

**Commonwealth Office of Technology (COT)  
Standard Process**

**Standard Process Number:** COT-009

**Effective Date:** 06/28/2007

**Revision Date:** 06/01/2011

**Reviewed Date:** 11/10/2014

**Subject:** Change Management

**Standard Process Statement:** COT and the Commonwealth of Kentucky personnel, under agreement with COT for IT Services, shall follow the standard process described below when involved with handling Information Technology (IT) Resources for the Commonwealth.

**Purpose:** This standard process describes the responsibilities and processes to be followed by COT when making changes or recording events to the Commonwealth of Kentucky's IT infrastructure. The IT infrastructure supported by COT is expanding and continuously becoming more complex. As the interdependency between Information Technology resources grows, the need for a strong change management process is essential. The Commonwealth Office of Technology is tasked with maintaining infrastructure stability and reliability for the Commonwealth of Kentucky. The purpose of the Change Management process is to ensure all changes are reviewed and implemented in a rational and predictable manner in order to increase efficiency, minimize the impact of Change related incidents upon service quality, and consequently improve day-to-day operations of the organization.

**Standard Process Maintenance Responsibility:** The Change Management Branch within the Office of Infrastructure Services (OIS) is responsible for maintaining and updating the Change Management Standard Processes.

**Review Cycle:** This Standard Process will be reviewed at least every two years.

**Applicability:** This standard process is to be adhered to by all staff, including employees, contractors, consultants, temporaries, volunteers, vendors and other workers that install, operate or maintain Information Technology resources maintained by COT.

**Unauthorized Change:** Each agency, office, division, branch should make staff members and users under their authority aware of the provisions of this Standard Process. The Standard Process outlined herein should be followed in both spirit and letter by all parties engaged in Change Management. Failure to do so may result in actions to bring about adherence and/or corrective actions subject to progressive disciplinary steps under applicable state personnel law and Kentucky administrative policies and regulations.

**Definition(s):**

**Asset:** any item of IT equipment for which COT has responsibility. This includes, but is not limited to: servers, desktop computers, laptops, switches, routers, hubs, printers and multifunction devices, scanners, data storage systems, data backup equipment, mainframe computer systems, telecommunications equipment, and the associated racks, cables and power conditioning equipment used by these devices<sup>1</sup>.

**Information Technology Resource:** any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-

held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines and printers. Additionally, it is the processes, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

*Note... "Assets" are a subset of "IT Resources", therefore all Assets are IT Resources, but not all IT Resources are considered Assets.*

Change: the addition, modification, or removal of approved, supported, or baseline hardware, network, software, application, environment, system, desktop build, or associated documentation.

Event: any activity outside of the normal operating processes that could have a real or potential impact on the stability and reliability of the infrastructure, i.e. a request to keep a system up during a normal shutdown period.

*Note... "Change" and "Event" will be used interchangeably throughout this document.*

Category/Sub-Category/Subcategory: a classification within the ticketing application that allows records to be searched and grouped by the type of change being performed.

Change Advisory Board (CAB): a group of people who can give expert advice to Change Management on the implementation of changes. This board is likely to be made up of representatives from all areas within IT and representatives from business units.

Change Advisory Board/Emergency Committee (CAB/EC): similar to the CAB defined above, however; this committee is convened as needed to address/approve emergency changes that cannot wait for the next regularly scheduled CAB meeting. The emergency committee often represents a smaller community of experts that can be referenced on an emergency basis for review of changes that meet the emergency criteria of an Emergency Change and are categorized as "Major" change.

Priority: addresses the overall impact and urgency of the Change Request to the business operations of an organization. The priority levels used by the Commonwealth of Kentucky are the same for Incident and Change; however, each has their own definition. The priority levels are (1) Critical, (2) Serious, (3) Important, (4) Needed and (5) Low.

Urgency: addresses how soon the Change Request must be reviewed and deployed to meet customer business needs. The Urgency levels used by COT are (1) High, (2) Medium and (3) Low.

Impact: addresses the impact the change will have on business functions and/or infrastructure. The Impact levels used by COT are (1) High, (2) Medium and (3) Low.

Type: describes the amount of effort and possible impact to the infrastructure needed to complete the change. Change Type will be determined by Change Management staff with the assistance of subject matter experts as needed. The change types used by COT are Standard/Pre-approved, Minor, Significant and Major. Change Type will be used by Change Management to assist in determining the proper levels of approval needed for a Change Request.

Emergency Change: a change that must be implemented immediately and cannot be scheduled. Immediate action is required, and resources are allocated immediately to build the change. The Emergency change must meet Priority 1 and Urgency = High/1 criteria listed above.

