



DELIVERING IT...

JITSD Operations Framework

Change Management Function

Version 1.0

Published: October 2013

The Microsoft Operations Framework 4.0 is provided with permission from Microsoft Corporation.

Continuous Process Improvement

Contents

DOJ ITSD (JITSD) use of Microsoft Operations Framework (MOF)	1
Position of the Change Management Function Within the JOF	1
Why Use the Change IMF?	2
Change IMF Overview	2
Goals of Change Management	3
Roles and Responsibilities	4
Key Terms	5
Change Types	6
Change Management Process Flow	8
Step 1: Baseline the Configuration	9
Step 2: Initiate the Change	10
Step 3: Classify the Change.....	12
Step 4: Plan and Design the Change.....	15
Step 5: Build, Test and Review the Change	17
Step 6: Approve and Schedule the Change	18
Step 7: Release the Change.....	22
Step 8: Review the Change	24
Conclusion.....	25
Implementation Checklist Example	26

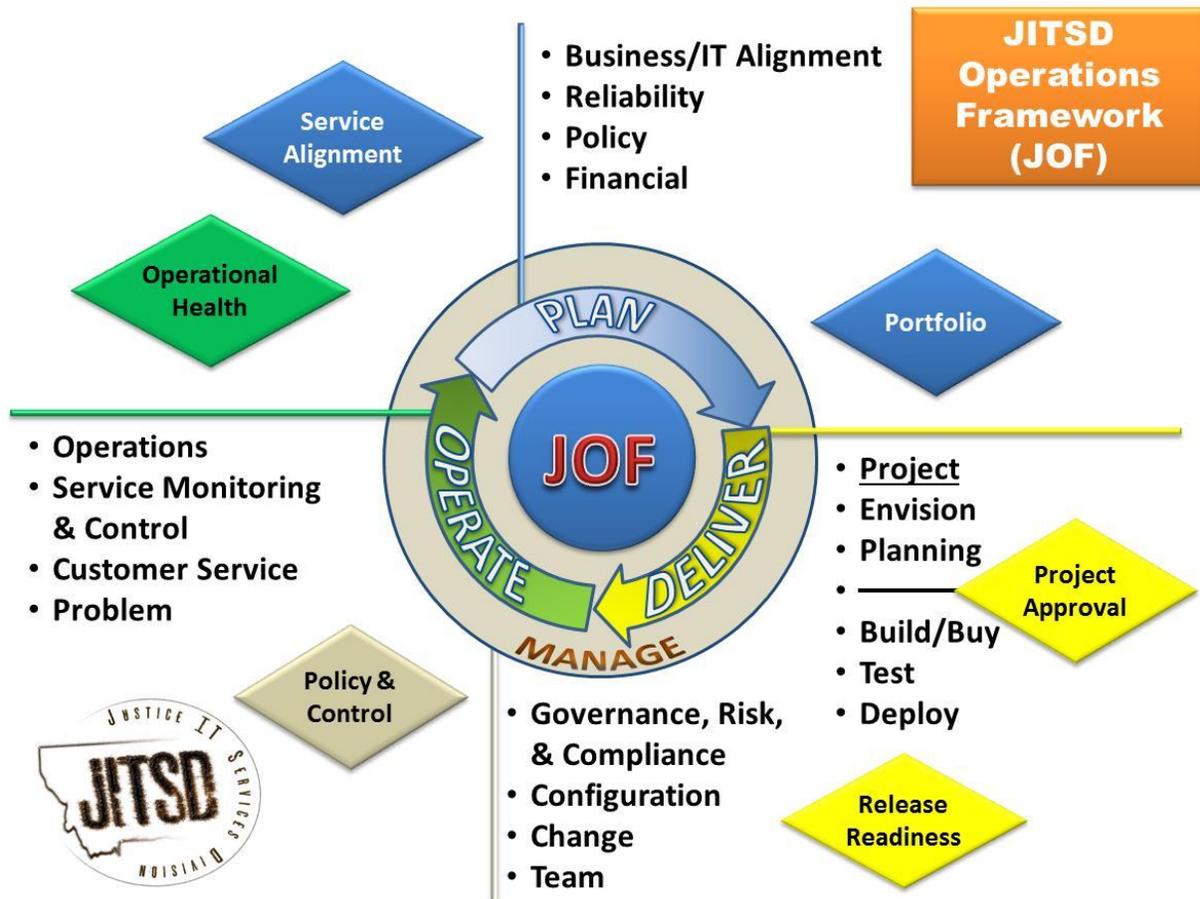
DOJ ITSD (JITSD) use of Microsoft Operations Framework (MOF)

DOJ ITSD (JITSD) uses Microsoft Operation Framework (MOF) as a starting and reference point for developing the DOJ Information Technology (IT) management, governance, and process improvement framework called the JITSD Operations Framework, or JOF for short. JOF will be used to document various IT Management Functions (IMFs) such as Customer Service, Change Management, etc that will serve as guidelines for how IT is managed in JITSD.

Position of the Change Management Function Within the JOF

The IT lifecycle encompasses all of the activities and processes involved in managing IT: conception, development, operation, maintenance, and ultimately retirement. JOF organizes these activities and processes into IT Management Functions (IMFs) such as Customer Service, Change Management, etc, which are grouped together in lifecycle phases (plan, deliver, operate, and manage). Each IMF is anchored within a lifecycle phase and contains a unique set of goals and outcomes supporting the objectives of that phase. The IMFs can be used as stand-alone sets of processes, but it is when IMFs are used together that they are most effective in ensuring service delivery at the desired quality and risk level.

The Change IMF belongs to the Manage Layer, the foundation of the JOF IT service lifecycle. The following figure shows the place of the Change IMF within the Manage Layer, as well as the location of the Manage Layer within the IT lifecycle.



Why Use the Change IMF?

- Reduce risk of negative impact to the organization from changes.
- Manage changes.

Change IMF Overview

In the IT industry, over 80% of outages are caused by unauthorized or uncoordinated changes. To reduce overall user downtime and the number of DOJ system outages, JITSD will **implement, monitor, measure, and continuously improve** a change management process. Change management is critical to delivering reliable and effective IT systems. JITSD must ensure that **change is planned and purposeful. Change in any form carries risk**—risk of failure, cultural resistance, disruption of operations, technical challenges, resource constraints, and unanticipated consequences.

