple systems and applications; includes verification that transmitted data was received unaltered.
B10.811.603	General Government	Information sharing	Data Warehouse	Defines the set of capabilities to support the archiving and storage of large volumes of data
B10.811.604	General Government	Information sharing	Meta Data Management	Support the maintenance and administration of data that describes data
B10.811.608	General Government	Information sharing	Data Recovery	Defines the set of capabilities to support the restoration and stabilization of data sets to a consistent, desired state
B10.811.673	General Government	Information sharing	Community Management	Defines the set of capabilities to support the administration of online groups that share common interests
B10.811.339	General Government	Information sharing	Information Mapping / Taxonomy / Categorization	Information Mapping/ Taxonomy/ Categorization defines the set of capabilities to support the creation and maintenance of relationships between data entities, naming standards and categorization and allow classification of data and information into specific layers or types to support an organization.
B10.812.576	General Government	Knowledge management	Knowledge Capture	Defines the set of capabilities to facilitate collection of data and information
B10.812.577	General Government	Knowledge management	Knowledge Distribution and Delivery	Defines the set of capabilities to support the transfer of knowledge to the end customer.
B10.813.108	General Government	Support delivery of federal services	Customer Services	Customer Services supports activities associated with providing an agency's customers with information regarding the agency's service offerings and managing the interactions and relationships with those customers.
B10.813.120	General Government	Support delivery of federal services	Help Desk Services	Help Desk Services involves the management of a service center to respond to government and contract employees' technical and administrative questions.
B10.813.139	General Government	Support delivery of federal services	IT Infrastructure Maintenance	IT Infrastructure Maintenance involves the planning, design, and maintenance of an IT Infrastructure to effectively support automated needs (i.e. platforms, networks, servers, printers, etc.).

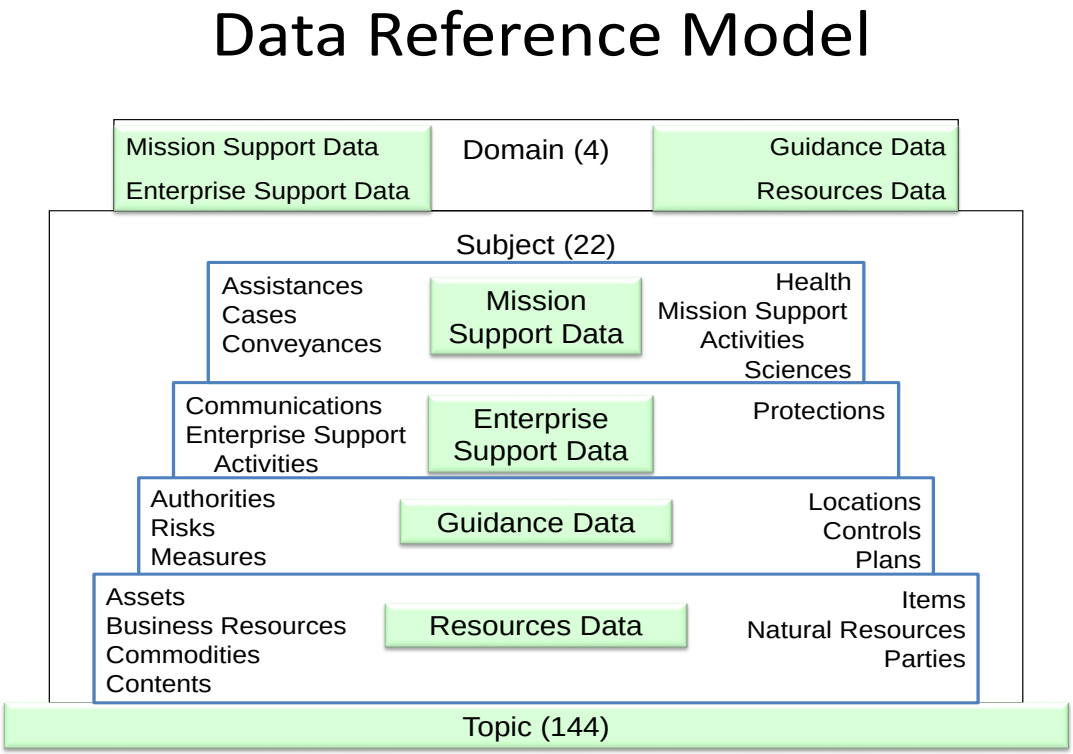
B10.813.263	General Government	Support delivery of federal services	System and Network Monitoring	System and Network Monitoring supports all activities related to the real-time monitoring of systems and networks for optimal performance.
B10.813.314	General Government	Support delivery of federal services	Assistive Technology Services	Assistive Technology Services is composed of hardware and software that help people who are physically or visually impaired, as well as ensuring electronic and information technology is accessible to people with disabilities, including employees and members of the public (i.e. 508 Compliant). This includes developing standards for all electronic and information technology.
B10.813.318	General Government	Support delivery of federal services	Business Analytics	Business analytics includes all forms of data analysis of extremely large, complex data sets (big data) that are manipulated for business (mission) consumption.
B10.813.326	General Government	Support delivery of federal services	IT System Development / Integration Support	IT System Development / Integration Support includes the software services enabling elements of distributed business applications to interoperate and the software development necessary to facilitate such integration. These elements can share function, content, and communications across heterogeneous computing environments.
B10.813.327	General Government	Support delivery of federal services	Enterprise Licenses and Software	Enterprise Licenses and Software includes License Management and Software Distribution; it supports the purchase, upgrade and tracking of legal usage contracts for system software and applications and supports the propagation, installation and upgrade of written computer programs, applications and components.
B10.813.341	General Government	Support delivery of federal services	Web Infrastructure	Web Infrastructure includes equipment/services to support delivery of services over the Internet or similar networks. These include supporting: Network Services which consists of protocols defining the format and structure of data and information either accessed from a directory or exchanged through communications; Service Transport which consists of protocols defining the format and structure of data and information either accessed from a directory or exchanged through communications.

B10.813.343	General Government	Support delivery of federal services	Audio / Video Conferencing	Audio / Video Conferencing entails communication across long distances with audio and / or video contact that may also include graphics and data exchange and includes all equipment, software, hardware, networks, etc. necessary to perform these functions.
B10.813.344	General Government	Support delivery of federal services	Content Management	Content Management includes Content Authoring, Content Review and Approval, Tagging and Aggregation, Content Publishing and Delivery and Syndication Management.
B10.813.518	General Government	Support delivery of federal services	Customer Feedback	Collect, analyze and handle comments and feedback from an organization's customers, both before and after a product or service is offered.
B10.813.530	General Government	Support delivery of federal services	Process Tracking	Defines the set of capabilities to manage business processes, including business process mapping, remapping, reengineering, and business process improvement efforts.
B10.813.531	General Government	Support delivery of federal services	Case Management	Manages the lifecycle of a particular claim or investigation within an agency to include creating, routing, tracing, assigning, and closing of a case. Includes the monitoring of activities within the business cycle and supporting the conclusion of contention or differences within the business cycle.
B10.813.538	General Government	Support delivery of federal services	Program / Project Management	Defines the set of capabilities to manage and control a particular effort of an organization. This includes intra-agency work.
B10.813.659	General Government	Support delivery of federal services	Email	Defines the set of capabilities to support the transmission of communications over a network. Includes instant messaging
B10.813.661	General Government	Support delivery of federal services	Document Management and workflow	Defines the set of capabilities to support the creation, use, archiving and deletion of unstructured data. This includes the set of capabilities to support the design, generation and maintenance of electronic or physical forms and templates

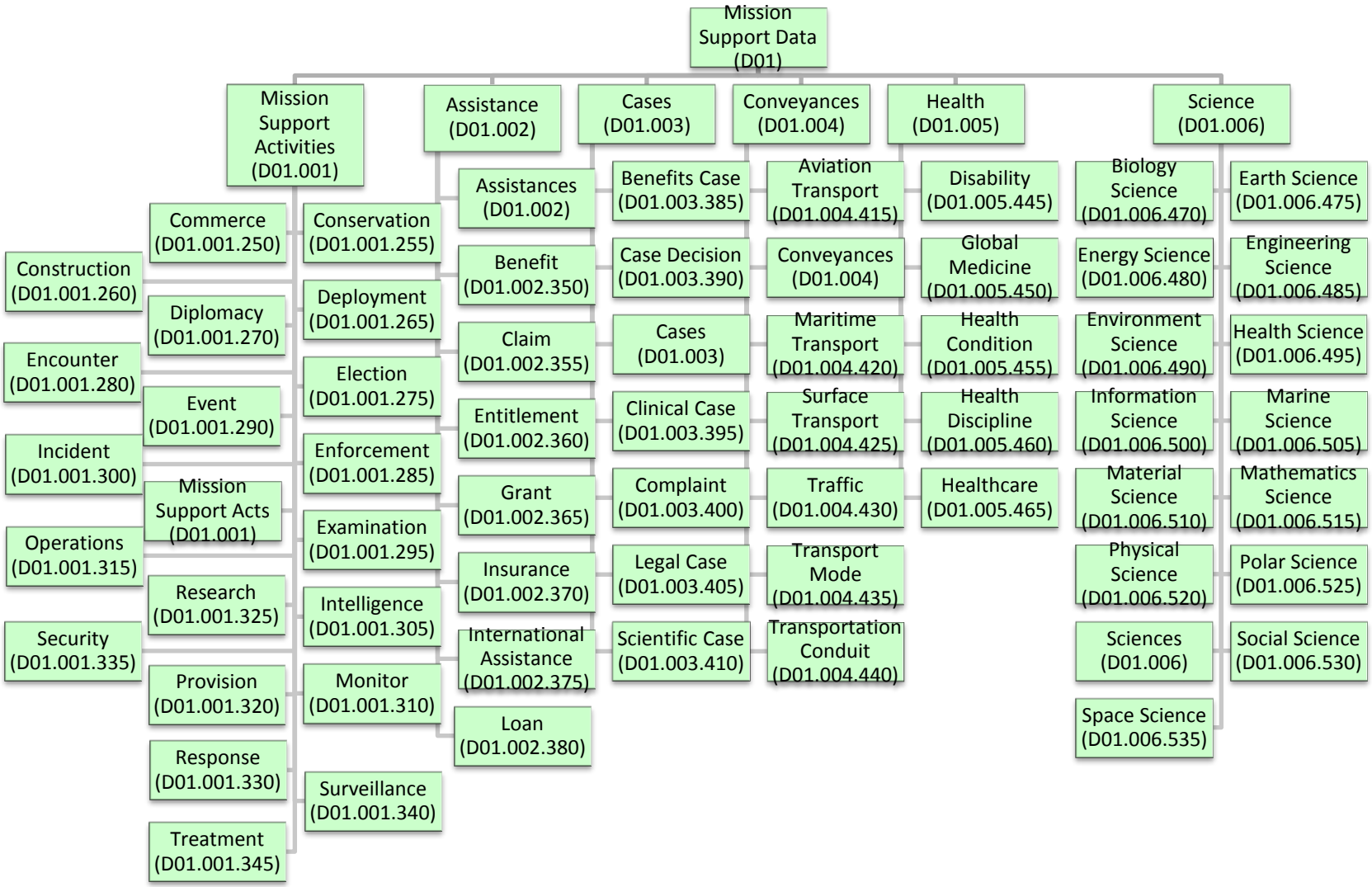
B10.813.675	General Government	Support delivery of federal services	Voice Communications	Defines the set of capabilities to provide telephony or other voice communications
B10.813.678	General Government	Support delivery of federal services	System Resource Usage	Support the balance and allocation of memory, usage, disk space and performance on computers and their applications.
B10.813.680	General Government	Support delivery of federal services	Issue Tracking	Defines the set of capabilities to receive and track user-reported issues and problems in using IT systems, including help desk calls

Appendix I: Data Reference Model Taxonomy with Definitions

The Data Reference Model (DRM) taxonomy is defined by a hierarchy in three layers, as illustrated below. The top rank of the hierarchy consists of four Domains. The middle layer of the hierarchy contains twenty-two Subject elements and the lowest rank of the hierarchy includes one hundred and forty-four Topic elements. The DRM provides a structure and vocabulary for agencies to form a consensus as to how, at a Federal level, to categorize, describe, and share data.



In the sections below, each DRM Domain is shown as a tree diagram, followed by definitions of the taxonomy elements in the corresponding tree.


Mission Support Data (D01)
Mission Support Activities (D01.001)
Assistance (D01.002)
Cases (D01.003)
Conveyances (D01.004)
Health (D01.005)
Science (D01.006)
Construction (D01.001.260)
Encounter (D01.001.280)
Incident (D01.001.300)
Operations (D01.001.315)
Security (D01.001.335)
Commerce (D01.001.250)
Diplomacy (D01.001.270)
Event (D01.001.290)
Mission Support Acts (D01.001)
Research (D01.001.325)
Provision (D01.001.320)
Response (D01.001.330)
Treatment (D01.001.345)
Conservation (D01.001.255)
Deployment (D01.001.265)
Election (D01.001.275)
Enforcement (D01.001.285)
Examination (D01.001.295)
Intelligence (D01.001.305)
Monitor (D01.001.310)
Surveillance (D01.001.340)
Assistances (D01.002)
Benefit (D01.002.350)
Claim (D01.002.355)
Entitlement (D01.002.360)
Grant (D01.002.365)
Insurance (D01.002.370)
International Assistance (D01.002.375)
Loan (D01.002.380)
Benefits Case (D01.003.385)
Case Decision (D01.003.390)
Cases (D01.003)
Clinical Case (D01.003.395)
Complaint (D01.003.400)
Legal Case (D01.003.405)
Scientific Case (D01.003.410)
Aviation Transport (D01.004.415)
Conveyances (D01.004)
Maritime Transport (D01.004.420)
Surface Transport (D01.004.425)
Traffic (D01.004.430)
Transport Mode (D01.004.435)
Transportation Conduit (D01.004.440)
Disability (D01.005.445)
Global Medicine (D01.005.450)
Health Condition (D01.005.455)
Health Discipline (D01.005.460)
Healthcare (D01.005.465)
Biology Science (D01.006.470)
Energy Science (D01.006.480)
Environment Science (D01.006.490)
Information Science (D01.006.500)
Material Science (D01.006.510)
Physical Science (D01.006.520)
Sciences (D01.006)
Space Science (D01.006.535)
Earth Science (D01.006.475)
Engineering Science (D01.006.485)
Health Science (D01.006.495)
Marine Science (D01.006.505)
Mathematics Science (D01.006.515)
Polar Science (D01.006.525)
Social Science (D01.006.530)

Mission Support Data (D01)				
Mission Support Data created and used by the enterprise is unique to the primary purpose(s) served by the enterprise, in that either the data is not typically used in other enterprises or is used in a significantly different manner than is typical.				
Code	**Domain**	**Subject**	**Topic**	**Definition**
D01.001	Mission Support Data	Mission Support Activities		Data describing the support required for an action, function, connection, relationship, or outcome involving parties, guidance and/or resources relevant to a mission or purpose.
D01.001.250	Mission Support Data	Mission Support Activities	Commerce	Data about activities for exchange or buying and selling of commodities on a large scale involving transportation from place to place.
D01.001.255	Mission Support Data	Mission Support Activities	Conservation	Data about activities to support the actions and kinds of natural resources being conserved.
D01.001.260	Mission Support Data	Mission Support Activities	Construction	Data about activities involved with the building occupation or industry.
D01.001.265	Mission Support Data	Mission Support Activities	Deployment	Data about activities to position, deliver or control resources or things in response to military, emergency, enforcement or other governmental requirements.
D01.001.270	Mission Support Data	Mission Support Activities	Diplomacy	Data about activities supporting the conduct by government officials of negotiations and/or relations between nations.
D01.001.275	Mission Support Data	Mission Support Activities	Election	Data about activities for the selection of a person or persons for office by vote, and the governing of associated activity by candidates and voters.
D01.001.280	Mission Support Data	Mission Support Activities	Encounter	Data about activities supporting the interaction between a person, organization or thing and a representative of the federal government or device for a specific purpose.
D01.001.285	Mission Support Data	Mission Support Activities	Enforcement	Data about activities involved with applying, executing, and implementing laws and regulations.
D01.001.290	Mission Support Data	Mission Support Activities	Event	Data about the support of a planned, non-emergency activity occurring in a particular place during a particular interval of time.
D01.001.295	Mission Support Data	Mission Support Activities	Examination	Data about activities supporting a thorough analysis, review, or evaluation of a person, place, object, or event in reference to a standard or requirement.

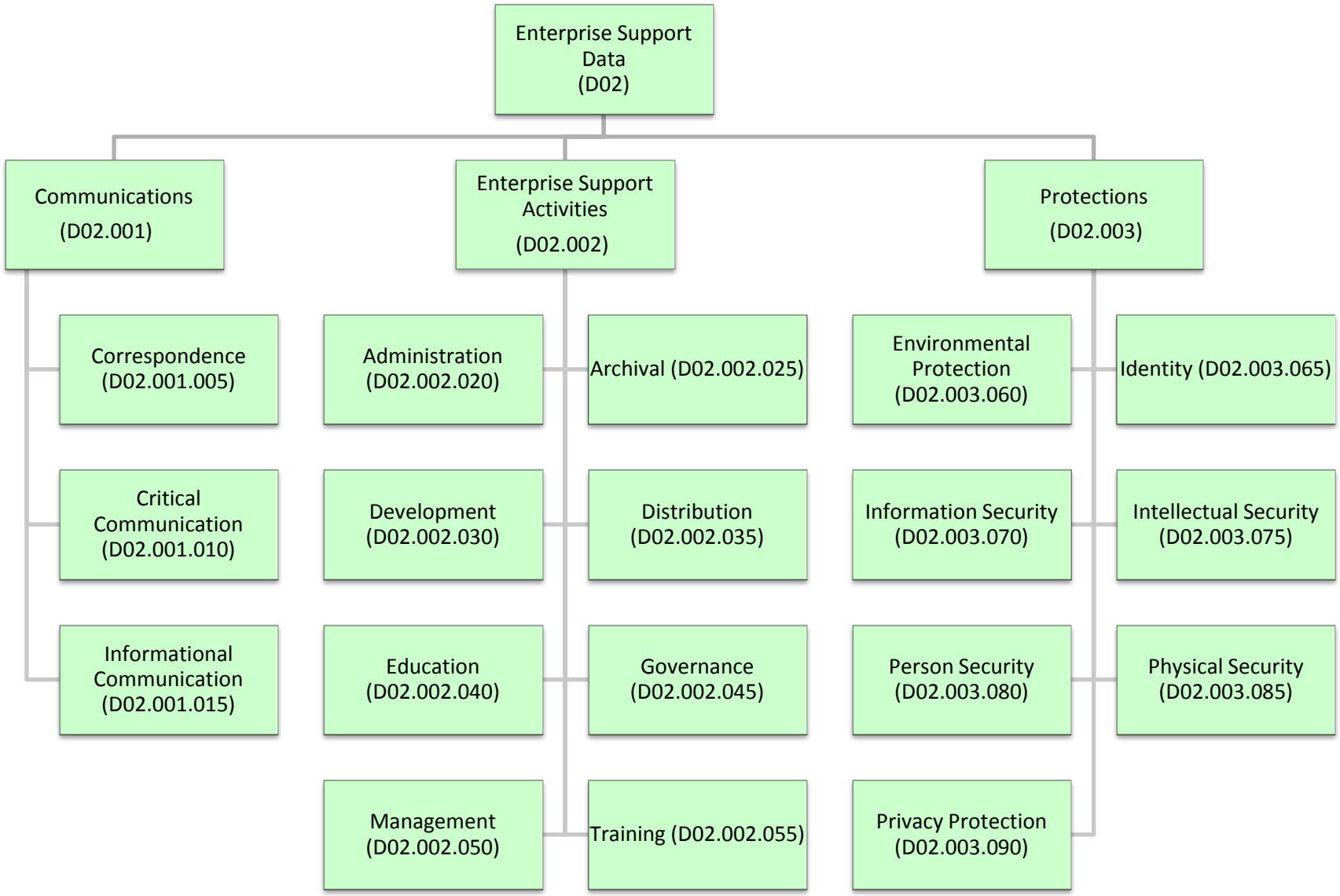
D01.001.300	Mission Support Data	Mission Support Activities	Incident	Data about an unplanned or spontaneous activity or set of activities occurring in a particular place with a start and end time.
D01.001.305	Mission Support Data	Mission Support Activities	Intelligence	Data about activities supporting the collection, analysis, and dissemination of information or knowledge of an event, circumstance or threat that may cause injury, disruption or impact National interests.
D01.001.310	Mission Support Data	Mission Support Activities	Monitor	Data about activities related to the continuous or repeated observation, measurement, surveying, and evaluation of activities or conditions for defined purposes, according to prearranged schedules, and using comparable methods for sensing and data collection.
D01.001.315	Mission Support Data	Mission Support Activities	Operations	Data about the support of a planned security, national threat or emergency engagement occurring in a particular place during a particular interval of time.
D01.001.320	Mission Support Data	Mission Support Activities	Provision	Data about activities or actions taken to plan for, respond to, and repair the effects of all incidents or events whether natural or man-made that may cause injury or death.
D01.001.325	Mission Support Data	Mission Support Activities	Research	Data about activities supporting a scientific undertaking or investigation of interest to one of the governmental or scientific communities or sectors.
D01.001.330	Mission Support Data	Mission Support Activities	Response	Data about activities or actions taken to safeguard, secure or respond to an incident or inquiry.
D01.001.335	Mission Support Data	Mission Support Activities	Security	Data about activities or actions taken to protect, secure, stabilize or prevent exposure, injury, damage, or destruction.
D01.001.340	Mission Support Data	Mission Support Activities	Surveillance	Data about activities or actions taken to closely observe, monitor and analyze a person, group, population or object, especially one under suspicion or concern.
D01.001.345	Mission Support Data	Mission Support Activities	Treatment	Data about activities taken to control, prevent or eradicate chemical, medical or biological threats.
D01.002	Mission Support Data	Assistances		Data describing the resources available for promoting or enhancing the well-being of parties through permissions, privileges, monies, goods, or services transferred to eligible parties.
D01.002.350	Mission Support Data	Assistances	Benefit	Data describing a resource supporting, promoting or enhancing the well-being of a party.

