IT Change Management Process Training

Before you begin:
This course was prepared for all IT professionals with the goal of promoting awareness of the process. Those taking this course will have varied knowledge of handling IT Changes. As such, this course aims to deliver information that is easily understood and relevant to everyone. We invite your specific questions or comments and encourage you to follow up directly with your manager.

Course Objectives

This course explains the following:

- Value of Change Management to the Enterprise
- Key Definitions for Change Management
- Roles and Responsibilities
- The Five Phases of the Change Management Process

Additional Information & Resources

Throughout this course you will have access to the **Change Management Process** document. This document provides the detailed definitions, roles and responsibilities, and process activities that are performed during the Change Management Process.

You can access this information any time during the course by clicking the icon at the top right-hand of the course. Go ahead and try it now!

Click here to Bookmark the **Change Management Process** in your browser.

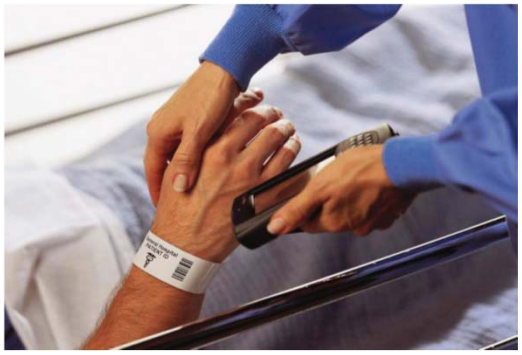
A Real Life Story and the Value of Change Management to the Enterprise

A request was made to deploy new print servers to support the EPIC 2012 upgrade. The change was implemented and shortly afterwards, the Service Desk started receiving calls that the Pharmacy was unable to print medication bar code labels. As a result, medication had to be administered without the bar code labels for 11 hours and placed patient safety at risk!

A post implementation review was conducted and it was determined that no request for change (RFC) was submitted into the Change Management System. This meant the change was implemented without following the Change Management Process. There were no documented plans, such as change plan, validation plan, and back-out plan. Furthermore, the Change did not get proper review and approval, and the Service Desk was not made aware of the change.

The Change Management Process provides value to the Enterprise by enabling Changes to be made with minimum disruption to IT Services by ensuring change procedures are completed , reviewed and approved prior to implementation.

"Failure to Plan" equals "Plan for Failure"



Key Definitions

A **Change** is any modification to the systems, infrastructure, or applications that comprise the UCSF IT production environment.

RFC is an acronym for *Request for change* – A request to implement a Change within the UCSF IT production environment

CMS is an acronym for *Change Management System* – Software tool utilized for the request, approval, tracking and details of changes. We use ServiceNow.

CI is an acronym for Configuration Item – A component that needs to be managed under the Change Process in order to deliver an IT Service.

CAB is an acronym for *Change Advisory Board* – Meets regularly to help the change manager assess, prioritize and schedule changes.

PIR is an acronym for *Post Implementation Review* - A review that is conducted when an RFC implementation has not been successful.

Change Management is an IT Service Management Process that aims to control the lifecycle of all changes. The primary objective of the Change Management Process is to enable Changes to be made with minimum disruption to IT Services.

Change Management Policy

To ensure the integrity, consistency and availability of UCSF IT Services, all changes to the UCSF IT production environment will be tracked via a Request for Change (RFC). RFCs will be entered into and managed via ServiceNow to ensure Changes are centrally tracked, approved, reported upon, and enforced in a reliable and consistent manner. RFCs must be reviewed and approved by the Change Advisory Board (CAB) prior to execution to ensure a proposed Change does not compromise the stability of the production environment.

Zero tolerance for unauthorized changes!

Roles & Responsibilities

Within the Change Management process, specific roles and functions have been defined. Each role is responsible for completing specific tasks within the process, ***however, all roles contribute to the success of the process.***

The Roles include:

- Change Assignee
- Peer Reviewer
- Group Manager Approver
- IT Director Approver
- Change Manager
- Change Advisory Board (CAB)

Change Assignee

The **Change Assignee** is the individual making the changes in the environment.

Responsibilities of the Change Assignee include :

- Ensuring that a detailed and accurate change request has been submitted.
- Obtain technical Peer Review and other required approvals prior to the implementation time.
- Represent the change to the CAB
- Implement the change as planned, including validation, and closure of the change before the scheduled end date/time.
- Participate in Post Implementation Reviews (PIR).

