fruition
PARTNERS

Yale University Change Management Process Guide

Learn more:

(888) 440-2730 x702
info@FruitionPartners.com
www.FruitionPartners.com

Table of Contents

Introduction

Purpose

This document will serve as the official process of Change Management for Yale University. This document will introduce a Process Framework and will document the workflow, roles, procedures, and policies needed to implement a high quality process and ensure that the processes are effective in supporting the business. This document is a living document and should be analyzed and assessed on a regular basis.

Scope

The scope of this document is to define the Change Management Process, and process inputs from, and outputs to, other process areas. Other service management areas are detailed in separate documentation. This document includes the necessary components of the Process that have been confirmed for the organization.

Change Management Overview

What is Change Management?

- Process to coordinate the change needed by business
- Authorizes changes and coordinates change timelines to avoid conflict
- Responsible for governance, not execution activities
- Ultimately to support the change owner and the implementation of a successful change

Why is Change Management Important?

- Manages risk and priority
    - On average, 80% of incidents caused by change
    - Compliance (SOX, ISO9000, etc)
    - Prioritizes to implement most important changes first
    - Rapid change capability for business
- Maintains a complete view of change in the organization

Change Management Key Concepts

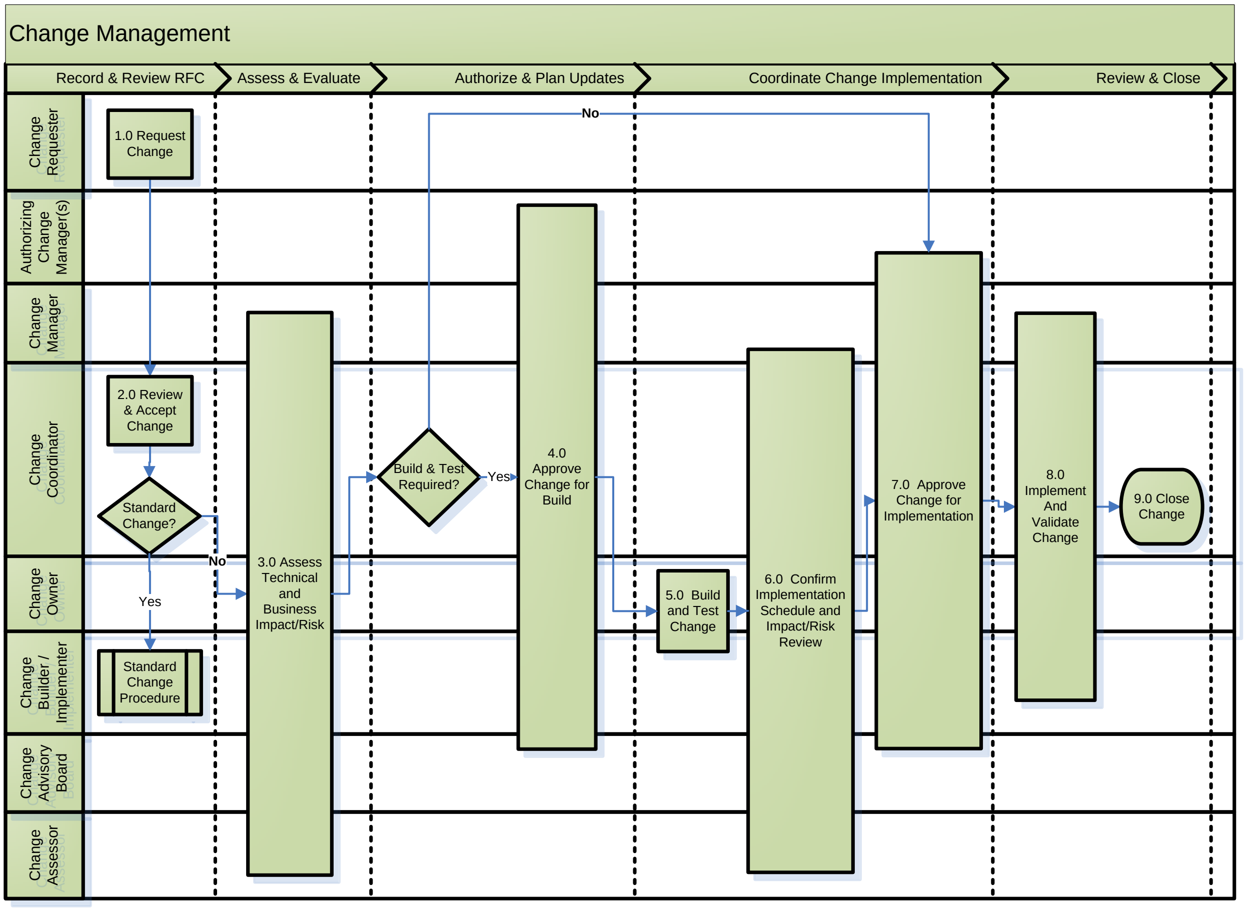
Change Request	• Optimize risk exposure. • Minimize the severity of any impact and disruption. • Proactive: Improve services, reduce costs, maintenance/prevention. • Reactive: Resolve known errors and adapt to business changes.
Service Request	• Something that can usually be planned for… • Standard, low/known risk, highly repetitive changes. • Well-defined activities that result in the fulfillment. • Access to an existing service, requests for information, or something that has been pre-approved by the Change Advisory Board.
Configuration Item	• Any Component that needs to be managed in order to deliver an IT Service. • An IT asset that is deemed valuable to track and manage through change control. • Either a physical (e.g. server) or logical (e.g. policy) record representing the actual asset. • CI's are controlled through the change process (or through request management when changes are deemed to be standard).
Release (and Deployment) Management	• Release and Deployment Management aims to build, test and deliver the capability to provide the services specified by Service Design and that will accomplish the stakeholders' requirements and deliver the intended objectives. • Packaging/bundling of Changes. • Provides additional QA and oversight to ensure successful releases.
Request for Change (RFC)	• A Request for Change • Represents what is being changed, optimally expressed as a CI, who owns the change, when/where the change is occurring and how it is being implemented
Forward Schedule of Change (FSC)	• Forward Schedule of Change • A Document that lists all approved Changes and their planned implementation dates. • Typically shows upcoming (i.e. non-implemented) changes
Submission Priority	• The relative priority that a change needs to be implemented defined by its proposed implementation date/time and the time the change was submitted • Changes logged without optimal time to assess are typically defined as urgent changes
Change Type	• The scope and criticality of a given change, derived from the technical impact and risk • Often requires some form of assessment to be conducted, covering a number of key areas to derive a consolidated value

Change Advisory Board (CAB)	• Change Advisory Board • Assists the change manager in prioritization, approval / authorization activities • Assess business consequences of an unsuccessful change • Assist in scheduling the change, taking into account FSC and external factors (e.g. resource availability)
Jurisdiction	• An organizational entity that may have accountability over specific IT scope • Organizations with multiple jurisdictions typically have multiple CIOs • IT supported directly by the business is not a condition for multiple jurisdictions

Change Management Policies

The Change Owner is ultimately accountable for the success of their respective change.
The approving Change Manager is accountable for the successful execution of the process, as a means to mitigate impact and risk for stakeholders/customers.
Change Management will manage all changes made to the production environment, including the operational test environment. This includes changes implemented by vendors and external organizations.
Effective Risk and Impact Assessment is enforced and is considered the foundation of Change Management.
All customers are informed of changes that affect the Service(s) they receive prior to change implementation.
There is a mechanism to implement URGENT changes to the managed environment with minimum destabilization of that environment.
The number of changes deemed URGENT is reduced to a pre-specified and progressive metric through proper planning.
A CAB exists and the Change Manager is the ultimate decision making authority within the CAB.
A Change implementation plan is required prior to change deployment.
All Service Providers will fulfill their roles in compliance with the Change Management process.
An RFC should not be approved for implementation unless relevant back-out plans are in place.

Change Management Process Flow


Change Management
Record & Review RFC
Assess & Evaluate
Authorize & Plan Updates
Coordinate Change Implementation
Review & Close
Change Requester
Authorizing Change Manager(s)
Change Manager
Change Coordinator
Change Owner
Change Builder / Implementer
Change Advisory Board
Change Assessor
1.0 Request Change
2.0 Review & Accept Change
Standard Change?
No
Yes
Standard Change Procedure
3.0 Assess Technical and Business Impact/Risk
Build & Test Required?
Yes
No
4.0 Approve Change for Build
5.0 Build and Test Change
6.0 Confirm Implementation Schedule and Impact/Risk Review
7.0 Approve Change for Implementation
8.0 Implement And Validate Change
9.0 Close Change

Roles and Responsibilities

The following roles have been identified within the Incident Management Process.

