

# Change Management Policies and Procedures Guide

## Contents

Executive Summary – IT Change Management Policy .....	2
Objective .....	2
Fundamentals .....	3
IT Change Management Defined .....	3
The IT Change Management Process.....	3
Scope .....	5
In Scope .....	5
Out of Scope .....	5
Workflow Tasks .....	6
Initiating the Change (New Request for a Change) .....	6
Analysis and Initial Approval Phase .....	7
Creating a Request for Change (RFC) .....	8
Assigning the Change Category .....	9
Assigning the Change Priority .....	9
Development Phase .....	10
Developing the Business Case Justification .....	11
Technical Impact Analysis .....	11
Business Risk and Impact Analysis .....	13
Risk Level Based Lead Times .....	16
Lead Time Guidelines .....	17
Developing the Backout Plan .....	17
IT Business Unit Manager Review and Approval .....	17
Testing .....	17
Conducting the Peer Approval .....	17
Change Approval Phase .....	18
Implementation and Documentation Phase.....	19
Final Planning .....	19
Scheduling and Notifications.....	19
Change Implementation .....	20
Testing, Validation, and Acceptance .....	20
Change Review and Acceptance .....	20
Monitor Change in Production Environment .....	21

Hold Post -Implementation Review .....	21
Accept Issues and Continue.....	21
Measuring Quality in the Change .....	22
Change Reports .....	22
Change Compliance .....	22
Roles and Responsibilities.....	22
Change Manager .....	23
Change Administrator.....	24
Change Initiator .....	24
Change Coordinator .....	24
Change Task Assignee or Change Implementer .....	24
Change Management System Administrator .....	25
Change Advisory Board .....	25
CAB Membership .....	25
CAB Meetings.....	26
Voting Rules.....	26
Key Definitions .....	27

## Executive Summary – IT Change Management Policy

Ensuring effective change management is important in ensuring quality delivery of IT services. The intent of this Policy and Procedures Guide is to ensure the effective management of change while reducing risk.

Key components to the company’s Change Management program include:

- **Accurate Documentation** – Identify the information relevant to a specific change that needs to be collected throughout the change management process.
- **Continuous Oversight** – Change Advisory Board (CAB) The CAB is tasked with balancing the need for change with the need to minimize risks.
- **Formal, Defined Approval Process** – All changes will follow the established multiple level approval process to ensure routine changes are completed with minimum restrictions while complex, high impact changes receive the oversight necessary to guarantee success.
- **Scope** – Establish the specific areas that this policy will cover.

## Objective

The primary objective of this document is to provide standardized methods and procedures to meet the change management requirements supporting the company’s operations. The business processes detailed in this document meet the foundation requirements for industry best practices as detailed within the Information Technology Infrastructure Library (ITIL) directly relating to IT change management.

It is important to note that not all the ITIL best practices for IT change management are included in this document.

Following these guidelines will ensure all information technology changes satisfy the Control Objectives for Information and Related Technologies (COBIT) elements related to IT change management. This will ensure the day-to-day IT functions performed to provide effective change management to satisfy including Sarbanes-Oxley corporate governance audit requirements. In addition to meeting all of the audit requirements, these guidelines will provide a process for efficient and prompt handling of all IT changes completed by the IT organization.

#### Key Goals:

- Establish clearly defined best practice processes to ensure compliance with the SOX requirements as measured using standard COBIT measurement elements
- Improve efficiency using automated tools and a centralized data depository
- Improve communication through automated escalations and notifications
- Ensure proper level of approvals
- Reduce risk associated with completing changes
- Reduce the impact of changes on the IT and business organizations

### Fundamentals

This section describes the definition, basic processes, and scope of Change Management for the IT Change Management organization.

#### IT Change Management Defined

IT Change Management is the process of requesting, analyzing, approving, developing, implementing, and reviewing a planned or unplanned change within the IT infrastructure. The Change Management Process begins with the creation of a Change Request within the company's selected technology platform. It ends with the satisfactory implementation of the change and the communication of the result of that change to all interested parties.

#### The IT Change Management Process

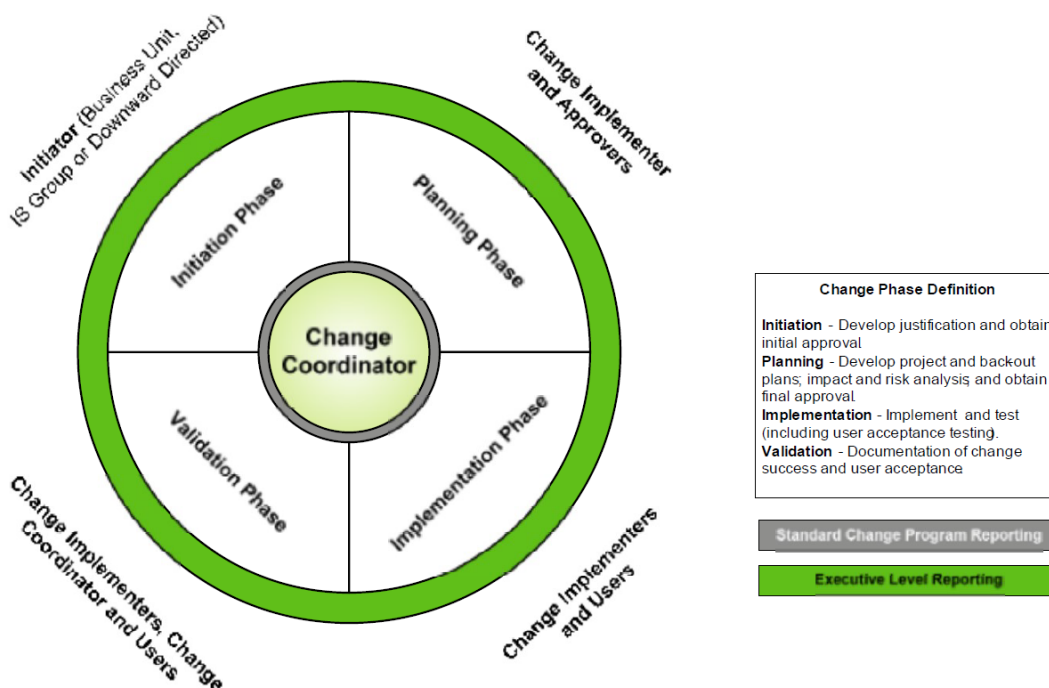
The primary goal of the IT change management organization is to accomplish IT changes in the most efficient manner while minimizing the business impact, costs, and risks. All IT changes within the company will be documented in the company's selected technology platform. To achieve this, the change management process includes the following primary steps (note that all information collected in the steps below is documented in a Change Record created in the company's selected technology platform):

- **Formally Request a Change.** All requests for change will be documented within the company's selected technology platform by creating a new change record. The completion of a new request for change will be completed by the Change Coordinator with input from the Change Requester.
- **Categorize and Prioritize the Change.** The Change Coordinator will assess the

urgency and the impact of the change on the infrastructure, end user productivity, and budget.