The Change Management IMF offers **guidance** to help manage change through repeatable, predictable, and measured processes while addressing risk. An organization's tolerance for risk determines the appropriate level of detail and formality to apply to change processes for each type, size, and timing of change.

Benefits of restricting changes include more efficient work, more stable environment, and minimized impact to related services, all of which have financial and timing implications.

Change management is applied at the appropriate level throughout the IT lifecycle and establishes boundaries and flexibility.

Standard changes provide agility within the boundaries of change management in the Operate Phase. Every organization should develop a collection of standard changes, ensuring predictability and the efficient use of resources by using a “tried, tested, and true” standard process for common change requests. This is accomplished by identifying common recurring changes and optimizing their execution. Ideally, 80 percent or more of all Operate Phase changes should be standard, this signals a mature change management process.

A standard change begins as a minor, significant, or major change. After the change has been thoroughly tested, deployed, and validated and the execution steps have been documented, a change may become standard. Examples of standard changes include desktop refresh, standard software deployment, password reset, and patch management.

As changes are approved and implemented, it is critical to record an accurate picture of the production environment configuration before and after each change is made. With configuration information readily available, IT is better equipped to:

- Evaluate proposed changes.
- Understand the current state of the production environment.
- Troubleshoot problems by analyzing recent changes made to the production environment.
- Return the configuration to a previously known state to address chronic problems or to meet regulatory requirements.
- Test changes outside of the production environment with the confidence that the production environment will be similar to the test environment.

Goals of Change Management

The primary goal of Change Management is to create an environment where changes can be made with the **least amount** of **risk** and **impact** to the organization.

Outcomes	Measures
Have a repeatable, predictable, measurable process for managing changes to the production environment to improve system reliability and customer satisfaction.	<ul style="list-style-type: none"> • Improved reliability of systems. • Improved customer satisfaction.
Eliminate unnecessary change.	<ul style="list-style-type: none"> • Reduction in cancelled projects. • Reduction in reversed changes.
Reduce unintended side effects.	<ul style="list-style-type: none"> • Reduction in production failures.
Enable IT to revert to a previous environment state in response to service disruptions by keeping accurate knowledge of the changes made.	<ul style="list-style-type: none"> • Number of managed service maps compared to the number of services offered. • Number of items in the Configuration Management System (CMS) with historical state records. • Date range of historical data maintained within the CMS (for example, previous states for the past 6 months).
Enable troubleshooting problems through an analysis of recent changes.	<ul style="list-style-type: none"> • Changes to production are known. • Decrease time to resolve problems.

Roles and Responsibilities

Role / Responsible Person(s)	Responsibilities
Change Process Manager: Application Services Bureau Chief (ASBC)	<ul style="list-style-type: none"> Manages the change management process for JITSD. Manages the change management system for JITSD.
Requester: IT Staff, Customer, User, or Vendor	<ul style="list-style-type: none"> Provides input to appropriate JITSD staff for a requested change.
Change Manager (CM): Any JITSD staff	<ul style="list-style-type: none"> Leads for all aspects of a change from beginning to end. The Change Manager may not do everything, but is accountable to ensure all things are completed. The CM could be any staff member. Fills out/modify Change Request (CR) and other required documentation through entire process. Implements the change or assigns to an implementer
Implementer: Any JITSD staff	<ul style="list-style-type: none"> Implements the change. Usually the change manager, but it could be any JITSD staff.
Technical Systems Lead (TSL): Different for each system. Consult Systems list to obtain appropriate person.	<ul style="list-style-type: none"> Tracks specific system configuration items (CIs) and updates the configuration management system (CMS) used to manage that system's configuration. The CMS could be a spreadsheet, but JITSD will work to use one system as much as possible and integrate separate CMSs that cannot be consolidated. Tracks what is changing and assist with the change impact. Ensures a known state at all times for their system.
Change Advisory Board (CAB): System Owner, CIO, Application Services Bureau Chief (ASBC), Systems Support Bureau Chief (SSBC), Information Security Officer (ISO)	<ul style="list-style-type: none"> Reviews, request more information, and (dis)approves CRs. Ensures changes are made with the least amount of risk and impact to the organization.
Extended CAB: Representative from each JITSD section as determined by the bureau chief.	<ul style="list-style-type: none"> Provide feedback and recommendations on changes.
Business Lead	<ul style="list-style-type: none"> The field is automatically populated with the name of Business Lead when the system is selected. The Change Request workflow uses the business lead information for automated notifications to the owner of the system and the name originates from the CMS Systems List data. It is the responsibility of the Change Manager to document the Change Request approval from the Business Lead if approval is given outside of the Change Management tool. For example, if Lisa Wanke sends an email approving the implementation of 14.3 then the Change Manager will need to add the email as an attachment to the Change Request.

Key Terms

Term	Definition
Change	The addition, modification, or removal of approved, supported, or baselined hardware, software, equipment, or associated documentation.
Change advisory board (CAB)	A cross-functional group set up to evaluate change requests for business need, priority, cost/benefit, and potential impacts to other systems or processes.
Change type	The category of a change determined by complexity, resources required (people, money, and time), risk, and urgency. Change types include Standard, Minor, Major and Emergency.
Change management system (ChMS)	A system use to track Change Requests (CRs) progress from submission, through review, approval, implementation, and closure.
Change Request (CR)	The formal change request, including a description of the change, components affected, business need, cost estimates, risk assessment, resource requirements, and approval status.
Configuration item (CI)	An IT component that is under configuration management control. Each CI can be composed of other CIs. CIs may vary widely in complexity, size, and type. Their scope can range from an entire system (including all hardware, software, and documentation) to a single software module or a minor hardware component.
Configuration management system (CMS)	A set of tools that is used to manage IT item and system configurations such as location, hardware/software versions, relationships, dependencies on other items and systems, changes, releases, known errors, and incidents related to items and systems.
Definitive software library (DSL)	A secure software library where all versions of software CIs that the CAB has approved for deployment are held in their definitive, quality-controlled form.
Schedule of Change (SoC)	A record of upcoming and recent approved changes to help staff understand the impact that already approved changes might have on any new proposed changes and to assist with current outages or incidents.
Post-implementation review (PIR)	A review that occurs after release of a new or updated system or major change. This review evaluates and measures the success of the release in the production environment and provides lessons learned.
Release (aka implementation)	A collection of one or more changes that includes new and/or changed configuration items that are tested and then introduced into the production environment.
Risk	The risk level (low, medium, or high) of a change is based on the PROBABILITY that a change could cause system failure, and if it does, what is the IMPACT to the business.
System diagram	A representation of a system from the perspective of the business and user that shows critical dependencies, settings, and areas of responsibility.