D01.002.355	Mission Support Data	Assistances	Claim	Data describing a request or demand for payment in accordance with an insurance policy, a workers' compensation law or other benefit or entitlement program.
D01.002.360	Mission Support Data	Assistances	Entitlement	Data describing a package of compensation provided to a party.
D01.002.365	Mission Support Data	Assistances	Grant	Data describing a form of monetary or other non-emergency aid provided to a party.
D01.002.370	Mission Support Data	Assistances	Insurance	Data describing a resource for assisting individuals or entities that provides protection or support against specified risks in order to meet or achieve social objectives.
D01.002.375	Mission Support Data	Assistances	International Assistance	Data describing aid, privileges, monetary help, and/or development projects provided to foreign governments to assist in meeting government goals and objectives.
D01.002.380	Mission Support Data	Assistances	Loan	Data describing a resource, usually monetary, temporarily furnished to a party with the understanding it will be returned, possibly for a fee.
D01.003	Mission Support Data	Cases		Data about a particular party or parties used to determine an outcome or course of action either legal, clinical or scientific, and ensure compliance with applicable laws and regulations.
D01.003.385	Mission Support Data	Cases	Benefits Case	Data describing the steps or processes for providing benefits, grants and other means of assistance such as veterans or welfare-related as part of a legal or government program.
D01.003.390	Mission Support Data	Cases	Case Decision	Data describing the outcome of a case or hearing based on the determination of the evidence and arguments presented.
D01.003.395	Mission Support Data	Cases	Clinical Case	Data describing the steps or processes performed and for documenting the observed symptoms and course of a disease.
D01.003.400	Mission Support Data	Cases	Complaint	Data describing the steps or processes for responding to or rectifying problems or issues associated with benefits, grants and other means of assistance or services.
D01.003.405	Mission Support Data	Cases	Legal Case	Data describing the steps or processes for resolving a dispute between opposing parties or administering a law and is resolved by a court, or by some equivalent legal process. There is a defendant and an accusing or opposing party either a person or organization.

D01.003.410	Mission Support Data	Cases	Scientific Case	Data describing the steps or processes for the collection of data through observation and experiment, and the formulation and testing of hypotheses.
D01.004	Mission Support Data	Conveyances		Data describing the business processes and the means of transportation from one place to another place.
D01.004.415	Mission Support Data	Conveyances	Aviation Transport	Design, development, production, operation, and use of aviation equipment and infrastructure.
D01.004.420	Mission Support Data	Conveyances	Maritime Transport	Design, development, production, operation, and use of maritime equipment and infrastructure.
D01.004.425	Mission Support Data	Conveyances	Surface Transport	Design, development, production, operation, and use of land/surface transport equipment and infrastructure.
D01.004.430	Mission Support Data	Conveyances	Traffic	A collection of people, things, and/or conveyances in transit via a transportation conduit.
D01.004.435	Mission Support Data	Conveyances	Transport Mode	A type of transportation object or method used to move people or objects.
D01.004.440	Mission Support Data	Conveyances	Transportati on Conduit	A specific infrastructure or route where people, things, and/or conveyances move and are controlled.
D01.005	Mission Support Data	Health		Data describing the business functions and things related to diseases and medical or clinical support services, processes or provisioning activities.
D01.005.445	Mission Support Data	Health	Disability	Data describing the mental and / or physical disabilities, providing services for people with disabilities, detection of disabilities, and improving access and fulfillment of ADA requirements.
D01.005.450	Mission Support Data	Health	Global Medicine	Data describing the medical or clinical information specific to international situations.
D01.005.455	Mission Support Data	Health	Health Condition	Data describing the level of functional or metabolic efficiency of a living being.
D01.005.460	Mission Support Data	Health	Health Discipline	Data describing the disciplines that specifically relate to medical or clinical specializations.
D01.005.465	Mission Support Data	Health	Healthcare	Data describing the medical or clinical information specific to the care of an individual.
D01.006	Mission Support Data	Sciences		Data describing any domain of knowledge accumulated by scientific study and organized by general principles.

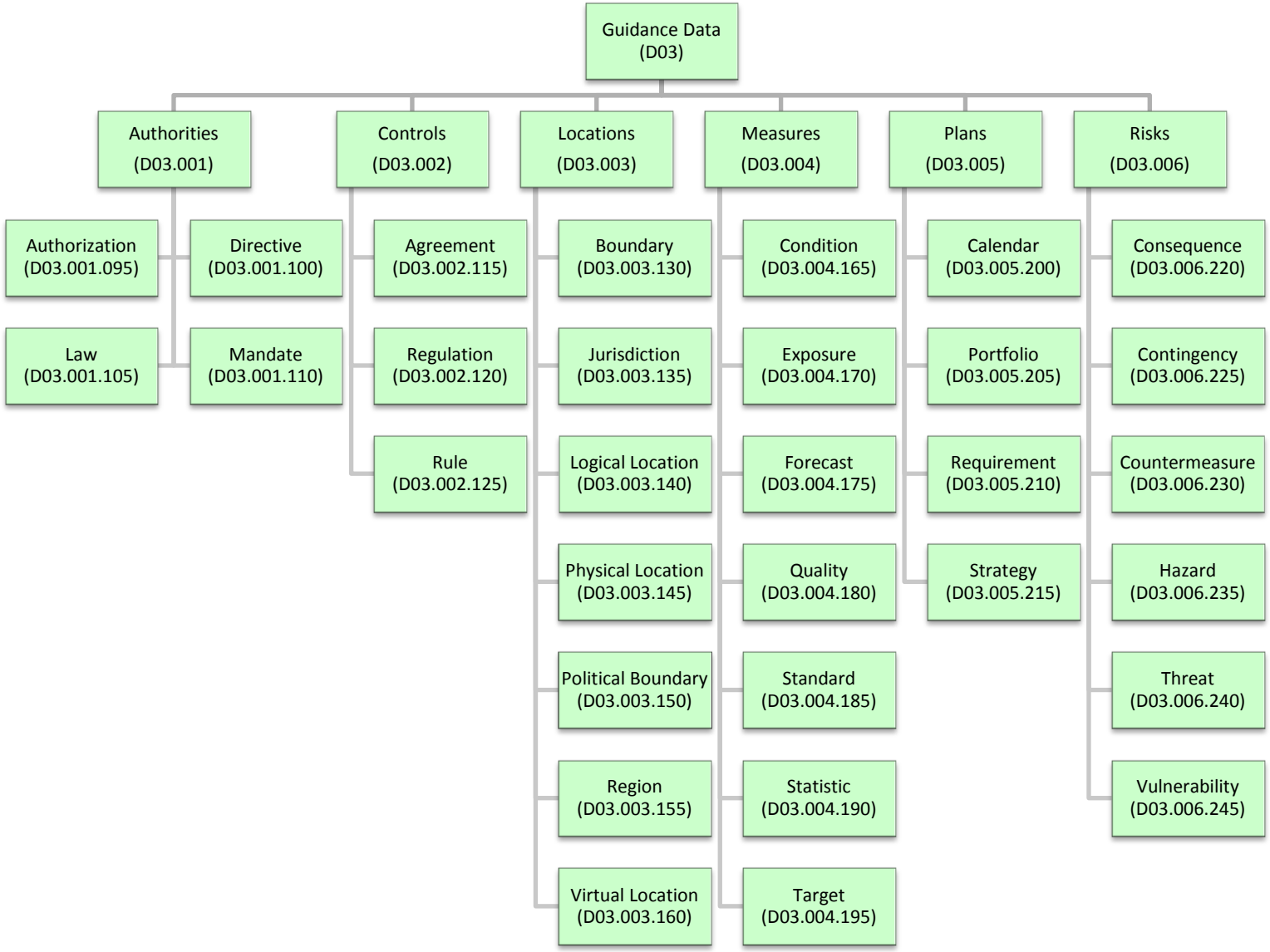
D01.006.470	Mission Support Data	Sciences	Biology Science	Data describing the discipline that deals with the science of life and life processes; includes the study of structure, origin, evolution, and distribution of living organisms.
D01.006.475	Mission Support Data	Sciences	Earth Science	Data describing the discipline for all sciences related to the study of the Earth and the materials of which it is made. This includes the atmospheric sciences and meteorology, geology, geophysics, seismology, volcanology, oceanography and related marine sciences, such as hydrology.
D01.006.480	Mission Support Data	Sciences	Energy Science	Data describing the discipline for applying scientific knowledge to energy problems.
D01.006.485	Mission Support Data	Sciences	Engineering Science	Data describing the discipline for applying scientific knowledge to practical problems.
D01.006.490	Mission Support Data	Sciences	Environment Science	Data describing the discipline for the interactions between the physical, chemical, and biological components of the environment, including their effects on all types of organisms.
D01.006.495	Mission Support Data	Sciences	Health Science	Data describing the discipline for diagnosing, treating, or preventing disease and other damage to the body or mind.
D01.006.500	Mission Support Data	Sciences	Information Science	Data describing the interdisciplinary science primarily concerned with the analysis, collection, classification, manipulation, storage, retrieval and dissemination of information and knowledge.
D01.006.505	Mission Support Data	Sciences	Marine Science	Data describing the discipline concerned with oceans, marine biology and related marine sciences.
D01.006.510	Mission Support Data	Sciences	Material Science	Data describing the discipline for the study of the structure and properties of any material, as well as using this body of knowledge to create new types of materials, and to tailor the properties of a material for specific uses.
D01.006.515	Mission Support Data	Sciences	Mathematics Science	Data describing the discipline that deals with numbers, quantities, shapes, patterns measurement, and the concepts related to them, and their relationships.
D01.006.520	Mission Support Data	Sciences	Physical Science	Data describing the discipline for studying the science of matter and energy and their interactions; includes chemistry, physics, and astronomy.
D01.006.525	Mission Support Data	Sciences	Polar Science	Data describing the discipline of study that deals with the science of Arctic and Antarctic regions, including exploration and research.

D01.006.530	Mission Support Data	Sciences	Social Science	Data describing the discipline for the branch of science that studies society and the relationships of individuals within a society.
D01.006.535	Mission Support Data	Sciences	Space Science	Data describing the discipline for the study of life and structures in space including space exploration, space medicine, and planetary science.


Enterprise Support Data (D02)
Communications (D02.001)
Enterprise Support Activities (D02.002)
Protections (D02.003)
Correspondence (D02.001.005)
Critical Communication (D02.001.010)
Informational Communication (D02.001.015)
Administration (D02.002.020)
Development (D02.002.030)
Education (D02.002.040)
Management (D02.002.050)
Archival (D02.002.025)
Distribution (D02.002.035)
Governance (D02.002.045)
Training (D02.002.055)
Environmental Protection (D02.003.060)
Information Security (D02.003.070)
Person Security (D02.003.080)
Privacy Protection (D02.003.090)
Identity (D02.003.065)
Intellectual Security (D02.003.075)
Physical Security (D02.003.085)

Enterprise Support Data (D02)				
Enterprise Support Data includes categories for data created or used for common or corporate purpose(s), in that the data is typically used in most enterprises in support of more mission-specific activities.				
Code	**Domain**	**Subject**	**Topic**	**Definition**
D02.001	Enterprise Support Data	Communications		Data describing the creation, distribution and delivery of data, information or messages either verbal, electronic or written targeted at a specific audience.
D02.001.005	Enterprise Support Data	Communications	Correspondence	Data describing the form of written communication sent or received in the course of affairs intended to deliver timely information.
D02.001.010	Enterprise Support Data	Communications	Critical Communication	Data describing a notice or message that needs to be delivered expeditiously due to its content, such as a notice of an imminent threat, impending hazard, risk or incident posing a threat to life or property or a message providing coordination information to emergency responders.
D02.001.015	Enterprise Support Data	Communications	Informational Communication	Data describing the memo or message containing information publicly available to any member of the public.
D02.002	Enterprise Support Data	Enterprise Support Activities		Data describing the support required for an action, function, connection, relationship, or outcome involving parties, guidance and/or resources relevant to enterprise.
D02.002.020	Enterprise Support Data	Enterprise Support Activities	Administration	Data about activities to manage or supervise the execution, use, or conduct of laws, regulations and standards.
D02.002.025	Enterprise Support Data	Enterprise Support Activities	Archival	Data about activities to support development and support of archives and / or museums of historical and cultural artifacts.
D02.002.030	Enterprise Support Data	Enterprise Support Activities	Development	Data about activities to create, conduct, promote or market something over time.
D02.002.035	Enterprise Support Data	Enterprise Support Activities	Distribution	Data about activities involved with delivering, disseminating or conveying information or things.

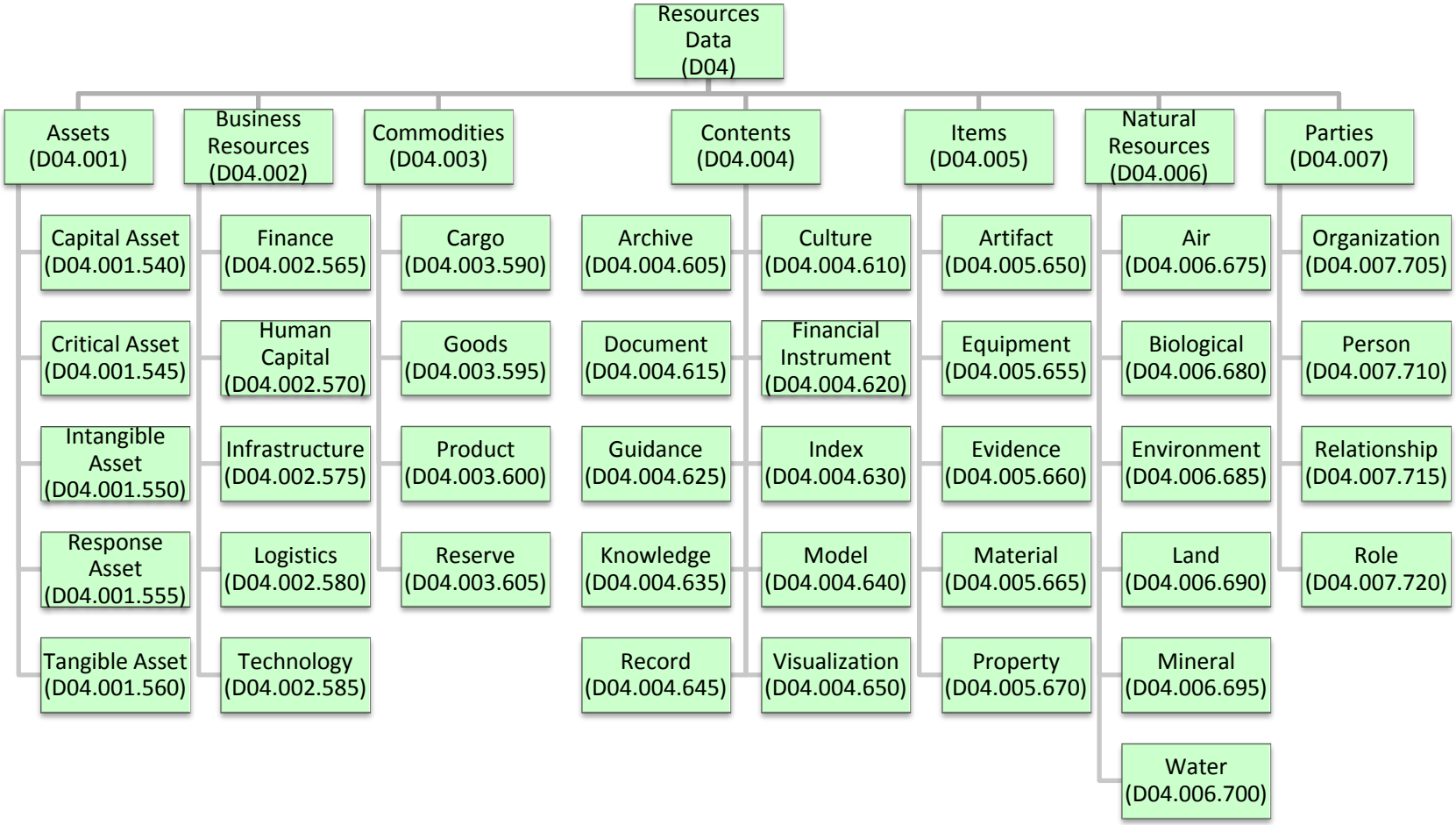
D02.002.040	Enterprise Support Data	Enterprise Support Activities	Education	Data about activities for the imparting or acquiring of general knowledge, developing the powers of reasoning and judgment, and preparing intellectually.
D02.002.045	Enterprise Support Data	Enterprise Support Activities	Governance	Data about activities supporting the systematic method of exercising authority by guiding actions and conduct to achieve desired outcomes and/or compliance.
D02.002.050	Enterprise Support Data	Enterprise Support Activities	Management	Data about activities connected with conducting or supervising something or someone.
D02.002.055	Enterprise Support Data	Enterprise Support Activities	Training	Data about activities performed for the purpose of education or instruction to develop skill or understanding in serving a business need.
D02.003	Enterprise Support Data	Protections		Data describing the identification of precautions or protection required to guard against damage, crime, attack, or accident in order to protect, defend, monitor and provide a sense of safety.
D02.003.060	Enterprise Support Data	Protections	Environmental Protection	Data describing the protection of the environmental resources.
D02.003.065	Enterprise Support Data	Protections	Identity	Data describing the protection of the set of uniquely distinguishing characteristics by which an entity is definitively recognizable or known.
D02.003.070	Enterprise Support Data	Protections	Information Security	Data describing the protection of information, detection capabilities, support and internet-related systems and services from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users.
D02.003.075	Enterprise Support Data	Protections	Intellectual Security	Data describing the protection of ideas, art and other intellectual property.
D02.003.080	Enterprise Support Data	Protections	Person Security	Data describing the protection of individuals, detection capabilities and support services.
D02.003.085	Enterprise Support Data	Protections	Physical Security	Data describing the protection of physical structures, detection capabilities and support services.
D02.003.090	Enterprise Support Data	Protections	Privacy Protection	Data describing the protection of confidential personal or organizational information whose exposure would cause harm or injury.


Guidance Data (D03)
Authorities (D03.001)
Controls (D03.002)
Locations (D03.003)
Measures (D03.004)
Plans (D03.005)
Risks (D03.006)
Authorization (D03.001.095)
Directive (D03.001.100)
Law (D03.001.105)
Mandate (D03.001.110)
Agreement (D03.002.115)
Regulation (D03.002.120)
Rule (D03.002.125)
Boundary (D03.003.130)
Jurisdiction (D03.003.135)
Logical Location (D03.003.140)
Physical Location (D03.003.145)
Political Boundary (D03.003.150)
Region (D03.003.155)
Virtual Location (D03.003.160)
Condition (D03.004.165)
Exposure (D03.004.170)
Forecast (D03.004.175)
Quality (D03.004.180)
Standard (D03.004.185)
Statistic (D03.004.190)
Target (D03.004.195)
Calendar (D03.005.200)
Portfolio (D03.005.205)
Requirement (D03.005.210)
Strategy (D03.005.215)
Consequence (D03.006.220)
Contingency (D03.006.225)
Countermeasure (D03.006.230)
Hazard (D03.006.235)
Threat (D03.006.240)
Vulnerability (D03.006.245)

Guidance Data (D03)				
Guidance Data consists of categories for data about management, control and guidance of activities performed by the enterprise and not typical to a specific or unique mission.				
Code	**Domain**	**Subject**	**Topic**	**Definition**
D03.001	Guidance Data	Authorities		Data describing the governing instruments that create legal consent and authorization for private, public, and international organizations to conduct business or other activities in support of a mission or goal.
D03.001.095	Guidance Data	Authorities	Authorization	Data describing the act of empowering a requesting person or organization to undertake an action, usually after an examination of the request and formalized through the issuance of a license or certificate.
D03.001.100	Guidance Data	Authorities	Directive	Data describing a statement of a policy, mission, program, or activity's purpose, scope, and authority, establishes and delegates responsibilities, and set forth policies and procedures.
D03.001.105	Guidance Data	Authorities	Law	Data describing a rule of conduct or actions prescribed or formally recognized as binding or enforced by a controlling authority within the government.
D03.001.110	Guidance Data	Authorities	Mandate	Data describing an official authoritative order or command.
D03.002	Guidance Data	Controls		Data describing the rules and regulations derived from law and/or agreements, that ensure compliance with applicable laws as intended through the supervision and oversight of operations and programs, the protection of systems and resources, and the prevention of waste, fraud and abuse.
D03.002.115	Guidance Data	Controls	Agreement	Data describing the formal or informal mutual understanding between two or more parties regarding the obligations, actions, terms, conditions, etc. the respective parties have agreed to.
D03.002.120	Guidance Data	Controls	Regulation	Data describing the rule or order issued by an executive authority or regulatory agency of a government and having the force of law.
D03.002.125	Guidance Data	Controls	Rule	Data describing the statement or statements that define or constrain an entity and always resolves to either a true or false conclusion or result.
D03.003	Guidance Data	Locations		Data describing logical, physical, and virtual places ranging in type, scale, name, and addressability.