Role	Description
Change Requestor	• The individual asking for a change to be made. May or may not be the change owner. • The requestor should be the person sponsoring or advocating the change, usually business.
Change Owner	• Individual stakeholder ultimately accountable for the end result of change, seeing it through its lifecycle. Ex: A Network Engineer may be the change owner for a router upgrade
Approving Change Manager	• Approves changes for build-test and implementation for changed owned by their jurisdiction • Accountable for the execution of the change process in support of the change owner • Conducts CAB meetings • Oversees change process
Change Advisory Board (CAB)	• A body that exists to support the authorization and approval of changes • Assists Change Management with assessment / prioritization feedback • Provides guidance to the Change Manager

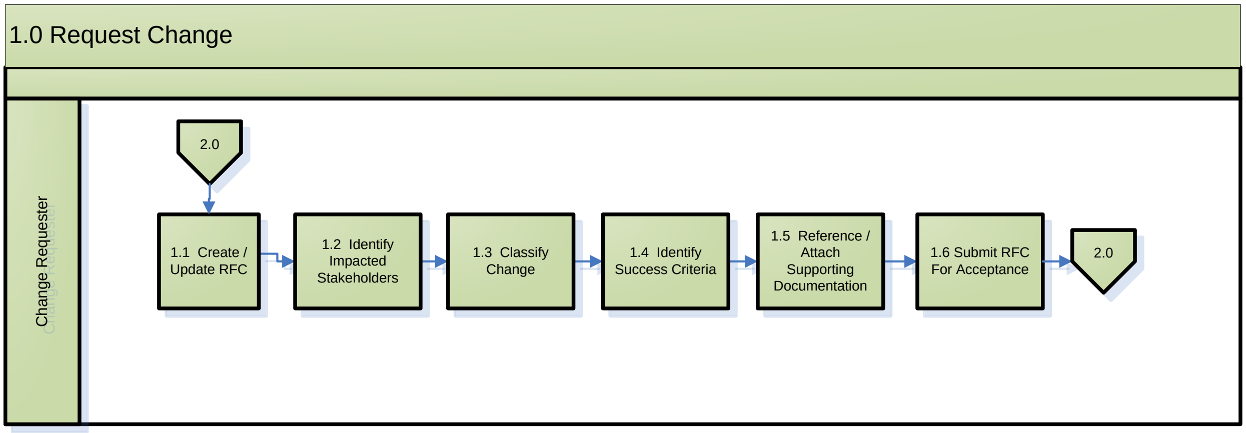
Role	Description
Change Coordinator	- Facilitates changes process - Assists the Change Manager and Change Owner throughout the change process
Change Assessor	- Responsible for contributing to the business and technical risk and impact assessment of a change for their domain
Change Builder / Implementer	- Individual responsible for performing the build/test and/or implementation
Authorizing Change Manager(s)	- Authorizes changes where their jurisdiction is impacted - Participates in CAB meetings as required

The following illustrates the Responsibility, Accountability, Consulted and Informed (RACI) matrix related to the key Change Management Activities:

	Change Requester	Authorizing Change Manager(s)	Approving Change Manager	Change Coordinator	Change Owner	Change Builder / Implementer	Change Advisory Board	Change Assessor	Change Process Owner
1.0 Request Change	AR								
2.0 Review & Accept Change	C		AR	R					
3.0 Assess Technical and Business Impact/ Risk				R	AR			R	
4.0 Approve Change for Build		R	AR	R	R		R		
5.0 Build and Test Change					AR	R			
6.0 Confirm Implementation Schedule and Impact / Risk Review			R	R	AR			R	
7.0 Approve Change for Implementation		R	AR	R	R		R		
8.0 Implement and Validate Change					AR	R			
9.0 Close Change	C		AR	R	R		C		
Process Maturity and Evolution	C	R	R	R	C	C	C	C	A

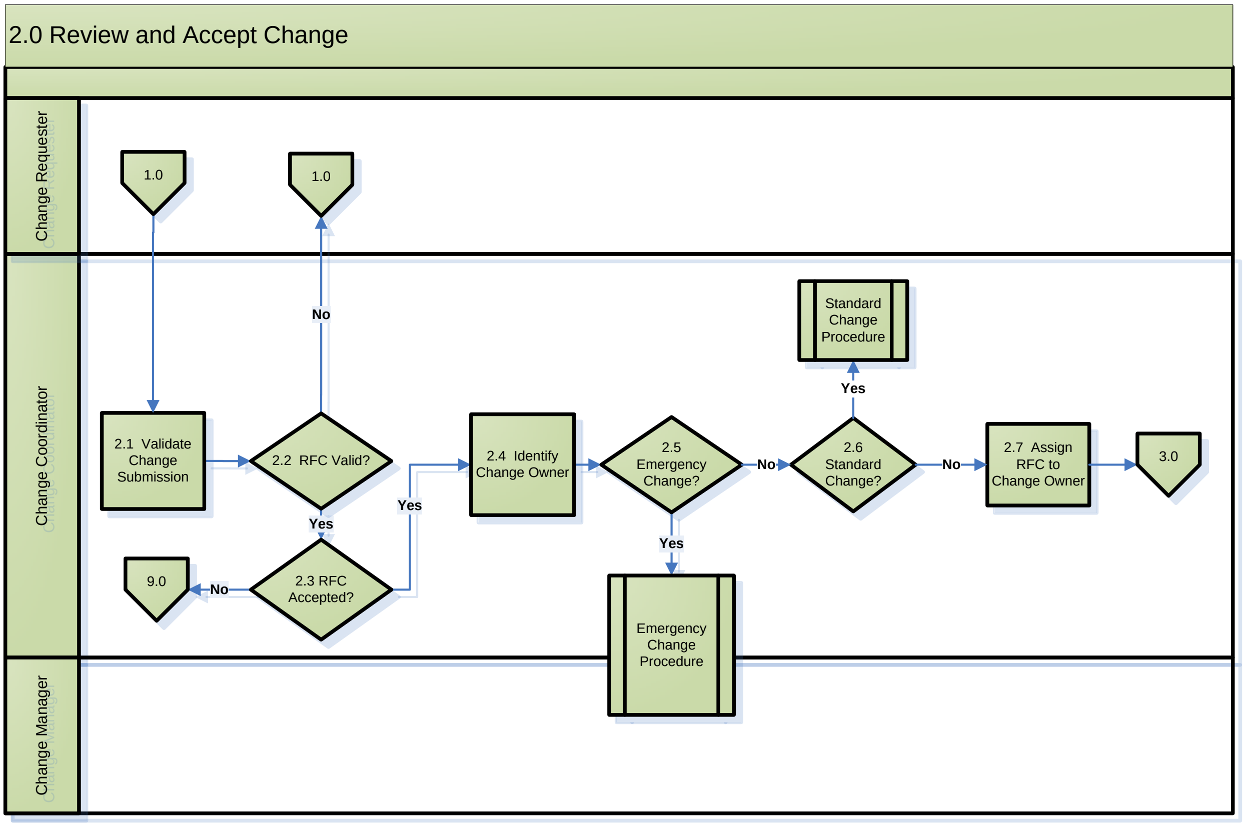
Process Procedures

1.0 Request Change


1.0 Request Change
Change Requester
2.0
1.1 Create / Update RFC
1.2 Identify Impacted Stakeholders
1.3 Classify Change
1.4 Identify Success Criteria
1.5 Reference / Attach Supporting Documentation
1.6 Submit RFC For Acceptance
2.0

Step	Activities
1.1 Create / Update RFC	Identify required information, such as contact information, requested schedule business rationale (eg. Functional enhancement to an application or service, increased performance/capacity/availability, resolution/fix to a known error…). It is possible some of these values may be updated by the change coordinator/manager and/ or owner.
1.2 Identify Impacted Stakeholders	Identify impacted stakeholders by identifying impacted CI's & services and indicate if they are located in other jurisdictions (change authorization required). Identify if resources will be required from other jurisdiction(s) to assist in the change.
1.3 Classify Change	Change requestor will provide the initial classification elements. This includes completing an initial impact/risk assessment to determine the change type.
1.4 Identify Success Criteria	Identify the Business objectives that will be used by to Validate Change Success after the change has been implemented and prior to closure.
1.5 Reference / Attached Supporting Documentation	Include all documentation appropriate to the nature of the change Project Charter, Business Case, detailed Change Description , etc) Note: If build-test is in-scope an Implementation plan, back-out plan, communication plan etc. may be included at this time, but are not mandatory.
1.6 Submit RFC for Acceptance	Once the request is complete, submit for acceptance.