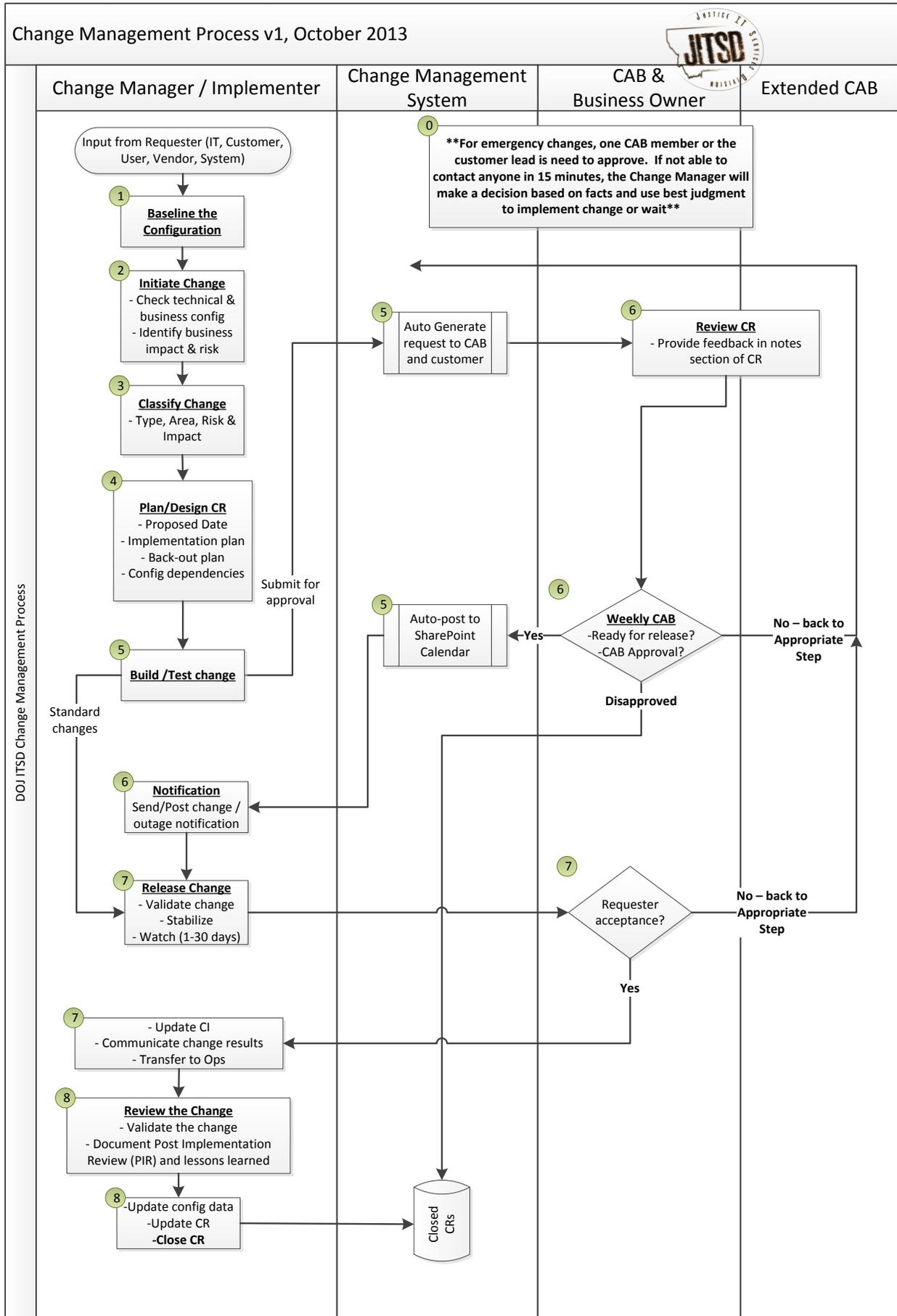
Change Types

Change	Definition
Standard	<p>Change that is pre-approved and does NOT require CAB approval and can proceed directly to release. Standard changes are nearly identical every time and have occurred and will occur many more times in the future and are low risk.</p> <ul style="list-style-type: none"> • Approval = Change manager • Change mgt system automated notification = none • Customer notifications = Only if there will be an outage • Post Implementation Review (PIR) = None • Examples <ul style="list-style-type: none"> • Group 1 software updates. • MERLIN minor releases. • III Sync
Minor	<p>Change that is not standard, but is low risk because the scope (number of systems/users and complexity) of the change is small.</p> <ul style="list-style-type: none"> • Approval = CAB • Change mgt system automated notification = none • Customer notifications = Yes • Post Implementation Review (PIR) = Only if other than “Successfully Implemented” • Examples <ul style="list-style-type: none"> • HVAC maintenance. • Adding new content farms. • Stylesheet changes • Incremental programming changes • Adding an OU to AD • Deprecating an AD DC • Crystal report updates
Major	<p>Change that is complex, wide ranging and/or the risk to the mission or business (operations or money loss) is high, if the change fails.</p> <ul style="list-style-type: none"> • Approval = CAB • Change mgt system automated notification = yes • Customer notifications = Yes • Post Implementation Review (PIR) = Only if other than “Successfully Implemented” • Examples <ul style="list-style-type: none"> • MERLIN major release. • SmartCop major release. • Replacement of SAN. • Key network node change. • Key (public safety) database or server change.
Emergency	<p>Change that is required immediately due to an outage, imminent outage or security vulnerability.</p> <ul style="list-style-type: none"> • Approval = one CAB member or the system owner within 15 minutes. If neither is available or does not call back, then the change manager can authorize the change. • Change mgt system automated notification = Yes • Customer notifications = if possible • Post Implementation Review (PIR) = Yes • Examples <ul style="list-style-type: none"> • Server outage and configuration change is needed to restore system. • Imminent security threat. • Data updates to public safety systems. • RESTORATION of existing operational items (hardware, software, etc) to their original state, IS NOT A CHANGE and does not require use of this process.