Normal Change (One Time Only): a change that follows the full, predefined change management process for review by Change Manager and regularly scheduled Change Advisory Board (CAB) when required.

Configuration Item (CI): the database record that represents the physical item or component in the IT environment. It may be a piece of hardware, software, network device, system, or documentation and may vary in complexity, size and type.

Forward Schedule of Change (FSC): a document containing/listing changes approved for implementation and their proposed dates of implementation. The FSC is to be referenced during CAB meeting reviews for potential conflicts to future changes. The FSC is a document for communicating scheduled changes to the user community at large.

Changes listed on the FSC should meet at least one of the following requirements:

- Change Requests requiring CAB approval,
- Change Requests affecting multi-users/multi-agencies,
- Change Requests typed as “Significant” or “Major”,

Standard Pre-Approved Change (One Time Only Standard): a change that is repeated and repeatable, that follows an established path, is relatively common, and is the accepted solution to a specific requirement or set of requirements. Standard implementation, roll-back, testing, and communication plans are established.

Minor Change: defined as a low risk change with impact limited to one production service and/or system and the ability to adequately test prior to implementation. Minor Changes will also have the ability to be easily backed-out in the event an issue arises. Minor Changes require the approval of the IS Manager of the group building or performing the change.

Significant Change: defined as medium risk, may involve complex changes to one system or common changes to multiple systems presenting greater risk for an associated outage. Due to the complexity and/or scope of significant changes, they are difficult to adequately test prior to implementation. Significant changes require the approval of the Change Manager and the Division Director of the group building or performing the change.

Major Change: defined as high risk, involving complex changes that can impact multiple production services and/or systems or present difficulty in back-out/recovery options. Major changes require the approval of the Change Advisory Board.

### **Roles and Responsibilities:**

Requestor: The individual who is making (not necessarily submitting) the change request of the Support Staff to meet an identified need. A “requestor” can be anyone inside or outside of COT and Support Staff.

Change Advisory Board Meeting: The role of the meeting is to share information, concerns, comments, etc. in a cooperative environment in order to assess impact and advise the Change Manager of potential issues and/or disruptions of service to COT customers.

Change Manager: The Change Management process leader with oversight responsibility and authority for all change requests and change process enforcement. The Change Manager, in combination with the CAB, has approval/rejection rights over submitted change requests.

**Change Coordinator:** The party with oversight responsibility for individual, approved change requests. This individual takes an oversight role to ensure successful coordination and implementation of the submitted change request. The Coordinator works with appropriate functional experts, as needed, to develop any required implementation, roll-back, communication, and test plans along with completing risk and security assessments for the requested change. Additionally, the Coordinator delegates the required tasks based upon the plans and assessments for implementation of the change. The Change Coordinator shall not be assigned “Approval” authority if the coordinator is also the requester. The approval task shall be assigned to the next level manager in those instances.

**Asset Manager vs. Configuration Manager:** Although often regarded as similar, these roles are responsible for two distinct activities within the Commonwealth Office of Technology organization. The asset manager is responsible for recording information about items in the infrastructure and accounting for those items within the Finance organization and eMARS, this information is housed in an Asset Database. The configuration manager’s responsibilities focus on the relationships between the items in the infrastructure and recorded in the Configuration Management Database.

**Approver:** Individual assigned (or delegated as alternate) the obligation to review and allow (approve) a request to proceed to the implementation phase. Approvers are generally within a COT leadership role.

**Task Implementer:** The individual given the duty to perform specific activities for the successful completion of a Change Request. The completion of the collective tasks, in a predetermined order, results in the completion of the change. Each task implementer is responsible for the successful completion of their activities as defined by the task within the Change Request in the order defined and the change window provided.

**Withdrawn Approvals:** Tickets that have tasks that have been completed without approval. The approval will be marked as “withdrawn” and a notation will be placed in the Journal notes stating the reason. A report will be generated monthly and will be presented to executive management.

**Change Management Objectives:** Certify all changes are reviewed and implemented in an efficient and prompt manner in order to minimize the impact of Change related incidents upon service quality, and consequently improve day-to-day operations of the organization<sup>2</sup>.

- Ensure that the Change Management process provides oversight for the effective introduction of approved changes into the environment quickly and with minimal disruption of service.
- Audit the roles and responsibilities of the Change Advisory Board (CAB) to ensure compliance to Change Management Policy.
- Ensure Requests for Change follow a defined assessment process that is inherently business driven.
- Specify that Requests for Change follow an approval process.
- Ensure that all Changes are recorded through the Change Management tool.
- Report the current status, history, and Forward Schedule of Change.
- Provide customer and management metrics (key performance indicators) to report on all Changes.
- To facilitate the most efficient manner of managing changes with an appropriate amount of acceptable risk, minimizing the occurrence of Change related Incidents.