- **Analyze and Justify the Change.** The Change Coordinator works with the change requester and the change initiator to develop specific justification for the change and to identify how the change may impact the infrastructure, business operations, and budget. The Change Coordinators use this information to further research and develop an extensive risk and impact analysis. When completing the analysis of the change, the Change Coordinator must ensure they consider the business as well as the technical impacts and risks.
- **Approve and Schedule the Change.** The Change Coordinator uses the company's selected technology platform to record an efficient process for routing the Request for Change (RFC) to the Change Coordinator, technical approvers, business approvers and, in the event of a major or significant change, to the Change Advisory Board (CAB) for approval or rejection of the change.
- **Plan and Complete the Implementation of the Change.** This process includes developing the technical requirements, reviewing the specific implementation steps and then completing the change in a manner that will minimize impact on the infrastructure and end users.
- **Post -Implementation Review.** A post-implementation review is conducted to ensure whether the change has achieved the desired goals. Post-implementation actions include deciding to accept, modify or back-out the change; contacting the end user to validate success; and finalizing the change documentation within the company's selected technology platform.

The figure below shows the change management phases.



## Scope

Because the Change Management Process deals with the management of changes in the production environment, it is imperative that both customers and the company's change organization understand the events that are considered within the scope of the process. In this section, the scope is described and includes areas which are both within and outside of the change management process scope.

## In Scope

The intended scope of the Change Management Process is to cover all of the company's or clients computing systems and platforms. The primary functional components covered in the Change Management process include (Note: Following are examples only – your specific areas may differ):

- SDLC – Changes handled through the formal software development life cycle will be included within the company's change management program.
- Hardware – Installation, modification, removal or relocation of computing equipment.
- Software – Installation, patching, upgrade or removal of software products including operating systems, access methods, commercial off-the-shelf (COTS) packages, internally developed packages and utilities.
- Database – Changes to databases or files such as additions, reorganizations and major maintenance.
- Application – Application changes being promoted to production as well as the integration of new application systems and the removal of obsolete elements.
- Moves, Adds, Changes and Deletes – Changes to system configuration.
- Schedule Changes - Request s for creation, deletion, or revision to job schedules, back-up schedules or other regularly scheduled jobs managed by the company's IT organization.
- Telephony – Installation, modification, de-installation, or relocation of PBX equipment and services.
- Desktop – Any modification or relocation of desktop equipment and services.
- Generic and Miscellaneous Changes – Any changes that are required to complete tasks associated with normal job requirements.

## Out of Scope

There are many IT tasks performed at the company, either by the IT department or by the end users that do not fall under the policies and procedures of Change Management. Tasks that require an operational process, but are outside the initial scope of the company's Change Management process includes:

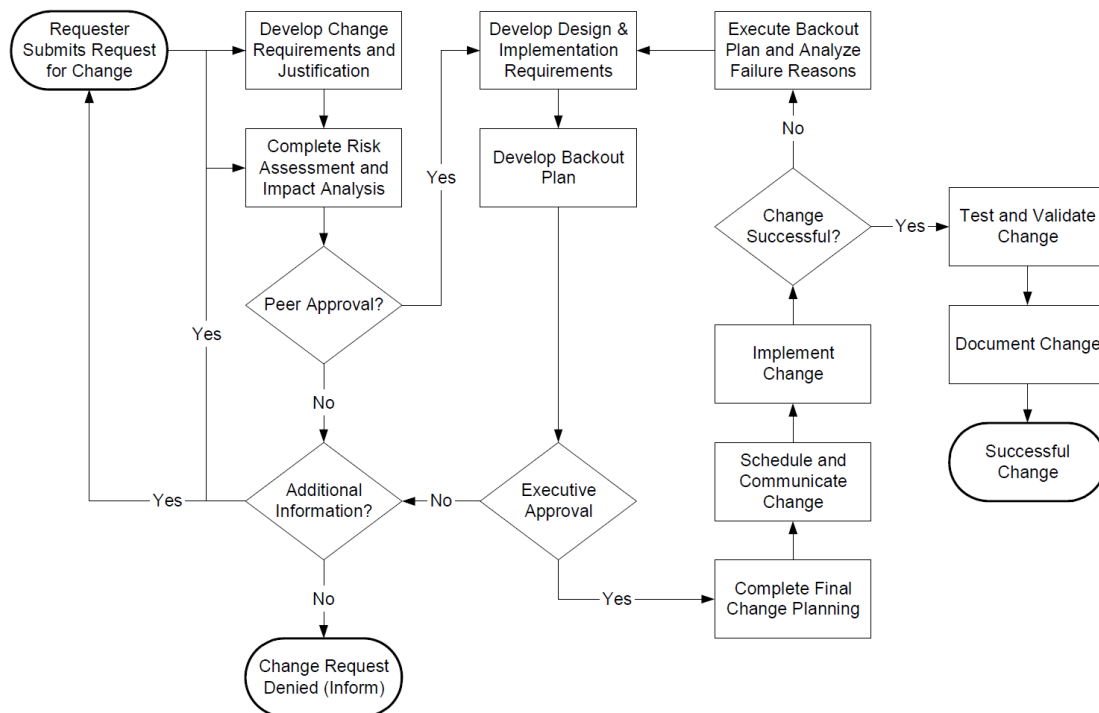
- Contingency/ Disaster Recovery
- Changes to non-production elements or resources
- Changes made within the daily administrative process. Examples of daily administrative tasks are:

- Password resets
- User adds/ deletes
- User modifications
- Adding, deleting or revising security groups
- Rebooting machines when there is no change to the configuration of the system
- File permission changes

The Change Advisory Board (CAB) may modify the scope periodically to include items in the scope of the company's overall Change Management process.

## Workflow Tasks

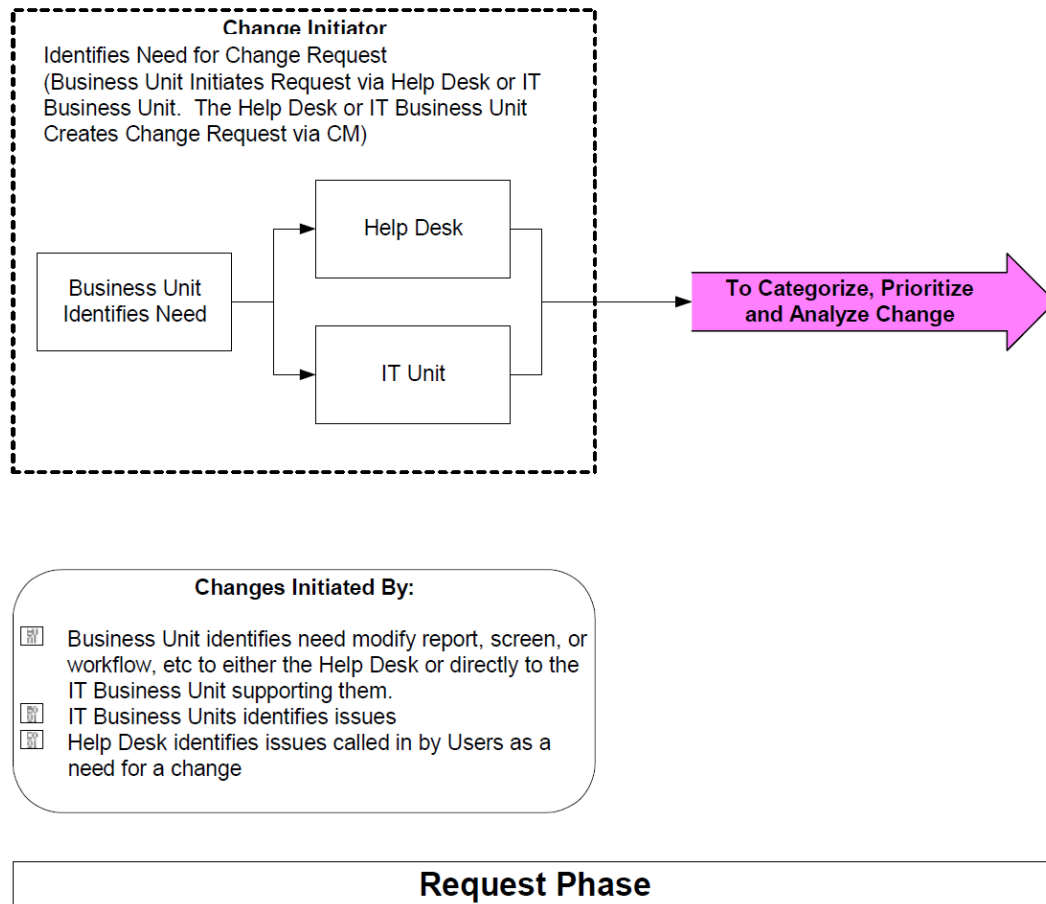
This section describes the basic tasks associated with the Change Management processes for the company. The following diagram provides a high level overview of the workflow for the change management tasks.