Change	Definition
Unauthorized	A change that has bypassed the change process and has come to light because of system failure or discovery after the change occurred.

Change Management Process Flow

Change Management Process v1, October 2013



DOJ ITSD Change Management Process

Step 1: Baseline the Configuration

As you begin the process of initiating and implementing a change, your first step should be to baseline the configuration around the change so that the starting configuration is known. This baseline may be needed for rollback, disaster recovery, and understanding the impact of the proposed change.

In order to successfully manage change, we must also manage the configuration of the production environment. **The most effective way to do this is to baseline the configuration before and after each change.**

A configuration baseline is a snapshot of the IT environment that identifies its structure and underlying dependencies. The data from this snapshot should be captured and recorded in a configuration management system (CMS). A CMS can be as simple as a spreadsheet or as complex as an integrated set of tools that includes a database.

A CMS provides:

- A way to understand, control, and predict the consequences of change.
- An accurate and comprehensive representation of the state of the production environment.
- A history of previous states to support efforts to analyze and remedy problems.

A CMS contains information about configuration items (CIs), which are IT components that are important in understanding the state of the production environment. Each CI may be composed of other CIs and can vary widely in complexity, size, and type—from an entire system (including all hardware, software, and documentation) to a single software module or a minor hardware component. Baseline configuration can be a major undertaking. In JITSD we will baseline as we make changes so that eventually the entire production configuration is known.

Activities	Considerations
Define and collect the configuration data to track in the CMS	<p>Key questions:</p> <ul style="list-style-type: none"> • What information should be captured? • Which users need access to service and/or system component information? • In what format would the information be most useful to each user? • Does any information in the CMS need to have restricted access? <p>Inputs:</p> <ul style="list-style-type: none"> • Change requirements. • List of needed and desired CMS reporting requirements. • Internal policies. <p>Outputs:</p> <ul style="list-style-type: none"> • CR and CMS requirements. <p>Best practices:</p> <ul style="list-style-type: none"> • Define both business (services interdependencies) and technical (system components) use of data. • To obtain the most complete idea of needs, involve all relevant people in assessment and planning. This group might include individuals from ASB, SSB, Service Desk, and the business.

Step 2: Initiate the Change

Activities	Considerations
Initiate a change request (CR)	<p>Key questions:</p> <ul style="list-style-type: none"> • What kind of information is to be included in the change description? For example, the service that will be affected, the business benefit, and the exact description of the configuration items to be changed. • How are CRs interlinked and cross-referenced? • Is there a specific CR for common or standard changes? <p>Inputs:</p> <ul style="list-style-type: none"> • Requests for a change can come from: <ul style="list-style-type: none"> • End-users • Projects • Business initiatives • IT initiatives • Problems • Service monitoring • Requirements for a change • Description of the change <p>Output:</p> <ul style="list-style-type: none"> • New CR (Open new CR and ensure status is “In Planning.”) <p>Best practices:</p> <ul style="list-style-type: none"> • Keep CR forms as simple as possible while capturing sufficient information to manage risk. • <u>The CR will be continually updated throughout the process</u>; it can be initiated without a thorough analysis or detailed information about the change and then updated later.
Check the technical configuration	<p>Key questions:</p> <ul style="list-style-type: none"> • Has the CR identified all CIs that will be affected or that will require a change? • How many actual CIs will be affected? If this is a global change such as a software update, is there an accurate account of all services or production devices that will be affected? • When looking at the system configuration information, are there additional CIs that may be affected? • What will need to change to accommodate this CR? • What applications will be affected by this CR? <p>Inputs:</p> <ul style="list-style-type: none"> • CIs • Service map • Impacted services gathered from the CR <p>Output:</p> <ul style="list-style-type: none"> • Affected system(s) documented in CR. • CIs impacted by the CR

Activities	Considerations
Identify the business impact	<p>Key questions:</p> <ul style="list-style-type: none"> • Which users and business groups need to know about this change? • What business processes are potentially affected by this proposed change? • What are the risks associated with this change such as change to business and impact if the change fails? <p>Inputs:</p> <ul style="list-style-type: none"> • Request for a change • Identification of the IT system and business group impacted by the change <p>Output:</p> <ul style="list-style-type: none"> • Affected system(s) documented in CR. • Communication with affected system(s) leaders to give them a heads-up on the change. • Documentation of a clearly stated business reason and the impact and risk of the change request. <p>Best practices:</p> <ul style="list-style-type: none"> • Dependencies on business processes and functionality must be identified. If you change the workflow or how the application is used, the business must be involved to identify impacts. • Consider systems, services, process, and impacted applications when considering what communications are required.

Step 3: Classify the Change

After the CR is initiated, the next step is to classify the request.

Activities	Considerations
Identify the Type of change	<p>Key questions:</p> <ul style="list-style-type: none"> • What Type of change is it? Consult Change Types at the beginning of this document. <p>Types take into account the resource requirements for the change, the impact to the business of doing or not doing the change, organizational experience with the change, and new technology or processes and are:</p> <ul style="list-style-type: none"> • Standard change. This type is low risk because it has been proven to be successful, it has minimal business impact, and it has a known set of release procedures. • Minor change. This type affects a small percentage of users and resources. Also, the risk of an outage is less because of the organization's experience in implementing this type of change. • Major change. With a high risk this type involves the greatest potential impact on users and resources. It might also affect a business-critical system and could involve downtime of the service. • Emergency change. This type is high risk because of the urgency of release and the minimal time in which to test it. It is relatively uncertain if the change will succeed, and there is a big impact on the business if it fails. • Unauthorized. A change that has bypassed the change process and has come to light because of system failure or discovery after the change occurred. <p>Inputs:</p> <ul style="list-style-type: none"> • Change information. • Knowledge base / list of standard and previous changes to compare to. <p>Output:</p> <ul style="list-style-type: none"> • Type of change entered into the CR <p>Best practices:</p> <ul style="list-style-type: none"> • Effective use of standard changes is important for keeping the process manageable and usable. Evaluate minor changes that go through the CAB process for recategorization as future standard changes. • Be as specific as possible in defining what is and is not a particular type of change.