D03.003.130	Guidance Data	Locations	Boundary	Data describing something or somewhere that indicates a border or area limit.
D03.003.135	Guidance Data	Locations	Jurisdiction	Data describing the set of limits or territory within which authority may be exercised.
D03.003.140	Guidance Data	Locations	Logical Location	Data describing a place that exists with intangible or non-physical characteristics or properties.
D03.003.145	Guidance Data	Locations	Physical Location	Data describing a place that exists with tangible or material characteristics or properties.
D03.003.150	Guidance Data	Locations	Political Boundary	Data describing an area or dividing line established by a legislature or other government body to encapsulate or divide the earth's surface according to recognized dominion or authority.
D03.003.155	Guidance Data	Locations	Region	Data describing a large, usually continuous segment of a surface or space or an area of interest, activity or conflict.
D03.003.160	Guidance Data	Locations	Virtual Location	Data describing a place or entity occurring or existing primarily electronically or having a universal identifier or address.
D03.004	Guidance Data	Measures		Data describing the dimensions, quantity, capacity, or conditions as ascertained by comparison with a standard or unit or measure.
D03.004.165	Guidance Data	Measures	Condition	Data describing a particular mode of being for a person or thing; existing state; situation with respect to circumstances.
D03.004.170	Guidance Data	Measures	Exposure	Data describing the amount of radiation or pollutant present in a given environment that represents a potential health threat to living organisms.
D03.004.175	Guidance Data	Measures	Forecast	Data describing a predicted measure value.
D03.004.180	Guidance Data	Measures	Quality	Data describing the standard or process used to assess and compare the quality of a structure, process, or outcome.
D03.004.185	Guidance Data	Measures	Standard	Data describing the accepted or approved instance or example of a quantity or quality against which others are judged or measured or compared.
D03.004.190	Guidance Data	Measures	Statistic	Data describing the numerical value, such as standard deviation or mean, that characterizes the sample or population from which it was derived.
D03.004.195	Guidance Data	Measures	Target	Data describing an accepted or approved measure value tied to a goal or an objective (the target).

D03.005	Guidance Data	Plans		Data describing an organized and anticipated strategy for programs, courses of action and/or methods for the accomplishment of a mission, goal, or objective.
D03.005.200	Guidance Data	Plans	Calendar	Data describing a system that organizes time for administrative and planning purposes.
D03.005.205	Guidance Data	Plans	Portfolio	Data describing a set of related projects with a scope supporting goals and objectives.
D03.005.210	Guidance Data	Plans	Requirement	Data describing a stated quantifiable objective to satisfy a need.
D03.005.215	Guidance Data	Plans	Strategy	Data describing a course of action that describes a method for achieving a specified goal or objective.
D03.006	Guidance Data	Risks		Data describing a level of real or potential threat for an unwanted outcome from an incident, event, or occurrence, as determined by its probability and consequences.
D03.006.220	Guidance Data	Risks	Consequence	Data describing the effect or impact of an event, incident, or occurrence.
D03.006.225	Guidance Data	Risks	Contingency	Data describing a planned response to an event or risk that might unexpectedly occur in the future.
D03.006.230	Guidance Data	Risks	Countermeasure	Data describing an action, measure, or device that reduces an identified risk.
D03.006.235	Guidance Data	Risks	Hazard	Data describing a natural or man-made source or cause of harm or difficulty.
D03.006.240	Guidance Data	Risks	Threat	Data describing a natural or human-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment and/or property.
D03.006.245	Guidance Data	Risks	Vulnerability	Data describing a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.


Resources Data (D04)
Assets (D04.001)
Business Resources (D04.002)
Commodities (D04.003)
Contents (D04.004)
Items (D04.005)
Natural Resources (D04.006)
Parties (D04.007)
Capital Asset (D04.001.540)
Critical Asset (D04.001.545)
Intangible Asset (D04.001.550)
Response Asset (D04.001.555)
Tangible Asset (D04.001.560)
Finance (D04.002.565)
Human Capital (D04.002.570)
Infrastructure (D04.002.575)
Logistics (D04.002.580)
Technology (D04.002.585)
Cargo (D04.003.590)
Goods (D04.003.595)
Product (D04.003.600)
Reserve (D04.003.605)
Archive (D04.004.605)
Document (D04.004.615)
Guidance (D04.004.625)
Knowledge (D04.004.635)
Record (D04.004.645)
Culture (D04.004.610)
Financial Instrument (D04.004.620)
Index (D04.004.630)
Model (D04.004.640)
Visualization (D04.004.650)
Artifact (D04.005.650)
Equipment (D04.005.655)
Evidence (D04.005.660)
Material (D04.005.665)
Property (D04.005.670)
Air (D04.006.675)
Biological (D04.006.680)
Environment (D04.006.685)
Land (D04.006.690)
Mineral (D04.006.695)
Water (D04.006.700)
Organization (D04.007.705)
Person (D04.007.710)
Relationship (D04.007.715)
Role (D04.007.720)

Resource Data (D04)				
Resource Data categorizes data about parties, places, objects and ideas used by the enterprise in performance of the mission but that are not unique to that mission.				
Code	**Domain**	**Subject**	**Topic**	**Definition**
D04.001	Resource Data	Assets		Data describing the resources that have value or an option for potential value, and that possess such critical importance as to require protection or that provide essential assistance in emergencies.
D04.001.540	Resource Data	Assets	Capital Asset	Data describing a business resource with an estimated useful life of two years or more.
D04.001.545	Resource Data	Assets	Critical Asset	Data describing a specific entity whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on national or economic security.
D04.001.550	Resource Data	Assets	Intangible Asset	Data describing a resource or asset that does not have a physical form but has a determined value, such as patents, trademarks and software.
D04.001.555	Resource Data	Assets	Response Asset	Data describing a person or organization with specialized skills, equipment, fund or facility required to react to an incident or event.
D04.001.560	Resource Data	Assets	Tangible Asset	Data describing an asset held for use rather than for processing or resale and is subject to depreciation.
D04.002	Resource Data	Business Resources		Data describing a group of support services, mission support services, and information technology services that empower and enable any organization's mission and operations.
D04.002.565	Resource Data	Business Resources	Finance	Data describing a discipline involving the management of money and other assets.
D04.002.570	Resource Data	Business Resources	Human Capital	Data describing an individual employed, contracted or engaged in an activity that provides a skill or capability in support of business or emergency processes.
D04.002.575	Resource Data	Business Resources	Infrastructure	Data describing the basic physical and organizational structures (e.g. buildings, roads, power supplies) needed for the operation of a society or enterprise.
D04.002.580	Resource Data	Business Resources	Logistics	Data describing a process involving the management of the flow of goods, information and other resources.

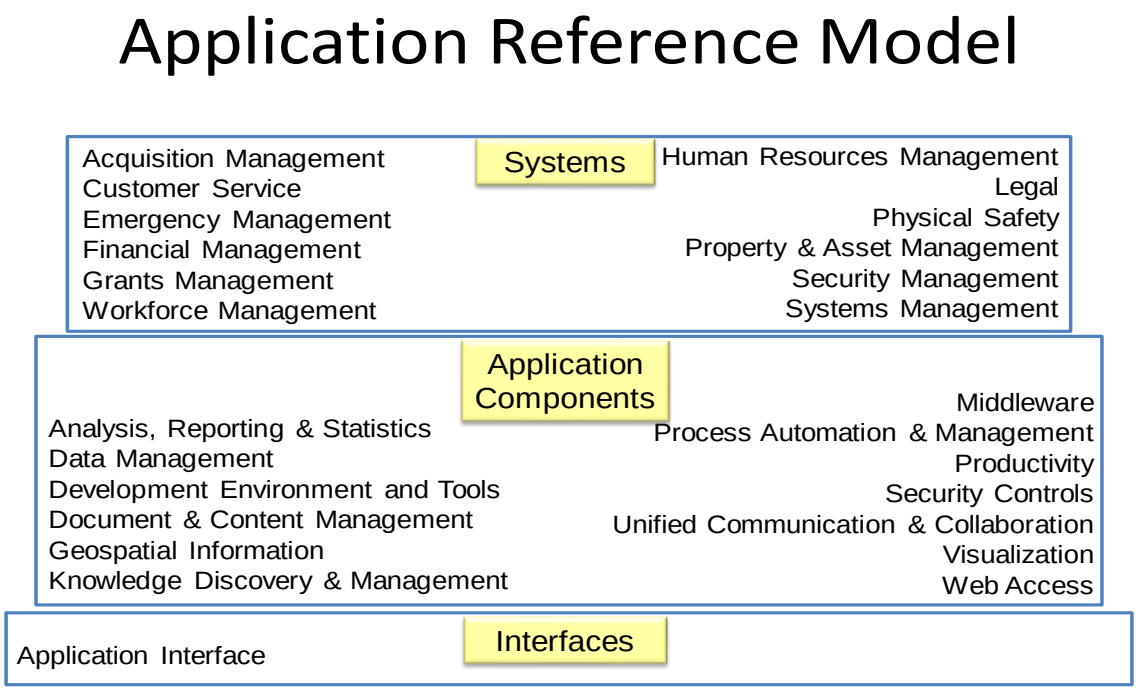
D04.002.585	Resource Data	Business Resources	Technology	Data describing a sequence of operations or capabilities for accomplishing a task especially using technical processes, methods, or knowledge.
D04.003	Resource Data	Commodities		Data describing the resources related to the import, export, storage, extracting, or harvesting of raw materials, products and goods, including the establishment, planning, supply, and maintenance of such operations.
D04.003.590	Resource Data	Commodities	Cargo	Data describing the goods or merchandise conveyed in a ship, airplane, or other conveyance.
D04.003.595	Resource Data	Commodities	Goods	Data describing a product or something that is intended to satisfy some wants or needs of a consumer and thus has economic utility.
D04.003.600	Resource Data	Commodities	Product	Data describing an idea, method, information, object, or service that is the end result of a process and serves as a need or want satisfier.
D04.003.605	Resource Data	Commodities	Reserve	Data describing the total estimated amount of products, goods and or capital available for consumption or insurance.
D04.004	Resource Data	Contents		Data describing the collections of written, printed, or electronic information that constitute a body of knowledge, policies, directives, memoranda, and/or guidance supporting a business function or activity.
D04.004.605	Resource Data	Contents	Archive	Data describing the resource for the data or information no longer actively used but retained for secondary use.
D04.004.610	Resource Data	Contents	Culture	Data describing the set of shared attitudes, values, goals, and practices that characterizes a social, religious, racial group; institution; or organization.
D04.004.615	Resource Data	Contents	Document	Data describing the resource for containing a collection of written, printed, or electronic information.
D04.004.620	Resource Data	Contents	Financial Instrument	Data describing a document with monetary value or that represents a legally enforceable agreement between two or more parties regarding a right to payment on money.
D04.004.625	Resource Data	Contents	Guidance	Data describing the directions, advice or a formal written collection of instructions from external agencies, which provides interpretations of statutory or regulatory requirements.
D04.004.630	Resource Data	Contents	Index	Data describing the alphabetic listing or numeric order of things that guide decision making and facilitate or point out references.
D04.004.635	Resource Data	Contents	Knowledge	Data describing the content, method or technique that is captured, processed, stored and published for its particular specialization and recognized value.

D04.004.640	Resource Data	Contents	Model	Data for a graphical, mathematical or physical representation of a concept or an object, with the representation typically intentionally abstracted to ignore certain details while emphasizing others.
D04.004.645	Resource Data	Contents	Record	Data describing the documentary materials regardless of physical form or characteristics, made or received by an agency of the United States government under federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the informational value of data in them.
D04.004.650	Resource Data	Contents	Visualization	Data describing the method or methods of making the data or content displayable in order to help readers better understand the information and put it in a business context.
D04.005	Resource Data	Items		Data describing the thing or quantity of things of interest to a person or organization.
D04.005.650	Resource Data	Items	Artifact	Data describing the man-made object which gives information about the culture or history of its creator and users. The artifact may change over time in what it represents, how it appears and how and why it is used as the culture changes over time.
D04.005.655	Resource Data	Items	Equipment	Data describing the items needed for a particular purpose or in an operation or activity including supplies and tools used for work.
D04.005.660	Resource Data	Items	Evidence	Data describing a set of information presented as proof of facts at issue including the testimony of witnesses, records, documents, or objects.
D04.005.665	Resource Data	Items	Material	Data describing a material thing or set of things of attention, concern, or interest to the case, mission or objective.
D04.005.670	Resource Data	Items	Property	Data describing a set of things that a party owns.
D04.006	Resource Data	Natural Resources		Data describing the ecological, cultural, historical, archaeological, energy, recreational, etc. resources and the support of planning and management activities to ensure their adequacy and availability.
D04.006.675	Resource Data	Natural Resources	Air	Data describing the mixture of gases, mainly nitrogen and oxygen, that forms the Earth's atmosphere.
D04.006.680	Resource Data	Natural Resources	Biological	Data describing the wildlife, marine, plants and any other biological entity or system.

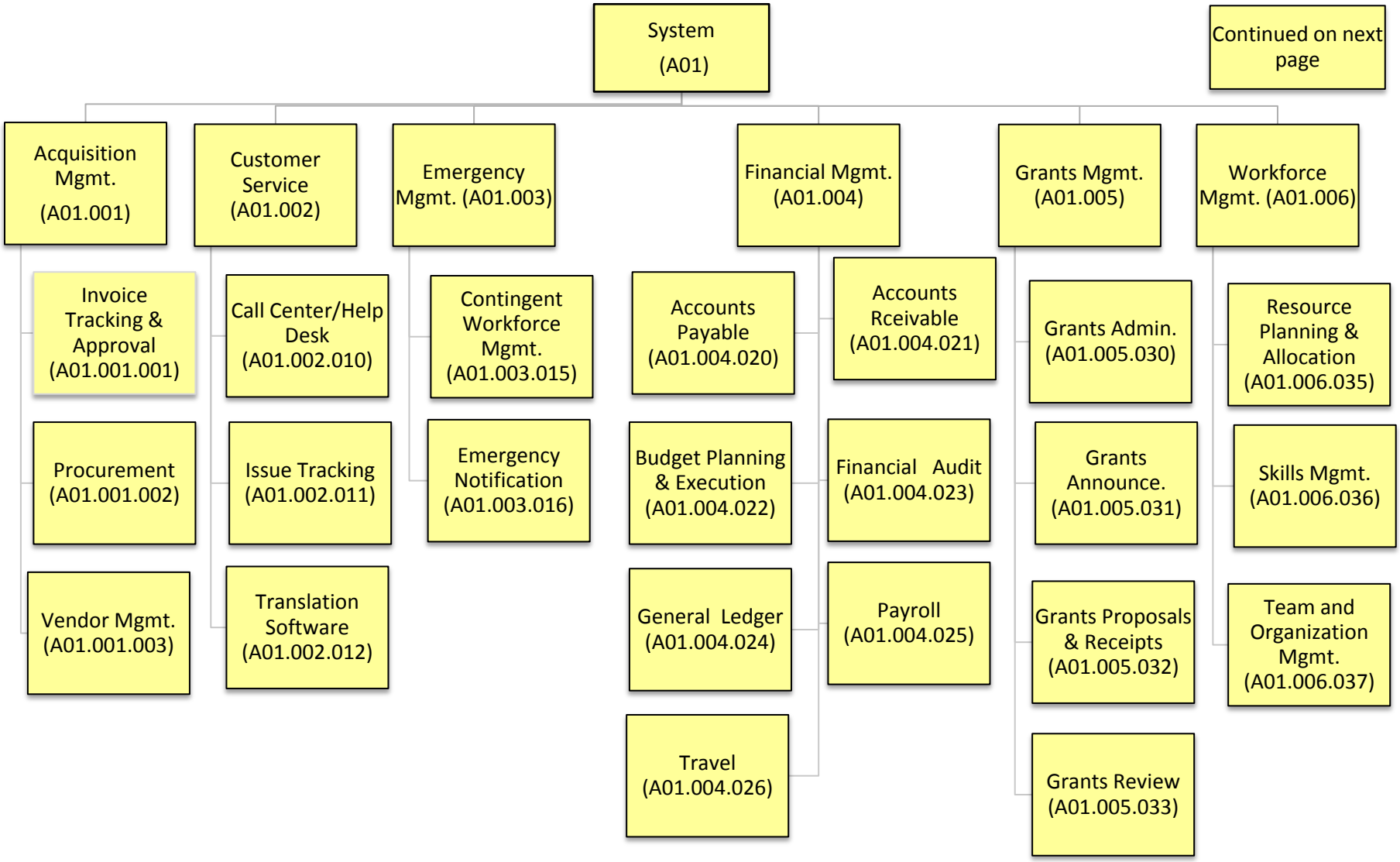
D04.006.685	Resource Data	Natural Resources	Environment	Data describing the surroundings or conditions in which a person, animal, or plant lives or operates.
D04.006.690	Resource Data	Natural Resources	Land	Data describing the geology, composition, condition, and type of the soil for a geospatially bounded land area.
D04.006.695	Resource Data	Natural Resources	Mineral	Data describing any naturally occurring substance formed through geologic processes that have a characteristic chemical composition, a highly ordered atomic structure, and specific physical properties.
D04.006.700	Resource Data	Natural Resources	Water	Data describing the nation's water resources and the partnerships developed to nourish a healthy environment and sustain a vibrant economy.
D04.007	Resource Data	Parties		Data describing the people, organizations or things associated by a common or specific idea, purpose, role or action.
D04.007.705	Resource Data	Parties	Organization	Data describing an association of parties established formally or informally to represent interests or issues or to conduct an activity.
D04.007.710	Resource Data	Parties	Person	Data describing a human being or a unique individual.
D04.007.715	Resource Data	Parties	Relationship	Data describing the association of one party to another.
D04.007.720	Resource Data	Parties	Role	Data describing a proper or customary function or characteristic assigned to a person, organization or thing.

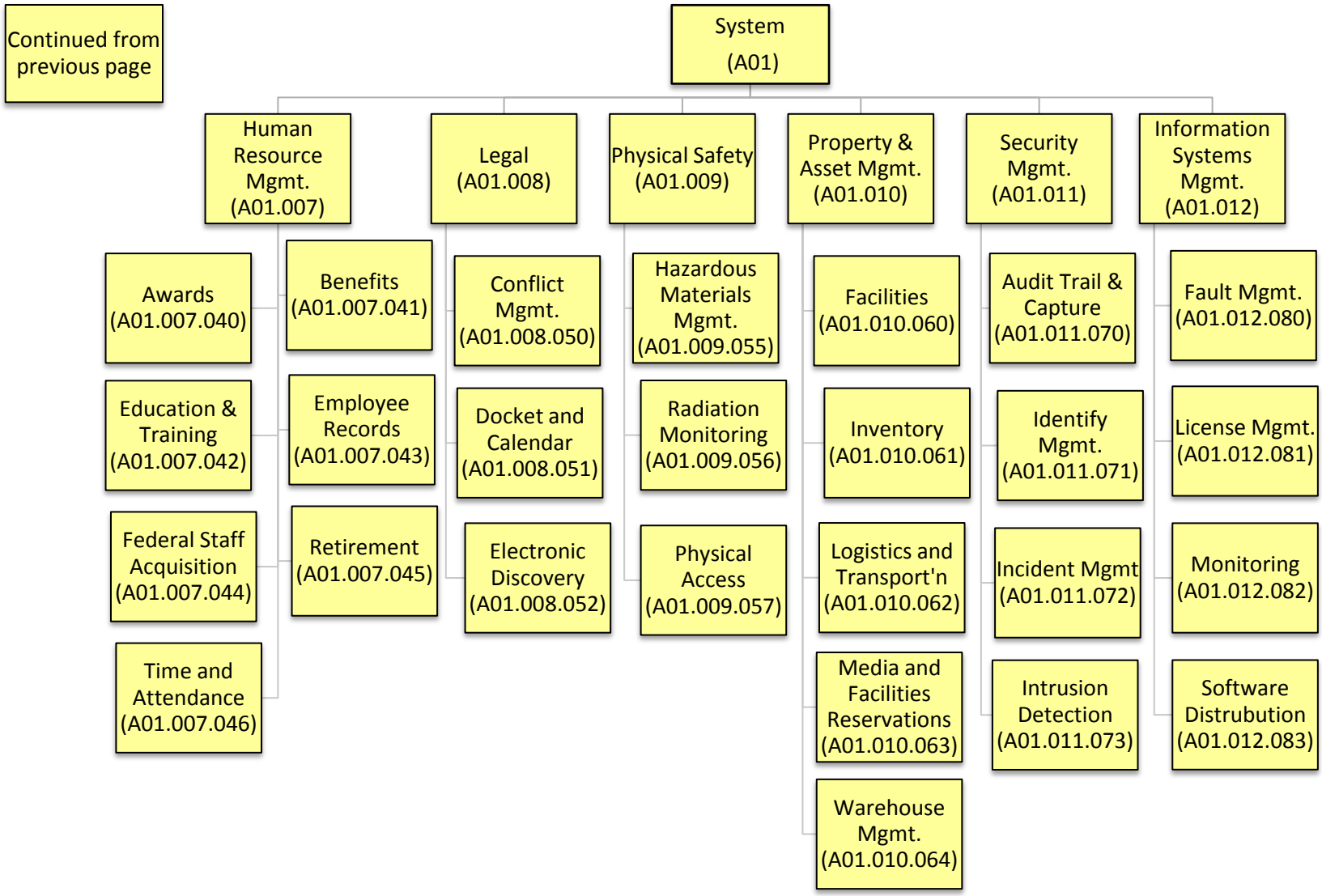
Appendix J: Application Reference Model Taxonomy with Definitions

The Federal Enterprise Architecture Application Reference Model (ARM) has three areas: Systems, Application Components, and Interfaces. Systems are discrete sets of information resources, organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information in support of a business process. Application Components are self-contained software that can be aggregated or configured to support (or contribute to achieving) many different business objectives. Interfaces are protocols used to transfer information between systems.



In the sections below, each ARM Area is shown as a tree diagram, followed by definitions of the taxonomy elements in the corresponding tree.