**Basic Change Management Workflow**

## Initiating the Change (New Request for a Change)

Within the company, changes are identified by the business unit or help desk within an IT business unit. Anyone identifying a requirement for a change functions as the Change Initiator and is responsible for providing the necessary information to identify the basic requirements associated with the change.



It is critical that the Change Management Process is consistent in quality and completeness and discards irrelevant requests. Although a change request can be submitted by anyone within a business or IT unit, it will receive an initial review by the Change Coordinator within the appropriate IT business unit. Change Initiator's can identify the need for a change through the Customer Help Desk or directly to a Change Coordinator in the IT Business Unit by phone or email. The Change Coordinator will determine if there is sufficient information to create the change request and will create a new change request within the Service Center Change module. They will contact the Change Initiator if additional information is required.

**Note 1:** In the current Customer change process, the IT Business Unit normally initiates changes based on their findings or a conversation with the relevant business unit. In these cases, the person in the IT Business Unit will function in the role of Change Initiator and may also function in the role of the Change Coordinator.

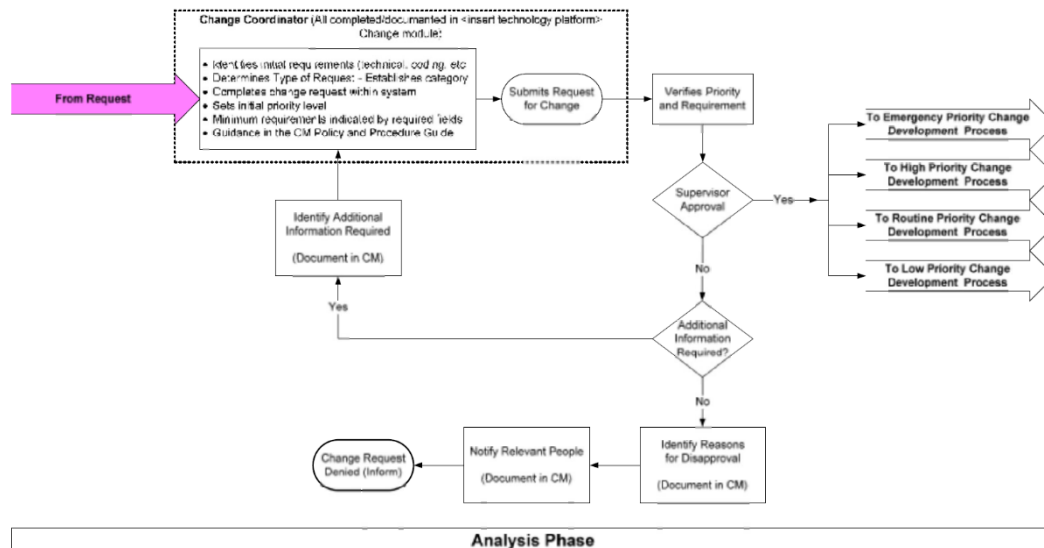
**Note 2:** Future enhancements will provide the ability for Change Initiators to submit an initial request for change using a web based tool.

## Analysis and Initial Approval Phase

During the creation of the new change request, the Change Coordinator will collect additional information to help them further define the change parameters. This additional information includes identifying specific coding or other technical



requirements as well as establishing the initial priority and category. The diagram below shows a more detailed workflow of the analysis phase which includes the actual creation of the change request, establishment of the initial priority level, and the approval at the IT business unit level.



## Creating a Request for Change (RFC)

The Request for Change (RFC) is the standard document created by the Change Coordinator within the company's selected technology platform that captures all the relevant information about the proposed change. This information may range from basic facts about the change to more complex technical specifications necessary to complete the change. The Change Coordinators will work with the Change Initiators to identify as much of the following information as possible:

- The Change Initiator's name and contact information
- The Change Coordinator's name and contact information
- An accurate description of the change required including the specific request, reason the change is required and the required timeframe
- The priority and category of the change based on the information available
- Incident tracking number of any issue that relates to the change
- Description and clarification of any items to be changed, including identification of the Configuration Item if known
- A cost-benefit analysis of the change and budgetary approval, if required
- Business impact and resource assessment
- Location of the release and a suggested implementation plan with timescale
- Impact on business continuity and contingency plans
- Risk involved in making the change



## Assigning the Change Category

The Change Coordinator will initially categorize the Change. The following change categories and subcategories will initially be available:

Category	Sub-Category
Systems - Hardware	Accessories
Systems - Hardware	AS400
Systems - Hardware	Database
Systems - Hardware	Mainframe
Systems - Hardware	Network
Systems - Hardware	Servers
Systems - Hardware	Telco
Production Migration	AS400
Production Migration	Client/ Server
Production Migration	Database
Production Migration	Mainframe
Production Migration	Network
Production Migration	NT Notes
Production Migration	Unix/ Linux

Category	Sub-Category
RFC -	business applications
RFC -	facilities
RFC -	imac
RFC -	network
RFC -	other
RFC -	procurement
RFC -	security
RFC -	service management
RFC -	shared infrastructure
RFC -	telecoms
RFC -	training
RFC -	user admin

Category	Sub-Category
Software	Accounting Apps
Software	Business Planning Apps
Software	E-Commerce Apps
Software	Human Resources Apps
Software	Logistics Apps
Software	Other Database Apps
Software	Other Mainframe Apps
Software	Other Network Apps
Software	Payroll Apps
Software	Purchase Apps
Software	Store Apps
Software	Supply Chain Apps

Category	Sub-Category
SDLC	Accounting Apps
SDLC	Business Planning Apps
SDLC	E-Commerce Apps
SDLC	Human Resources Apps
SDLC	Logistics Apps
SDLC	Other Database Apps
SDLC	Other Mainframe Apps
SDLC	Other Network Apps
SDLC	Payroll Apps
SDLC	Purchase Apps
SDLC	Store Apps
SDLC	Supply Chain Apps

Category	Sub-Category
Systems -	Accessories
Systems -	AS400
Systems -	Database
Systems -	Mainframe
Systems -	Network
Systems -	Servers
Systems -	Telco

Category	Sub-Category
Scheduling	Client/ Server
Scheduling	Database
Scheduling	Mainframe
Scheduling	Network
Scheduling	NT Notes
Scheduling	Unix/ Linux

Additional change categories will be added as the new change forms are created to meet specific business needs.