Activities	Considerations								
<p>Identify the Area to be changed</p>	<p>Key questions:</p> <ul style="list-style-type: none"> • What Area will be changed as a result of this CR? <ul style="list-style-type: none"> • Hardware. This includes servers, workstations, printers, and other hardware changes • Software. This includes custom or commercial software, database, web or any other software type changes. • Network. This includes routers, switches, and other networking types of changes. • Security. This includes system access changes for users and systems and other type of security changes. • Business. This includes process, documentation and other types of changes that do not fall into the above categories. <p>Inputs:</p> <ul style="list-style-type: none"> • CR and other information. <p>Output:</p> <ul style="list-style-type: none"> • Change Area entered into the CR 								
<p>Identify the Risk of the change</p>	<p>Key questions:</p> <ul style="list-style-type: none"> • What is the Risk of the change? Use the following seven questions to assist in determining the risk level. <ol style="list-style-type: none"> 1. Is the change implementation plan documented to a level so that more than one individual could execute it? 2. Is the roll-back plan documented to a level so that more than one individual could execute a roll-back? 3. Is there a written verification test plan that will be executed immediately following the conclusion of the change to verify success? 4. Has the change been tested in a non-production environment? 5. Will this change be implemented outside of core business hours? 6. Is there no system outage? 7. Is there no additional user training required because of this change? <p>A “No” answer to each of the questions above elevates the risk associated with the change. .</p> <table border="1" data-bbox="509 1375 1203 1560"> <thead> <tr> <th>Risk Level</th> <th>Calculated Value of Questions</th> </tr> </thead> <tbody> <tr> <td>High</td> <td>6-7 “No” Answers</td> </tr> <tr> <td>Medium</td> <td>3-5 “No” Answers</td> </tr> <tr> <td>Low</td> <td>1-2 “No” Answer</td> </tr> </tbody> </table> <p>Inputs:</p> <ul style="list-style-type: none"> • System configuration • Business operations • Probability that a change could cause system failure <p>Output:</p> <ul style="list-style-type: none"> • Risk of the change entered into the CR 	Risk Level	Calculated Value of Questions	High	6-7 “No” Answers	Medium	3-5 “No” Answers	Low	1-2 “No” Answer
Risk Level	Calculated Value of Questions								
High	6-7 “No” Answers								
Medium	3-5 “No” Answers								
Low	1-2 “No” Answer								

Activities	Considerations																
<p>Identify the Impact of the change</p>	<p>Key questions:</p> <ul style="list-style-type: none"> • What is the size of the impact of this change? How many users are affected and what might be the cost (safety, financial or public trust) be if the change fails? <p>Inputs:</p> <ul style="list-style-type: none"> • Impact to business (operations, monetary, regulatory, public trust, etc) if failure occurs. • System configuration. • Business operations. <p>Output:</p> <ul style="list-style-type: none"> • Impact of the change entered into the CR <table border="1" data-bbox="488 674 1192 1058"> <thead> <tr> <th>Impact Level</th> <th>Affected Users / Cost</th> </tr> </thead> <tbody> <tr> <td> <ul style="list-style-type: none"> • High </td> <td> <ul style="list-style-type: none"> • >100 Users • Critical business system (CJIN, SmartCop, MERLIN) </td> </tr> <tr> <td> <ul style="list-style-type: none"> • Medium </td> <td> <ul style="list-style-type: none"> • 10-100 Users • Significant business system (SharePoint, HOPE card, etc) </td> </tr> <tr> <td> <ul style="list-style-type: none"> • Low </td> <td> <ul style="list-style-type: none"> • <10 Users • Standard business system (Contracts library, consumer alert) </td> </tr> </tbody> </table>	Impact Level	Affected Users / Cost	<ul style="list-style-type: none"> • High 	<ul style="list-style-type: none"> • >100 Users • Critical business system (CJIN, SmartCop, MERLIN) 	<ul style="list-style-type: none"> • Medium 	<ul style="list-style-type: none"> • 10-100 Users • Significant business system (SharePoint, HOPE card, etc) 	<ul style="list-style-type: none"> • Low 	<ul style="list-style-type: none"> • <10 Users • Standard business system (Contracts library, consumer alert) 								
Impact Level	Affected Users / Cost																
<ul style="list-style-type: none"> • High 	<ul style="list-style-type: none"> • >100 Users • Critical business system (CJIN, SmartCop, MERLIN) 																
<ul style="list-style-type: none"> • Medium 	<ul style="list-style-type: none"> • 10-100 Users • Significant business system (SharePoint, HOPE card, etc) 																
<ul style="list-style-type: none"> • Low 	<ul style="list-style-type: none"> • <10 Users • Standard business system (Contracts library, consumer alert) 																
<p>Severity: Will be automatically calculated.</p>	<p>The severity (low, medium, or high) will be automatically calculated based on the Risk and the IMPACT input on the CR.</p> <table border="1" data-bbox="701 1213 1154 1465"> <thead> <tr> <th>Risk Impact</th> <th>Low</th> <th>Med</th> <th>High</th> </tr> </thead> <tbody> <tr> <th>High</th> <td>Med</td> <td>High</td> <td>High</td> </tr> <tr> <th>Med</th> <td>Low</td> <td>Med</td> <td>High</td> </tr> <tr> <th>Low</th> <td>Low</td> <td>Low</td> <td>Med</td> </tr> </tbody> </table>	Risk Impact	Low	Med	High	High	Med	High	High	Med	Low	Med	High	Low	Low	Low	Med
Risk Impact	Low	Med	High														
High	Med	High	High														
Med	Low	Med	High														
Low	Low	Low	Med														