Continued from previous page
System (A01)
Human Resource Mgmt. (A01.007)
Legal (A01.008)
Physical Safety (A01.009)
Property & Asset Mgmt. (A01.010)
Security Mgmt. (A01.011)
Information Systems Mgmt. (A01.012)
Awards (A01.007.040)
Benefits (A01.007.041)
Education & Training (A01.007.042)
Employee Records (A01.007.043)
Federal Staff Acquisition (A01.007.044)
Retirement (A01.007.045)
Time and Attendance (A01.007.046)
Conflict Mgmt. (A01.008.050)
Docket and Calendar (A01.008.051)
Electronic Discovery (A01.008.052)
Hazardous Materials Mgmt. (A01.009.055)
Radiation Monitoring (A01.009.056)
Physical Access (A01.009.057)
Facilities (A01.010.060)
Inventory (A01.010.061)
Logistics and Transport'n (A01.010.062)
Media and Facilities Reservations (A01.010.063)
Warehouse Mgmt. (A01.010.064)
Audit Trail & Capture (A01.011.070)
Identify Mgmt. (A01.011.071)
Incident Mgmt (A01.011.072)
Intrusion Detection (A01.011.073)
Fault Mgmt. (A01.012.080)
License Mgmt. (A01.012.081)
Monitoring (A01.012.082)
Software Distrubution (A01.012.083)

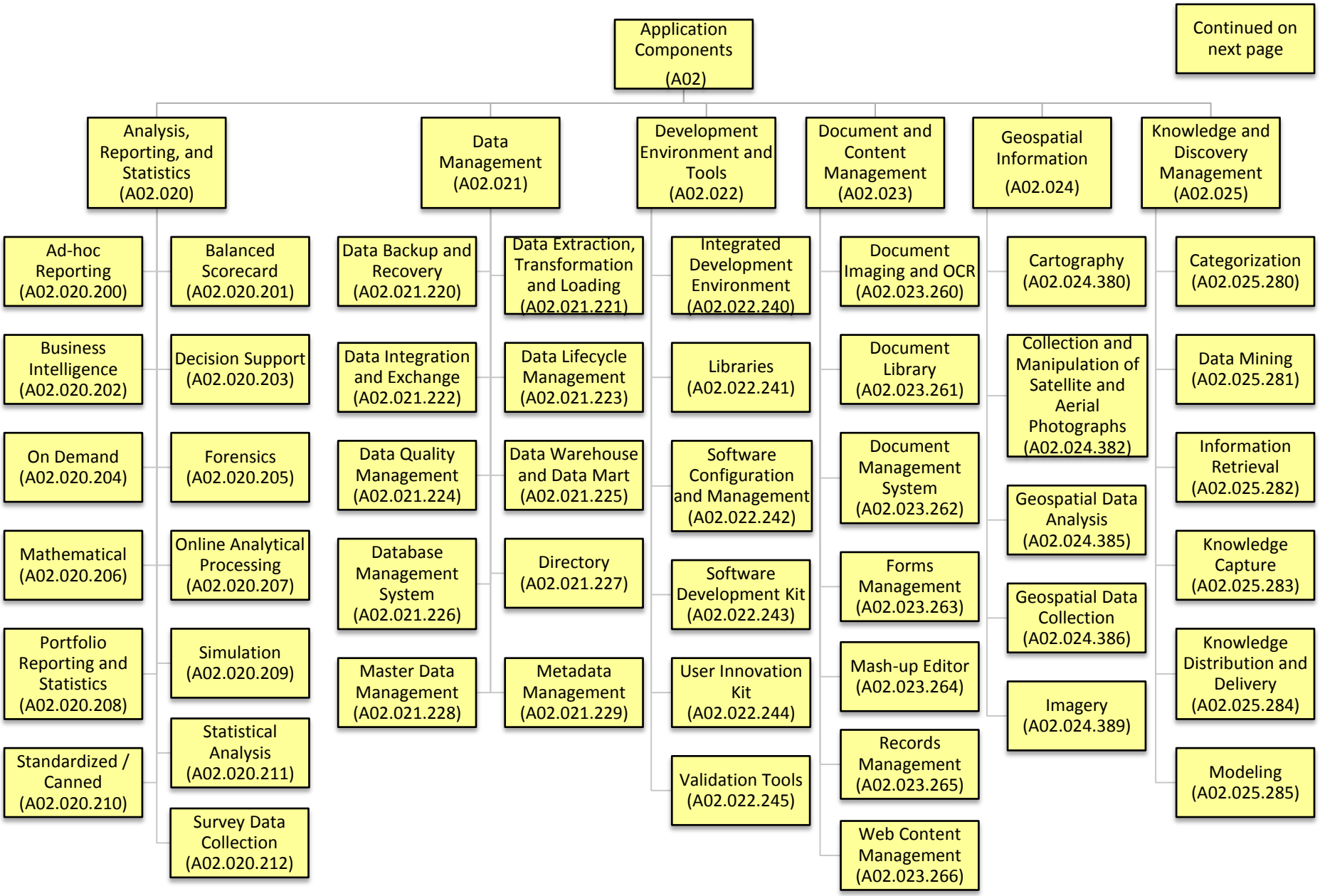
SYSTEM (A01)				
Systems are discrete sets of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information in support of a specific business process.				
Code	**Domain**	**Area**	**Category**	**Description**
A01.001.001	System	Acquisition Management	Invoice Tracking and Approval	Software that manages inflow and outflows of "products", as well as data about the level of "products" on hand.
A01.001.002	System	Acquisition Management	Procurement	Software used in the acquisition of goods or services and management of the contracts.
A01.001.003	System	Acquisition Management	Vendor Management	Software used to build a list of vendors or measure satisfaction of relationship.
A01.002.010	System	Customer Service	Call Center / Help Desk	Software that supports the management of a service center to respond to government and contract employees' technical and administrative questions.
A01.002.011	System	Customer Service	Issue Tracking	Software that supports activities associated with providing an agency's customers with information regarding the agency's service offerings and managing the interactions and relationships with those customers.
A01.002.012	System	Customer Service	Translation Software	Software that supports or enables translation functionality. This does not include software for other purposes that can be used in multiple languages.
A01.003.015	System	Emergency Management	Contingent Workforce Management	Software that supports the continuity of operations for an organization's business through the identification of surge or temporary personnel in addition to federal staff.
A01.003.016	System	Emergency Management	Emergency Notification	Software that enables designated individuals to communicate critical information to many individuals across multiple devices.
A01.004.020	System	Financial Management	Accounts Payable	Software that manages and pays the funds owed.
A01.004.021	System	Financial Management	Accounts Receivable	Software that supports collections and receivables, including deposits, fund transfers, and receipts for sales or service.

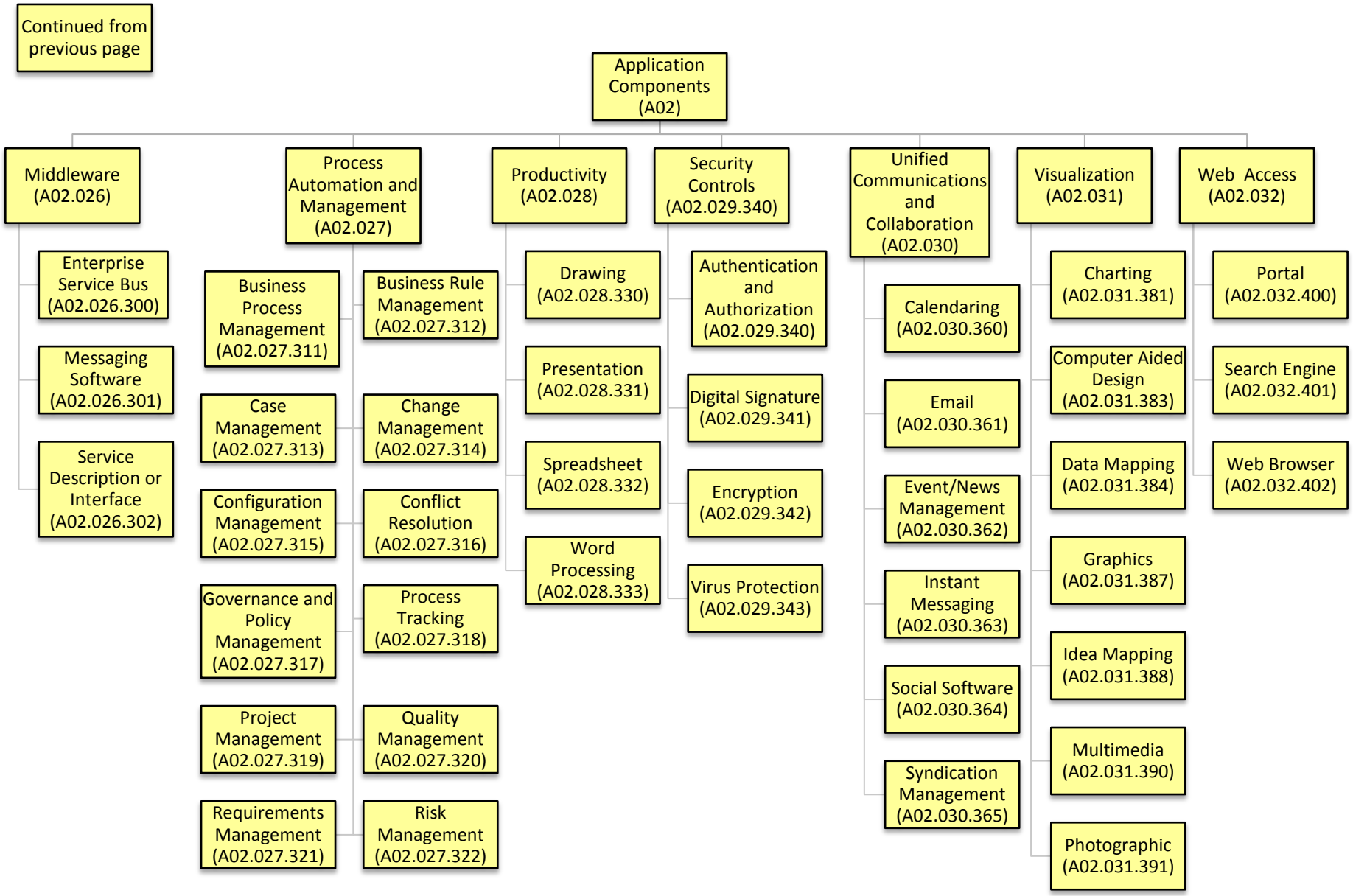
A01.004.022	System	Financial Management	Budget Planning and Execution	Software that supports all activities undertaken to determine priorities for future spending and to develop an itemized forecast of future funding and expenditures during a specified period of time. This includes the collection and use of performance information to assess the effectiveness of programs and develop budget priorities and the legal (apportionment) and managerial (allotment and sub-allotment) distribution of budget authority to achieve results consistent with the formulated budget.
A01.004.023	System	Financial Management	Financial Audit	Software used to track and manage financial audits.
A01.004.024	System	Financial Management	General Ledger	Software that supports accounting for assets, liabilities, fund balances, revenues and expenses associated with the maintenance of federal funds and expenditure of federal appropriations (salaries and expenses, operations and maintenance, procurement, working capital, trust funds, etc.), in accordance with applicable federal standards (e.g., FASAB, Treasury, OMB, GAO, etc.).
A01.004.025	System	Financial Management	Payroll	Software that supports the administration and determination of employee compensation.
A01.004.026	System	Financial Management	Travel	Software that supports activities associated with planning, preparing, and monitoring of business-related travel expenses. This may include employees and others supporting the work of the government.
A01.005.030	System	Grants Management	Grant Administration	Software that supports the administration and monitoring of grants.
A01.005.031	System	Grants Management	Grant Announcement	Portal that posts and publishes announcements of grants to be funded.
A01.005.032	System	Grants Management	Grant Receipt of Proposals	Portal for the receipt of grant proposals.
A01.005.033	System	Grants Management	Grant Review	Software that supports the review process for grants.

A01.006.035	System	Workforce Management	Resource Planning and Allocation	Software that supports the processes for identifying the workforce competencies required to meet the agency's strategic goals and for developing the strategies to meet these requirements. The software also supports procedures for attracting and selecting high-quality, productive employees with the right skills and competencies, in accordance with merit system principles. This includes developing a staffing strategy and plan; establishing an applicant evaluation approach; announcing the vacancy, sourcing and evaluating candidates against the competency requirements for the position; initiating pre-employment activities; and hiring employees.
A01.006.036	System	Workforce Management	Skills Management	Software that supports the proficiency of employees in the delivery of an organization's products or services.
A01.006.037	System	Workforce Management	Team and Organization Management	Software that supports the hierarchy structure and identification of employees within the various sub-groups of an organization.
A01.007.040	System	Human Resource Management	Awards	Software that supports the administration of employee bonus and monetary awards programs. Also includes software used to design, develop, and implement pay for performance compensation programs to recognize and reward high performance, with both base pay increases and performance bonus payments.
A01.007.041	System	Human Resource Management	Benefits	Software that supports the design, development, and implementation of benefits programs for agency employees. This includes establishing and communicating benefits programs, processing benefits actions, and interacting as necessary with third party benefits providers.
A01.007.042	System	Human Resource Management	Education / Training	Software that supports the design, development, and implementation of a comprehensive employee development and training approach to ensure that agency employees have the right competencies.
A01.007.043	System	Human Resource Management	Employee Records	Software that manages employee personnel records and files.
A01.007.044	System	Human Resource Management	Federal Staff Acquisition	Software that supports the procedures for attracting and selecting high-quality, productive employees with the right skills and competencies, in accordance with merit system principles. This includes developing a staffing strategy and plan, and establishing an applicant evaluation.

A01.007.045	System	Human Resource Management	Retirement	Software that supports development of policies and management of retirement benefits, pension benefits, and income security for retirees.
A01.007.046	System	Human Resource Management	Time and Attendance	Software that supports the set of capabilities to support the submission, approval and adjustment of employee hours.
A01.008.050	System	Legal	Conflict Management	Software that supports negotiation, bargaining, mediation, or arbitration proceedings.
A01.008.051	System	Legal	Docket and Calendar	Software that supports management of legal resource scheduling.
A01.008.052	System	Legal	Electronic Discovery	Software that supports the analysis of electronically stored information and its exchange, including digital forensics analysis.
A01.009.055	System	Physical Safety	Hazardous Materials Management	Software that supports the management of, and mechanisms for, interaction and oversight for controlling biological, chemical, and radiological materials and wastes. This includes addressing identification of materials that need special handling and processes to minimize the risk of their unsafe use and improper disposal.
A01.009.056	System	Physical Safety	Radiation Monitoring	Software that supports measurement and monitoring to protect people and goods from risks of radiation.
A01.009.057	System	Physical Safety	Physical Access	Software to regulate entry to turnstiles, gates, campuses, and doors.
A01.010.060	System	Property and Asset Management	Facilities	Software that supports facilities management including the maintenance, administration, certification, and operation of office buildings that are possessions of the federal government.
A01.010.061	System	Property and Asset Management	Inventory	Software that supports the tracking of information related to procured assets and resources with regard to quantity, quality, and location.
A01.010.062	System	Property and Asset Management	Logistics and Transportation	Software that supports the planning and tracking of personnel and their resources in relation to their availability and location.
A01.010.063	System	Property and Asset Management	Media and Facilities Reservations	Software that supports arrangements to track and secure the use of media and facilities.

A01.010.064	System	Property and Asset Management	Warehouse Management	Software that controls the movement, storage, shipping and receiving of materials.
A01.011.070	System	Security Management	Audit Trail and Capture	Software that supports the set of capabilities to support the identification and monitoring of activities within an application, system, or network.
A01.011.071	System	Security Management	Identity Management	Software that identifies individuals in a system and controls access to the resources in that system by placing restrictions on the established identities of the individuals.
A01.011.072	System	Security Management	Incident management	Software that supports the set of capabilities to provide active response and remediation to a security incident that has allowed unauthorized access to a government information system.
A01.011.073	System	Security Management	Intrusion Detection	Hardware or software products that gather and analyze information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations.)
A01.012.080	System	Systems Management	Fault management	Software that detects, isolates, and corrects malfunctions in a telecommunications network and compensates for environmental changes. This includes maintaining and examining error logs, accepting and acting on error detection notifications, tracing and identifying faults, carrying out sequences of diagnostics tests, correcting faults, reporting error conditions, and localizing and tracing faults by examining and manipulating database information.
A01.012.081	System	Systems Management	License Management	Software that supports enterprise license management. It supports the purchase, upgrade and tracking of legal usage contracts for system software and applications, written computer programs, and components.
A01.012.082	System	Systems Management	Monitoring	Software that continuously records performance, capacity use, throughput of computer hardware or software and provides notification about deviations from normal.
A01.012.083	System	Systems Management	Software Distribution	Software that supports distribution of software, propagation, installation and upgrade of written computer programs, applications and components.


Application Components (A02)
Continued on next page
Analysis, Reporting, and Statistics (A02.020)
Data Management (A02.021)
Development Environment and Tools (A02.022)
Document and Content Management (A02.023)
Geospatial Information (A02.024)
Knowledge and Discovery Management (A02.025)
Ad-hoc Reporting (A02.020.200)
Business Intelligence (A02.020.202)
On Demand (A02.020.204)
Mathematical (A02.020.206)
Portfolio Reporting and Statistics (A02.020.208)
Standardized / Canned (A02.020.210)
Balanced Scorecard (A02.020.201)
Decision Support (A02.020.203)
Forensics (A02.020.205)
Online Analytical Processing (A02.020.207)
Simulation (A02.020.209)
Statistical Analysis (A02.020.211)
Survey Data Collection (A02.020.212)
Data Backup and Recovery (A02.021.220)
Data Integration and Exchange (A02.021.222)
Data Quality Management (A02.021.224)
Database Management System (A02.021.226)
Master Data Management (A02.021.228)
Data Extraction, Transformation and Loading (A02.021.221)
Data Lifecycle Management (A02.021.223)
Data Warehouse and Data Mart (A02.021.225)
Directory (A02.021.227)
Metadata Management (A02.021.229)
Integrated Development Environment (A02.022.240)
Libraries (A02.022.241)
Software Configuration and Management (A02.022.242)
Software Development Kit (A02.022.243)
User Innovation Kit (A02.022.244)
Validation Tools (A02.022.245)
Document Imaging and OCR (A02.023.260)
Document Library (A02.023.261)
Document Management System (A02.023.262)
Forms Management (A02.023.263)
Mash-up Editor (A02.023.264)
Records Management (A02.023.265)
Web Content Management (A02.023.266)
Cartography (A02.024.380)
Collection and Manipulation of Satellite and Aerial Photographs (A02.024.382)
Geospatial Data Analysis (A02.024.385)
Geospatial Data Collection (A02.024.386)
Imagery (A02.024.389)
Categorization (A02.025.280)
Data Mining (A02.025.281)
Information Retrieval (A02.025.282)
Knowledge Capture (A02.025.283)
Knowledge Distribution and Delivery (A02.025.284)
Modeling (A02.025.285)


Continued from previous page
Application Components (A02)
Middleware (A02.026)
Enterprise Service Bus (A02.026.300)
Messaging Software (A02.026.301)
Service Description or Interface (A02.026.302)
Process Automation and Management (A02.027)
Business Process Management (A02.027.311)
Business Rule Management (A02.027.312)
Case Management (A02.027.313)
Change Management (A02.027.314)
Configuration Management (A02.027.315)
Conflict Resolution (A02.027.316)
Governance and Policy Management (A02.027.317)
Process Tracking (A02.027.318)
Project Management (A02.027.319)
Quality Management (A02.027.320)
Requirements Management (A02.027.321)
Risk Management (A02.027.322)
Productivity (A02.028)
Drawing (A02.028.330)
Presentation (A02.028.331)
Spreadsheet (A02.028.332)
Word Processing (A02.028.333)
Security Controls (A02.029.340)
Authentication and Authorization (A02.029.340)
Digital Signature (A02.029.341)
Encryption (A02.029.342)
Virus Protection (A02.029.343)
Unified Communications and Collaboration (A02.030)
Calendaring (A02.030.360)
Email (A02.030.361)
Event/News Management (A02.030.362)
Instant Messaging (A02.030.363)
Social Software (A02.030.364)
Syndication Management (A02.030.365)
Visualization (A02.031)
Charting (A02.031.381)
Computer Aided Design (A02.031.383)
Data Mapping (A02.031.384)
Graphics (A02.031.387)
Idea Mapping (A02.031.388)
Multimedia (A02.031.390)
Photographic (A02.031.391)
Web Access (A02.032)
Portal (A02.032.400)
Search Engine (A02.032.401)
Web Browser (A02.032.402)

APPLICATION COMPONENTS (A02)				
Application components are self-contained software that can be aggregated or configured to support (or contribute to achieving) many different business objectives.				
Code	**Domain**	**Area**	**Category**	**Description**
A02.020.200	Application Components	Analysis, Reporting and Statistics	Ad hoc Reporting	Software tools that support the creation and display of individually designed and structured reports with self-service access to meaningful data.
A02.020.201	Application Components	Analysis, Reporting and Statistics	Balanced Scorecard	A semi-standard structured report, supported by proven design methods and automation tools, that can be used by managers to keep track of the execution of activities by the staff within their control and to monitor the consequences arising from these actions.
A02.020.202	Application Components	Analysis, Reporting and Statistics	Business Intelligence	Software to support identifying, extracting, and analyzing business data, such as performance and cost metrics to support better business decision-making.
A02.020.203	Application Components	Analysis, Reporting and Statistics	Decision Support	Software that supports business or organizational decision-making activities. Supports the management, operations, and planning levels of an organization and helps to make decisions, which may be rapidly changing and not easily specified in advance.
A02.020.204	Application Components	Analysis, Reporting and Statistics	On Demand	Software tools which support estimating the quantity of a product or service that will be required.
A02.020.205	Application Components	Analysis, Reporting and Statistics	Forensics	Software that supports the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.
A02.020.206	Application Components	Analysis, Reporting and Statistics	Mathematical	Software that provides an environment for statistical analysis, predictive and descriptive modeling, data mining, forecasting, optimization, simulation.
A02.020.207	Application Components	Analysis, Reporting and Statistics	Online Analytical Processing (OLAP)	Software that supports a process to swiftly answer multi-dimensional analytical (MDA) queries and enable users to interactively analyze multidimensional data from multiple perspectives. An OLAP consists of three basic analytical operations: consolidation, drill-down, and slicing and dicing.