**Emergency Change Objectives:** Emergency changes are to be handled with the highest priority and level of urgency in fulfilling the requirements.

**Standard, Pre-Approved Change Objectives:** Plans, assessments, and approvals have all been evaluated and completed in the past and a level of assurance and comfort is maintained for this type of

change. Standard, Pre-Approved Changes have been implemented through the full change life-cycle in the past, gaining all levels of required approval, and have been proven to be repeated and repeatable with a manageable level of risk. The Category/Sub-category matrix defines requests appropriate for this pre-approved path and does not require manager or Change Manager Approval; nor is it reviewed by the CAB prior to implementation. Request deemed worthy of pre-approval status should be submitted for the first time as Normal Changes and coordinated for pre-approval designation with the Change Manager. Upon agreement of “pre-approval”, appropriate administrative activities will update the ticket management application for future submissions of like requests.

Criteria questions for “Standard, Pre-Approved” designation should include, but are not limited to:

- Has this change been implemented successfully in the past?
- Will this change be submitted frequently?
- Are the tasks always consistent on each implementation – repeated and repeatable?
- Have plans (implementation, testing, back-out, etc.) been defined and proven effective? Plans should be accessible for reference on all future changes.
- Will this change ever be submitted as an “Emergency”? Generally speaking, if this is answered “yes”, it would likely, but not in all cases, indicate that this should not be considered standard, pre-approved.
- Has/will implementation training be completed by support staff, allowing any member of the appropriate support teams to implement this change in a similar manner?

**Scope:** The defined Change Management processes (“Emergency”, “Standard”, or “Normal”) cover any and all changes that may alter normal operations on hardware, software, and applications affecting production environments. Sources of change include, but are not limited to, the following list:

- Maintenance
- User requested changes – modify, add, remove
- Upgrades (hardware and commercial or in-house developed software)
- Unforeseen events – incidents/problems
- Proactive modifications and improvements
- Operations schedule and/or hours of availability

If you are unsure if a change ticket is needed, please contact the COT Change Manager or the Commonwealth Service Desk prior to taking action.

#### **Guidelines:**

Managers are responsible for pro-active planning of their managed IT environments to include any cabinet level pre-approval requirements prior to submitting a change request. Change Requests should be submitted to the Commonwealth Service Desk in a timely fashion, allowing for up to 48 hours (two working days) processing time. This time may vary within that range depending on the complexity, impact and research necessary for ticket preparation. Note that this period exists independent of the time necessary for final approvals and task implementation.

Managers are required to develop internal best practices, processes, and checklists to enhance and support the overall Change Management processes detailed below in addition to completing the appropriate research prior to change submission.

For adjustments to submitted, but not yet implemented changes, notification must be made to the designated Coordinator as soon as possible. The Coordinator and Change Manager will assess the adjustment and make a determination as to whether the submitted change can proceed with the update or a new change must be submitted to initiate reviews again. In the event a new change is required, the original should be identified with the status “resolved” and the closure code “cancelled” and then related to the new request.

COT employs maintenance windows for regularly scheduled system maintenance. Changes requesting implementation during a defined maintenance window must include a valid business case and will be reviewed and coordinated accordingly.

Vendor required changes affecting COT managed IT systems will follow the defined Change Management processes; championed by their designated COT contact.

Emergency changes are the likely result of identified, or potential, incidents. Where possible, an emergency change should be related to the initiating incident. Emergency changes may also be initiated as a result of pro-active maintenance of the environment. Clear identification of the impending issue to be resolved by the emergency change should be captured within the tracking ticket.

The Change Coordinator monitors and manages the lifecycle, implementation, and testing of all Changes. The Change Coordinator is to provide progress updates to COT IT Management, key contacts and customers, and within the ticket management application. Updates for minor tickets shall be provided to branch manager, significant tickets to division director and major tickets to CAB/EC.

Per the defined processes, submitted changes should only be confirmed as “emergency” by the assigned Change Coordinator in step 6 of the Normal Change process during ticket evaluation.

Changes classified as “Emergency” will automatically place the Change Management team as the Change Coordinator. The Change Management team will transfer the coordination of duties to the appropriate staff as Change Coordinator upon the ticket being placed in “accepted” status.

COT Change Management reserves the right to deny any and all changes so long as proper justification can be produced supporting the reason for denial. This includes the right to establish periods of change inactivity for the purpose of protecting critical business processes from change associated reduction or loss of service. These moratoriums of change must first be discussed and approved by the CAB or the CAB/EC.

#### **Process:**

##### ***Submission and Planning Phase (Non-Pre-approved Changes)***

In the submission and planning phase, the information required for the requested change is logged in the ticket management/tracking system through the Commonwealth Service Desk.