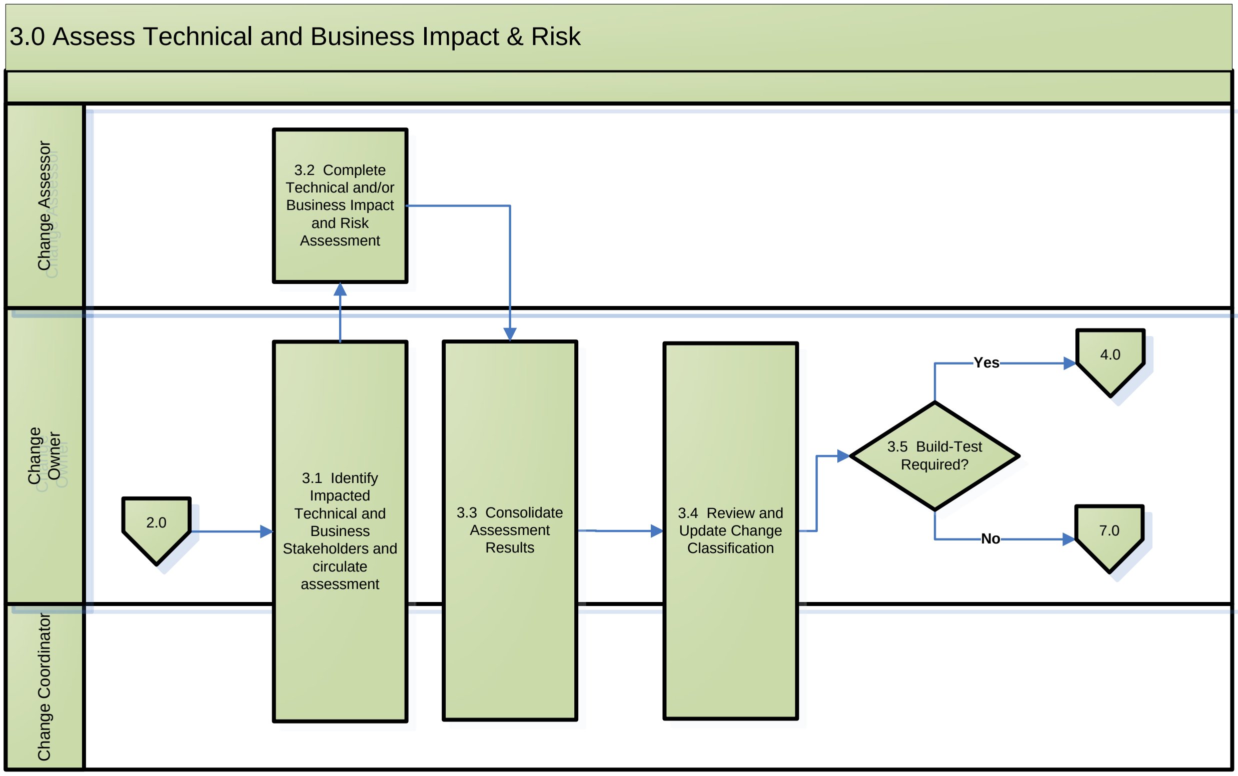
2.0 Review and Accept Change


2.0 Review and Accept Change
Change Requester
Change Coordinator
Change Manager
1.0
1.0
No
Standard Change Procedure
Yes
2.1 Validate Change Submission
2.2 RFC Valid?
2.4 Identify Change Owner
2.5 Emergency Change?
No
2.6 Standard Change?
No
2.7 Assign RFC to Change Owner
3.0
Yes
Yes
Yes
9.0
No
2.3 RFC Accepted?
Emergency Change Procedure

Step	Activities
2.1 Validate Change Submission	Verify that all information required to process the RFC has been provided.
2.2 RFC Valid?	Verify that the RFC complies with Change Management Standards and any jurisdiction-specific policies and business requirements. Refer exceptions to Change Requestor for correction, otherwise notify the Change Manager.
2.3 RFC Accepted?	Verify that this is a legitimate RFC. If not, reject the RFC and if so, continue processing. It is possible to meet all validation requirements in 2.2 but still not be considered legitimate. This could include changes outside the scope of IT.
2.4 Identify Change Owner	Change Coordinator identifies the Change Owner and confirms the accuracy of the selection with the Change Owner. If the Change Owner will come from another jurisdiction, the Change Coordinator will request the Change Manager/Coordinator from that jurisdiction to identify the Change Owner.
2.5 Emergency Change?	Determine if change meets emergency change criteria . If change is emergency, Chance Coordinator notifies approving Change Manager who invokes local emergency change procedures, otherwise change is processed under normal procedures .
2.6 Standard Change?	Verify that this is a legitimate "standard" change and defer the to the Standard Change Procedures.

Step	Activities
2.7 Assign RFC to Change Owner	Assign RFC to Change Owner for subsequent Review and Assessment.

3.0 Assess Technical and Business Impact & Risk

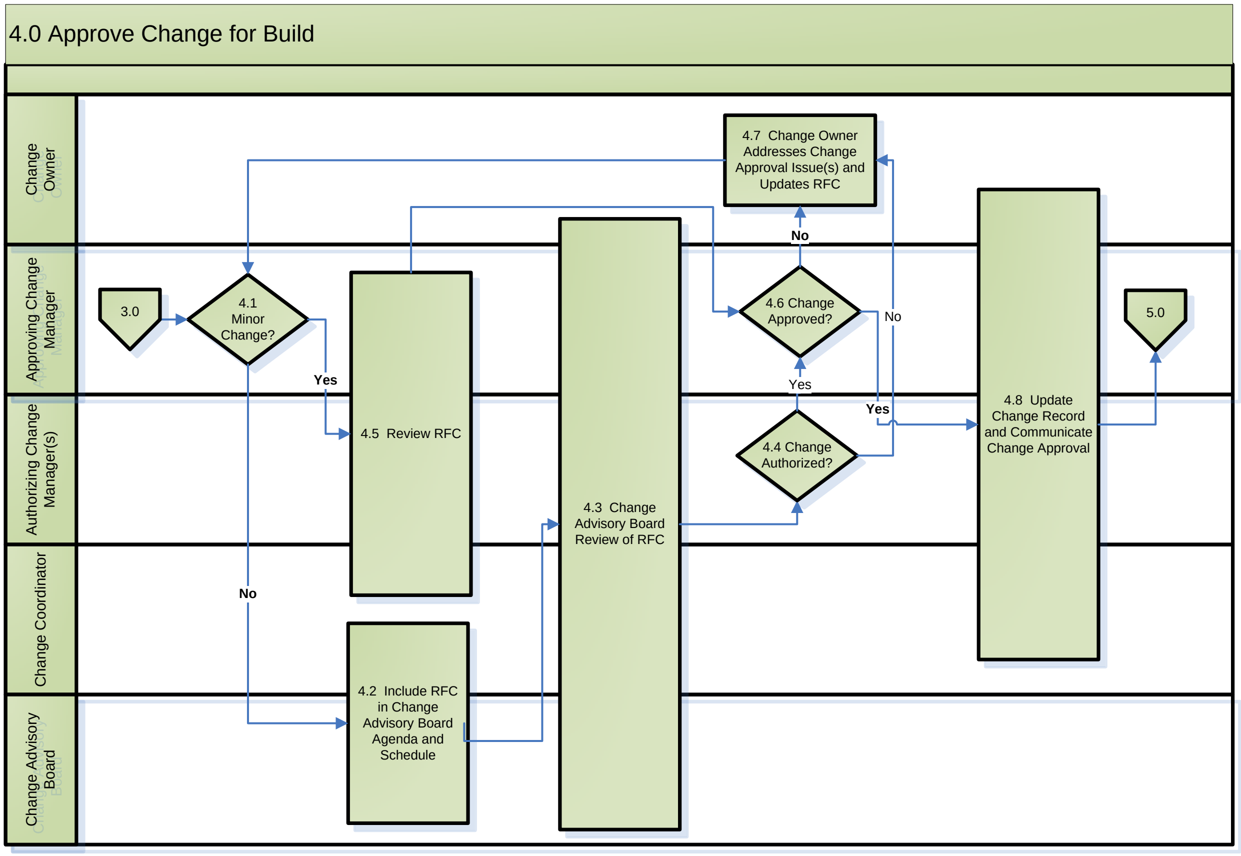


3.0 Assess Technical and Business Impact & Risk
Change Assessor
Change Owner
Change Coordinator
3.2 Complete Technical and/or Business Impact and Risk Assessment
2.0
3.1 Identify Impacted Technical and Business Stakeholders and circulate assessment
3.3 Consolidate Assessment Results
3.4 Review and Update Change Classification
3.5 Build-Test Required?
Yes
No
4.0
7.0

Step	Activities
3.1 Identify Impacted Technical and Business Stakeholders and circulate assessment	With the assistance of the change owner jurisdiction, the change Owner requests appropriate participation to assess the change using the standard risk/impact assessment (RIA) model. If RFC impacts other jurisdictions, the Change Owner requests their Change Managers to coordinate a the jurisdictional assessment. By default a single assessment task is sent to each jurisdiction but this may prompt additional tasks to be created by the jurisdictional change coordinator. A specific “Release” task will be sent to the release manager to determine if release coordination activities are required for this specific change. Release criteria will be defined and managed separately.
3.2 Complete Technical and/or Business Impact and Risk Assessment	• Change Owner uses the RIA model to conduct both Business Risk-Impact assessments and Technical Risk-Impact assessments. This may be updated following responses from assessors in 3.3. • This may be a Re-Assessment prior to Implementation approval if significant scope change encountered during Build-test • Operational procedures resolve conflicts with scheduling.