A02.020.208	Application Components	Analysis, Reporting and Statistics	Portfolio Management	Software that provides the set of capabilities to support the administration of a group of investments held by an organization.
A02.020.209	Application Components	Analysis, Reporting and Statistics	Simulation	Software that helps manipulate information to identify patterns and create possible changes.
A02.020.210	Application Components	Analysis, Reporting and Statistics	Standardized / Canned	Software that supports the creation and display of standard reports with self-service access to meaningful data.
A02.020.211	Application Components	Analysis, Reporting and Statistics	Statistical Analysis	Software that supports the study of a collection, organization, analysis, and interpretation of data.
A02.020.212	Application Components	Analysis, Reporting and Statistics	Survey Data Collection	Software that supports methods to collect information from a sample of individuals in a systematic way for empirical research in social sciences, marketing and official statistics.
A02.021.220	Application Components	Data Management	Data Backup and Recovery	Software that creates copies of data which may be used to restore the original after a data loss event or to restore and stabilize data sets to a consistent, desired state.
A02.021.221	Application Components	Data Management	Data Extraction, Transformation and Loading	Software that supports the extraction of data from a database, the manipulation and change of data to a different format and the population of another database with the data.
A02.021.222	Application Components	Data Management	Data Integration and Exchange	Software services that enable elements of distributed business applications to interoperate and the software development necessary to facilitate such integration. These elements can share function, content, and communications across heterogeneous computing environments.
A02.021.223	Application Components	Data Management	Data Lifecycle Management	Software that supports a policy-based approach to managing the flow of an information system's data throughout its life cycle: from creation and initial storage to the time when it becomes obsolete and is deleted.
A02.021.224	Application Components	Data Management	Data Quality Management	Software to ensure that data are fit for their intended uses in operations, decision making and planning and to ensure internal consistency of the data.

A02.021.225	Application Components	Data Management	Data Warehouse & Data Mart	Database used for reporting and analysis, where the data stored in the warehouse is uploaded from the transactional systems.
A02.021.226	Application Components	Data Management	Database Management System	Software that supports the storage, modification, extraction, and search for information within a database.
A02.021.227	Application Components	Data Management	Directory	Software that supports the listing of employees and their whereabouts.
A02.021.228	Application Components	Data Management	Master Data Management	Software that supports a set of processes and tools that consistently define and manage the non-transactional data entities of an organization, which may include reference data. It has the objective of providing processes for collecting, aggregating, matching, consolidating, quality-assuring and distributing such data throughout an organization to ensure consistency and control in the ongoing maintenance and application use of this information.
A02.021.229	Application Components	Data Management	Metadata Management	Software that supports the maintenance and administration of data that describes data.
A02.022.240	Application Components	Development Environment and Tools	Integrated Development Environment	Software that provides comprehensive facilities to computer programmers for software development.
A02.022.241	Application Components	Development Environment and Tools	Libraries	A collection of resources used to develop software which may include pre-written code and subroutines, classes, values or type specifications.
A02.022.242	Application Components	Development Environment and Tools	Software Configuration Management	Software to track and control changes in the software including the establishment of baselines and revision control
A02.022.243	Application Components	Development Environment and Tools	Software Development Kit	Software development tools that allow for the creation of applications for a certain software package, software framework, hardware platform, computer system, video game console, operating system, or similar platform.
A02.022.244	Application Components	Development Environment and Tools	User Innovation Toolkit	Software toolkit based on the idea that manufacturers possess the knowledge of the solution possibilities, while the users possess the knowledge about needs.

A02.022.245	Application Components	Development Environment and Tools	Validation Tools	Software tools that check web pages for accessibility and syntactical correctness of code.
A02.023.260	Application Components	Document and Content Management	Document Imaging and OCR	Software that supports the document scanning and the interpretation of images into text.
A02.023.261	Application Components	Document and Content Management	Document Library	On line repository of documents, letters, speeches, web sites, books, or articles to be shared.
A02.023.262	Application Components	Document and Content Management	Document Management System	Software used to track, store and retrieve electronic documents and/or images of paper documents. It is usually capable of keeping track of the different versions created by different users (history tracking).
A02.023.263	Application Components	Document and Content Management	Forms Management	Software that supports the creation, modification, and usage of physical or electronic documents used to capture information within the business cycle.
A02.023.264	Application Components	Document and Content Management	Mash-up Editor	Software that uses and combines data, presentation or functionality from two or more sources to create new services. The main characteristics of the mash-up are combination, visualization, and aggregation.
A02.023.265	Application Components	Document and Content Management	Records Management	Software that supports the management and stewardship of a type of information by the federal government in order to facilitate communication and information archival.
A02.023.266	Application Components	Document and Content Management	Web Content Management	Software that provides content authoring, content review and approval, tagging and aggregation, content publishing and delivery, and syndication management.
A02.024.280	Application Components	Knowledge and Discovery Management	Categorization	Software that supports the creation and maintenance of relationships between data entities, naming standards and categorization and allows classification of data and information into specific layers or types to support an organization.
A02.024.380	Application Components	Geospatial Information	Cartography	Software that supports the creation of maps.

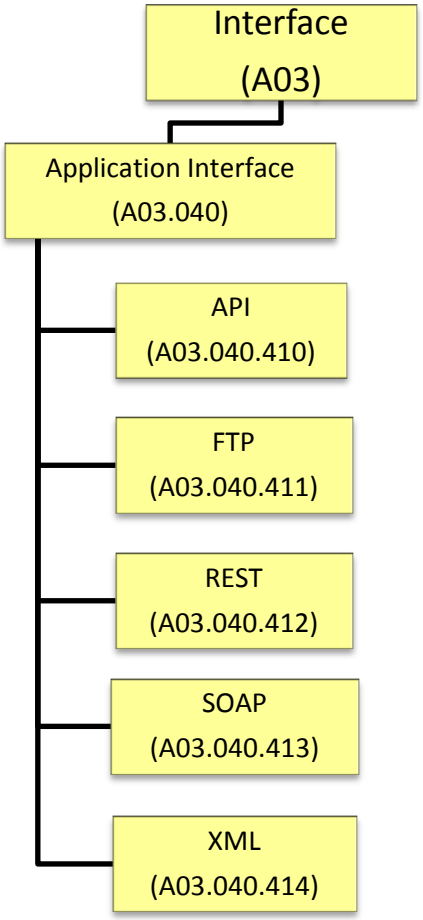
A02.024.382	Application Components	Geospatial Information	Collection and Manipulation of Satellite and Aerial Photographs	Software which supports the modification or analysis of imagery information.
A02.024.385	Application Components	Geospatial Information	Geospatial Data Analysis	Supports the application of statistical analysis and other informational techniques to geographically based data.
A02.024.386	Application Components	Geospatial Information	Geospatial Data Collection	Software that supports the collection or management of geospatial information.
A02.024.389	Application Components	Geospatial Information	Imagery	Software that supports the collection of information via satellite and aerial photography.
A02.025.281	Application Components	Knowledge and Discovery Management	Data Mining	Software that provides for the efficient discovery of non-obvious, valuable patterns and relationships within a large collection of data.
A02.025.282	Application Components	Knowledge and Discovery Management	Information Retrieval	Software that provides access to data and information for use by an organization and its stakeholders.
A02.025.283	Application Components	Knowledge and Discovery Management	Knowledge Capture	Software that facilitates collection of data and information.
A02.025.284	Application Components	Knowledge and Discovery Management	Knowledge Distribution and Delivery	Software that supports the transfer of knowledge to the end customer.
A02.025.285	Application Components	Knowledge and Discovery Management	Modeling	Software to develop descriptions that adequately explain relevant data for the purpose of prediction, pattern detection, exploration or general organization of data.
A02.026.300	Application Components	Middleware	Enterprise Service Bus	Software used for designing and implementing the interaction and communication between mutually interacting software applications in Service Oriented Architecture (SOA).
A02.026.301	Application Components	Middleware	Messaging Software	Software that enables passing of information message between different systems and IT assets using different communications technologies.

A02.026.302	Application Components	Middleware	Service Description or Interface	Software that enables various services available in SOA. It is designed to be interrogated by Simple Object Access Protocol (SOAP) messages and to provide access to Web Services Description Language (WSDL) documents describing the protocol bindings and message formats required to interact with the web services listed in its directory.
A02.027.311	Application Components	Process Automation and Management	Business Process Management	Software that allows organizations to abstract business process from technology infrastructure and support the managerial approach through enabling technology, bridging organizational and technology silos. Business Process Management applications and software include items such as: Process Engine, Business Analytics, Content Management, and Collaboration Tools.
A02.027.312	Application Components	Process Automation and Management	Business Rule Management	Software used to define, deploy, execute, monitor and maintain the variety and complexity of decision logic that is used by operational systems within an organization or enterprise. This logic, also referred to as business rules, includes policies, requirements, and conditional statements that are used to determine the tactical actions that take place in applications and systems.
A02.027.313	Application Components	Process Automation and Management	Case Management	Software that manages the life cycle of a particular claim or investigation within an organization to include creating, routing, tracing, assignment and closing of a case as well as collaboration among case handlers
A02.027.314	Application Components	Process Automation and Management	Change Management	Software that controls the process for updates or modifications to the existing documents, software or business processes of an organization.
A02.027.315	Application Components	Process Automation and Management	Configuration Management	Software that controls the hardware and software environments, as well as documents of an organization.
A02.027.316	Application Components	Process Automation and Management	Conflict Resolution	Software that supports the conclusion of contention or differences within the business cycle.
A02.027.317	Application Components	Process Automation and Management	Governance and Policy Management	Software the supports decisions, actions, business rules and other matters that govern an organization

A02.027.318	Application Components	Process Automation and Management	Process Tracking	Software that monitors the activities within the business cycle
A02.027.319	Application Components	Process Automation and Management	Project Management	Software that provides capabilities for cost estimation and planning, scheduling, cost control and budget management, resource allocation, collaboration, communication, quality management and documentation or administration systems, which are used to deal with the complexity of large projects.
A02.027.320	Application Components	Process Automation and Management	Quality Management	Software that ensures an organization or product is consistent based on quality planning, quality control, quality assurance and quality improvement.
A02.027.321	Application Components	Process Automation and Management	Requirements Management	Software used to document, analyze, trace, prioritize and agree on requirements for an initiative and communicate with the relevant stakeholders.
A02.027.322	Application Components	Process Automation and Management	Risk Management	Software that allows planners to explicitly address uncertainty by identifying and generating metrics, setting parameters, prioritizing, and developing mitigations, and tracking risk.
A02.028.330	Application Components	Productivity	Drawing	Software used to create or edit a graphical object.
A02.028.331	Application Components	Productivity	Presentation	Software used to display information, normally in the form of a slide show.
A02.028.332	Application Components	Productivity	Spreadsheet	Software used to create, update and/or read a two-dimensional matrix of rows and columns.
A02.028.333	Application Components	Productivity	Word Processing	Software used for the composition, editing, formatting and/or possibly printing of print material.
A02.029.340	Application Components	Security Controls	Authentication and Authorization	Software that supports obtaining information about parties attempting to log on to a system or application for security purposes and the validation of those users.
A02.029.341	Application Components	Security Controls	Digital Signature	Software to use and manage electronic signatures to support.
A02.029.342	Application Components	Security Controls	Encryption	Software to convert plaintext to ciphertext through the use of a cryptographic algorithm.
A02.029.343	Application Components	Security Controls	Virus Protection	Software used to prevent, detect, and remove self-replicating programs that run and spread by modifying other programs or files.

A02.030.360	Application Components	Unified Communications and Collaboration	Calendaring	Software that provides users with an electronic version of a calendar**,** an appointment book, address book, and/or contact list.
A02.030.361	Application Components	Unified Communications and Collaboration	Email	Software that supports the transmission of memos and messages over a network.
A02.030.362	Application Components	Unified Communications and Collaboration	Event / News Management	Software that provides users with frequently updated content to which they subscribe.
A02.030.363	Application Components	Unified Communications and Collaboration	Instant Messaging	Software that supports text, voice and/or video communications between two or more users.
A02.030.364	Application Components	Unified Communications and Collaboration	Social Software	Software that supports the capturing, storing and presentation of communication, usually written but may include audio and video as well. Interactive tools handle mediated interactions between a pair or group of users. They focus on establishing and maintaining a connection among users, facilitating the mechanics of conversation and talk.
A02.030.365	Application Components	Unified Communications and Collaboration	Syndication Management (RSS Feeds)	A family of web feed formats used to publish frequently updated works, such as blog entries, news headlines, audio, and video, in a standardized format.
A02.031.381	Application Components	Visualization	Charting	Software to develop graphical representation of data in which the data is represented by symbols such as bars, lines, slices, dots, size, etc.
A02.031.383	Application Components	Visualization	Computer Aided Design (CAD)	Software that supports the use of computer technology for the process of design and design-documentation and includes software or environments which provide the user with input-tools for the purpose of streamlining design processes; drafting, documentation, and manufacturing processes.
A02.031.384	Application Components	Visualization	Data Mapping	Software that supports the process of creating data element mappings between two distinct data models. Data mapping is used as a first step for a wide variety of data integration tasks.
A02.031.387	Application Components	Visualization	Graphics	Software that enables a person to manipulate static, animated or video visual images on a computer.
A02.031.388	Application Components	Visualization	Idea Mapping	Software that is used to create diagrams of relationships between concepts, ideas or other pieces of information.

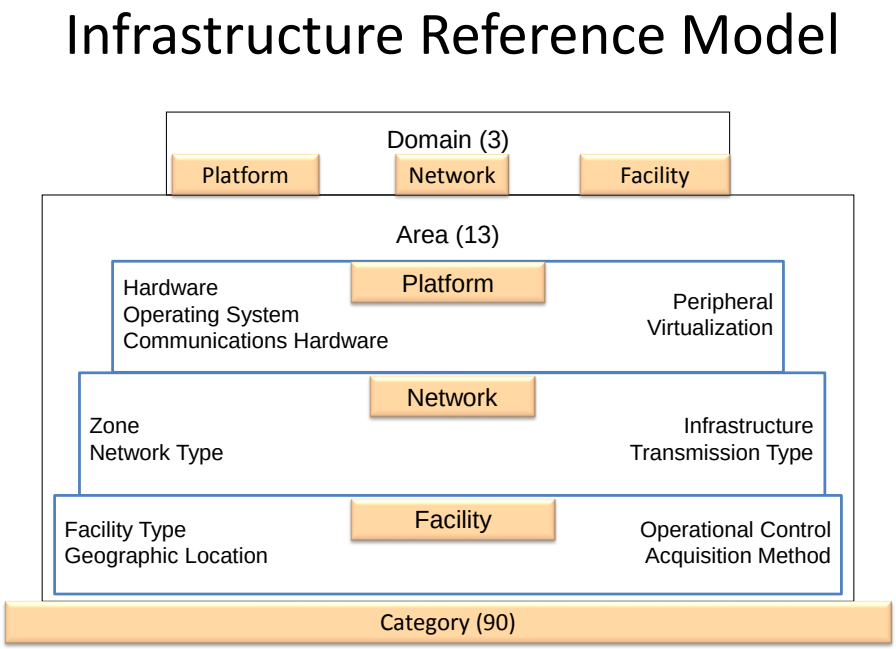
A02.031.390	Application Components	Visualization	Multimedia	Software to manage, develop and manipulate content from a combination of different content forms such as text, audio, still images, animation, video, or interactivity.
A02.031.391	Application Components	Visualization	Photographic	Software that supports the capture, storage, and manipulation of photographic images.
A02.032.400	Application Components	Web Access	Portal	Software that provides central view to manage and provide access to projects and documents.
A02.032.401	Application Components	Web Access	Search Engine	Software that includes query capabilities, precision or recall ranking, classification and pattern matching.
A02.032.402	Application Components	Web Access	Web Browser	Software used to locate, retrieve and also display content on the World Wide Web, including web pages, images, video and other files.


Interface
(A03)
Application Interface
(A03.040)
API
(A03.040.410)
FTP
(A03.040.411)
REST
(A03.040.412)
SOAP
(A03.040.413)
XML
(A03.040.414)

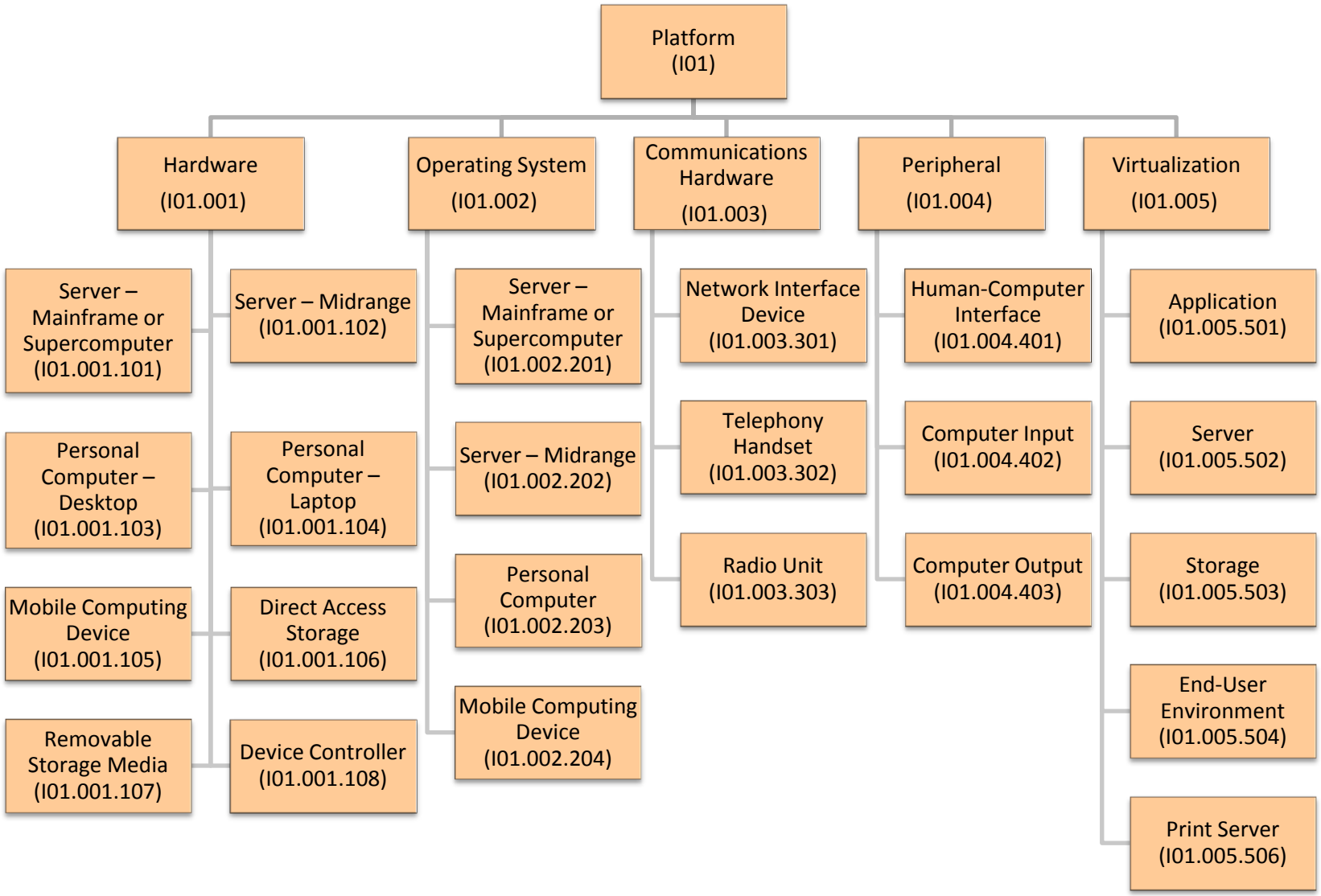
INTERFACE (A03)				
Interfaces are protocols used to transfer information from system to system.				
Code	**Domain**	**Area**	**Category**	**Description**
A03.040.010	Interface	Application Interface	API	Source code based specification intended to be used as an interface by software components to communicate with each other. An application programming interface (API) may include specifications for routines, data structures, object classes, and variables (e.g., per Wikipedia).
A03.040.011	Interface	Application Interface	FTP	Standard network protocol used to transfer files from one host to another host over a TCP-based network, such as the Internet. File Transfer Protocol (FTP) is built on a client-server architecture and uses separate control and data connections between the client and server.
A03.040.012	Interface	Application Interface	REST	Representational State Transfer (REST) is a style of software architecture for distributed hypermedia systems such as the World Wide Web.
A03.040.013	Interface	Application Interface	SOAP	Simple Object Access Protocol (SOAP) is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks. It relies on Extensible Markup Language (XML) for its message format, and usually relies on other Application Layer protocols, most notably Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP), for message negotiation and transmission.
A03.040.014	Interface	Application Interface	XML	Extensible Markup Language (XML) defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. It is defined in the XML 1.0 Specification produced by the World Wide Web Consortium (W3C), and several other related specifications, all gratis open standards.