1. The following Change ticket elements/data are captured from the requestor, along with the name of the configuration item (CI) to be changed.
  - a. Urgency
  - b. Priority
  - c. Category
  - d. Sub-Category
  - e. Name (of requestor)
  - f. Associated Incident number(s) and Problem number(s), if exist(s)
  - g. Application name, if Change is for software
  - h. Name of COT final approver, if applicable
  - i. Estimated Start/End dates and time
  - j. Summary (Not to include sensitive or confidential data. Additional information on proper treatment of such data may be found in COT enterprise policies and standards and the COT Security Manual. For general staff members and vendor responsibilities to protect such data, see References section of this document.) Examples of sensitive data include IP addresses, server names, Social Security numbers, passwords, etc. When in doubt, please contact the COT Security Office through the Change Manager.

- k. Description details of expected required activities
  - l. Any other system identified required field elements
  - m. Risk Assessment
  - n. Backout Plan
2. The Request for Change (RFC) is assigned to the Change Management team and initial review occurs for accuracy and completeness of data.
  3. Upon automated Front Range notification, Change Management performs the following initial steps:
    - a. Change Management team determines if change is an “Emergency”, “Standard”, or “Normal” change and directs the request along the appropriate path.
    - b. Links the proper hardware and/or software Configuration Item(s) to the Change Ticket
    - c. Add a Change Management approval to the ticket as a placeholder until the final COT approver(s) name is added later
    - d. Set up a ticket coordination task, normally in the name of the COT staff member requesting the creation of the ticket
    - e. Implementation, testing, back-out, and communication plans are verified as they pertain to the change request.
    - f. Proposed start and end dates for implementation activities according to change details are verified.
    - g. At this point, the status of the ticket will be changed from ‘Evaluated’ to ‘Accepted’, and the ticket is ready for the Change Coordinator to further work the ticket preliminaries. Creation of the task(s) may be the responsibility of the sub-delegated Change Coordinator.
  4. The Change Coordinator creates the appropriate tasks for implementation of the change request.

### **Assessment Phase**

During assessment, the request is reviewed by the Change Management team and it is confirmed that all relevant information is provided so approvers have a clear understanding of what they are approving in the next phase. It must be noted that if any of the required information is not supplied, the change request will be rejected.

5. The assigned coordinator performs risk, impact, criticality, and security assessments.
6. As more information is required, the needed resources are contacted.
7. Upon completion of all details, the request for change moves to the approval phase of the lifecycle.

### **Approval Phase**

This phase secures authorization from the appropriate organizational approvers and the CAB as needed.

8. Based upon the request’s defined change type, the approval tasks are added to the change for review by the appropriate approvers.
9. The approvers can determine if CAB approval is required. If so, the request is available for review by CAB members and is presented at the weekly CAB meeting for discussion.
10. Upon approval, the change moves to the scheduling and notification phase. Rejection of the request results in documentation, notification to the requestor, and cancellation of the ticket.

### **Scheduling and Notification Phase**

Within this phase of the request lifecycle, the approved change request is scheduled and implemented and notification of the expected implementation date is communicated.

11. The appropriate date and time for implementation has been finalized and is communicated to the organization via the Forward Schedule of Change (FSC).
12. The requestor is notified of the request's approval and anticipated implementation.
13. The Change Coordinator hands off the RFC for implementation.

### **Closure Phase**

The change process lifecycle concludes with confirmation from the team implementing the change that the request has been successfully implemented.

14. The Change Coordinator receives notification of successful/unsuccessful implementation, provides update(s) within the ticket, and communicates the resolution to the requestor.
15. The ticket is closed with the appropriate closure classification.
16. Post implementation review is conducted during the next scheduled CAB meeting to review successes, best practices, lessons learned, etc. from this Change. Additionally changes posted on FSC for previous week will be made available for discussion.

### **References:**

(Note: some documents have restricted access; please contact the Change Manager for assistance if needed.)

- COT-F011 – COT Acknowledgement of Confidentiality Agreement  
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-1920/>
- COT-F015 – COT Acknowledgement of Responsibility  
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-617/>
- OAD-DPM-BP-001\_Production Implementation Best Practices  
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-110209/>
- COT-F053 Production Cutover form for zSeries Systems  
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-392602/>
- COT-F052 Production Cutover form for Distributed Systems  
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-392601/>

**\*\*End\*\***

---

<sup>1</sup> Definition provided is based upon accepted and approved definition presented in Asset Management Standard Procedures documentation.

<sup>2</sup> Best Practices for Service Support – ITIL The Key to Managing IT Services; The Stationary Office on behalf of OGC; 2000; page 165