Step 4: Plan and Design the Change

Activities	Considerations
Plan the change date	<p>Key questions:</p> <ul style="list-style-type: none"> • What date best fits the change based on user system, user, operational, and IT requirements? • Is any other system change schedule for same/nearby date? <p>Inputs:</p> <ul style="list-style-type: none"> • Business and user requirements for the solution. • Usage scenarios. • Operational and system requirements. <p>Output:</p> <ul style="list-style-type: none"> • Proposed change date (located at the top of the CR form)
Develop Implementation and Back-out plans	<p>Key questions:</p> <ul style="list-style-type: none"> • What needs to be done when and by whom? • Does the design address operational requirements? • Does the design address system requirements? • Who in the business is most likely to be affected by this change in terms of either its success or failure? • Who has the most relevant IT technical knowledge? • Who would best understand the implications to the business of not making this change? • What could go wrong and what are the plans to overcome those problems? • Who will best understand the security and privacy implications? • What is the procedure to revert back to the starting configuration? • Who makes the decision to revert back or continue forward if the change goes past the outage window. <p>Inputs:</p> <ul style="list-style-type: none"> • Business and user requirements for the solution • Usage scenarios • Operational and system requirements <p>Output:</p> <ul style="list-style-type: none"> • Implementation plan • Back-out plan

Activities	Considerations
Identify configuration dependencies	<p>Key questions:</p> <ul style="list-style-type: none"> • Are there other CIs that have dependencies on or that could be affected by the proposed change? • Does the proposed change have dependencies on other changes? In other words, does completing the proposed change require other changes to be made first? • Are all changes (both the prerequisites and the ultimate change) recorded in the CMS? <p>Input:</p> <ul style="list-style-type: none"> • Information about other proposed changes in the CMS <p>Output:</p> <ul style="list-style-type: none"> • A CMS entry in the “Notes” field showing CI dependencies that might be affected by or have an effect on the proposed change
Update the CR	<p>Key questions:</p> <ul style="list-style-type: none"> • Have updates been made to reflect such things as the planned release date, backout plans and any reasons for a backout (if one was required), support requirements, rollout plan, test results, observed problems, and date of the post-implementation review (PIR)? • Have status updates and monitoring been done throughout the process? • Has the change initiator been able to view the CR throughout the process to get status? <p>Input:</p> <ul style="list-style-type: none"> • Updates about the change <p>Output:</p> <ul style="list-style-type: none"> • Updated CR <p>Best practice:</p> <ul style="list-style-type: none"> • The Change Manager should be monitoring open changes that are pending release in order to ensure information gets updated.

Step 5: Build, Test and Review the Change

Activities	Considerations
Build and test the change	<p>Key questions:</p> <ul style="list-style-type: none"> • Does the built change meet the customer's specifications? • Is there a way to test the change in a test environment? • Has the development team prepared an issue-tracking process? • Have the development and test teams worked together to prepare a test specification? • Has the team created multiple release candidates and tested each to see whether it is fit to release to a pilot group? • Has the team completed user acceptance testing? • Has the team piloted the solution and collected feedback? <p>Inputs:</p> <ul style="list-style-type: none"> • Functional specification • Customer requirements • Code • Equipment • Test specification document • Test plan • Test environment • Issue tracking database and issue tracking policies and procedures <p>Outputs:</p> <ul style="list-style-type: none"> • Release candidate to be tested • Test results <p>Best practices:</p> <ul style="list-style-type: none"> • Resolve all known issues, whether the resolutions are fixes or deferrals. • Define and communicate standards for issue priority and severity to all team members. • Provide an issues database to training and support staff so that they can have a deeper insight into the history of the solution and the problems found in development. • Schedule regular meetings with those responsible for development and testing to review issues and plan strategies for resolving them.

Step 6: Approve and Schedule the Change

Activities	Considerations
Submit change for approval	<p>Key question:</p> <ul style="list-style-type: none"> • Is everything completed on the CR? <p>Input:</p> <ul style="list-style-type: none"> • CR information. • Approved processes. <p>Outputs:</p> <ul style="list-style-type: none"> • CR submitted for approval (Change CR Status to “Submitted for Approval”) • Standard changes given to the Change Manager <p>Best practices:</p> <ul style="list-style-type: none"> • In addition to standing CAB members, include personnel and experts from parts of the organization affected by the change or who can add value to the discussion of the change. These additional members are chosen on a case-by-case basis. • Beware of the “this is obvious, just do it” decision. Solicit sufficiently broad input by involving a variety of parties in the approval body so that there is rigor in identifying trade-offs.
Process standard changes to release	<p>Key questions:</p> <ul style="list-style-type: none"> • Has this change been classified as a standard change? • Are the change tasks well known and proven? • When this standard change has been performed, has it always resulted in expected outcomes? • Will this change occur after the next CAB? If not, reschedule change until after next CAB. <p>Inputs:</p> <ul style="list-style-type: none"> • The CR under consideration • List of approved standard changes <p>Outputs:</p> <ul style="list-style-type: none"> • Identified standard changes proceed directly to development or to release • Documentation of a standard change having passed through previous approval. <p>Best practices:</p> <ul style="list-style-type: none"> • “Tried, Tested, and True”. These are characteristics of standard changes. There is a high level of predictability and confidence that a standard change will yield expected results, without exception. • Because the types of changes that have been pre-approved as standard changes are known to have a low impact on the environment and are a low risk to it, they do not need to be reviewed again by the CAB or even the Change Manager. This, however, means that care must be taken during the initial screening to ensure that a change request that has been categorized as standard is, indeed, one of the pre-approved change types and fits in the change window.

Activities	Considerations
Review CR	<p>Key questions:</p> <ul style="list-style-type: none"> • Is all information available to review the change? • Does the change make sense? • Does the change really need to be made? • Is the timing right to make the change or is there a better change window? Examples such as critical business operations such as elections or tax or hunting season; current state or world events; severe weather forecasted; heightened terrorist or hacker alerts, etc. Do any of the reviewers have questions? If so, add them to the “Notes” section of the CR. The Change Manager should reply with an answer inside the notes field as well. • Have all stakeholders been involved? • Does the implementation and back-out plan look thorough? <p>Input:</p> <ul style="list-style-type: none"> • The CR • CR review times are seven (7) days before CAB for major changes and five (5) days for minor changes. <p>Output:</p> <ul style="list-style-type: none"> • Questions in “Notes” field of CR • Communication between stakeholders <p>Notes Field in the ChMS:</p> <ul style="list-style-type: none"> • The Notes field is to be used for technical comments regarding the change. The Change Manager (CM) is responsible for addressing any issues or concerns that have been documented here and make appropriate updates within the notes field. For example, if a CAB or Extended CAB member has either a question or concern regarding the change, the CM needs to add that note to the Change Request. The CM must either manually monitor the Change or configure a SharePoint alert on the notes field. The CM must provide timely updates to any documented questions or concerns.
CAB Review	<p>The CAB and Extended CAB have a standing, weekly meeting. All changes are routed to the CAB for approval. In addition to reviewing and (dis)approving changes, the CAB performs the following functions:</p> <ul style="list-style-type: none"> • Provide enterprise risk management, communications management, and process compliance management to the change process environment. • Ensure that changes to the DOJ enterprise are reviewed and processed in accordance with this Change Management Process. • Ensure all changes adhere to state and DOJ policy and are documented, tested, and approved prior to implementation. <p>Input:</p> <ul style="list-style-type: none"> • The CR <p>Output:</p> <ul style="list-style-type: none"> • Approved, disapproved or more information required for the CR • Communication to affected groups