## Assigning the Change Priority

The Change Management system has been designed to default to a routine priority for the end user community. The Change Coordinator will have authority to adjust the priority level as required to meet the business needs. There are four levels of Change priorities which include:

- Emergency – A change that, if not implemented immediately, will leave the organization open to significant risk (for example, applying a security patch).
- High – A change that is important for the organization and must be implemented soon to prevent a significant negative impact to the ability to conduct business.
- Routine – A change that will be implemented to gain benefit from the changed service.
- Low – A change that is not pressing but would be advantageous.

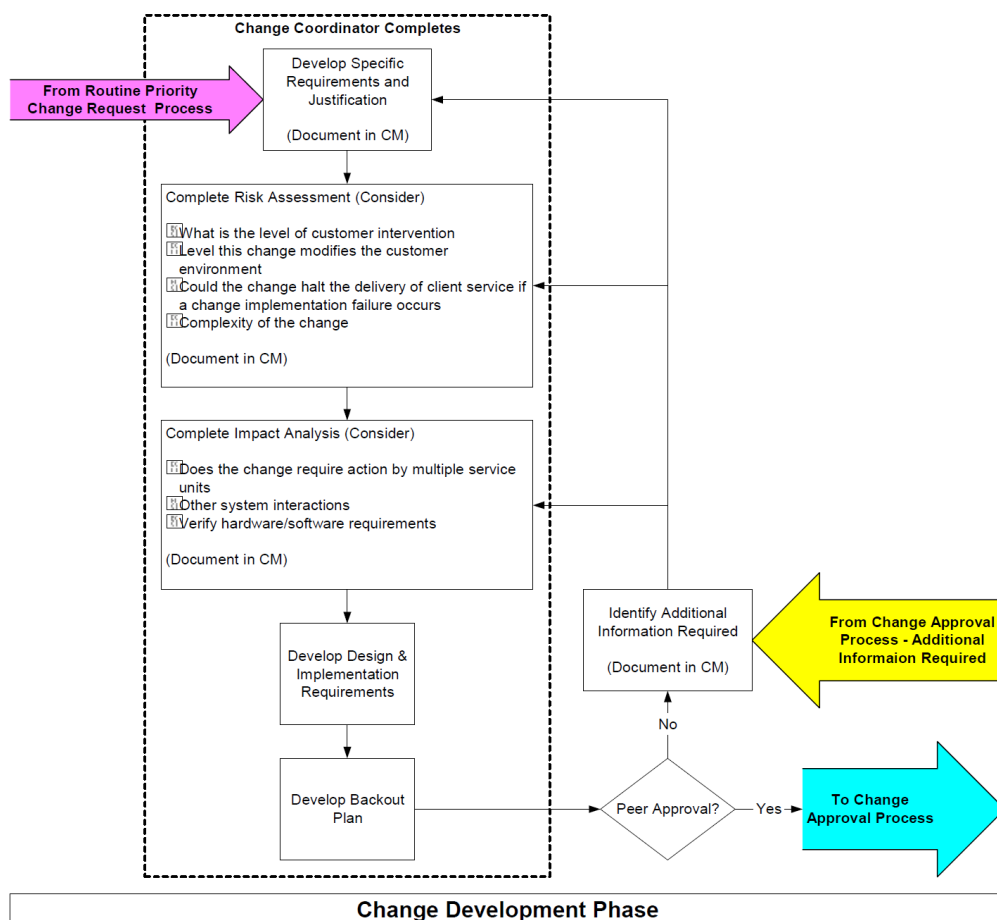
Note: Emergency changes must be kept to an absolute minimum due to the increased risk involved in implementing them.

## Development Phase

The diagram below shows the detailed steps for developing the business case justification, including:

- Completing a risk and impact analysis
- Developing specific change requirements
- Identifying a back-out plan and receiving peer approval

Note that all the information collected during these stages should be documented in the company's selected technology platform.



## Developing the Business Case Justification

For all change categories, the Change Coordinator must develop a Business Case Justification, including the requirements of the change that will be attached to the RFC for consideration in the analysis portion of the process. The business case information is documented in the “Change Description” field within the company’s selected technology platform. The following questions are relevant information that should be addressed during development of the business justification:

- The requirements and detailed description of the change
- Describe the impact the change will make on the business unit’s operation
- Describe the effect the change may have upon the end user, business operation, and infrastructure if known
- Describe the impact on other services that run on the same infrastructure (or on software development projects)
- Describe the effect of not implementing the Change
- Estimate the IT, business and other resources required to implement the Change, covering the likely costs, the number and availability of people required, the elapsed time, and any new infrastructure elements required
- Estimate any additional ongoing resources required if the Change is implemented

## Technical Impact Analysis

This section describes the criteria a technical reviewer must consider when evaluating the technical impact of a change. The technical impact and risk analysis is documented within the company’s selected technology platform module’s “Impact” fields. After the Change Coordinator reviews, categorizes, and prioritizes the RFC, they will assign a resource depending on the type of change and complexity, to perform a technical analysis of the change. This process is intended to evaluate and validate the technical feasibility, risk and effect a change will have on the production environment and end user productivity.

The Technical Approver should consider the following criteria while reviewing any change:

- Evaluate the change plans to gauge the impact and effect of the change during and immediately following the change implementation.
- Review the technical completeness of the change plan, including anticipated assets changed, impact on start-up or shut down of systems, impact on disaster recovery plans, back-up requirements, storage requirements, and operating system requirements.
- Evaluate the technical feasibility of the change and the whole impact of the change in terms of:
  - Performance
  - Capacity
  - Security

- Operability
- Validate technical aspects, feasibility, and plan.

After the technical impact assessment is complete, the reviewer must assign a technical impact level to the change. The technical impact levels are described in the sections below.

- Low – For routine categories, the technical impact default is low. If the evaluation of the technical impact corresponds with the criteria below, the technical impact will be designated as “low.” The technical impact criteria include:
  - Involves IT resources from one workgroup within same IT division
  - Low complexity – no technical coordination required
  - Low risk to system availability (system/ service outage affecting clients during Non-Prime Time)
  - Easy implementation and back-out
  - No impacts to service level agreements
- Medium – The components of a medium technical impact include:
  - Involves IT resources from more than one workgroup within same IT division
  - Significant complexity – technical coordination required from one or more functional groups
  - Moderate risk to system availability (system/ service outage exposure during Prime/ Peak Times, outage primarily expected during Non-Prime Time)
  - Some complexity to implementation and back-out plans, back-out not expected to extend the window timeframe
  - Affects application, data or server security
  - Impacts service level agreements (e.g. Business Non-Prime Time) and internal support required
- High – A technical impact is classified as high if the following criteria apply to the change:
  - Involves IT resources from more than two workgroups, crosses IT divisions
  - High complexity – complex technical coordination required with one or more functional groups
  - High risk to system availability (system/ service outage expected during Prime/Peak Times)
  - Complex implementation and back-out plans, back-out likely to extend the window timeframe
  - Affects security of data on infrastructure
  - Impacts service level agreements (e.g. Business Prime/Peak Time)
  - Outside vendor support is typically required

## Business Risk and Impact Analysis

This section details the potential infrastructure and business risks and impacts associated with a change, and the criteria necessary to assign a risk level to a change. The Change Coordinator works with the business units closely associated or impacted by the proposed change to conduct a business risk and impact analysis. The business risk and impact analysis is completed when a new change record is created. The business risk and impact process evaluates the impact of the change as it relates to the ability of the company to conduct business. The key objective is to confirm that the change is consistent with current business objectives. The following points should be considered while performing the business risk and impact assessment:

- Evaluate business risk/ impact of both doing and not doing the change
- Analyze timing of the change to resolve any conflicts and minimize impact
- Ensure all affected parties are aware of the change and understand its impact
- Determine if the implementation of the change conflicts with the business cycle
- Ensure current business requirements and objectives are met.