Peer Reviewer

The **Peer Reviewer** is the technical peer with similar knowledge of the environment where the Change will take place.

Responsibilities of the Peer Reviewer include :

- Review the RFC and ensure that the specific technical steps planned appear to be correct.
- Update the RFC, indicating that they have reviewed the technical steps of the Change.
- Represent the RFC during CAB, if the Assignee is unavailable.
- Back up the assignee during the actual implementation.

Group Manager Approver

The **Group Manager Approver** is the manager who provides the first level of approval to a RFC, allowing it to go before the CAB for review. In most cases, this is the manager of the Change Assignee. If that is not possible, the Change Approver can be any IT manager or above.

Responsibilities of the Group Manager Approver include:

- Review all RFC submitted by staff members of their group
- Ensure all necessary communication, coordination, documentation and testing has been completed properly on all RFC prior to approval
- Approve all RFC prior to them being submitted for review by the Change Advisory Board
- Represent the change during CAB if the Assignee and Peer Reviewer are unavailable.
- Participate in Post Implementation Reviews (PIR).

IT Director Approver

The **IT Director Approver** is the director who provides the second level of approval to a RFC that are high risk or requires to be expedited, allowing it to go before the CAB for review. In most cases, this is the director of the Change Assignee. If that is not possible, the IT Director Approver can be any IT director or above.

Responsibilities of the IT Director Approver include:

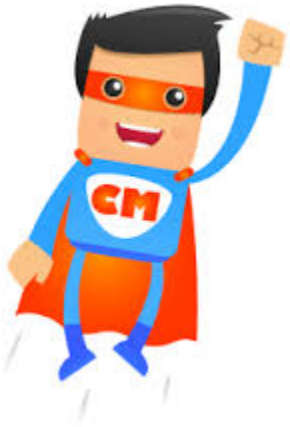
- Review all *high risk or expedited* RFCs submitted by staff members of their group
- Ensure all necessary communication, coordination, documentation and testing has been completed properly on all *high risk* or *expedited* RFCs prior to approval
- Represent the change during CAB if the Assignee, Peer Reviewer, and Group Manager are unavailable.
- Approve all *high risk or expedited* RFCs prior to them being submitted for review by the Change Advisory Board

Change Manager

The **Change Manager** is responsible for the overall facilitation of the Change Management process.

Responsibilities of the Change Manager include:

- Coordinate and chair the regularly scheduled meetings of the Change Advisory Board.
- Facilitate the resolution of any schedule conflicts that may arise.
- Maintain the policies and procedures necessary to carry necessary CM functions.



Change Advisory Board (CAB)

The **Change Advisory Board (CAB)** is a group of individuals that represent various IT units and Client communities. This group is responsible for final review and approval/rejection of all comprehensive RFCs. The CAB meets at a regularly scheduled interval to review all pending RFCs.

All Changes are reviewed by the CAB during its scheduled meeting. The CAB has the authority to do any of the following:

- Cancel or reject changes
- Approve RFC as presented
- Reassess the risk level of a Change
- Reassess the impact level of a Change
- Request additional information prior to approval

Change Types

One of the key descriptors of a Change is its *type*. The Change type dictates which of the process steps must be completed. There are five Change types: **routine**, **emergency**, **comprehensive**, **expedited comprehensive, and latent** . The process steps that are executed during a Change are adjusted based on type.

The Change types are defined as follows:

- A **Routine** change is a pre-approved change that is low in risk, relatively common, and follows a pre-defined procedure or work instruction. Routine changes require initial review and approval by the CAB, but once approved, no longer require individual CAB approval.
- An **Emergency** change is one that must be done immediately. It is of such a high priority that it is auto-approved and scheduling is not required. The Emergency Change must be related to an active high or critical priority incident.
- A **Comprehensive** change requires that all Change process steps be completed and reviewed for approval by the Change Advisory Board (CAB) prior to implementation.
- An **Expedited Comprehensive** change also requires that all Change process steps be completed, however, the change must be implemented in a time frame that does not allow them to go through the normal CAB approval cycle. Review and approval is done electronically.
- A **Latent** change that is logged after implementation and did not follow the Change Management process. A PIR is required for latent changes and must be reviewed at CAB. ***A Latent change is also known as an unauthorized change!***