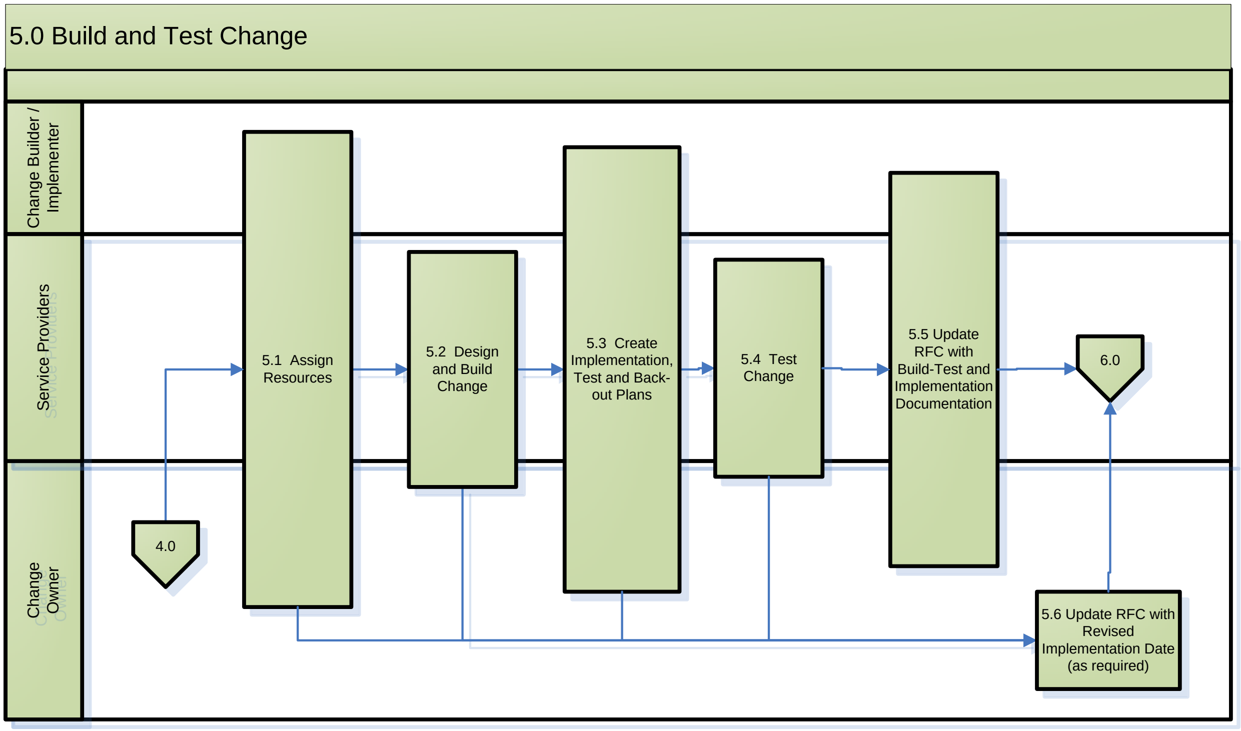
Step	Activities
3.3 Consolidate Assessment Results	Change Owner will consolidate input from all jurisdictions, which may inform updates to the overall impact and risk assessment. If Assessments are provided from multiple jurisdictions, Change Owner will: • Use worst case scenario to update the RIA to arrive at a single value for Risk, Impact and derived Change Type value. • Consolidate Operational Discovery feedback which may influence build/test and/or implementation plans.
3.4 Review and Update Change Classification	Following Assessment, Change Owner will confirm accuracy of Classification elements: • Jurisdiction(s) • Change Type reflects Risk-Impact value If Assessment tasks have identified additional impacted jurisdiction(s), the Change Owner will update RFC accordingly and request an assessment from each jurisdiction and reflect the input in final classification.
3.5 Build-Test Required?	If Build-test activities are not required, or if this is a re-assessment following Build-test completion, then request approval for Implementation.

4.0 Approve Change for Build


4.0 Approve Change for Build
Change Owner
Approving Change Manager
Authorizing Change Manager(s)
Change Coordinator
Change Advisory Board
3.0
4.1 Minor Change?
Yes
No
4.2 Include RFC in Change Advisory Board Agenda and Schedule
4.3 Change Advisory Board Review of RFC
4.4 Change Authorized?
Yes
No
4.5 Review RFC
4.6 Change Approved?
Yes
No
4.7 Change Owner Addresses Change Approval Issue(s) and Updates RFC
4.8 Update Change Record and Communicate Change Approval
5.0

Step	Activities
4.1 Minor Change?	Verify that this is a legitimate "minor" change.
4.2 Include RFC in CAB Agenda and Schedule	Take the steps necessary to include the RFC in the agenda for upcoming CAB meeting. This may be necessary across multiple CABs.
4.3 Change Advisory Board Review of RFC	CAB members review the RFC to provide additional input. The change owner may be requested to speak to these items, and provide additional details in the change as identified by the CAB prior to full change approval.
4.4 Change Authorized?	Impacted jurisdictions will review RFC, Risk-impact Assessment and associated documentation and provide authorization. CM will consider local assessment values to determine whether or not to involve their respective CAB. If impacted CM does not provide authorization, he/she must specify the conditions that would support authorization.
4.5 Review RFC	The RFC is reviewed for approval. This may include ensuring that all authorizations are provided should the minor change impact multiple jurisdictions.
4.6 Change Approved?	Prior to approval, CM will ensure that any conditions (from conditional Authorizations) are satisfied. Owner jurisdiction Change Manager approves start of Build-Test, involving CAB at his discretion. This can only occur if all jurisdictions have authorized the change.
4.7 Change Owner Addresses Change Approval Issue(s) and Updates RFC	If all avenues for approval have been exhausted, CM will deny the change and inform stakeholders.
4.8 Update Change Record and Communicate Change Approval	Update the record with all necessary information and ensure the approval of the change is approved accordingly.

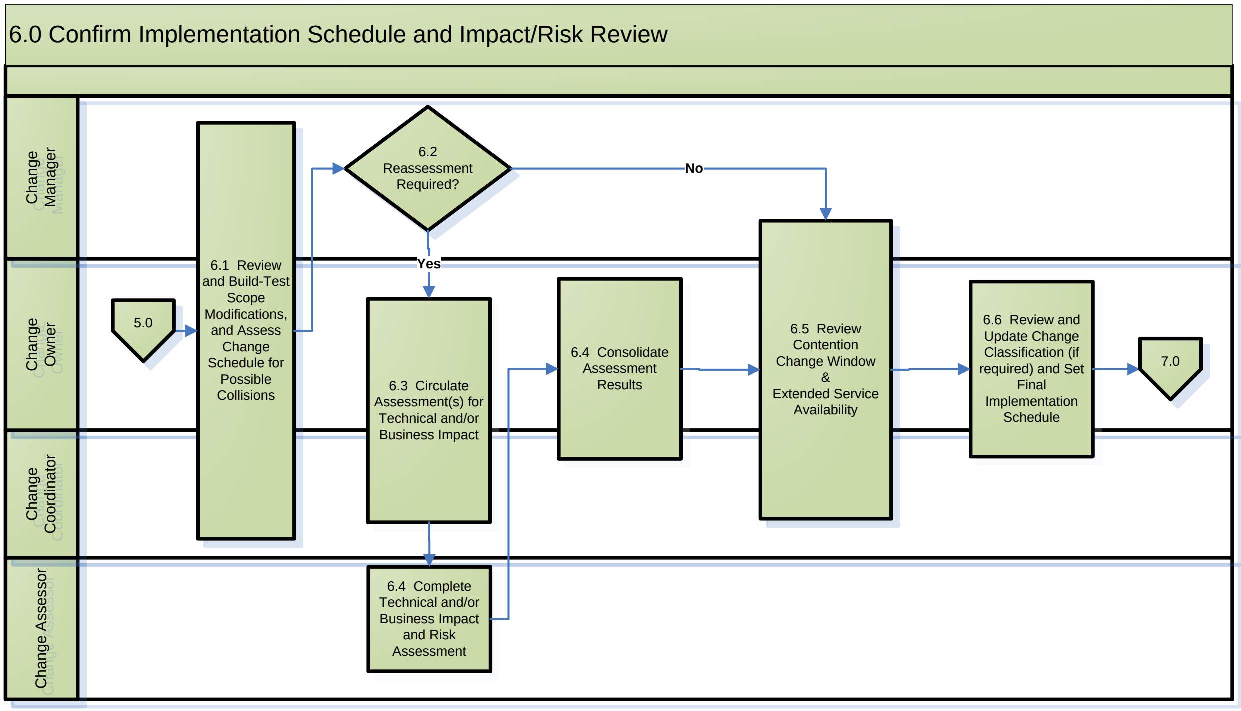
5.0 Build and Test Change


5.0 Build and Test Change
Change Builder / Implementer
Service Providers
Change Owner
4.0
5.1 Assign Resources
5.2 Design and Build Change
5.3 Create Implementation, Test and Back-out Plans
5.4 Test Change
5.5 Update RFC with Build-Test and Implementation Documentation
6.0
5.6 Update RFC with Revised Implementation Date (as required)

Step	Activities
5.1 Assign Resources	Change Owner and Builder ensures necessary resources (HW, SW, staff) are assigned to perform B-T activities, with assistance from other jurisdictions. Example: in addition to application development/testing, infrastructure resources may develop and test the Build Kit, while network resources test new router configurations.
5.2 Design and Build Change	Develop Build-test detailed schedule and review/agree with B-T resources from all jurisdictions . Build Team executes the build plan to develop the solution.
5.3 Create Implementation, Test and Back-out Plans	Change Owner ensures that the Build-test team prepares the Implementation Plan, containing the following: • Implementation instructions & estimated duration • Verification test instructions & estimated duration • Backout instructions, which must specify estimated duration , backout decision point & protocol, backout verification procedures • Communication protocol to communicate implementation, verification & backout results
5.4 Test Change	Testing scope includes everything from unit testing, through system testing up to & including Pre-Prod staging. The Implementation Plan is also tested (estimated timeframes are confirmed). The Change Owner may also request that Change Implementers assist in some of the above activity to familiarize themselves with what to expect during implementation.
5.5 Update RFC with Build-Test and Implementation	Prepare or update other collateral appropriate to the Change, including, at a minimum, Communication Plan (content approved for distribution) and Operations Discovery

Step	Activities
Documentation	Prepare description of Configuration Management data to be updated (may include documentation as well as HW/SW components)
5.6 Update RFC with Revised Implementation Data (as required)	If the previously scheduled Implementation Date is no longer achievable, due to Build-test slippage or external factors, the Change Owner requests that a revised Implementation date be scheduled asap. Note, this may require a reassessment in some cases.