When the Change Coordinator analyzes the change, they have the responsibility of initially assigning a risk level for all categories. Risk levels have been established based on the answers to the following questions:

### Customer and/or Client Impact

- o High (4) – Impacts several internal and/ or external customers, major disruption to critical systems or impact to mission critical services.
- o Moderate (3) – Impacts several internal customers, significant disruption to critical systems or mission critical services.
- o Low (2) – Impacts a minimal number of internal customers, minimal impact to a portion of a business unit or non- critical service.
- o No Risk (1) – No impact to internal customers, as well as no impact to critical systems or services.

### IT Resource Impact

- o High (4) – Involves IT resources from more than two workgroups and crosses IT divisions or involves expertise not currently staffed.
- o Moderate (3) – Involves IT resources from more than two workgroups within the same IT division or involves expertise that has limited staffing.
- o Low (2) – Involves IT resources from one workgroup within same IT division.
- o No Risk (1) – Involves a single IT resource from a workgroup.

### Implementation Complexity

- o High (4) – High complexity requiring technical and business coordination.
- o Moderate (3) – Significant complexity requiring technical coordination only.
- o Low (2) – Low complexity requiring no technical coordination.
- o No Risk (1) – Maintenance type of change

### Duration of Change

- o High (4) – Change outage greater than 1 hour and affecting clients during Prime/ Peak times. Lengthy install and back-out.
- o Moderate (3) – Change outage less than 1 hour during Prime/ Peak times or greater than 1 hour during Non-Prime times.
- o Low (2) – Change outage less than 1 hour during Non-Prime times and affecting clients during Non-Prime times.
- o No Risk (1) – No outage expected.

### Security

- o High (4) – Affects critical data or server security and the back-out would likely extend the window timeframe.
- o Moderate (3) – Affects non-critical data or server security and has a moderate back-out plan which would not extend window timeframe.
- o Low (2) – No security issues and easy back-out plan.
- o No Risk (1) – No back-out plan needed.

### Service Level Agreement Impact

- o High (4) – Impacts SLA during business Prime/ Peak times.
- o Moderate (3) – Impacts SLA during business Non-Prime times.
- o Low (2) – Little measurable effect on SLA times.
- o No Risk (1) – No effect on SLA times.

RANGE	RISK
24 – 19	High
18 – 11	Moderate
12 – 7	Low
6 – 1	No Risk

### Approvals Required for Change Based on Risk Level

Required approvals are based on the Change Category, Risk Level and the Priority. The required approvals are shown in the table below. The Peer Review approvals are conditional depending on the response to the question, “Peer Reviewer Requested?”

Change Category	Risk Level	Priority			
		Emergency	Urgent	Routine	Low
Production Migration	No Risk	Assignment group	Assignment group	Assignment group	Assignment group
	No Risk	Mgr of Assignment group	Mgr of Assignment group	Mgr of Assignment group	Mgr of Assignment group

		Priority			
Change Category	Risk Level	Emergency	Urgent	Routine	Low
Hardware	High	Assignment group based on subcategory, Peer Review, CAB	Assignment group based on subcategory, Peer Review, CAB	Assignment group based on subcategory, Peer Review, CAB	Assignment group based on subcategory, Peer Review, CAB
	Moderate	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review
	Low	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review
	No Risk	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review

		Priority			
Change Category	Risk Level	Emergency	Urgent	Routine	Low
Software	High	Assignment group based on subcategory, Peer Review, CAB	Assignment group based on subcategory, Peer Review, CAB	Assignment group based on subcategory, Peer Review, CAB	Assignment group based on subcategory, Peer Review, CAB
	Moderate	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review
	Low	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review
	No Risk	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory	Assignment group based on subcategory, Peer Review

		Priority			
Change Category	Risk Level	Emergency	Urgent	Routine	Low
Retail Systems	High	Assignment group based on subcategory, Peer Review, CAB	Assignment group based on subcategory, Peer Review, CAB	Assignment group based on subcategory, Peer Review, CAB	Assignment group based on subcategory, Peer Review, CAB
	Moderate	Assignment group based on subcategory,	Assignment group based on subcategory,	Assignment group based on subcategory,	Assignment group based on subcategory,



		Peer Review	Peer Review	Peer Review	Peer Review
	Low	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review
	No Risk	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory	Assignment group based on subcategory, Peer Review
Scheduling	High	Assignment group based on subcategory, Peer Review, CAB	Assignment group based on subcategory, Peer Review, CAB	Assignment group based on subcategory, Peer Review, CAB	Assignment group based on subcategory, Peer Review, CAB
	Moderate	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review
	Low	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review
	No Risk	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory, Peer Review	Assignment group based on subcategory	Assignment group based on subcategory, Peer Review

## Risk Level Based Lead Times

It is essential that requests for change are submitted and approved in a timely manner. This will allow completion of accurate documentation, change processing and obtaining the approvals in sufficient time prior to the requested implementation date.

Lead times are the number of days an action (Initiation or Approval) must be completed prior to the requested implementation date. The number of days will vary, depending on the priority and the risk level.

		Lead Time by Change Phase	
Priority	Risk Level	Initiation	Approval
Emergency	High	3	3
	Moderate	2	2
	Low	1	1
	No Risk	1	1
Urgent	High	6	3
	Moderate	4	2
	Low	2	1
	No Risk	1	1
Routine	High	20	10
	Moderate	15	7
	Low	10	5
	No Risk	5	3
Low	High	25	15

	Moderate	20	10
	Low	15	7
	No Risk	10	5

## Lead Time Guidelines

It is essential that requests for change are submitted and approved in a timely manner. This will allow completion of accurate documentation, change processing and obtaining the approvals in sufficient time prior to the requested implementation date, and provide for conflict resolution for scheduling of changes.

Lead times are the number of days an action (Initiation or Approval) must be completed prior to the requested implementation date. The number of days may vary depending on the priority and the risk level. The Risk Worksheet which is required to be completed for each change will assist Change Initiators to determine risk potential. Preferably, high risk and/ or large change requests should have several weeks (or even months) notice prior to the requested implementation date. Lead Times for each change will vary depending on the type of change. Change Initiators should plan lead times to allow sufficient time for planning, review, and approval. In some cases, lead times would also need to be planned to allow for standard implementation times that have been set for certain processes like the SDLC Approval process.

## Developing the Backout Plan

Development of the back-out plan is essential to ensuring effective recovery in the event of a failed change. The back-out plan is primarily based on the technical impact analysis and the implementation plan.

## IT Business Unit Manager Review and Approval

Following the submission of the new RFC, it will be screened by the IT business unit manager who determines whether to authorize or deny the change based on the information in the new change record. This screening process includes a reality check to ensure that the RFC is appropriate, and to ensure the request is complete. The manager can elect to approve, deny or request additional information from the change initiator. The Change Initiator is notified of the progress of their request at all stages.

## Testing

All change categories will undergo some level of testing depending on the complexity of the change. Once the change is built, configured and integrated in the development environment, the change is moved to the Test/ QA environment. This phase focuses on conducting testing and quality assurance to ensure reliability and performance of all components of the organization's technology infrastructure. The Change Coordinator will oversee the testing function, develop the test plan and report its findings back to the CAB for voting on whether to advance the change to the next step.