Appendix K: Infrastructure Reference Model Taxonomy with Definitions

The IRM taxonomy is intended to provide a categorization scheme for physical IT assets, the operating systems and firmware that run them, and the locations or facilities that host the physical IT assets. The IRM is divided into three levels. Level 1 of the hierarchy, called "Domain", consists of three entities, Platform, Network and Facility, which are linked and related to each other to enable analysis of IT assets across the three dimensions. Level 2 of the hierarchy, called "Area", consists of 13 total Areas (for example, "Hardware") linked to the three Domains in Level 1. Level 3 of the hierarchy, called "Category", consists of 90 total Categories (for example, "Personal Computer – Laptop") linked to the 13 Areas in Level 2.



In the below, each IRM section is shown as a tree diagram, followed by definitions of the taxonomy elements in the corresponding tree.


Platform
(I01)
Hardware
(I01.001)
Operating System
(I01.002)
Communications Hardware
(I01.003)
Peripheral
(I01.004)
Virtualization
(I01.005)
Server – Mainframe or Supercomputer (I01.001.101)
Server – Midrange (I01.001.102)
Personal Computer – Desktop (I01.001.103)
Personal Computer – Laptop (I01.001.104)
Mobile Computing Device (I01.001.105)
Direct Access Storage (I01.001.106)
Removable Storage Media (I01.001.107)
Device Controller (I01.001.108)
Server – Mainframe or Supercomputer (I01.002.201)
Server – Midrange (I01.002.202)
Personal Computer (I01.002.203)
Mobile Computing Device (I01.002.204)
Network Interface Device (I01.003.301)
Telephony Handset (I01.003.302)
Radio Unit (I01.003.303)
Human-Computer Interface (I01.004.401)
Computer Input (I01.004.402)
Computer Output (I01.004.403)
Application (I01.005.501)
Server (I01.005.502)
Storage (I01.005.503)
End-User Environment (I01.005.504)
Print Server (I01.005.506)

PLATFORM DOMAIN (I01)				
The Platform Domain includes a hardware architecture and a software framework, where the combination allows software, particularly application software, to run. For the purposes of the IRM, platforms include a computer's architecture, operating system, attached and internal devices, as well as software platforms that emulate entire hardware platforms (e.g., system virtualization).				
Code	**Domain**	**Area**	**Category**	**Definition**
I01.001	Platform	Hardware		Hardware, in a computer context, refers to the physical components that make up a computer system, including the basic machine itself. There are many different kinds of machines and different kinds of hardware that can be installed inside, and connected to the outside, of a computer.
I01.001.101	Platform	Hardware	Server – Mainframe or Supercomputer	A Server is a computer that provides data to other computers. It may serve data to systems on a Local Area Network (LAN) or a Wide Area Network (WAN) over the Internet. A Mainframe is a high-performance computer used for large-scale computing purposes that require greater availability and security. It often serves many connected terminals and is usually used by large complex organizations. A supercomputer is a high-performance computing machine designed to have extremely fast processing speeds. Supercomputers have various applications, such as performing complex scientific calculations, modeling simulations, and rendering large amounts of 3D graphics. The chief difference between a supercomputer and a mainframe is that a supercomputer channels all its power into executing a few programs as fast as possible, whereas a mainframe uses its power to execute many programs concurrently.
I01.001.102	Platform	Hardware	Server – Midrange	A midrange computer is a medium-sized computer system or server. Midrange computers encompass a very broad range and reside in capacity between high-end PCs and mainframes. Formerly called "minicomputers", which were hosts to dumb terminals connected over dedicated cables, most midrange computers today function as servers in a network.

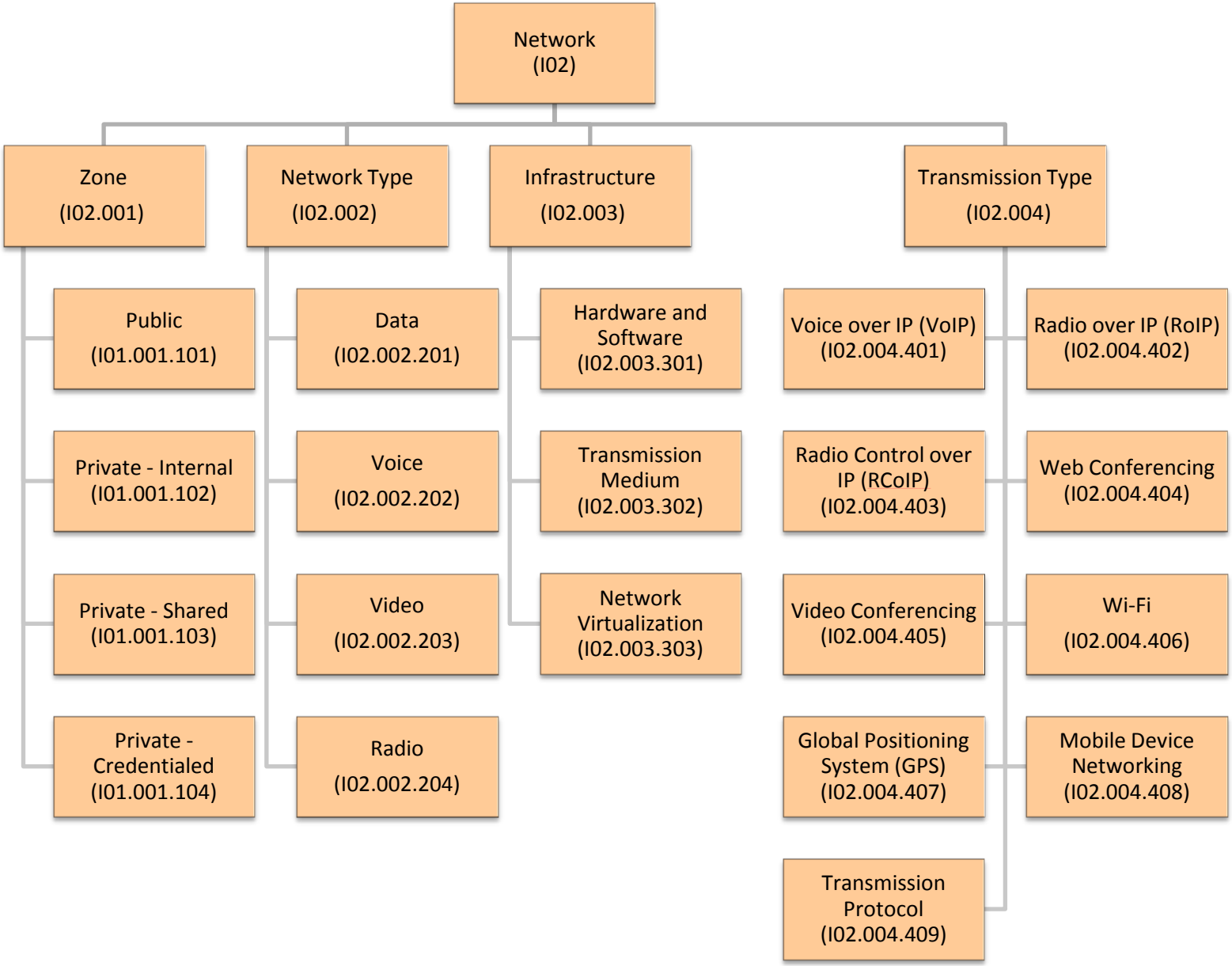
I01.001.103	Platform	Hardware	Personal Computer – Desktop	A desktop computer is a personal computer in a form intended for regular use at a single location, as opposed to a mobile laptop or portable computer. A Personal Computer (PC) is any general-purpose computer whose size, capabilities, and original sales price make it useful for individuals, and which is intended to be operated directly by an end-user with no intervening computer operator.
I01.001.104	Platform	Hardware	Personal Computer – Laptop	A laptop computer is a personal computer for mobile use. A Personal Computer (PC) is any general-purpose computer whose size, capabilities, and original sales price make it useful for individuals, and which is intended to be operated directly by an end-user with no intervening computer operator. A laptop integrates most of the typical components of a desktop computer, including a display, a keyboard, a pointing device such as a touchpad and speakers into a single unit.
I01.001.105	Platform	Hardware	Mobile Computing Device	A mobile computing device is a small, hand-held computing device, typically having a display screen with touch input and/or a miniature keyboard and weighing less than 2 pounds (0.91 kg). Such devices have an Operating System (OS), and can run various types of application software, known as apps. Most devices can also be equipped with WI-FI, Bluetooth and GPS capabilities that can allow connections to the Internet and other Bluetooth capable devices such as an automobile or a microphone headset. A camera or media player feature for video or music files can also be typically found on these devices along with a stable battery power source such as a lithium battery.
I01.001.106	Platform	Hardware	Direct Access Storage	Direct access storage device is a general term for magnetic disk storage devices and solid state storage devices. Within the IRM, the term refers to magnetic storage devices for mainframes, midranges, and PCs. "Direct access" means that all data can be accessed directly in about the same amount of time, rather than having to progress sequentially through the data.
I01.001.107	Platform	Hardware	Removable Storage Media	Removable storage media is any type of storage device that can be removed from a computer while the system is running.
I01.001.108	Platform	Hardware	Device Controller	A device controller is a part of a computer system that makes sense of the signals going to and coming from the CPU.

I01.002	Platform	Operating System		An Operating System (OS) is a computer program, implemented in either software or firmware, which acts as an intermediary between users of a computer and the computer hardware. The purpose of an operating system is to provide an environment in which a user can execute applications.
I01.002.201	Platform	Operating System	Server – Mainframe or Supercomputer	A mainframe or supercomputer operating system is, in simplest terms, a collection of programs that manage a computer system's internal workings - its memory, processors, devices, and file system. Mainframe operating systems are tailored to meet the substantially different architectures and purposes of mainframes as high-volume transaction processing devices, or the purposes of supercomputers as high-volume algorithmic processors.
I01.002.202	Platform	Operating System	Server – Midrange	A midrange computer operating system is, in simplest terms, a collection of programs that manage a computer system's internal workings - its memory, processors, devices, and file system. Midrange computers are almost universally known as servers to recognize that they often "serve" applications to end users at "client" computers, that they use a client/server computing model.
I01.002.203	Platform	Operating System	Personal Computer	For personal computers, operating systems are generally tailored to the needs of users on standalone machines that may or may not connect to a network, and are generally not servers of information to large numbers of other machines.
I01.002.204	Platform	Operating System	Mobile Computing Device	As with other operating systems, a mobile computing device Operating System (OS) is a computer program, implemented in either software or firmware, which acts as an intermediary between users of a computer and the computer hardware. The purpose of an OS is to provide an environment in which a user can execute applications.
I01.003	Platform	Communications Hardware		Communications Hardware refers broadly to hardware intended primarily to create a link to the network from the user or another computational device.
I01.003.301	Platform	Communications Hardware	Network Interface Device	For the purposes of the IRM, a Network Interface Device is a broad term that includes devices that serve as a demarcation point between the carrier's local loop and the customer's on-premises wiring, where the data wires end and a customer's premise wiring starts, and network interface controllers (also known as a network interface card, network adapter, LAN adapter and by similar terms) which may be internal or external to a piece of computer hardware.

I01.003.302	Platform	Communications Hardware	Telephony Handset	A telephony handset is a device the user holds to the ear to hear the audio sound, usually containing the phone's microphone.
I01.003.303	Platform	Communications Hardware	Radio Unit	A Radio unit is a device that transmits signals through free space by electromagnetic waves with frequencies significantly below visible light, in the radio frequency range, from about 3 kHz to 300 GHz. These devices may be analog or digital, and mobile or stationary.
I01.004	Platform	Peripheral		A peripheral is a device connected to a host computer, but not part of it. It expands the host's capabilities but does not form part of the core computer architecture. It is often, but not always, partially or completely dependent on the host. Usually, the word peripheral is used to refer to a device external to the computer case, but the devices located inside the computer case (particularly with laptops) are also technically peripherals. Devices that exist outside the computer case are called external peripherals, or auxiliary components. Devices that are inside the case such as internal hard drives or CD-ROM drives are also peripherals in technical terms and are called internal peripherals, but may not be recognized as peripherals by laypeople. For the purposes of the IRM, three different types of peripherals are recognized: Human-Computer Interface, Computer Input, and Computer Output. Storage devices, commonly a form of peripheral, are handled elsewhere.
I01.004.401	Platform	Peripheral	Human-Computer Interface	The human–computer interface can be described as the point of communication between the human user and the computer, and, as such, all devices that primarily facilitate such ongoing interactions are grouped here.
I01.004.402	Platform	Peripheral	Computer Input Device	Inputs are the signals or data received by the system, and outputs are the signals or data sent from it. For the purposes of the IRM, computer input devices are those that provide data to the machine/application combination for further processing or for manipulation by users through the human-computer interface devices.

I01.004.403	Platform	Peripheral	Computer Output Device	Inputs are the signals or data received by the system, and outputs are the signals or data sent from it. For the purposes of the IRM, computer output devices are those that provide data from the machine/application combination to other machines or to the user for asynchronous consumption.
I01.005	Platform	Virtualization		In computing, virtualization is the creation of a virtual (rather than actual) version of something, such as a hardware platform, Operating System (OS), storage device, or network resources. This section of the IRM categorizes those mechanisms to create virtual platforms.
I01.005.501	Platform	Virtualization	Application	For the purposes of the IRM, application virtualization encapsulates application from the underlying operating system on which they are executed. A fully virtualized application is not installed in the traditional sense, although it is still executed as if it were. The application is fooled at runtime into believing that it is directly interfacing with the original operating system and all the resources managed by it, when in reality it is not. In this context, the term "virtualization" refers to the artifact being encapsulated (application), which is quite different to its meaning in hardware virtualization, where it refers to the artifact being abstracted (physical hardware).
I01.005.502	Platform	Virtualization	Server	Virtual servers are virtual machines where each server, although running in software on the same physical computer as other customers' servers, is in many respects functionally equivalent to a separate physical computer. A virtual server is dedicated to the individual customer's needs, has the privacy of a separate physical computer, and is configured to run server software. The term cloud server is also used to describe the same concept, normally where such systems can be setup and re-configured on the fly.
I01.005.503	Platform	Virtualization	Storage	Storage virtualization applies virtualization concepts to enable better functionality and more advanced features within the storage system. Storage systems use special hardware and software along with disk drives in order to provide very fast and reliable storage for computing and data processing.
I01.005.504	Platform	Virtualization	End-User Environment	End-User Environment virtualization is a broad term including desktop and client virtualization. End-User virtualization separates a personal computer desktop or mobile computing environment from a physical machine using the client–server model of computing.

I01.005.506	Platform	Virtualization	Print Server	Print server virtualization extends the virtualization concept to the access to and management of print resources. For the purposes of the IRM, a print server can be a dedicated device, a standalone computer, specialized software, or some combination that handles receipt, queuing, delivery, and status of print jobs for printers on the network.


Network
(I02)
Zone
(I02.001)
Network Type
(I02.002)
Infrastructure
(I02.003)
Transmission Type
(I02.004)
Public
(I01.001.101)
Private - Internal
(I01.001.102)
Private - Shared
(I01.001.103)
Private - Credentialed
(I01.001.104)
Data
(I02.002.201)
Voice
(I02.002.202)
Video
(I02.002.203)
Radio
(I02.002.204)
Hardware and Software
(I02.003.301)
Transmission Medium
(I02.003.302)
Network Virtualization
(I02.003.303)
Voice over IP (VoIP)
(I02.004.401)
Radio Control over IP (RCoIP)
(I02.004.403)
Video Conferencing
(I02.004.405)
Global Positioning System (GPS)
(I02.004.407)
Transmission Protocol
(I02.004.409)
Radio over IP (RoIP)
(I02.004.402)
Web Conferencing
(I02.004.404)
Wi-Fi
(I02.004.406)
Mobile Device Networking
(I02.004.408)

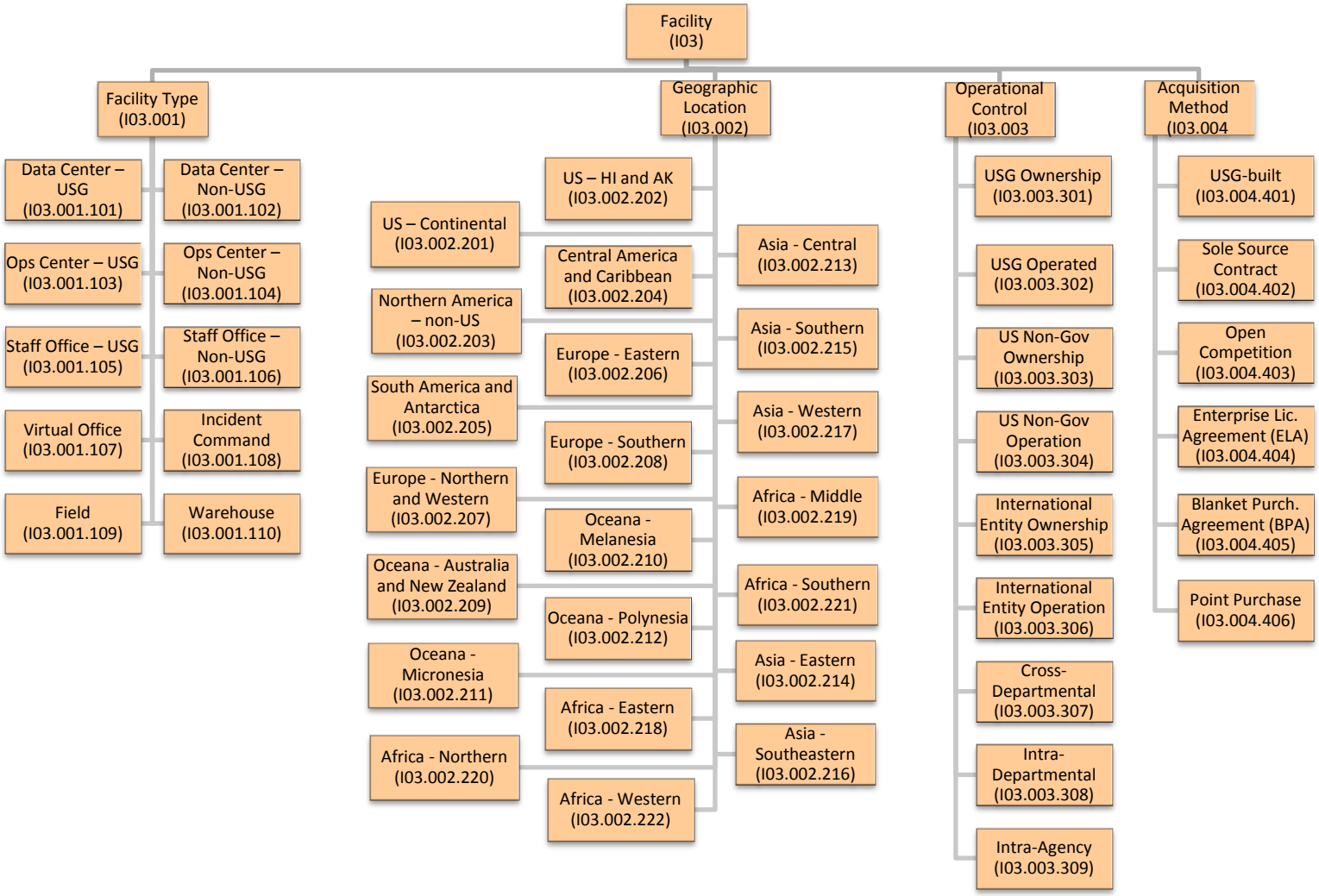
NETWORK DOMAIN (I02)				
The Network (Element Name) Domain (Level) describes the Network section of the IRM addresses how a particular IT asset accessed and used within the enterprise.				
Code	**Domain**	**Area**	**Category**	**Definitions**
I02.001	Network	Zone		For the purposes of the IRM, a Zone is a conceptual division of the network into areas that are separated (usually by security measures) from one another.
I02.001.101	Network	Zone	Public	Assets in the public zone are accessible to anyone, without credentials, from outside the boundaries of the organization.
I02.001.102	Network	Zone	Private - Internal	Assets in the private, internal zone are accessible only from within the boundaries of a single organization
I02.001.103	Network	Zone	Private - Shared	Assets in the private, shared zone are accessible to more than one major organization, but only within the boundaries of those participating organizations.
I02.001.104	Network	Zone	Private - Credentialed	Assets in the private, credentialed zone are accessible only with appropriate credentials from outside the boundaries of the organization.
I02.002	Network	Network Type		For the purposes of the IRM, a Network Type categorizes the major types of traffic on a given network. A single network may carry more than one type of traffic.
I02.002.201	Network	Network Type	Data	A data network type is an electronic communications process that allows for the orderly transmission and receptive of data, such as letters, spreadsheets, and other types of documents. What sets the data network apart from other forms of communication, such as an audio network, is that the data network is configured to transmit data only. This is in contrast to the audio or voice network, which is often employed for both voice communications and the transmission of data such as a facsimile transmission.
I02.002.202	Network	Network Type	Voice	Voice networks are sometimes dedicated, as in the original public switched telephone network (PSTN), but have changed to be a type of traffic carried on data networks using some form of packet-switching technology. Voice traffic is distinct from Data traffic in the delivery requirements (it needs to arrive nearly synchronously and be assembled in order without drop-outs) and bandwidth usage (which is high).