Activities	Considerations
Review the readiness of the change for release	<p>Key questions:</p> <ul style="list-style-type: none"> • Is there clear ownership of all activities and actions? • Has the appropriate management signed off on all plans? • Have required communications with all affected groups occurred? • Do the users and owners of dependent services know this change is scheduled and what the impact will be to them? • Are the functional users ready and committed to the new changes? • Is the testing complete? • Is SSB, ASB and the Service Desk ready for the release? <p>Input:</p> <ul style="list-style-type: none"> • Release candidate (software and/or hardware) • Testing results • Updated rollout schedule, plan, checklist, procedures, etc <p>Output:</p> <ul style="list-style-type: none"> • A go/no go decision about whether to release <p>Best practices:</p> <ul style="list-style-type: none"> • Ensure that the Release Manager is provided with the appropriate information in order to make a good decision. • Provide feedback and acknowledgement to those who have supported the release, and remind the organization of the expected benefits.
Send notifications	<p>Key questions:</p> <ul style="list-style-type: none"> • What do IT staff and users need to know about this change? <p>Input:</p> <ul style="list-style-type: none"> • Change date and details <p>Output:</p> <ul style="list-style-type: none"> • Notifications lead-time to users for system outages is SEVEN (7) CALENDER DAYS • Notifications should be geared toward the user and business and not be in IT talk. IT folks can get details in the CR. Example: <p style="text-align: center;">DOJ ITSD Service Interruption Wednesday, 11-Sep-2013 3:00 A.M. to 6:00 A.M. MDT MERLIN</p> <p>Description: MERLIN 14.5 upgrade.</p> <p>Change Overview: Upgrade MERLIN software to provide _____ (list major enhancements).</p> <p>Change Reason: Provide new capabilities (other examples: software end of life, increase security, enable faster system performance, cost savings, etc)</p> <p>Customer Impact: MERLIN will be unavailable during change time.</p> <p>Change Request Number: 99</p>

Activities	Considerations
Update the CR	<p>Key questions:</p> <ul style="list-style-type: none">• Have updates been made to reflect such things as the planned release date, backout plans and any reasons for a backout (if one was required), support requirements, rollout plan, test results, observed problems, and date of the post-implementation review (PIR)?• Have status updates and monitoring been done throughout the process?• Has the change initiator been able to view the CR throughout the process to get status?• Has there been formal communication at the point of release with the change initiator? <p>Input:</p> <ul style="list-style-type: none">• Updates about the change <p>Output:</p> <ul style="list-style-type: none">• Updated CR <p>Best practice:</p> <ul style="list-style-type: none">• The Change Manager should be monitoring open changes that are pending release in order to ensure information gets updated.

Step 7: Release the Change

Once the changed has been built, tested, and reviewed for release readiness, it is time to release the change.

Activities	Considerations
Release the change	<p>Key questions:</p> <ul style="list-style-type: none"> • Is the change stable enough to release? • Are IT and the users ready to release the change to production? <p>Inputs:</p> <ul style="list-style-type: none"> • Released change, including change deliverables and documentation. • Implementation plan. <p>Output:</p> <ul style="list-style-type: none"> • Released change <p>Best practice:</p> <ul style="list-style-type: none"> • Make decisions about the release strategy early in the process, possibly in the envisioning or project planning phases, to minimize risk.
Validate and stabilize the release	<p>Key questions:</p> <ul style="list-style-type: none"> • Does the team have a plan to monitor the solution during the watch period? This is the period when the project team is no longer active but does respond to issues as SSB escalates them to the team. Typical watch periods last from 15 to 30 days. • Is the release change stable? • Have all issues found by testing and through pilot feedback been resolved? • Has user acceptance testing been done? <p>Inputs:</p> <ul style="list-style-type: none"> • Test specification document • Master plan, including the test plan • Test scenarios and test cases • Interim builds, including: <ul style="list-style-type: none"> • Solution deliverables. • Documentation. • Issue-tracking database. • Issue-tracking policies and procedures <p>Outputs:</p> <ul style="list-style-type: none"> • Released change <p>Best practices:</p> <ul style="list-style-type: none"> • Use a formal issue-tracking system to track and report the status of bugs. • Document issue-tracking and reporting procedures during planning. • Define and agree on success criteria for testing the release candidate. • Do not release the candidate until the entire team signs off on its suitability.

Activities	Considerations
Get final customer approval of the change	<p>Key questions:</p> <ul style="list-style-type: none"> • Is the customer satisfied with the change and accept it? <p>Input:</p> <ul style="list-style-type: none"> • Released change <p>Output:</p> <ul style="list-style-type: none"> • Requester release acceptance sign off
Document the released change and communicate the impact to users	<p>Key questions:</p> <ul style="list-style-type: none"> • Have changes made to IT components during release been communicated and documented in the CR? • Has the team recorded in the CR any workarounds or requests for change submitted regarding the release? <p>Inputs:</p> <ul style="list-style-type: none"> • Information about the change • Service map <p>Outputs:</p> <ul style="list-style-type: none"> • Updated CR • A stable solution released into the production environment • A customer who is satisfied with and accepts the released solution • A solution that is successfully transferred from the change team to SSB <p>Best practice:</p> <ul style="list-style-type: none"> • Clearly communicate the change to all interested parties.
Transfer responsibility to SSB	<p>Key questions:</p> <ul style="list-style-type: none"> • Has the change solution been transferred successfully to operations (SSB)? • Has training been done to ensure that SSB personnel are prepared to manage and support the new configuration? <p>Input:</p> <ul style="list-style-type: none"> • Released change <p>Output:</p> <ul style="list-style-type: none"> • A managed and supported change
Update the CR and the configuration database	<p>Key questions:</p> <ul style="list-style-type: none"> • Has the CR been updated to reflect any changes made from the original request? • Have changes made to IT components been recorded in the CMS? • Have any workarounds or requests for a change submitted in support of the release been recorded in the CMS? <p>Inputs:</p> <ul style="list-style-type: none"> • Changes made in original request • Information about changed CIs <p>Outputs:</p> <ul style="list-style-type: none"> • Updated CR • Updated CMS <p>Best practice:</p> <ul style="list-style-type: none"> • When a change is moved to production, update the CMS current state so that an accurate picture is available for problem analysis and other CRs.