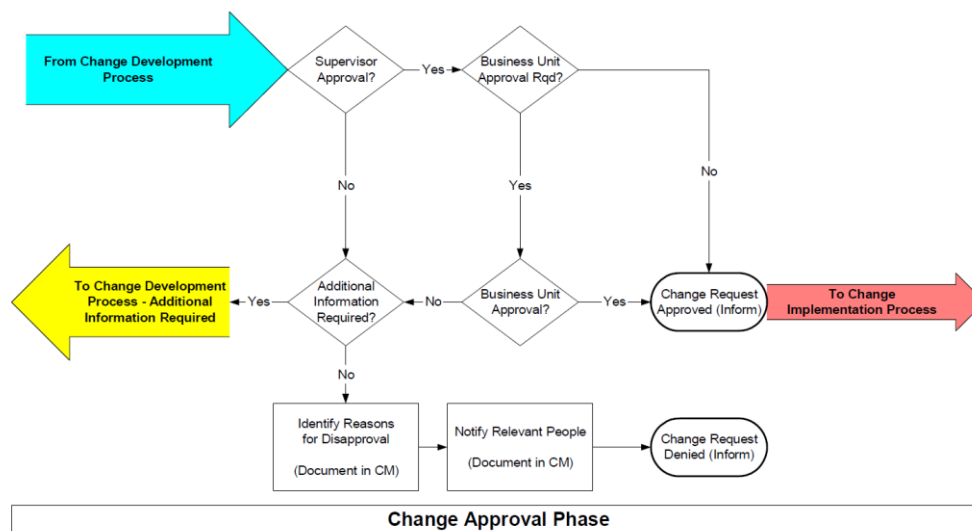
## Conducting the Peer Approval

Peer approvals are the last step of the Change Development Phase. Peer approvals are optional for all changes completed by a customer IT business unit. This step ensures that all the technical components and notifications have been completed as

required by the Change Advisory Board. This approval can be completed by anyone approved by the IT business unit manager and identified as a Peer Approver in the company's selected technology platform. Peer approvals are completed using a checklist which is attached to the change record.

## Change Approval Phase

After a minor, major or significant change has been correctly prioritized, categorized, and analyzed by the Change Coordinator and been through the Peer Review process, the change must be authorized for implementation. The diagram below identifies the workflow associated with change management approval at the company:



The process of authorizing a change request depends upon the category and priority of the change and will be handled in the following manner:

- Emergency priority changes are escalated to the appropriate IT business unit manager for fast-track approval. All emergency changes will be entered the company's selected technology platform (after the fact) and tracked by the CAB.
- Routine changes are approved by the appropriate IT Business Unit Manager and progress directly to the change implementation phase.
- Minor changes can be approved by the Change Coordinator or the appropriate IT Business Unit Manager or appropriate peer approval.
- All other major and significant changes must be approved by the established approval authority as identified in the change record. Approval authority level is dependent on the change category.
- Changes that are maintenance types of changes, usually within the operations and systems support areas, can be approved at the manager level, but will usually involve a peer review only.

In each case, the appropriate person or body decides on whether the change should be implemented based on the information supplied in the RFC.

If the RFC is rejected, the RFC is closed and the Change Initiator is informed of the

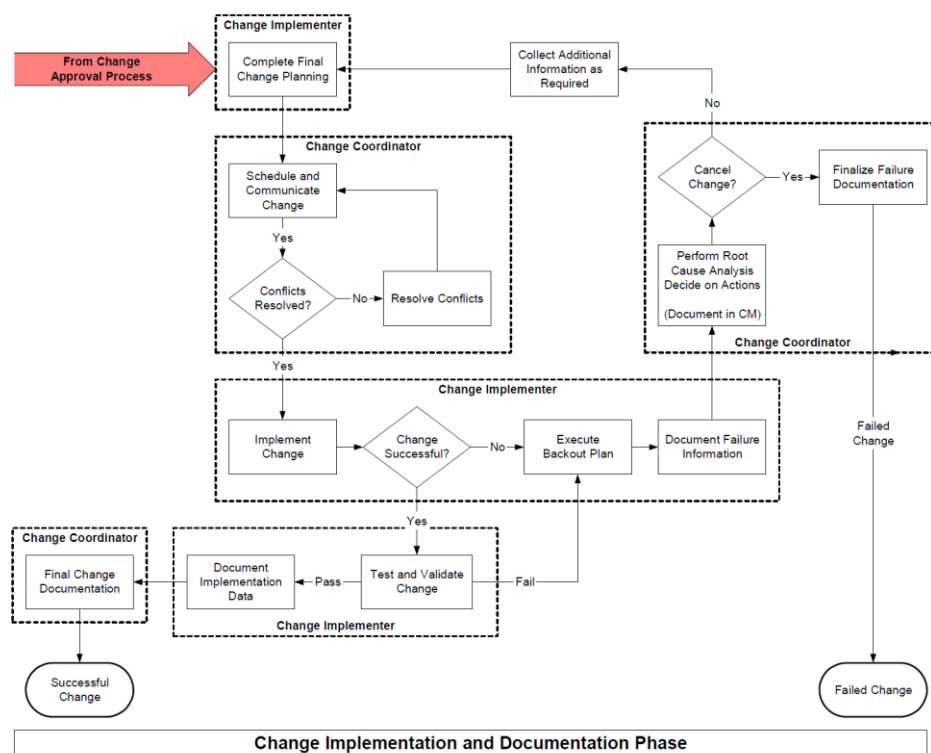
decision. The reasons for the rejection are added to the change record.

## Implementation and Documentation Phase

Once an RFC is approved, it moves into the Implementation and Documentation Phase. This phase is concerned with the steps necessary to successfully implement the change:

- Complete final planning
- Establish the schedule and complete required notifications
- Complete the change implementation
- Test, validate and accept the change
- Complete final change documentation

The diagram below shows the steps and workflow associated with completing the change:



## Final Planning

During this step the Change Coordinator reviews all comments and recommendations to ensure all required tasks have been completed. They conduct this review with the IT business unit manager, the change implementer and the change initiator. This phase is also used by the change implementer to complete any final change development necessary to complete the implementation

## Scheduling and Notifications

The Change Coordinator establishes the appropriate schedule for the

implementation of the change. The schedule is based on several factors including the change priority, other changes being implemented, and system availability. Once the schedule has been established the Change Coordinator ensures the change is noted on the consolidated change schedule and notifies all interested parties of the pending change.

### Change Implementation

The Change Implementer implements the change in accordance with the implementation plan and during the scheduled time. This is generally a technical implementation. Failure of an implementation at this level will normally require the Change Implementer to follow the back-out plan to ensure normal system operations. Significant changes within the environment that require a major program development effort will follow the guidelines established in the SDLC document and established Customer Project Management procedures. In general, these include the following requirements which all change implementations must follow:

- Developing an implementation project plan
- Verify testing was successful
- Applying the change to production
- Validating the change in production
- Resolving problems caused by the change
- Writing a summary of the results
- Updating the Change Management application with results of the implementation

### Testing, Validation, and Acceptance

Once a change has been implemented, the IT Business unit responsible for the change and end users who will be using the change will conduct testing following the test plan developed during the change development phase. Accurate documentation and analysis of any abnormalities is documented in the change record.