I02.002.203	Network	Network Type	Video	Video networks can be dedicated links devoted to video for large video conferencing installations. As with Voice traffic, Video is often a type of traffic carried on data networks using some form of packet-switching technology. Video traffic is distinct from Data traffic in the delivery requirements (it needs to arrive nearly synchronously and be assembled in order without drop-outs) and bandwidth usage (which is very high).
I02.002.204	Network	Network Type	Radio	Radio networks are transmitted through free space by radio waves. There are two types of radio networks currently in use around the world: the one-to-many broadcast network commonly used for public information and mass media entertainment; and the two-way type used more commonly for public safety and public services such as police, fire, taxicabs, and delivery services. Many of the same components and much of the same basic technology applies to both.
I02.003	Network	Infrastructure		For the purposes of the IRM, Infrastructure, as used here, is a broad term covering the various forms of basic hardware and software that comprise the foundation of a network.
I02.003.301	Network	Infrastructure	Hardware and Software	Specifically for Networks, Hardware and Software refers to many different kinds of devices and their firmware. These devices provide many things including routing, security, etc. The software included here is the firmware and/or Operating System (OS) associated with specific network devices.
I02.003.302	Network	Infrastructure	Transmission Medium	Transmission medium is the material and/or technology that carries signal from one location to another.
I02.003.303	Network	Infrastructure	Network Virtualization	A virtual network is a computer network that consists, at least in part, of virtual network links. A virtual network link is a link that does not consist of a physical (wired or wireless) connection between two computing devices but is implemented using methods of network virtualization. The two most common forms of network virtualization are protocol-based virtual networks (such as Virtual Local Area Networks (VLAN), Virtual Private Networks (VPN), and Virtual Private LAN Services (VPLS)) and virtual networks that are based on virtual devices (such as the networks connecting virtual machines inside a hypervisor).
I02.004	Network	Transmission Type		The Transmission Type category allows for identification of the low-level infrastructure "applications" that form the core of the network, as well as the foundational protocols.

I02.004.401	Network	Transmission Type	Voice over IP (VoIP)	Voice over IP (VoIP, or Voice over Internet Protocol) commonly refers to the communication protocols, technologies, methodologies, and transmission techniques involved in the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. Other terms commonly associated with VoIP are IP telephony, Internet telephony, Voice over Broadband (VoBB), broadband telephony, IP communications, and broadband phone. Internet telephony refers to communications services — voice, fax, SMS, and/or voice-messaging applications — that are transported via the Internet, rather than the Public Switched Telephone Network (PSTN). The steps involved in originating a VoIP telephone call are signaling and media channel setup, digitization of the analog voice signal, encoding, packetization, and transmission as Internet Protocol (IP) packets over a packet-switched network. On the receiving side, similar steps (usually in the reverse order) such as reception of the IP packets, decoding of the packets and digital-to-analog conversion reproduce the original voice stream. Even though IP Telephony and VoIP are terms that are used interchangeably, they are actually different; IP telephony has to do with digital telephony systems that use IP protocols for voice communication, while VoIP is actually a subset of IP Telephony. VoIP is a technology used by IP telephony as a means of transporting phone calls.
I02.004.402	Network	Transmission Type	Radio over IP (RoIP)	Radio over Internet Protocol (RoIP) is similar to VoIP, but augments two-way radio communications rather than telephone calls. From the system point of view, it is essentially VoIP with PTT (Push To Talk). To the user it can be implemented like any other radio network. With RoIP, at least one node of a network is a radio (or a radio with an IP interface device) connected via IP to other nodes in the radio network. The other nodes can be two-way radios, but could also be dispatch consoles either traditional (hardware) or modern (software on a PC), POTS telephones, softphone applications running on a computer such as a Skype phone, PDA, smartphone, or some other communications device accessible over IP. RoIP can be deployed over private networks as well as the public Internet.

I02.004.403	Network	Transmission Type	Radio Control over IP (RCoIP)	Radio Control over Internet Protocol (RCoIP) builds on the concepts of RoIP, but can be used in combination with analog radio units. In RCoIP, handsets and other mobile units are remotely controlled using IP-delivered commands.
I02.004.404	Network	Transmission Type	Web Conferencing	Web conferencing refers to a service that allows conferencing events to be shared with remote locations. In general the service is made possible by Internet technologies, particularly on TCP/IP connections. The service allows real-time point-to-point communications as well as multicast communications from one sender to many receivers. It offers information of text-based messages, voice and video chat to be shared simultaneously, across geographically dispersed locations. Applications for web conferencing include meetings, training events, lectures, or short presentations from any computer.
I02.004.405	Network	Transmission Type	Video Conferencing	Videoconferencing is the conduct of a videoconference (also known as a video conference or video teleconference) by a set of telecommunication technologies which allow two or more locations to communicate by simultaneous two-way video and audio transmissions. It has also been called 'visual collaboration' and is a type of groupware.
I02.004.406	Network	Transmission Type	Wi-Fi	Wi-Fi (/ˈwaɪfaɪ/, also spelled Wifi or WiFi) is a popular technology that allows an electronic device to exchange data wirelessly (using radio waves) over a computer network, including high-speed Internet connections. The Wi-Fi Alliance defines Wi-Fi as any "wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards". However, since most modern WLANs are based on these standards, the term "Wi-Fi" is used in general English as a synonym for "WLAN".
I02.004.407	Network	Transmission Type	Global Positioning System (GPS)	The Global Positioning System (GPS) is a space-based satellite navigation system that provides location and time information in all weather, anywhere on or near the Earth, where there is an unobstructed line of sight to four or more GPS satellites. It is maintained by the United States government and is freely accessible to anyone with a GPS receiver.

I02.004.408	Network	Transmission Type	Mobile Device Networking	Mobile Device Networking covers the sets of standards commonly used for mobile devices and mobile telecommunication services and networks that comply with specifications by the International Telecommunication Union. Such standards find applications in wireless voice telephony, mobile Internet access, fixed wireless Internet access, video calls and mobile TV, among others.
I02.004.409	Network	Transmission Type	Transmission Protocol	Transmission Protocol is a category that allows grouping and identification of various transmission standards, at a basic level in the OSI stack.


Facility (I03)
Facility Type (I03.001)
Geographic Location (I03.002)
Operational Control (I03.003
Acquisition Method (I03.004
Data Center – USG (I03.001.101)
Data Center – Non-USG (I03.001.102)
Ops Center – USG (I03.001.103)
Ops Center – Non-USG (I03.001.104)
Staff Office – USG (I03.001.105)
Staff Office – Non-USG (I03.001.106)
Virtual Office (I03.001.107)
Incident Command (I03.001.108)
Field (I03.001.109)
Warehouse (I03.001.110)
US – HI and AK (I03.002.202)
US – Continental (I03.002.201)
Central America and Caribbean (I03.002.204)
Northern America – non-US (I03.002.203)
Europe - Eastern (I03.002.206)
South America and Antarctica (I03.002.205)
Europe - Southern (I03.002.208)
Europe - Northern and Western (I03.002.207)
Oceana - Melanesia (I03.002.210)
Oceana - Australia and New Zealand (I03.002.209)
Oceana - Polynesia (I03.002.212)
Oceana - Micronesia (I03.002.211)
Africa - Eastern (I03.002.218)
Africa - Northern (I03.002.220)
Africa - Western (I03.002.222)
Asia - Central (I03.002.213)
Asia - Southern (I03.002.215)
Asia - Western (I03.002.217)
Africa - Middle (I03.002.219)
Africa - Southern (I03.002.221)
Asia - Eastern (I03.002.214)
Asia - Southeastern (I03.002.216)
USG Ownership (I03.003.301)
USG Operated (I03.003.302)
US Non-Gov Ownership (I03.003.303)
US Non-Gov Operation (I03.003.304)
International Entity Ownership (I03.003.305)
International Entity Operation (I03.003.306)
Cross-Departmental (I03.003.307)
Intra-Departmental (I03.003.308)
Intra-Agency (I03.003.309)
USG-built (I03.004.401)
Sole Source Contract (I03.004.402)
Open Competition (I03.004.403)
Enterprise Lic. Agreement (ELA) (I03.004.404)
Blanket Purch. Agreement (BPA) (I03.004.405)
Point Purchase (I03.004.406)

FACILITY DOMAIN (I03)				
The Facility (Element Name) Domain (Level) of the IRM addresses how and/or where a particular asset acquired, deployed, and operated.				
Code	**Domain**	**Area**	**Category**	**Definition**
I03.001	Facility	Facility Type		The particular kind of location in which the assets are deployed.
I03.001.101	Facility	Facility Type	Data Center – USG	A data center is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and security devices. In this instance, such operations center would be the primary responsibility of the US Government, with or without contract support.
I03.001.102	Facility	Facility Type	Data Center – Non-USG	A data center is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and security devices. Enterprises with large networks as well as service providers may use a third-party data center to shift the burden of data center operations onto the third party, with or without direct support of US Government employees.
I03.001.103	Facility	Facility Type	Operations Center – USG	An operations center is designed to monitor IT assets deployed elsewhere on an enterprise network. There are many different kinds of operations centers, including "Network Operations Center" (NOC) and "Security Operations Center" (SOC). In this instance, such operations center would be the primary responsibility of the US Government, with or without contract support.

FACILITY DOMAIN (I03)				
The Facility (Element Name) Domain (Level) of the IRM addresses how and/or where a particular asset acquired, deployed, and operated.				
Code	**Domain**	**Area**	**Category**	**Definition**
I03.001.104	Facility	Facility Type	Operations Center – Non-USG	An operations center is designed to monitor IT assets deployed elsewhere on an enterprise network. There are many different kinds of operations centers, including "Network Operations Center" (NOC) and "Security Operations Center" (SOC). Enterprises with large networks as well as service providers may use a third-party operations center to shift the burden of operational monitoring onto the third party, with or without direct support of US Government employees.
I03.001.105	Facility	Facility Type	Staff Office – USG	For the purposes of the IRM, a staff office is any physical location/building intended to be a destination for actual individuals to regularly report for work functions, including locations primarily devoted to research, development, and/or science. In this instance, such staff offices would be the primary responsibility of the US Government, with or without the addition of contract staff.
I03.001.106	Facility	Facility Type	Staff Office – Non-USG	For the purposes of the IRM, a staff office is any physical location/building intended to be a destination for actual individuals to regularly report for work functions, including locations primarily devoted to research, development, and/or science. In this instance, such staff offices would be the primary responsibility of a third party, where US Government employees may or may not be stationed.
I03.001.107	Facility	Facility Type	Virtual Office	For the purposes of the IRM, a Virtual Office is a workspace not set in a specific geographic location, but rather connected (via the Internet) to the wider enterprise. Virtual Offices include telework arrangements for US Government employees (when they are off-site), contract staff that works remotely, or some combination.

FACILITY DOMAIN (I03)				
The Facility (Element Name) Domain (Level) of the IRM addresses how and/or where a particular asset acquired, deployed, and operated.				
Code	**Domain**	**Area**	**Category**	**Definition**
I03.001.108	Facility	Facility Type	Incident Command	For the purposes of the IRM, an Incident Command includes smaller, often temporary locations for the management of forward operations or crisis / emergency management. In the military, such locations are often called "forward operating bases" (FOBs).
I03.001.109	Facility	Facility Type	Field	For the purposes of the IRM, the Field includes any active deployment outside of traditional staff facilities, including anything from the battlefield to on-site research and data-gathering.
I03.001.110	Facility	Facility Type	Warehouse	For the purposes of the IRM, Warehouse covers any place in which IT assets are stored or staged. The storage or staging may be for any purpose, including, but not limited to delivery to an eventual service location, disposal, or further decisions. The intent of this category is to identify IT assets not currently in active use.
I03.002	Facility	Geographic Location		Geographic location is the actual global region in which the IT asset is deployed, regardless of facility type. These divisions are derived from the UN listing of macro geographical regions, available at: http://unstats.un.org/unsd/methods/m49/m49regin.htm.
I03.002.201	Facility	Geographic Location	US – Continental	The Continentals US refers to the 48 contiguous states.
I03.002.202	Facility	Geographic Location	US – HI and AK	US - HI and AK geographic location refers to the 49th and 50th states, Alaska and Hawaii.
I03.002.203	Facility	Geographic Location	Northern America – non-US	North America – non-US refers specifically to: Bermuda, Canada, Greenland, Saint Pierre and Miquelon.

FACILITY DOMAIN (I03)				
The Facility (Element Name) Domain (Level) of the IRM addresses how and/or where a particular asset acquired, deployed, and operated.				
Code	**Domain**	**Area**	**Category**	**Definition**
I03.002.204	Facility	Geographic Location	Central America and Caribbean	Central America and Caribbean is the central geographic region of the Americas. Central America is the southernmost portion of the North American continent, which connects with South America on the southeast, and refers specifically to: Belize, Costa Rica, El Salvador, Guatemala, Honduras, Mexico, Nicaragua, Panama The Caribbean is a crescent-shaped group of islands more than 2,000 miles (3,200 km) long separating the Gulf of Mexico and the Caribbean Sea, to the west and south, from the Atlantic Ocean, to the east and north. From the peninsula of Florida on the mainland of the United States, the islands stretch 1,200 miles (1,900 km) southeastward, then 500 miles (800 km) south, then west along the north coast of Venezuela on the South American mainland. Caribbean refers specifically to: Anguilla, Antigua and Barbuda, Aruba, Bahamas, Barbados, Bonaire, Saint Eustatius and Saba, British Virgin Islands, Cayman Islands, Cuba, Curaçao, Dominica, Dominican Republic, Grenada, Guadeloupe, Haiti, Jamaica, Martinique, Montserrat, Puerto Rico, Saint-Barthélemy, Saint Kitts and Nevis, Saint Lucia, Saint Martin (French part), Saint Vincent and the Grenadines, Saint Maarten (Dutch part), Trinidad and Tobago, Turks and Caicos Islands, United States Virgin Islands

FACILITY DOMAIN (I03)				
The Facility (Element Name) Domain (Level) of the IRM addresses how and/or where a particular asset acquired, deployed, and operated.				
Code	**Domain**	**Area**	**Category**	**Definition**
I03.002.205	Facility	Geographic Location	South America and Antarctica	South America is a continent located in the Western Hemisphere, mostly in the Southern Hemisphere, with a relatively small portion in the Northern Hemisphere. South America refers specifically to: Argentina , Bolivia (Plurinational State of), Brazil, Chile, Colombia, Ecuador, Falkland Islands (Malvinas), French Guiana, Guyana, Paraguay, Peru, Suriname, Uruguay, Venezuela (Bolivarian Republic of) Antarctica is Earth's southernmost continent, containing the geographic South Pole. It is situated in the Antarctic region of the Southern Hemisphere, almost entirely south of the Antarctic Circle, and is surrounded by the Southern Ocean.
I03.002.206	Facility	Geographic Location	Europe - Eastern	Europe is one of the world's seven continents. Comprising the western most peninsula of Eurasia, Europe is bordered by the Arctic Ocean to the north, the Atlantic Ocean to the west, the Mediterranean Sea to the south, and the Black Sea and connected waterways to the southeast. Eastern Europe refers specifically to: Belarus, Bulgaria, Czech Republic, Hungary, Poland, Republic of Moldova, Romania, Russian Federation, Slovakia, Ukraine.

FACILITY DOMAIN (I03)				
The Facility (Element Name) Domain (Level) of the IRM addresses how and/or where a particular asset acquired, deployed, and operated.				
Code	**Domain**	**Area**	**Category**	**Definition**
I03.002.207	Facility	Geographic Location	Europe - Northern and Western	Europe is one of the world's seven continents. Comprising the western most peninsula of Eurasia, Europe is bordered by the Arctic Ocean to the north, the Atlantic Ocean to the west, the Mediterranean Sea to the south, and the Black Sea and connected waterways to the southeast. Northern Europe refers specifically to: Åland Islands, Channel Islands, Denmark, Estonia, Faeroe Islands, Finland, Guernsey, Iceland, Ireland, Isle of Man, Jersey, Latvia, Lithuania, Norway, Sark, Svalbard and Jan Mayen Islands, Sweden, United Kingdom of Great Britain and Northern Ireland Western Europe refers specifically to: Austria, Belgium, France, Germany, Liechtenstein, Luxembourg, Monaco, Netherlands, Switzerland
I03.002.208	Facility	Geographic Location	Europe - Southern	Europe is one of the world's seven continents. Comprising the western most peninsula of Eurasia, Europe is bordered by the Arctic Ocean to the north, the Atlantic Ocean to the west, the Mediterranean Sea to the south, and the Black Sea and connected waterways to the southeast. Southern Europe refers specifically to: Albania, Andorra, Bosnia and Herzegovina, Croatia, Gibraltar, Greece, Holy See, Italy, Malta, Montenegro, Portugal, San Marino, Serbia, Slovenia, Spain, The former Yugoslav Republic of Macedonia
I03.002.209	Facility	Geographic Location	Oceana - Australia and New Zealand	Oceania is a region centered on the islands of the tropical Pacific Ocean. Oceana – Australia and New Zealand refers specifically to: Australia, New Zealand, Norfolk Island

FACILITY DOMAIN (I03)				
The Facility (Element Name) Domain (Level) of the IRM addresses how and/or where a particular asset acquired, deployed, and operated.				
Code	**Domain**	**Area**	**Category**	**Definition**
I03.002.210	Facility	Geographic Location	Oceana - Melanesia	Oceania is a region centered on the islands of the tropical Pacific Ocean. Oceana - Melanesia refers specifically to: Fiji, New Caledonia, Papua New Guinea, Solomon Islands, Vanuatu.
I03.002.211	Facility	Geographic Location	Oceana - Micronesia	Oceania is a region centered on the islands of the tropical Pacific Ocean. Oceana - Micronesia refers specifically to: Guam, Kiribati, Marshall Islands, Micronesia (Federated States of), Nauru, Northern Mariana Islands, Palau
I03.002.212	Facility	Geographic Location	Oceana - Polynesia	Oceania is a region centered on the islands of the tropical Pacific Ocean. Oceana - Polynesia refers specifically to: American Samoa, Cook Islands, French Polynesia, Niue, Pitcairn, Samoa, Tokelau, Tonga, Tuvalu, Wallis and Futuna Islands
I03.002.213	Facility	Geographic Location	Asia - Central	Asia is the world's largest and most populous continent, located primarily in the eastern and northern hemispheres. Central Asia includes primarily former Soviet Republics that are typically culturally Islamic. Central Asia refers specifically to: Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan
I03.002.214	Facility	Geographic Location	Asia - Eastern	Asia is the world's largest and most populous continent, located primarily in the eastern and northern hemispheres. Eastern Asia excludes the far eastern districts of the Russian Federation, focusing on Mongolia, the various Chinese-associated countries and territories, the Koreas, and Japan. Eastern Asia refers specifically to: China , China - Hong Kong Special Administrative Region, China - Macao Special Administrative Region, Democratic People's Republic of Korea, Japan, Mongolia, Republic of Korea

FACILITY DOMAIN (I03)				
The Facility (Element Name) Domain (Level) of the IRM addresses how and/or where a particular asset acquired, deployed, and operated.				
Code	**Domain**	**Area**	**Category**	**Definition**
I03.002.215	Facility	Geographic Location	Asia - Southern	Asia is the world's largest and most populous continent, located primarily in the eastern and northern hemispheres. Southern Asia includes the Indian Sub-Continent, including Bangladesh in the East, the Himalayas south of China to the North, Sri Lanka and the Maldives to the South, and West through historical Persia (Iran). Southern Asia refers specifically to: Afghanistan, Bangladesh, Bhutan, India, Iran (Islamic Republic of), Maldives, Nepal, Pakistan, Sri Lanka
I03.002.216	Facility	Geographic Location	Asia - Southeastern	Asia is the world's largest and most populous continent, located primarily in the eastern and northern hemispheres. Southeastern Asia includes countries to the east of Bangladesh and the south of China. Southeastern Asia refers specifically to: Brunei Darussalam, Cambodia, Indonesia, Lao People's Democratic Republic, Malaysia, Myanmar, Philippines, Singapore, Thailand, Timor-Leste, Viet Nam
I03.002.217	Facility	Geographic Location	Asia - Western	Asia is the world's largest and most populous continent, located primarily in the eastern and northern hemispheres. Western Asia is also commonly known as "The Middle East", though it is part of the Asian continent. The region includes the historical Babylon (Iraq), the Arabian Peninsula, historical Palestine, the Asia Minor Sub-Continent, and the island of Cyprus. Western Asia refers specifically to: Armenia, Azerbaijan, Bahrain, Cyprus, Georgia, Iraq, Israel, Jordan, Kuwait, Lebanon, Occupied Palestinian Territory, Oman, Qatar, Saudi Arabia, Syrian Arab Republic, Turkey, United Arab Emirates, Yemen

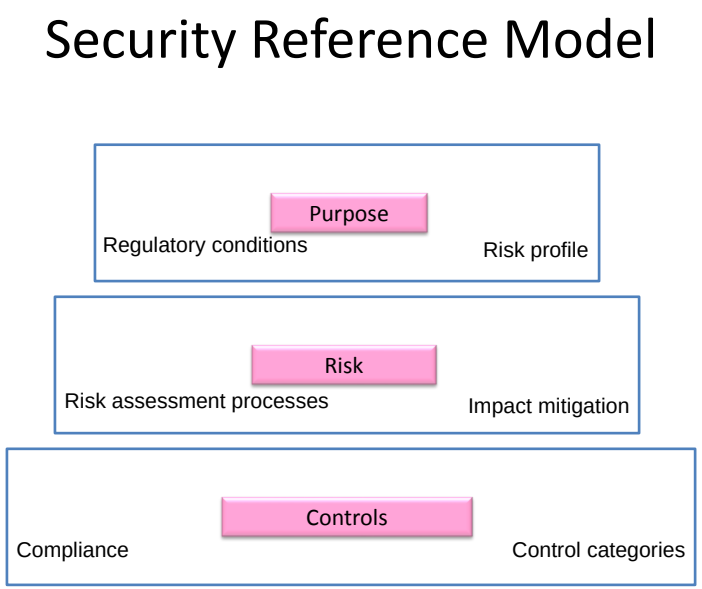
FACILITY DOMAIN (I03)				
The Facility (Element Name) Domain (Level) of the IRM addresses how and/or where a particular asset acquired, deployed, and operated.				
Code	**Domain**	**Area**	**Category**	**Definition**
I03.002.218	Facility	Geographic Location	Africa - Eastern	Eastern Africa is the easterly region of the African continent, variably defined by geography or geopolitics. Eastern Africa refers specifically to: Burundi, Comoros, Djibouti, Eritrea, Ethiopia, Kenya, Madagascar, Malawi, Mauritius, Mayotte, Mozambique, Réunion, Rwanda, Seychelles, Somalia, Uganda, United Republic of Tanzania, Zambia, Zimbabwe
I03.002.219	Facility	Geographic Location	Africa - Middle	Middle Africa, as defined by geography or geopolitics, includes 10 countries located in Central Africa. Middle Africa refers specifically to: Angola, Cameroon, Central African Republic, Chad, Congo, Democratic Republic of the Congo, Equatorial Guinea, Gabon, Sao Tome and Principe
I03.002.220	Facility	Geographic Location	Africa - Northern	Northern Africa refers to the northernmost region of the African continent, linked by the Sahara to Sub-Saharan Africa. Geopolitically, the United Nations definition of Northern Africa includes eight countries or territories. Northern Africa refers specifically to: Algeria, Egypt, Libya, Morocco, South Sudan, Sudan, Tunisia, Western Sahara
I03.002.221	Facility	Geographic Location	Africa - Southern	Southern Africa is the southernmost region of the African continent, variably defined by geography or geopolitics. Within the region are numerous territories, including the Republic of South Africa. Southern Africa refers specifically to: Botswana, Lesotho, Namibia, South Africa, Swaziland