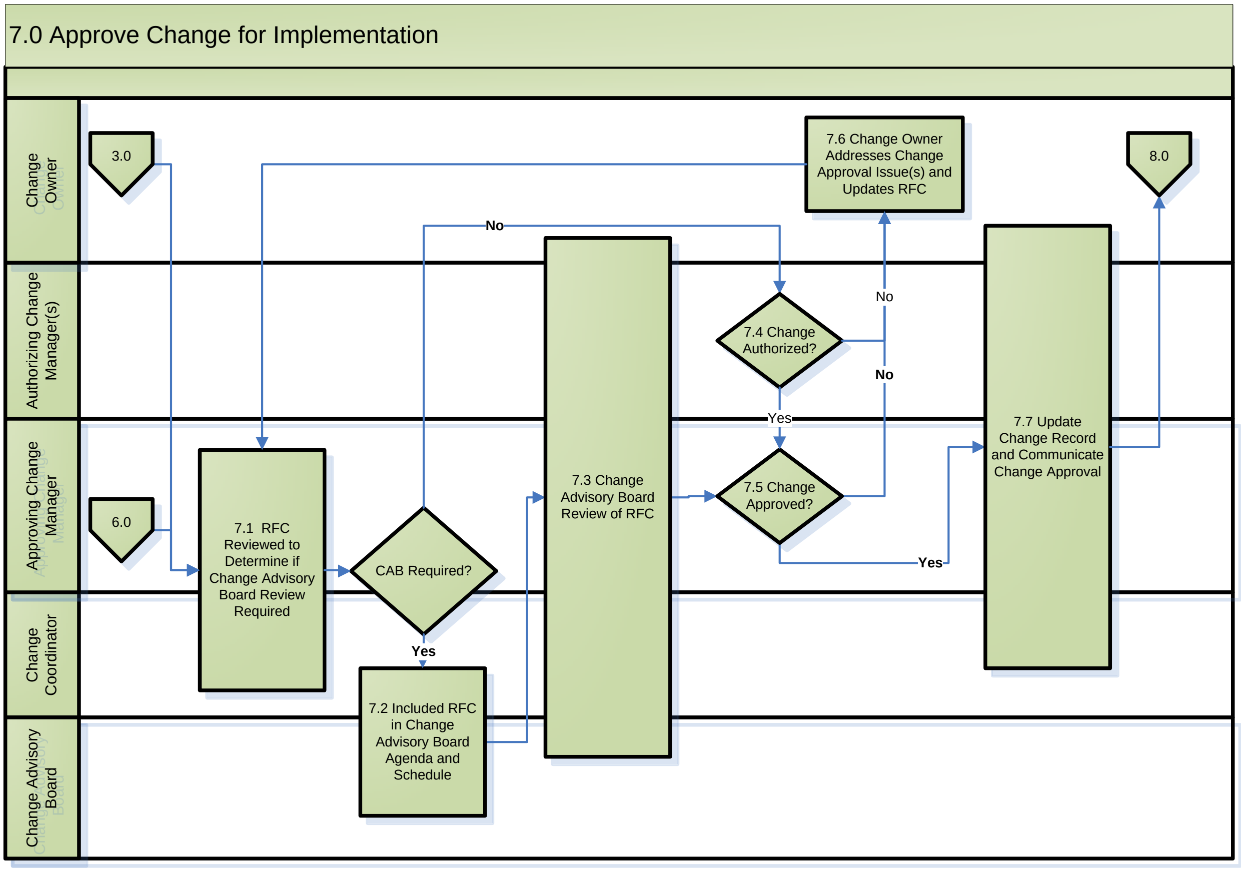
6.0 Confirm Implementation Schedule and Impact/Risk Review


6.0 Confirm Implementation Schedule and Impact/Risk Review
Change Manager
Change Owner
Change Coordinator
Change Assessor
5.0
6.1 Review and Build-Test Scope Modifications, and Assess Change Schedule for Possible Collisions
6.2 Reassessment Required?
No
Yes
6.3 Circulate Assessment(s) for Technical and/or Business Impact
6.4 Complete Technical and/or Business Impact and Risk Assessment
6.4 Consolidate Assessment Results
6.5 Review Contention Change Window & Extended Service Availability
6.6 Review and Update Change Classification (if required) and Set Final Implementation Schedule
7.0

Step	Activities
6.1 Review Build-Test Scope Modifications and Assess Change Schedule for Possible Collisions	Compare Build-test estimated effort against with assigned resources to determine reasonableness of proposed implementation date.
6.2 Reassessment Required?	Compare requested date against known scheduling constraints (ie freezes), and review scope of the original change request to determine if the change needs to be re-assessed. CM consults CAB based upon jurisdiction-specific detailed instructions if/as required.
6.3 Circulate Assessments(s) for Technical and/or Business Impact	CM requests impacted jurisdiction CM's to provide authorization.

Step	Activities
6.4 Complete Technical and/or Business Impact and Risk Assessment	• Change Owner & Change Assessors use the RIA model to conduct both Business Risk-Impact assessments and Technical Risk-Impact assessments • This may be a Re-Assessment prior to Implementation approval if significant scope change encountered during Build-test • Operational procedures resolve conflicts with scheduling.
6.5 Consolidate Assessment Results	Change Owner will consolidate input from all jurisdictions, which may inform updates to the overall impact and risk assessment. If Assessments are provided from multiple jurisdictions, Change Owner will: • Use worst case scenario to update the RIA to arrive at a single value for Risk, Impact and derived Change Type value. • Consolidate Operational Discovery feedback which may influence build/test and/or implementation plans.
6.6 Review Contention Change Window & Extended Service Availability	If conflicts or change window contention are acceptable, confirm requested date and inform Change Owner
6.7 Review and Update Change Classification (if required) and Set Final Implementation Schedule	Use priority and RIA to select candidate RFC's to be rescheduled and negotiate revised date(s) with the Change Owner(s) in order to minimize or eliminate contention and impact. If RFC being considered for change is in another jurisdiction, request CM from that jurisdiction to facilitate access to the CO