The Change Coordinator or the CAB designee will rate the change with one of the following ratings.

- Acceptance— with no comments
- Acceptance— with minor exceptions (note that these exceptions will either be fixed under the current change or may require the creation of another new change)
- Rejection— normally used only if the implemented change doesn't meet the required business needs. This results in a failed change determination and must be thoroughly reviewed to identify the root cause of the failure. This will normally result in the creation of a new change request.

### Change Review and Acceptance

Following a successful change implementation, a change review must be conducted to determine if the change resulted in the desired outcome. In most cases, this review process might be very brief. For a routine change, where the

effect has been small and the results relatively predictable, the review process will be limited to checking that the change has provided the user with the desired functionality.

### Monitor Change in Production Environment

To determine whether the deployed change has been effective, it is necessary to monitor the changes in the production environment. For a small change, this may consist of checking on the desired functionality. For larger changes, it might require the monitoring of network and server information, performance data, event logs, or response times. Several different tools and technologies are available for monitoring a change in the production environment. The actual tools used will depend on the nature of the change, the components of the IT infrastructure that are affected, and the skills and experience of personnel performing the monitoring activity. The Change Coordinator will typically determine the best tool needed based on the specific change.

### Hold Post -Implementation Review

The Change Coordinator is responsible for ensuring that a post-implementation review is completed and presented to the CAB. The findings of the post implementation review are documented within the company's selected technology platform record. After sufficient information has been gathered from monitoring to determine the effectiveness of the change, a post-implementation review is held.

The CAB Chairperson or Change Coordinator will schedule and moderate the review meeting for large changes. During the review, reference must be made to the original RFC, which states the objectives of the change and offers some measurable indicators for gauging the effectiveness of the change. The measured effects of the change can be compared with the desired effects to decide whether the change has met its objectives.

In addition to making a success or failure decision on the change implementation, the review will also consider how the change was deployed, and whether it was implemented on time and on budget. This exercise will result in the documentation of lessons learned from the change. Review feedback is then distributed to all parties involved in the change to encourage and enable future process improvements.

### Accept Issues and Continue

Even if a change has not fully met the desired objectives for the change, the review may still determine that the change should not be backed out and that it is not desirable or cost-effective to make more changes. Instead, there may be options available to work around the shortcomings of the system. Such workarounds should be documented. If they are user workarounds, the service desk should be informed so that the information can be easily made available to the users. If the workaround is an additional manual process that some IT staff needs to take, then they should be so informed.

In this case, the change log is updated with the reasons to accept the change and any workarounds that are implemented. The Change Initiator and other interested parties are informed and the RFC is closed.

## Measuring Quality in the Change

Reports from the company's selected technology platform will provide meaningful and concise information about past and current changes. This information will permit the evaluation of the impact of changes, dependencies, and trends.

## Change Reports

NOTE: These are currently recommended reports that should be developed. This section will need revision at semi-annual intervals. The Change Management Reports include:

- Reasons for Change (user requests, emergency, enhancements, business requirements, service call/ incident/ problem fixes, procedures/ training improvement, etc.)
- Number of successful changes
- Number of failed changes
- Number of changes backed-out, together with the reasons (e.g. incorrect assessment, bad build)
- Number of Incidents traced to the change and the reasons
- Number of RFCs (and any trends in origination)
- Number of implemented changes reviewed, and the size of review backlogs
- Data from previous periods (last period, last year) for comparison
- Number of RFCs rejected
- Number of changes per category

The above reports can be used as a basis for assessing the efficiency and effectiveness of the Change Management process.

## Change Compliance

This section describes the activities necessary for the Change Organization to audit their effectiveness of change. The Change Manager will conduct an annual audit that will include an examination of the following items:

- CAB minutes and Forward Scheduling Calendar (FSC)
- Review records for random RFCs and implemented changes
- When review and analyze Change Management reports based on the following criteria:
  - All RFCs have been correctly logged, assessed and executed
  - FSC has been adhered to, or there is a good reason why not
  - All items raised at CAB meetings have been followed up and resolved
  - All Change reviews have been carried out on time
  - All documentation is accurate, up-to-date and complete

## Roles and Responsibilities

Roles associated with the Change Management process are defined in the context of the management function and are not intended to correspond with organizational job



titles. Specific roles have been defined per industry best practices. In some cases, many persons might share a single role; and in other cases, a single person may assume many roles. The significant roles defined for the change management process are:

- Change Manager
- Change Initiator
- Change Coordinator
- Change Task Assignee or Change Implementer
- Change Management System Administrator

Committees are also defined in terms of the roles they play and the responsibilities they have in the context of the change management function. At a minimum, there are normally at least two committees established: The Change Advisory Board (CAB) and the Change Advisory Board Emergency Committee, which typically have management responsibilities for the change management process.

### Change Manager

The Change Manager is responsible for managing the activities of the change management process for the IT organization. This individual focuses on the process more than on any individual change. However, the Change Manager is involved in every step of the process – from receipt of an RFC to the implementation of the change in the IT environment. The Change Manager is ultimately responsible for the successful implementation of any change to the IT environment. The Change Manager's responsibilities include:

- Receiving RFCs and ensuring that they are properly recorded in the change management system technology platform.
- Selecting CAB members and facilitating CAB meetings jointly with the CAB Chairperson. Note that the Change Manager may initially serve as the CAB Chairperson.
- Preparing CAB meeting agendas and providing all necessary review information to the CAB members prior to the meetings.
- If necessary, assigning teams to conduct RFC impact analyses and risk assessments.
- Analyzing and prioritizing RFCs.
- Categorizing, assigning change Coordinators, and scheduling RFCs, subject to approval by the CAB.
- Approving requests for minor changes or assigning approval authority to others.
- Providing change notification to the Change Initiator and other affected parties.
- Monitoring the successful completion of all RFCs, including the change development project phases and ensuring that these processes follow the change schedule.
- Reviewing and evaluating the change process.

## Change Administrator

The Change Administrator directly supports the change manager and is responsible for all the administrative functions associated with the Change Management program. These duties include maintaining the CAB meeting schedule as well as preparing the agenda; publishing any reports required for the meeting, and publishing the CAB meeting minutes; updating the policies and procedures guide as required by the Change Manager; and assisting with the publishing of any change management reports required to support business management and the CAB.

## Change Initiator

The Change Initiator (normally someone within the IT Business Unit) originates changes by submitting a Request for Change (RFC) to the Help Desk or the Change Coordinator in the appropriate IT Business unit. Everyone is authorized to initiate an RFC. The Change Initiator is responsible for providing sufficient information on the change that the Change Coordinator can complete the new change form within the company's selected technology platform. This person is notified whether the change was approved and is kept up-to-date on the status of the RFC throughout the change process. The Change Initiator assists the Change Manager and CAB in determining the RFC priority and, after the change, participates in the post-implementation review.

## Change Coordinator

The Change Manager assigns (with the CAB's approval) an individual to be the Change Coordinator for a change - Change Coordinators will be assigned to each IT business unit. The Change Coordinator is responsible for planning and coordinating all the phases of the change from initiation through acceptance and documentation. The Change Coordinator will document all relevant information in the company's selected technology platform.

The Change Coordinator will routinely provide project status feedback to the Change Manager and identify any problems as they arise. The Change Coordinator presents all formal updates and proposals to the CAB after the CAB approves the RFC for passage through the various change implementation, review and closure phases.