FACILITY DOMAIN (I03)				
The Facility (Element Name) Domain (Level) of the IRM addresses how and/or where a particular asset acquired, deployed, and operated.				
Code	**Domain**	**Area**	**Category**	**Definition**
I03.002.222	Facility	Geographic Location	Africa - Western	Western Africa is the westernmost region of the African continent. Geopolitically, the United Nations definition of Western Africa includes the16 countries and an area of approximately 5 million square km. Western Africa refers specifically to: Benin, Burkina Faso, Cape Verde, Cote d'Ivoire, Gambia, Ghana, Guinea, Guinea-Bissau, Liberia, Mali, Mauritania, Niger, Nigeria, Saint Helena, Senegal, Sierra Leone, Togo
I03.003	Facility	Operational Control		Operational Control describes the three key aspects of IT asset operations: ownership, operations, and scope of use / re-use.
I03.003.301	Facility	Operational Control	USG Ownership	Owned by the US Government, through Government Services Agency (GSA) or another specific department or agency, etc.
I03.003.302	Facility	Operational Control	USG Operated	Operated by the US Government, through the Government Services Agency (GSA) or another specific department or agency, etc.
I03.003.303	Facility	Operational Control	US Non-Governmental Ownership	Owned by an entity based or controlled within the domestic US, and existing entirely outside of the US Government control.
I03.003.304	Facility	Operational Control	US Non-Governmental Operation	Operated by an entity based or controlled within the domestic US, and existing entirely outside of the US Government control.
I03.003.305	Facility	Operational Control	International Entity Ownership	Owned by an entity based or controlled outside of the domestic US, and existing entirely outside of the US Government control.
I03.003.306	Facility	Operational Control	International Entity Operation	Operated by an entity based or controlled outside of the domestic US, and existing entirely outside of the US Government control.
I03.003.307	Facility	Operational Control	Cross-Departmental	An asset that is provided for active use across more than one departmental boundary (for example, usage by both Department of Justice and Department of State).

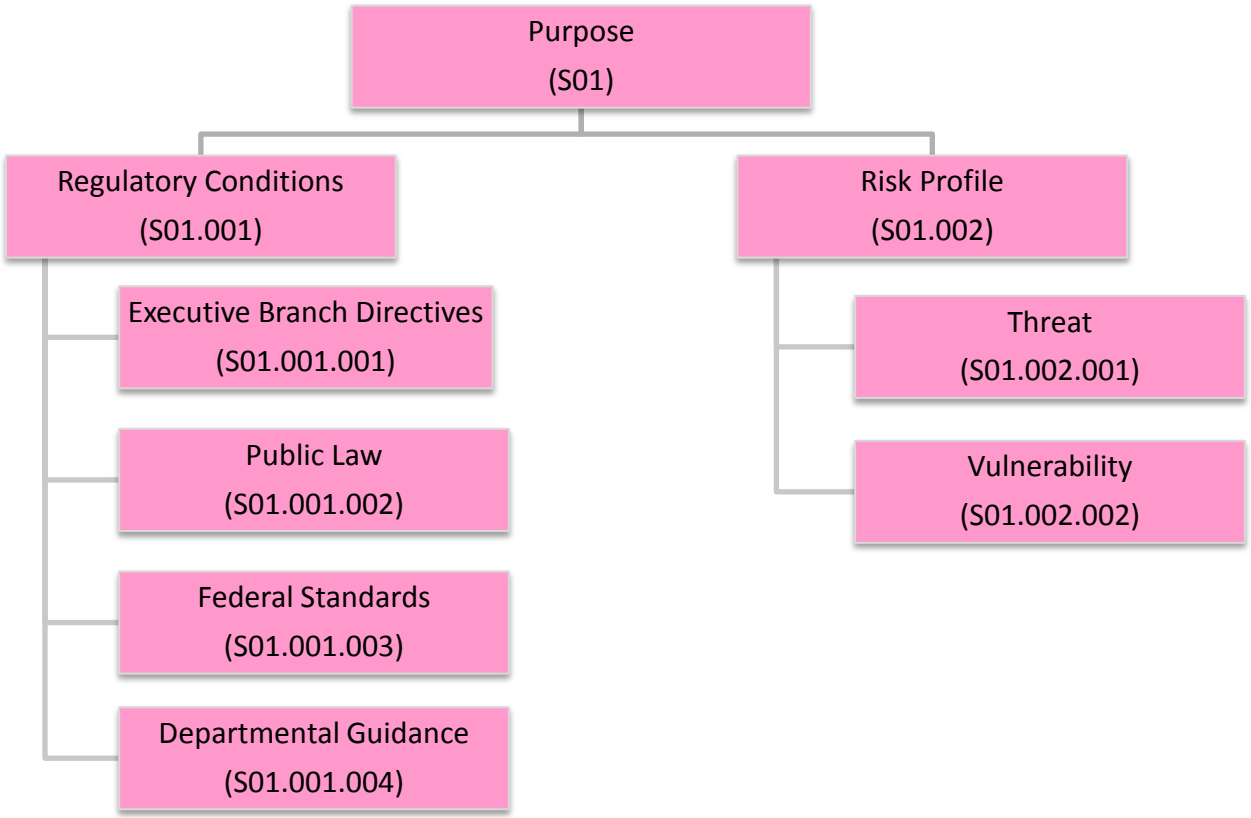
FACILITY DOMAIN (I03)				
The Facility (Element Name) Domain (Level) of the IRM addresses how and/or where a particular asset acquired, deployed, and operated.				
Code	**Domain**	**Area**	**Category**	**Definition**
I03.003.308	Facility	Operational Control	Intra-Departmental	An asset that is provided for active use by more than one sub-agency within a single US Government Department (for example, usage by National Oceanic and Atmospheric Administration (NOAA) and the National Institute of Standards and Technology (NIST) within Department of Commerce).
I03.003.309	Facility	Operational Control	Intra-Agency	An asset that is provided for active use only within a single sub-agency of a larger US Government department (for example, usage only by Internal Revenue Service (IRS) within Department of Treasury).
I03.004	Facility	Acquisition Method		The method by which IT assets are acquired.
I03.004.401	Facility	Acquisition Method	USG-built	Built by the U.S. Government; Government Off The Shelf (GOTS)
I03.004.402	Facility	Acquisition Method	Sole Source Contract	Sole Source means a contract for the purchase of supplies or services that is entered into or proposed to be entered into by an agency after soliciting and negotiating with only one source.
I03.004.403	Facility	Acquisition Method	Open Competition	Full and open competition, when used with respect to a contract action, means that all responsible sources are permitted to compete.
I03.004.404	Facility	Acquisition Method	Enterprise License Agreement (ELA)	An Enterprise License Agreement (ELA) is an agreement to license the entire population of an entity (employees, on-site contractors, off-site contractors) accessing a software or service for a specified period of time for a specified value. Consolidated contracts are often confused with ELAs. Consolidated contracts generally are limited by the number eligible to use the software or service.
I03.004.405	Facility	Acquisition Method	Blanket Purchasing Agreement (BPA)	A Blanket Purchase Agreement (BPA) is a simplified method of filling anticipated repetitive needs for supplies or services by establishing “charge accounts” with qualified sources of supply.
I03.004.406	Facility	Acquisition Method	Point Purchase	For the purposes of the IRM, Point Purchase is a broad term encompassing one-time, non-contract purchases that typically involve a smaller amount of money than ELAs, BPAs, or other longer-term contractual arrangements.

Appendix L: Security Reference Model Taxonomy with Definitions

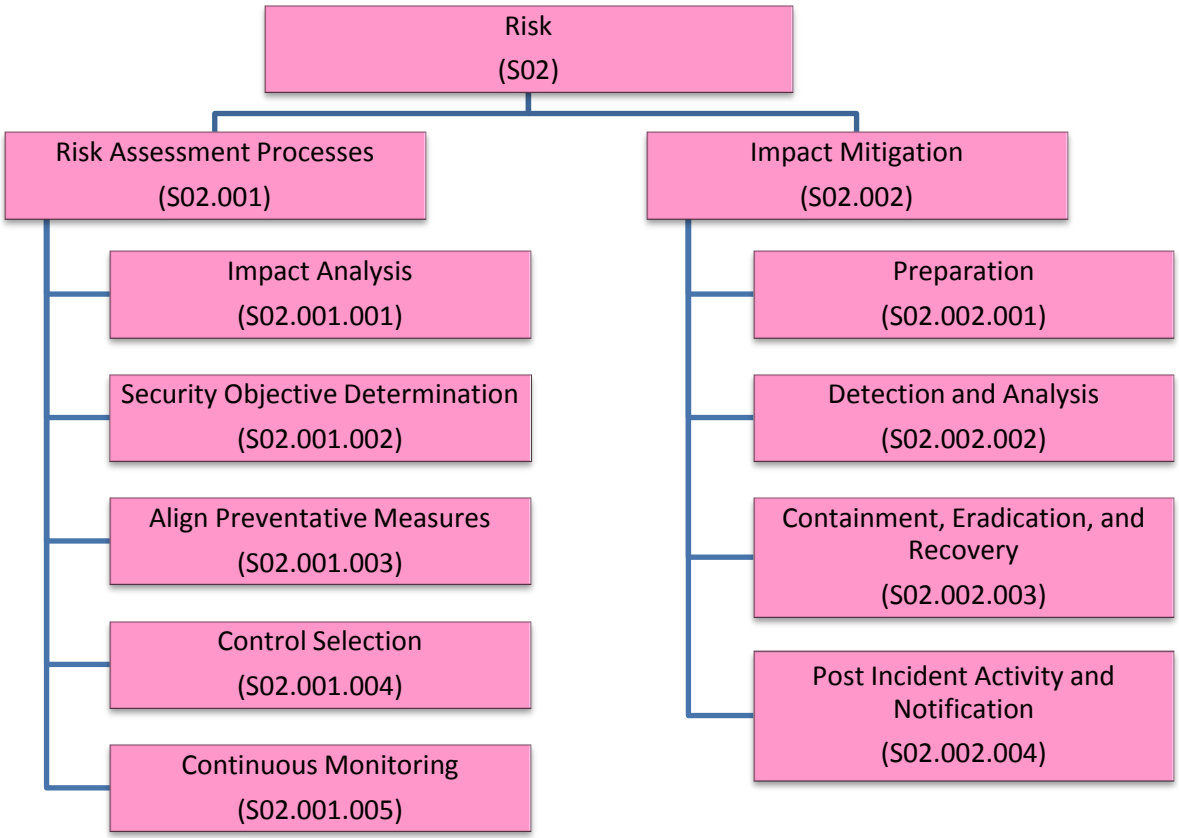
The Federal Security Reference Model (SRM) has three areas: Purpose, Risk, and Controls. These are divided into six subareas, as shown in the figure below. Each subarea must be addressed at the enterprise, agency, and system level. The SRM uses the information from the Purpose and Risk at each level of the enterprise to find and classify the correct Controls to secure the environment.



In the sections below, each SRM area is shown as a tree diagram, followed by definitions of the taxonomy elements in the corresponding tree.

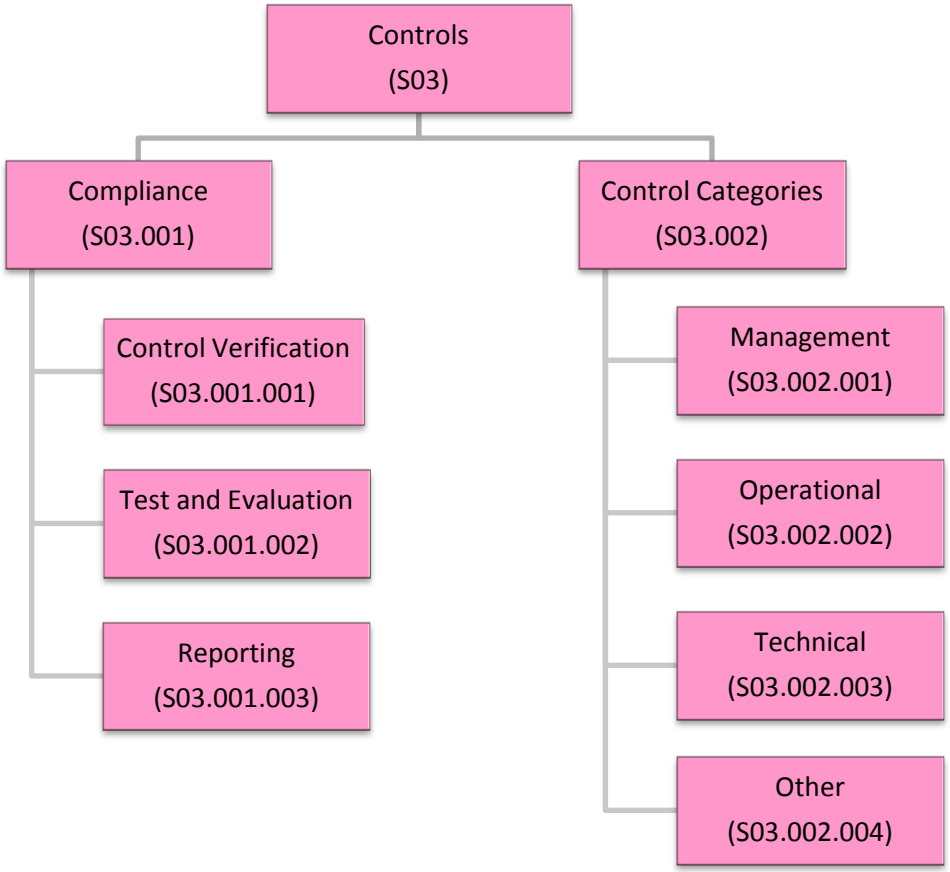

Purpose
(S01)
Regulatory Conditions
(S01.001)
Risk Profile
(S01.002)
Executive Branch Directives
(S01.001.001)
Public Law
(S01.001.002)
Federal Standards
(S01.001.003)
Departmental Guidance
(S01.001.004)
Threat
(S01.002.001)
Vulnerability
(S01.002.002)

PURPOSE (S01)				
The Purpose area describes the risk to business impact and regulatory environment that shapes the reasons and responsibilities for a security program.				
Code	**Area**	**Consideration**	**Context**	**Definition**
S01.001	Purpose	Regulatory Conditions		The regulatory conditions levied on an information system are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
S01.001.001	Purpose	Regulatory Conditions	Executive Branch Directives	Executive Orders, White House Memoranda, security directives regarding classification and protection of federal information or other security goals. See FIPS 200, NIST SP 800-53, NIST SP 800-53A, NIST SP 800-37, and CNSSI-4009.
S01.001.002	Purpose	Regulatory Conditions	Public Law	Public laws applicable to all government agencies regarding IT security.
S01.001.003	Purpose	Regulatory Conditions	Federal Standards	Mandatory and recommended security standards such as Federal Information Processing standards (FIPS) and guidelines required by FISMA legislation. See NIST SP 800-37.
S01.001.004	Purpose	Regulatory Conditions	Departmental Guidance	Any security-related guidance issued at an agency level that adds to or interprets federal standards, policies, laws and regulations. See NIST SP 800-37.
S01.002	Purpose	Risk Profile		Risk is the probability of a vulnerability being exploited, multiplied by the impact resulting from that vulnerability being exploited. Types of risk include: program or acquisition risk (e.g., cost, schedule, performance); compliance and regulatory risk); financial risk; legal risk; operational (e.g., mission or business) risk; political risk; project risk; reputational risk; safety risk; strategic planning risk; and supply chain risk.
S01.002.001	Purpose	Risk Profile	Threat	The potential for a threat source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability. See NIST SP 800-37.
S01.002.002	Purpose	Risk Profile	Vulnerability	A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. See NIST SP 800-37.


Risk
(S02)
Risk Assessment Processes
(S02.001)
Impact Mitigation
(S02.002)
Impact Analysis
(S02.001.001)
Security Objective Determination
(S02.001.002)
Align Preventative Measures
(S02.001.003)
Control Selection
(S02.001.004)
Continuous Monitoring
(S02.001.005)
Preparation
(S02.002.001)
Detection and Analysis
(S02.002.002)
Containment, Eradication, and Recovery
(S02.002.003)
Post Incident Activity and Notification
(S02.002.004)

RISK (S02)				
The Risk Area describes the practice of identifying, mitigating and controlling risk factors within an organization.				
Code	**Area**	**Consideration**	**Context**	**Definition**
S02.001	Risk	Risk Assessment Processes		Risk assessment processes are used to determine the risk to the business of government within the context of a program or IT system, the level of acceptable risk, and corresponding controls that would best reduce the risk to acceptable levels through preventative measures.
S02.001.001	Risk	Risk Assessment Processes	Impact Analysis	The process to identify potential impacts that could jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization. See NIST 800-60.
S02.001.002	Risk	Risk Assessment Processes	Security Objective Determination	This involves all functions pertaining to the protection of federal information and information systems from unauthorized access, use, disclosure, disruptions, modification, or destruction. See FISMA definition [44 U.S.C., Sec. 3542].
S02.001.003	Risk	Risk Assessment Processes	Align Preventative Measures	The protective measures prescribed to meet the security requirements (e.g., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. See NIST SP 800-53, NIST SP 800-37, FIPS 200, and CNSSI-4009.
S02.001.004	Risk	Risk Assessment Processes	Control Selection	The minimum security countermeasures to which protective measures, techniques, and procedures must be applied to information systems and networks based on risk, threat, vulnerability, system interconnectivity considerations, and information assurance needs. See NIST SP 800-53, NIST SP 800-37, FIPS 200, and CNSSI-4009.
S02.001.005	Risk	Risk Assessment Processes	Continuous Monitoring	The monitoring activities required to determine the effectiveness of security controls and the extent to which they comply with related laws, regulations, and policies.
S02.002	Risk	Impact Mitigation		Impact mitigation considers the activities needed to reduce the impact to the organization when vulnerability is exploited.

S02.002.001	Risk	Impact Mitigation	Preparation	The preparatory measures to ensure that an organization can respond effectively to security incidents. See NIST SP 800-61 and NIST SP 800-83.
S02.002.002	Risk	Impact Mitigation	Detection and Analysis	The capability needed to detect, validate, and assess impact and prioritize response to security incidents. See NIST SP 800-61.
S02.002.003	Risk	Impact Mitigation	Containment, Eradication, and Recovery	The activities needed to contain, eradicate and recover from a security incident, including documenting evidence, mitigation of exploits, elimination of vulnerability, and confirmation of normal operating functionality. See NIST SP 800-61.
S02.002.004	Risk	Impact Mitigation	Post Incident Activity and Notification	The process of conducting a robust assessment of lessons learned after incidents, identifying needed changes to security policy, and providing adequate reporting of all incidents. See NIST SP 800-61.


Controls
(S03)
Compliance
(S03.001)
Control Categories
(S03.002)
Control Verification
(S03.001.001)
Test and Evaluation
(S03.001.002)
Reporting
(S03.001.003)
Management
(S03.002.001)
Operational
(S03.002.002)
Technical
(S03.002.003)
Other
(S03.002.004)

CONTROLS (S03)				
Controls are the mechanisms by which vulnerabilities are mitigated, likelihood and impact of a security incident are reduced, and/or threat vectors are eliminated, including evaluation of their effectiveness.				
Code	**Area**	**Consideration**	**Context**	**Definition**
S03.001	Controls	Compliance		Compliance considers the activities needed to validate and report on the effectiveness of implemented controls.
S03.001.001	Controls	Compliance	Control Verification	The activities that support verification of control mechanisms.
S03.001.002	Controls	Compliance	Test and Evaluation	The activities that support the test and evaluation of security capabilities and requirements.
S03.001.003	Controls	Compliance	Reporting	The activities required to comply with security and privacy reporting requirements, performance metrics, associated costs and other information.
S03.002	Controls	Control Categories		Control categories consider the specific activities, technical implementations and processes instituted to reduce or eliminate known vulnerabilities.
S03.002.001	Controls	Control Categories	Management	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security. See FIPS 200.
S03.002.002	Controls	Control Categories	Operational	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people, as opposed to executed by systems. See FIPS 200.
S03.002.003	Controls	Control Categories	Technical	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. See FIPS 200.
S03.002.004	Controls	Control Categories	Other	Mandatory security controls not contained within FISMA, including FISCAM, HIPAA, OMB memoranda, Presidential Directives, and other federal security mandates (e.g. TIC, HSPD-12, and IPv6). See FIPS 200.