Five Phases of Change Management Process

Phase 1
Create Change

Phase 2
Conduct Reviews & Approvals

Phase 3
Schedule Change

Phase 4
Implement Change

Phase 5
Post Implementation Review and Close Change

Phase 1: Create Routine Change

1. Select an approved routine template to create a routine RFC.
   - Routine templates require an initial CAB approval in order for the RFC to become Routine
2. Select the responsible assignee to manage the Change
   - The Change Assignee can schedule the change and go straight to the implementation phase, however, they need to ensure there are no conflicts with other RFCs scheduled before implementing their routine Change

Phase 1: Create Emergency Change

1. Create an RFC in ServiceNow and select responsible assignment group and assignee to manage the Change
2. Relate the Change to an active High or Critical Incident.
3. Define the Change, Validation and Back-out plans:
   - The Change Plan should include enough detail to explain what will be done.
   - Validation plans should include steps to verify that the change fulfilled the technical and business objectives. It should also include steps to verify that existing functionality was not unintentionally affected.
   - Back-out plans should include the trigger that will be used by the assignee to transition from the implementation to the back-out procedure.
4. Document the impact to the business and assess the risk level.
5. Identify Configuration items (CIs) that will be added, removed, or modified by the change.
6. Define the change window, including implementation time, validation time and potential back-out time.

Phase 1: Create Comprehensive Change

1. Create an RFC in ServiceNow and select responsible assignment group and assignee to manage the Change
2. Define the Change, Validation and Back-out plans:
   - The Change Plan should include enough detail to explain what will be done.
   - Validation plans should include steps to verify that the change fulfilled the technical and business objectives. It should also include steps to verify that existing functionality was not unintentionally affected.
   - Back-out plans should include the trigger that will be used by the assignee to transition from the implementation to the back-out procedure.
3. Document the impact to the business and assess the risk level.
4. Identify Configuration items (CIs) that will be added, removed, or modified by the change.
5. Identify the Peer Reviewer, Manager Group Approver and if required IT Director Approver.
6. Define the change window, including implementation time, validation time and potential back-out time. ServiceNow will automatically determine if the Change Type is Comprehensive or Expedited Comprehensive.

Phase 2: Conduct Reviews & Obtain Approval

1. Once an RFC has been completed and is ready to be submitted for approval, the Change Assignee must request a review of the RFC from a technical peer with similar knowledge of the Change.
   - Peer Reviews are not required for Change Types: Routine or Emergency
2. The technical peer reviews the RFC to ensure the technical steps planned appear to be correct. Once this is verified, the peer reviewer will update the RFC, indicating that they have reviewed the technical steps of the Change
   - Keep in mind that the peer reviewer shares responsibility for the change!

Phase 2: Conduct Reviews & Obtain Approval

3. Once the RFC has been fully completed, submit the RFC for approval. The Change type dictates which approval steps must be completed.

Change Type:	Change Review and Approval:
Routine	• Pre-approved
Emergency	• Auto-approved
Comprehensive	• Peer Reviewer • Group Manager Approval • IT Director Approval (high risk only) • CAB
Expedited Comprehensive	• Peer Reviewer • Group Manger Approval • IT Director Approval* • Expedited CAB (Campus only)

* For Campus, IT Director Approval is only required for high risk Changes.
* For Med Center, in addition to high risk changes, all expedited comprehensive Changes also require IT Director Approval.

Phase 2: Conduct Reviews & Obtain Approval

4. The Group Manager reviews the RFC for Approve or Reject the request. Approval will advance the RFC to the next level of approval.
   - The Group Manager reviews the RFC for accuracy and to ensure the appropriate actions have taken place, including but not limited to peer review of the proposed solution, plan for notification of the user community if required, and coordination of change with appropriate teams.
5. For high risk Changes, the IT Director reviews the RFC and Approve or Reject the request. Approval will advance the RFC to the next level of approval.
   - IT Director approval is required for all Medical Center Expedited Comprehensive Changes and will advance to scheduled once approved.
6. The Change Advisory Board (CAB) will meet regularly for the purpose of reviewing all pending RFC. The CAB will either approve or reject the RFC during the course of the meeting. This is the final level of approval.
   - All Change Assignee who have a RFC pending must attend the CAB meeting or send a representative from their department who can properly represent and discuss the Change. Failure to do so may result in the automatic Rejection of the RFC.