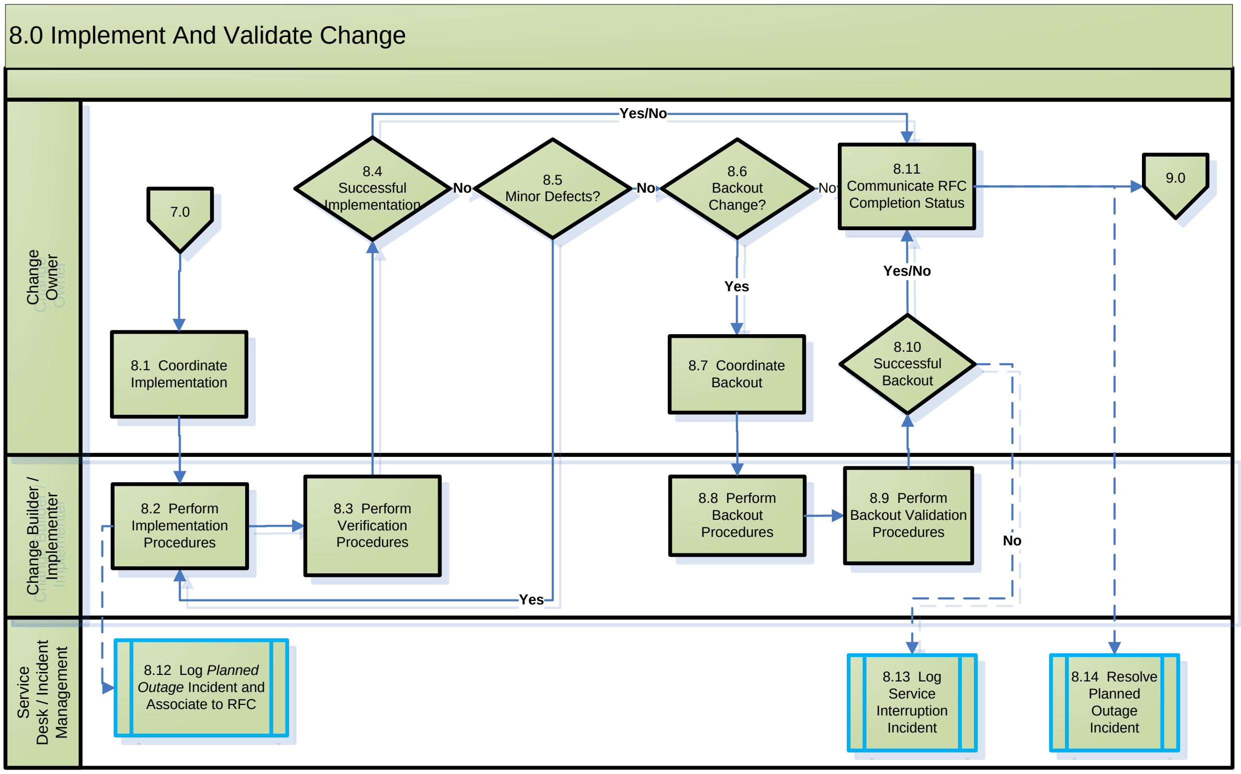
7.0 Approve Change for Implementation


7.0 Approve Change for Implementation
Change Owner
Authorizing Change Manager(s)
Approving Change Manager
Change Coordinator
Change Advisory Board
3.0
6.0
7.1 RFC Reviewed to Determine if Change Advisory Board Review Required
CAB Required?
Yes
No
7.2 Included RFC in Change Advisory Board Agenda and Schedule
7.3 Change Advisory Board Review of RFC
7.4 Change Authorized?
Yes
No
7.5 Change Approved?
No
Yes
7.6 Change Owner Addresses Change Approval Issue(s) and Updates RFC
7.7 Update Change Record and Communicate Change Approval
8.0

Step	Activities
7.1 RFC Reviewed to Determine if Change Advisory Board Review Required	CM determines if CAB approval is required to proceed to implementation.
7.2 Include RFC in Change Advisory Board Agenda and Schedule	If CAB approval is required, take the steps necessary to include the RFC in the agenda for upcoming CAB meeting. This may be necessary across multiple CABs.
7.3 Change Advisory Board Review of RFC	CAB reviews all RFC to approve the change for implementation.
7.4 Change Authorized?	Impacted jurisdictions will review RFC, Risk-impact Assessment and associated documentation and provide authorization. CM will consider local assessment values to determine whether or not to involve CAB . If impacted CM does not provide authorization, he/she must specify the conditions that would support authorization.
7.5 Change Approved?	Prior to approval, CM will ensure that any conditions (from conditional Authorizations) are satisfied. Owner jurisdiction Change Manager approves implementation, involving CAB at his or her discretion. This can only occur if all jurisdictions have authorized the change.

Step	Activities
7.6 Change Owner Addresses Change Approval Issue(s) and Updates RFC	If all avenues for approval have been exhausted, CM will deny the change and inform stakeholders.
7.7 Update Change Record and Communicate Change Approval	Update the record with all necessary information and ensure the approval of the change is approved accordingly.

8.0 Implement and Validate Change

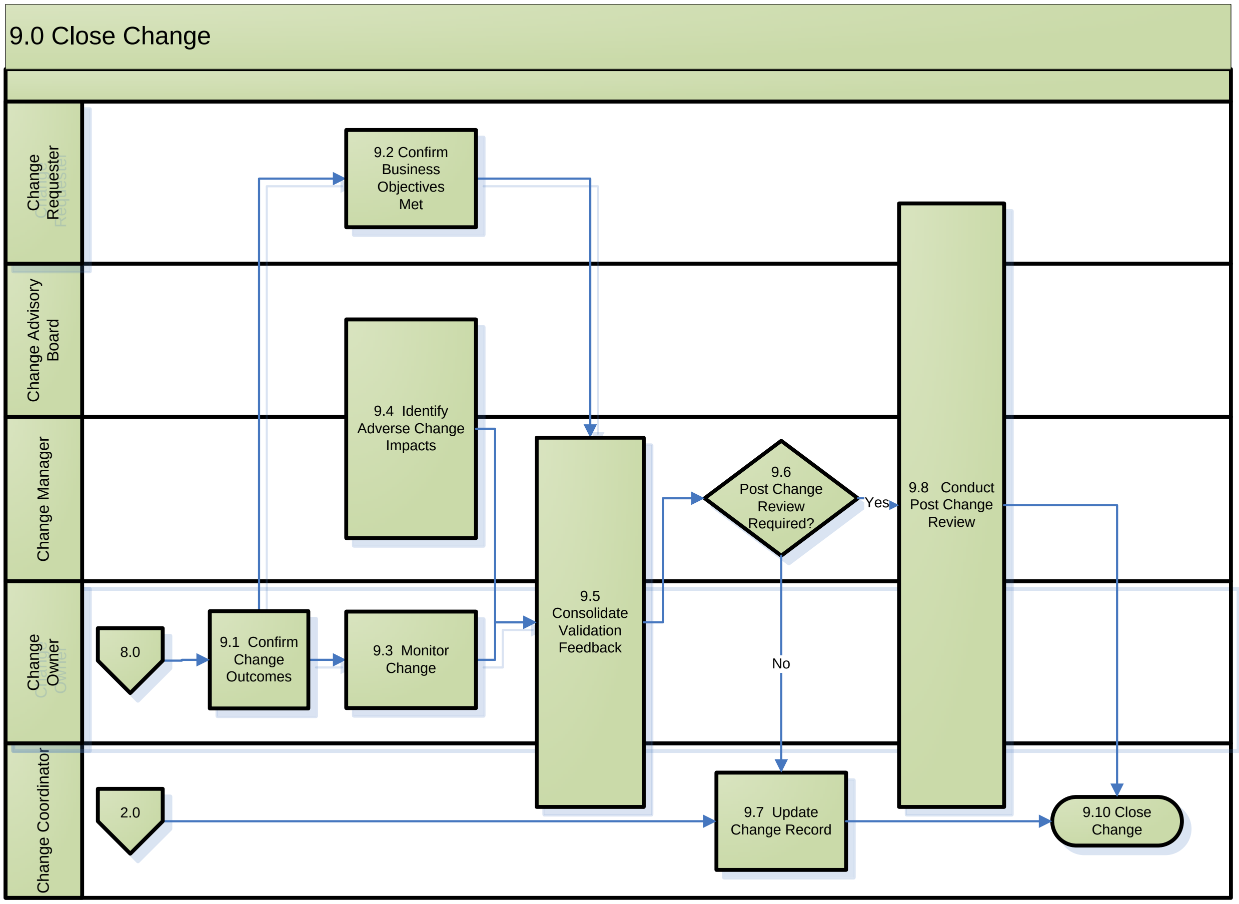

8.0 Implement And Validate Change
Change Owner
Change Builder / Implementer
Service Desk / Incident Management
7.0
8.1 Coordinate Implementation
8.2 Perform Implementation Procedures
8.3 Perform Verification Procedures
8.4 Successful Implementation
No
8.5 Minor Defects?
No
Yes
8.6 Backout Change?
No
Yes
Yes/No
8.7 Coordinate Backout
8.8 Perform Backout Procedures
8.9 Perform Backout Validation Procedures
8.10 Successful Backout
Yes/No
No
8.11 Communicate RFC Completion Status
9.0
8.12 Log *Planned Outage* Incident and Associate to RFC
8.13 Log Service Interruption Incident
8.14 Resolve Planned Outage Incident

Step	Activities
8.1 Coordinate Implementation	Confirms that any prerequisite prep work has been performed and implementation resources: • are available at scheduled times • have documented implementation, verification, and backout plans • understand their implementation tasks • are aware of implementation task dependencies • are aware of communication protocols • are aware of change window timelines, backout go/no-go decision point • have necessary parts, files, media • have necessary logical & physical access • if multiple Change Implementers involved ensure a lead is assigned
8.2 Perform Implementation Procedures	Execute Implementation tasks per approved, documented implementation plan. Documents and resolves any minor deviations/corrections in the implementation procedures (eg. Used HTTP-S instead of HTTP). Reports implementation results to Change Owner.