Step 8: Review the Change

After the team has successfully released the change into the production environment, the next important step is to validate the release and then review it. **The goal of validation is to verify that the change has actually been released as expected.** The goal of reviewing the change, called a Post-Implementation Review (PIR), is to determine whether the change has had the desired effect and has met the requirements from the original CR.

Determining whether the released change has been effective and has achieved the desired results requires monitoring the change in the production environment. For a small change, this might be a matter of checking on the desired functionality. Larger changes might require monitoring of network and server information, performance data, event logs, and response times.

After the release of the change has been validated, the PIR can be performed. The results of the PIR should include:

- A success/failure decision on the change implementation.
- A review of how the change was released and whether it was implemented on time and on budget.
- Documentation of the lessons learned from the change process.

Activities and Considerations for Validating and Reviewing the Change

Activities	Considerations
Validate the technical success or failure of the change	<p>Key questions:</p> <ul style="list-style-type: none"> • Did the change meet the technical requirements? This may be verified in different ways based on the type of change. For example: <ul style="list-style-type: none"> • User testing • IT testing • Monitoring tools • Are all site deployments complete and stabilized? • Was the stabilization period uneventful or were numerous incidents documented? <p>Input:</p> <ul style="list-style-type: none"> • Data about the technical success of the change <p>Output:</p> <ul style="list-style-type: none"> • Post Implementation Review (PIR) report • Updated CR Implementation Results <ul style="list-style-type: none"> • Successfully Implemented • Implemented with Issues • Partially Implemented • Failed and Backed out • Postponed • Lessons learned into the CR. What was learned from this change that could improve the process the next time? <p>Best practices:</p> <ul style="list-style-type: none"> • Incidents related to the change are a reactive indicator of the success of the change. • For minor changes, a phone call, walk around check-in, or email after a change is made are proactive verifications.

Activities	Considerations
Validate the business success or failure of the change	<p>Key questions:</p> <ul style="list-style-type: none"> • Did the change meet the business requirements and objectives? • Are customers and users satisfied with the solution and its release? • Are customers and users happy with the results? • Have there been any unexpected side effects? <p>Inputs:</p> <ul style="list-style-type: none"> • Feedback regarding technical aspects of the change. • Feedback regarding business requirements aspects of the change. <p>Output:</p> <ul style="list-style-type: none"> • Validation of the change
Audit the configuration system	<p>Key questions:</p> <ul style="list-style-type: none"> • How accurate is the data about the change that has been stored in the CMS? • Who updates the CMS, and what happens if the data is incorrect? <p>Input:</p> <ul style="list-style-type: none"> • Information about the changed CIs. <p>Output:</p> <ul style="list-style-type: none"> • Accurate and updated information in the CMS.
Communicate and record the change	<p>Key questions:</p> <ul style="list-style-type: none"> • Has the team documented the results of the change? • Has the team provided feedback (including issues and a summary of the PIR) about the change to the appropriate parties? For example: <ul style="list-style-type: none"> • CAB members • Customers and users who are affected • The change management and release management teams • IT management • IT staff <p>Input:</p> <ul style="list-style-type: none"> • Information about the change <p>Output:</p> <ul style="list-style-type: none"> • Communications about and a record of the change.
Update and close the CR	<p>Key questions:</p> <ul style="list-style-type: none"> • Has the CR been updated to include feedback from the PIR? • Does the CR accurately reflect the change just completed? • Have Lessons Learned been documented? <p>Input:</p> <ul style="list-style-type: none"> • Updated information about the change <p>Output:</p> <ul style="list-style-type: none"> • Closed CR

Conclusion

The Change IMF describes the process for understanding and gaining control over the changes made in IT. CI and CR data is collected and used in this process. Change requested are reviewed, approved, implemented, and analyzed.

Implementation Checklist Example

Implementation Checklist			
For Proposed Scheduled Date of :4-Oct-2012 through 7-Oct-2012			
Date Due	Person Responsible	Task	Comments
Pre Deploy	Jack	Send service interruption notice	
Pre Deploy	Service Desk	Send AM/AP service interruption notice	done
Pre Deploy	John	Create LUN(s) on Compellent SAN	done
Pre Deploy	John	Attach LUN to DOJHLNITSD541	done
Pre Deploy	CPI	Verify System B is configured for fail-over	done
----	----	----	----
10/4/2012 5:00	John / CPI	Fail OpenFox services from System A to System B	done
10/4/2012 5:15	Service Desk	Confirm services have been restored.	done
10/4/2012 8:00	John	Upgrade OS on DOJHLNITSD540	in work
10/4/2012 13:00	John	Install, relocate to fiber chassis, and flash HBA on DOJHLNITSD540	done
10/4/2012 15:00	John	Attach LUN to DOJHLNITSD540	
----	----	----	
----	----	----	----
10/7/2012 8:00	John / CPI	Add LUNS to NFS vgs (/CPI /CPX /E2E /FOXVG	
10/7/2012 9:00	John / CPI	Initiate consistent disk mirror process	
10/7/2012 12:00	John / CPI	Break mirror and detach NFS mounts	
10/7/2012 13:00	CPI	Modify FOX scripts on 540/541	which scripts does Matt need to modify?
10/7/2012 ???	John / CPI	Perform fail-over to 540	Send AM/AP
10/7/2012 ???	Service Desk	Confirm services have been restored (RQ, DQ, FQ, KQ, PAQ)	
10/7/2012 ???	JC	Confirm CHOPRS interface is functioning	This needs to be coordinated with MII.