Phase 3: Schedule Change

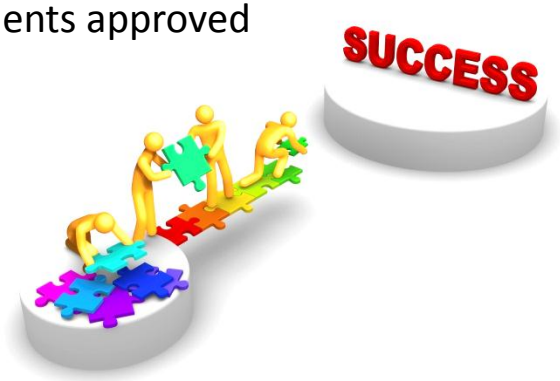
1. Once the final approval is received, the Change Manager will change the status to scheduled.
2. If an update to the CI is required, a task will be created and must be completed before the change can be closed.
3. The Change Assignee notifies the Service Desk and provide sufficient details to enable them to respond to calls from users who may be impacted by the change.
4. The Change Assignee or IT Service Desk sends required notifications to the user community.

Phase 4: Implement Change

1. Before initiating the actual change activity, the Change assignee should change the status from Scheduled to WIP. The change cannot go to WIP before the scheduled start date/time.
2. After changing the status to WIP, the assignee should enter the actual start date/time.
3. The Change Assignee executes the Change
   - Change Assignee should document activities in the Work Log. Examples of the kind of information that would be appropriate are:
     - Reaching key milestones in the implementation
     - Unexpected issues with the implementation
     - The start/stop of validation as well as any unexpected results
     - The reasons for backing out a change or closing the record as incomplete
4. The CI Support Group updates the CI if required and closes their task.

Phase 5: Conduct Post Implementation Review & Close Change

1. Once the Change is completed, the Change Assignee notifies the Service Desk and advise them of the success or failure as well as the current state of the impacted environment.
2. The Change Assignee should complete the RFC within 24 hours of the Change execution by selecting a Results Code for the Change. The result codes are:
   - **Successful**: Implemented within the approved change window and all of the approved components for the change were implemented (no more, no less)
   - **Backed out**: Started, but caused issues that required a reversal of the implementation
   - **Completed with issues**: Implemented with issues that did not require a back out. *Changes that are also completed outside the approved change window is considered completed with issues*
   - **Incomplete**: Partially implemented; not all of the components approved for the Change were implemented



Phase 5: Conduct Post Implementation Review & Close Change

3. Any result code that is not *Successful* is considered an exception and will require the Group Manager Approver to conduct a Post Implementation Review (PIR) of the exception. The PIR should document:
   - A description summarizing why the change was not successful
   - A description of the business impact
   - A description of effort that will be put in place to prevent a similar exception

Test Question 1

Which one of the following statement is incorrect?

A. Assessing risks is key to effective change management

B. Some unauthorized change should be permitted to maintain flexibility

C. The Peer Reviewer is the technical peer with similar knowledge of the environment where the Change will take place

D. A successful change does not require a PIR

Test Question 2

The primary objective to the Change Management Process is to enable changes to be made with minimum disruption to IT Services.

True or False

Test Question 3

Who is responsible for the success of a High Risk Change?

A. Group Manager only
B. IT Director only
C. Assignee and Peer Reviewer
D. Assignee, Peer Reviewer, Group Manager, IT Director, Change Manager, CAB

Test Question 4

A change that was implemented without issues but ran beyond the approved planned end date and time is considered successful.

True or False

Test Question 5

What is the correct sequence of the Change Phases?

A. Create Change, Conduct Post Implementation Review and Close Change, Conduct Reviews & Obtain Approvals, Schedule Change, Implement Change

B. Create Change, Conduct Reviews & Obtain Approvals, Schedule Change, Implement Change, Conduct Post Implementation Review and Close Change

C. Create Change, Schedule Change, Conduct Reviews & Obtain Approvals, Implement Change, Conduct Post Implementation Review and Close Change

Test Question 6

What does the acronym CI stand for in relation to Change Management?

A. Caller ID

B. Clinical Investigation

C. Configuration Item

D. Change Item

Test Question 7

Which change type is considered an unauthorized Change?

A. Comprehensive
B. Emergency
C. Latent
D. Expedited Comprehensive
E. Routine

Test Question 8

The IT Director, Group Manager or the Peer Reviewer could represent the RFC at CAB if the Assignee is unavailable? True or False

Test Question 9

Peer Review is required all Comprehensive and Expedited Change regardless of risk level.

True or False

Test Question 10

What is required in every RFC?

A. Change Plan
B. Validation Plan
C. Back-out Plan
D. A and B only
E. A,B and C