Step	Activities
8.3 Perform Verification Procedures	Execute Verification tasks per approved, documented verification plan and reports verification results to Change Owner.
8.4 Successful Implementation?	Check to see if successfully implemented as planned. If yes, go to "Update RFC Completion Status" and if no, go to "Backout Change?"
8.5 Minor Defects?	If the cause of verification failure is known, and corrective action is minor in scope, the Change Owner may direct Change Implementer to fix the defects and re-conduct verification Testing. The Change Implementer must document any deviations/extra steps performed during this activity. At no time can the corrective action jeopardize the ability to execute the backout plan within the originally approved Change Window.
8.6 Backout Change?	Determine whether the change can/should be backed out or whether it will be left in a partially implemented state. Change requestor/implementers may be consulted to assist in this decision if the direction to contact the Change Requestor is detailed in the change verification/backout plans.
8.7 Coordinate Backout	Communicate backout decision to implementation team Ensures that implementation resources • understand their backout tasks • are aware of backout task dependencies • are aware of communication protocols • are aware of change window timelines
8.8 Perform Backout Procedures	Perform the backout plan and report backout results and any deviations to Change Owner.
8.9 Perform Backout Validation Procedures	Execute validation tasks per approved, documented plan and report results to Change Owner. Document any deviations and send results to the change owner.
8.10 Successful Backout?	Determine whether change appears to have been successfully backed out as planned. If yes, goto "Update RFC Completion Status" and if no, go to "Unsuccessful Change" and also Update the RFC completion status.
8.11 Communicate RFC Completion Status	Change Owner (or delegate) will: • inform Service Desk and other stakeholders of Change completion status., as explicitly described in the Implementation Plan communication protocol. • Update RFC completion codes (Successful or not) • notify Configuration Management to update Configuration Data to reflect the change
8.12 Log Planned Outage Incident and Associate to RFC	Create a Service Outage Incident that serves as the Master Incident linked to the RFC and any incoming incidents can be associated with.
8.13 Log Service Interruption Incident	Contact Service Desk and report Incident associated to RFC and include details in the Incident that describe the deficiencies in the production environment resulting from the partially implemented change (ie. functionality, performance, outage)

Step	Activities
8.14 Resolve Planned Outage Incident	Resolve the Planned Service Outage Incident that was previously created.

9.0 Close Change


9.0 Close Change
Change Requester
Change Advisory Board
Change Manager
Change Owner
Change Coordinator
9.2 Confirm Business Objectives Met
9.4 Identify Adverse Change Impacts
9.5 Consolidate Validation Feedback
9.6 Post Change Review Required?
Yes
No
9.8 Conduct Post Change Review
8.0
9.1 Confirm Change Outcomes
9.3 Monitor Change
2.0
9.7 Update Change Record
9.10 Close Change

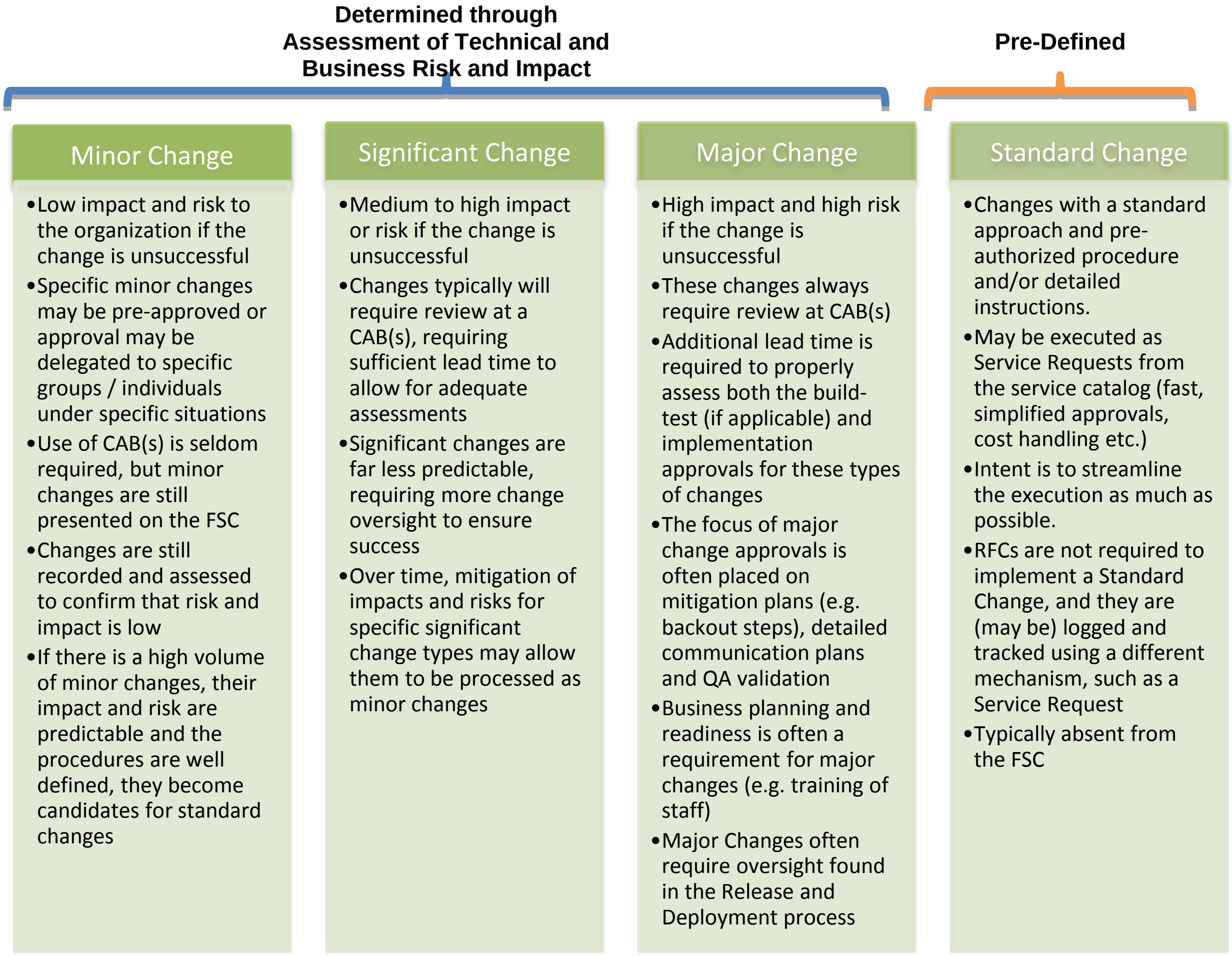
Step	Activities
9.1 Confirm Change Outcomes	Change owner asks Change Requester and impacted jurisdiction CM's to validate the change success from their perspectives.
9.2 Confirm Business Objectives Met	Change Requestor uses Validation criteria to confirm that requested business objectives were met.
9.3 Monitor Change	Determine if any adverse affects resulted from Change that were not encountered during verification testing . If related issues exist, Incidents should have been reported
9.4 Identify Adverse Change Impacts	Determine if the change introduced adverse service impact on impacted jurisdictions either during the change window (eg. Impact to unintended CI's) or following implementation.
9.5 Consolidate Validation Feedback	Consolidate input received (to be used by PIR). Note that feedback may indicate unacceptable impact, which could lead to logged Incident and subsequent RFC to remediate or backout the change. Set the change closure code with an initial value.
9.6 Post Change Review Required?	Review results from validation task. Use the following criteria to determine if formal PIR should be considered: • Implemented - Without approval • Implemented - Not as planned • Service impact exceeds those approved • Implemented - Partially implemented • Backed out

Step	Activities
	• Urgent Change • Latent Change • Failed Standard Change • Negative indication from Validate task • Business Objectives not met • Incidents from Impacted Jurisdictions
9.7 Update Change Record	Change record is updated accordingly, including the change closure code if necessary.
9.8 Conduct Post Change Review	Summarize post change review details and attach to Change Record. • Analyze Change - perform root cause analysis and determine why change did not meet objectives • Recommend improvements - remedial actions for Change Owner to address root cause, Change Procedure suggestions for Change manager, suggestions for other processes (eg. SDLC) • Distribute PIR Report
9.9 Close Change	Ensure appropriate documentation is attached to RFC (updated IVB instructions, PIR collateral, etc), update RFC State=closed and confirm closure code is populated.

Change Process Components

Change Types

Change types are important as different types may follow slightly different procedures, such as different levels of approval.



Determined through Assessment of Technical and Business Risk and Impact

Pre-Defined

Minor Change

- Low impact and risk to the organization if the change is unsuccessful
- Specific minor changes may be pre-approved or approval may be delegated to specific groups / individuals under specific situations
- Use of CAB(s) is seldom required, but minor changes are still presented on the FSC
- Changes are still recorded and assessed to confirm that risk and impact is low
- If there is a high volume of minor changes, their impact and risk are predictable and the procedures are well defined, they become candidates for standard changes

Significant Change

- Medium to high impact or risk if the change is unsuccessful
- Changes typically will require review at a CAB(s), requiring sufficient lead time to allow for adequate assessments
- Significant changes are far less predictable, requiring more change oversight to ensure success
- Over time, mitigation of impacts and risks for specific significant change types may allow them to be processed as minor changes

Major Change

- High impact and high risk if the change is unsuccessful
- These changes always require review at CAB(s)
- Additional lead time is required to properly assess both the build-test (if applicable) and implementation approvals for these types of changes
- The focus of major change approvals is often placed on mitigation plans (e.g. backout steps), detailed communication plans and QA validation
- Business planning and readiness is often a requirement for major changes (e.g. training of staff)
- Major Changes often require oversight found in the Release and Deployment process

Standard Change

- Changes with a standard approach and pre-authorized procedure and/or detailed instructions.
- May be executed as Service Requests from the service catalog (fast, simplified approvals, cost handling etc.)
- Intent is to streamline the execution as much as possible.
- RFCs are not required to implement a Standard Change, and they are (may be) logged and tracked using a different mechanism, such as a Service Request
- Typically absent from the FSC

Risk and Impact

Risk and Impact analysis is used to determine the type of Change.