The Change Coordinator must work with the Change Initiator to ensure that the change meets the Change Initiator's requirements and that it successfully corrects any problems or provides the correct system enhancements intended by the RFC. After implementing the change, the Change Coordinator assists the Change Manager in evaluating the change process as it applies to the change. The Change Coordinator also coordinates and presents the post-implementation review analysis to the CAB.

## Change Task Assignee or Change Implementer

Change Task Assignees are responsible for executing individual tasks within a change and ensuring they are completed per the implementation plan. For example, the technician who performs the actual upgrade of the operating system would complete the tasks associated with completing the upgrade.

The Change Coordinator when developing the planning and implementation tasks will assign the appropriate Change Task Assignee to perform the tasks required to plan and implement the change. (Note: When using a standard change category established technology platform, the tasks and Task Assignees are already identified. The Change Coordinator can make modifications as required to meet specific requirements.)

### Change Management System Administrator

The Change Management System Administrator is responsible for modifying and maintaining the company's selected technology platform, including the development and administration of the Change Management reports.

### Change Advisory Board

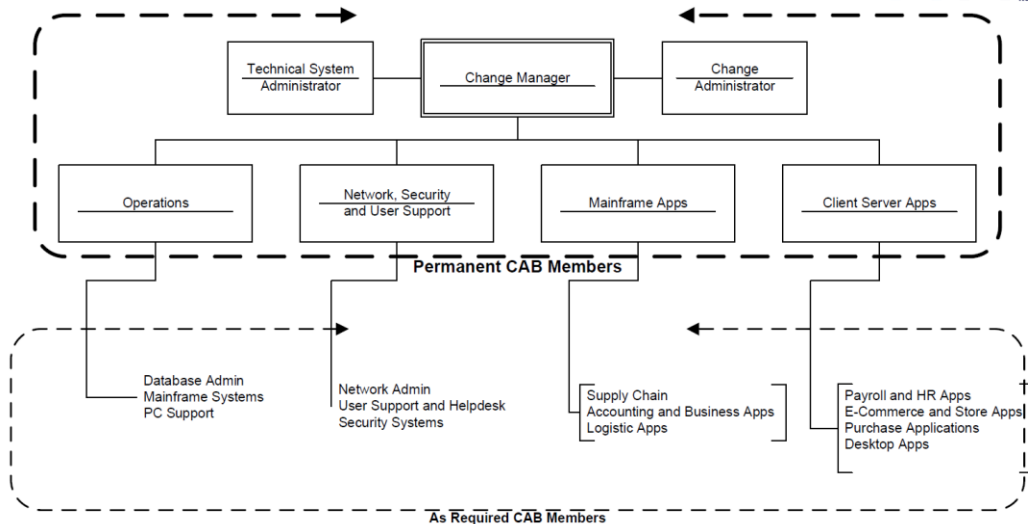
The Change Advisory Board (CAB) is the change management decision-making authority for the IT organization. The primary responsibilities of the CAB are to:

- Establish and manage overall change management policies and provide guidance
- Oversee the Scheduling Calendar (this is a report generated from within the company's selected technology platform)
- Review and approve all pending requests for high-risk and high-impact changes (The CAB may grant approval authority at levels lower than the CAB)
- Review completed changes and make recommendations for approval
- Appoint people to key roles within the Change Management program

### CAB Membership

The CAB is made up of individuals with stakeholder interest in the IT production environment. Since RFCs can impact any part of IT and any organizational group, the makeup of the CAB reflects the focus of the RFC being reviewed. In general, the CAB is composed of individuals who have a wide range of expertise and are familiar with business requirements, the user community, and IT system technology.

The organization chart below shows the general structure of the Customer Change Advisory Board:



It's important to note that additional CAB members may be required per the RFCs being considered and if necessary may include input from security, services, vendors and customer user groups. The CAB Chairperson, will make these decisions and notify resources if they need to attend the regularly scheduled CAB or an emergency session.

## CAB Meetings

The CAB is scheduled to hold an extensive meeting monthly with update meetings held on a weekly basis or as required. The monthly and weekly meetings will provide an overall review of the technical and business impact, prioritization, approval, and scheduling of pending RFCs. The monthly meetings will also include review of the key change management reports, discussion on the change management program, and a review of any failed changes or changes requiring modifications during the implementation phase to ensure a successful change. A few days before each CAB meeting, the CAB Chairperson will send out a meeting notification and agenda e-mail to all CAB members. The contents of this e-mail include:

- Date, time, and location (if relevant) of the meeting.
- Format of the meeting. As an alternative to holding face-to-face meetings, CAB meetings may be held using a conferencing software or by telephone conference calls. Net Meeting is preferred because it enables CAB members to share documentation and use electronic whiteboards.
- The reviewing order for RFCs (agenda). CAB members may be interested in only a small number of the proposed changes and might join the meeting only when necessary.
- A link to all the RFCs being reviewed at the meeting and a forward schedule of the change calendar for discussion.

## Voting Rules

This section establishes the voting rules for RFCs requiring approval of the CAB. The standard change categories developed and included in the company's selected technology platform include a recommended approval process. If the specific

change being completed does not have established approval requirements, the CAB Chairperson will assign a minimum of two CAB members as the approval authorities for that change. These approval authorities are then added to the RFC documentation in the change record.

## Key Definitions

Key definitions for change management used in this document include:

**Change Advisory Board (CAB)** – The CAB is a cross-functional group set up to evaluate change requests for business need, priority, cost/ benefit, and potential impacts to other systems or processes. Typically, the CAB will make recommendations for implementation, further analysis, deferment, or cancellation.

**CAB Emergency Committee (CAB/ EC)** – This is a subset of the CAB that deals only with emergency changes. It is established to be able to meet on short notice to authorize or reject changes with emergency priority.

**Change** – Any new IT component deliberately introduced to the IT environment that may affect an IT service level or otherwise affect the functioning of the environment or one of its components.

**Change Category** – The measurement of the potential impact a change may have on IT and the business. The change complexity and resources required, including people, money, and time, are measured to determine the category. The risk of the deployment, including potential service downtime, is also a factor.

**Change Coordinator** – The role that is responsible for planning and implementing a change in the IT environment. The Change Coordinator role is assigned to an individual for a change by the Change Coordinator and assumes responsibilities upon receiving an approved RFC. The Change Coordinator is required to follow the approved change schedule.

**Change Requester** – A person who initiates a Request for Change; this person can be a business representative or a member of the IT organization.

**Change Initiator** – A person who receives a request for change from the Change Requester and enters the request for change in the Change Management process; this person is typically a member of the IT organization.

**Change Manager** – The role that has the overall management responsibility for the Change Management process in the IT organization.

**Change Priority** – A change classification that determines the speed with which a requested change is to be approved and deployed. The urgency of the need for the solution and the business risk of not implementing the change are the main criteria used to determine the priority.

**Change Record** – The record within the company's selected technology platform that contains all the information relative to a change. This information includes

justification, risk and impact analysis, approvals, phases, and tasks associated with accomplishing the change.

**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, from an entire system (including all hardware, software, and documentation) to a single software module or a minor hardware component.

**Forward Schedule of Changes (FSC)** – The FSC shows when all changes are to take place within the entire Customer IT infrastructure. This single glance at the change schedule makes it possible to see the available change windows. Scheduling changes against the FSC also ensures that multiple, interdependent changes are not scheduled at the same time.

**Release** – 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.

**Request for Change (RFC)** – This is the formal change request, including a description of the change, components affected, business need, cost estimates, risk assessment, resource requirements, and approval status.