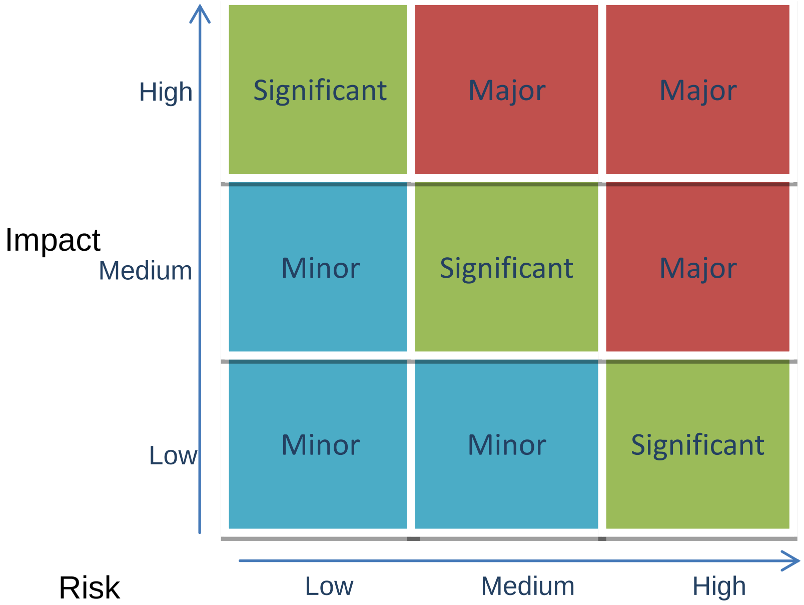
Risk

- Scope: Technical Impact
- Scope: Business Impact
- Readiness: Change Conflicts
- Tolerance / Confidence: Implementation & Backout Plans
- Awareness / Confidence: Service Support Model
- Awareness: Training
- Confidence: New Technology

Impact

- Scope: Impact to Service Availability Awareness
- Scope: Impact to Business Users
- Scope/Awareness: Impact to Business Services
- Tolerance: Impact to Business if Change is Not Implemented
- Confidence/Readiness: Resource Impacts

The following matrix illustrates how the rating of impact and risk results in the Change Type.



Impact			
High	Significant	Major	Major
Medium	Minor	Significant	Major
Low	Minor	Minor	Significant
Risk	Low	Medium	High

Change Source

Incident	• Typically the result of an emergency change where a change to a CI is required to restore service. Sometimes executed prior to a change formally being raised, requiring a latent change to be logged.
Problem	• Changes driven from the problem management process, as a means to remove the problem from the production environment.
Service Modification	• A modification to an existing service, potentially to enhance service.
New Service	• A net new service activation. These types of changes are often classified as major changes.
Decommissioning	• The deactivation of one or more service components
Unauthorized	• The result of an authorized change to a production CI, often recorded as a latent change.
Other	• Any other change source or driver.

Change Submission Priorities

Planned Change	Urgent Unplanned	Urgent Emergency	Latent
• The change has been planned for and is submitted prior to lead time criteria for the applicable change type	• The change does not require emergency change handling however it has been submitted within the lead time criteria for the applicable change type.	• The change requires immediate escalation and approvals, often as a result of an incident during business hours.	• The change has already been executed, either a result of an emergency or to record the details of an unauthorized change.

Assessment Condition Codes

Request for BT CAB Agenda

- A change has been assessed and requires Build-Test approval, and is waiting to be scheduled for an upcoming CAB meeting

Scheduled on BT CAB Agenda

- A change has been scheduled for Build-Test Approval at an upcoming CAB

Request for IMPL CAB Agenda

- A change has been assessed and requires Implementation approval, and is waiting to be scheduled for an upcoming CAB meeting

Scheduled on IMPL CAB Agenda

- A change has been scheduled for Build-Test Approval at an upcoming CAB

<<Blank Value>>

- Change did not require CAB approval (e.g. Minor Change), or the Change Owner is in the process of consolidating assessment feedback

Task Completion Codes

Completed

- The task was successfully completed, and contains details that may aid the change owner (e.g. assessment recommendations, build-test activities completed, implementation successfully executed etc.)

Not Completed (No Impact)

- The task was closed, often due to the result of a completed assessment where no impact was identified, or if other tasks were called off by the Change Owner.

Partially Complete

- The task was partially completed. This is often an indication that the task recipient was unable to fully complete the task objective(s) (e.g. partially completed implemented task).

Approval Condition Codes

Approved Conditionally	•The Change Is approved for Build-Test or Implementation, pending the outcome of some outstanding criteria (e.g. completion of test cases that are currently in-progress)
Approved Release Schedule	•The Change Is approved and will execute against a release schedule, which may include multiple dates where implementation activities will occur
Approved	•The change is approved for Build-Test or Implementation
Exempt	•The change may proceed but is not in-scope for approvals (e.g. regulatory change)
Not Approved	•The change has not been approved **with specific criteria** that, if met, would result in a future approval once addressed (e.g. implementation plan issues that must be addressed)
Advisory	•The change is raised purely for advisory / informational purposes (e.g. Telco planned maintenance that will affect all Telco customers)

Completion / Implementation Codes

Implemented - As Planned	•The change implementation proceeded to plan issues encountered.
Implemented - Not As Planned	•The change was ultimately implemented but with some issues encountered and resolved, or activities that had to be adjusted during the change window (e.g. minor defects).
Implemented – Partially	•The change could not be fully implemented. Some actives were successfully completed.
Not Implemented - Backed Out	•The change could not be implemented and was backed out. Note, the backout may have been unsuccessful as noted in the closure condition codes.
Not Implemented	•The change could not be implemented and was not attempted due to external factors (e.g. implementer was sick, major incident drew resources away from the implementation team etc.).

Closure Condition Codes

Successful

- The change was successful and met the defined business objectives defined by the change requestor.

Partially Successful

- Some aspects of the change were successful and met the business objectives defined by the requestor however, not all outcomes were achieved (e.g. change partially addressed a service degradation incident).

Unsuccessful - Not Backed Out

- The change was unsuccessful but could not be backed out, or the backout attempt failed. This condition often leads to incidents that should be analyzed through problem management. Unsuccessful changes that have no backout opportunity would also take on this closure code.

Unsuccessful - Backed Out

- The change was unsuccessful and the change was successfully backed out.

Cancelled

- The change was cancelled by the change owner at some point in the change lifecycle. This could be the result of budget cuts, changing business needs etc.

Rejected

- While the change may have been successfully validated by a change coordinator, the change does not meet organizational policies for the change process (e.g. a change to business processes, or staffing allocation).

Process Metrics

The following table describes the Incident Management KPIs identified.

KPI Name	ServiceNow Operational Metric / Filters
Ref#: 5 % of RFCs incorrectly classified as emergency RFCs	Changes should never be accepted as emergency if they do not meet emergency change criteria (i.e. to resolve a problem). See proposal for urgent-unplanned below.
Ref#: 9&10 % of RFCs closed by CAB	CAB does not close changes. Recommend KPI *Volume of Implemented Changes*
Ref#: 14 & 15 % of RFCs pending for review by (E)CAB past SLA targets	Recommend against SLA targets
Ref#: 16 Total number of outages during changes	Clarification, is this the same as changes causing an incident where the incidents are major incidents?
Ref#: 17 Total number of failed changes with no backout plan	For discussion – recommend change success rate (all changes should have a backout plan if one is possible)
Ref#: 6 % of problems that generated emergency RFCs	Volume of changes with a problem association + change source = problem + change submission priority = emergency
Ref#: 7 % of RFCs approved by CAB	Change volume where date populated for implementation approval + submission priority ≠ emergency or latent + advisory flag = false
Ref#: 8 % of RFCs approved by ECAB	Change volume where date populated for implementation approval + submission priority = emergency
Ref#: 11 % of unauthorized changes implemented during the period	Volume of Implemented Changes where change source = unauthorized
Ref#: 12 % of RFCs pending for review by CAB	Volume of changes + submission priority ≠ emergency + state=assessed or approved BT + assessment condition code = *scheduled* values
Ref#: 13 % of RFCs pending for review by ECAB	Volume of changes + submission priority = emergency + state=assessed + assessment condition code = *scheduled* values
Ref#: 18 % of changes causing an incident	Volume of incidents associated to problems with an association to changes + change source = problem
Ref#: 22-25 % of changes causing a problem	Changes associated to problems + change priority + problem source = change management
Proposed	Average time to process change (accepted → implemented)
Proposed	Average time to approve change (accepted → approved BT or Impl if BT required = false)
Proposed	Approval backlog (BT and Implementation) + advisory flag = false
Proposed	Change Success Rate (volume of successful changes / unsuccessful changes) + advisory flag = false
Proposed	Volume of urgent – unplanned and urgent – emergency changes + advisory flag = false
Proposed	Volume of rescheduled changes + advisory flag = false
Added in day 3 workshop	# of associated tasks past due date (in the moment) and # of tasks that went past due.

Document History

Version	Date	Changes	Author
01	01/26/2012	Initial Document	Angie Massicotte / Michael Oas
02	01/30/2012	Minor Updates	Michael Oas