



Process Guide

Change Management

Version: 1.2
CALGARY Release

Table of Contents

1 Introduction	3
1.1 Overview	3
1.2 Process Description	3
1.3 Process Goal	3
1.4 Process Objectives	3
1.5 Relationship with Other Processes	4
1.6 Principles and Basic Concepts	4
2 Process Roles	6
2.1 RACI Matrix	8
3 Change Management Activity Description	10
3.1 Process Overview	10
3.2 Standard Change	12
3.3 Normal Change	15
3.4 Emergency Change	21
4 Process Control	25
4.1 KPIs	25
4.2 Operational Data	25
4.3 Reports and Homepages	25
Appendix A: Diagram Convention	27
Appendix B: Glossary of Terms and Acronyms	28
Appendix C: Standard Change Guidelines	33
Appendix D: Risk Assessment	34
Appendix E: Scheduling Assessment	35
Appendix F: Emergency Change Guidelines	36
Appendix G: Expedited Change Guidelines	37

List of Figures

Figure 1. Process Overview	10
Figure 2. Standard Change	12
Figure 3. Normal Change	15
Figure 4. Emergency Change	21

1 Introduction

The concepts described in this guide are aligned with ITIL 2011 and may reference capabilities that are dependent upon other ServiceNow applications. These references will be noted by *blue italicized font*.

1.1 Overview

A process is defined as a set of linked activities that transform specified inputs into specified outputs, aimed at accomplishing an agreed-upon objective in a measurable manner. The process definition laid out in this document further breaks down these activities into actions and the role(s) responsible for their execution.

This document also describes how ServiceNow supports the change management process with its abilities to manage the creation, assessment, approval, scheduling, and implementation of changes to minimize risk to the IT environment.

1.2 Process Description

A change is the addition, modification, or removal of anything that could have an effect on an IT service. Change management is the process responsible for controlling the life cycle of all changes to minimize the risk of disruption to IT services.

1.3 Process Goal

The goal of the change management process is to enable beneficial changes to be made with minimum disruption to business operations, thus ensuring that the best possible levels of service quality and availability are maintained. This is accomplished through a formal approach that assesses the risk and business continuity, impact, and resource requirements of the change against its realizable business benefits.

1.4 Process Objectives

The objectives of change management are to:

- Respond to the customer's changing business requirements while maximizing value and reducing incidents, disruption, and rework.
- Respond to the business and IT requests for change that will align the services with the business needs.
- Ensure the changes are recorded and evaluated, and that authorized changes are prioritized, planned, tested, implemented, documented, and reviewed in a controlled manner.
- Ensure that all changes to configuration items (CIs) are recorded in the *Configuration Management Database (CMDB)*.

1.5 Relationship with Other Processes

Process	Relation Description	Input	Output
Incident Management	A request for change (RFC) can be initiated when a CI change is required to resolve an incident.	X	
	<ul style="list-style-type: none"> Change management is responsible for keeping the service desk informed of all scheduled changes. Access to recent change information can be used to determine the cause of current incidents. 		X
Problem Management	A RFC is initiated when a CI change is required to remove a detected or known error.	X	
	Problem management is informed of the status and progress of submitted RFCs.		X
Configuration Management	Information from configuration management (CMDB) is used to evaluate the risk and impact of changes to business services or CIs.	X	
	Change management ensures that CI information is updated following a change implementation.		X

1.6 Principles and Basic Concepts

Policies

Policies are formally documented management expectations and intentions that are used to direct decisions and ensure consistent and appropriate implementation of processes, standards, roles, and activities. Policies may also dictate specific tool requirements. Examples of common change management policy topics include:

- Creating a culture of change management across the organization where there is zero tolerance for unauthorized change.
- Evaluating possible risk and performance impact of all changes on the service capability.
- Defining emergency change criteria and authorization requirements.
- Ensuring that changes create business value and that the benefits are measured and reported.
- Segregating duty controls for security and error mitigation.
- Defining change windows – enforcement and authorization for exceptions.

Methods of Raising an RFC

There are several ways to generate a new change record in ServiceNow:

- Create a change manually through the Change application.
- Request a change through the [Service Catalog](#).
- Initiate a change from an [incident](#).
- Initiate a change from a [problem](#).
- Generate a change from a pre-configured inbound email. See [inbound email action](#) in the ServiceNow Wiki for a description of how to utilize this feature.

Configuration Management Interface

The configuration management database (CMDB) supports the change management process by providing reliable, quick, and easy access to accurate configuration information to:

- Perform impact assessment
- Identify high-risk, high-impact CIs
- Identify related CIs that will be affected by the change
- Populate the change record with relevant CI information
- Capture CIs, configuration baselines, and releases
- Link CIs to past changes

A well-planned integration between the configuration management system (CMS) and change management is a best practice that enables optimal process efficiency and effectiveness.

Types of Change Requests

Different types of changes require different levels of process rigor and control. The ServiceNow application provides workflows for three different types of service changes:

- **Standard:** a low risk change to a service or other CI for which the approach is pre-authorized by change management and follows an accepted and established procedure or work instruction. See **Appendix C** for standard change guidelines and considerations.
- **Emergency:** a change that must be implemented as soon as possible to eliminate an error that is negatively impacting the business to a high degree, or could do so in the future. See **Appendix F** for emergency change guidelines and considerations.
- **Normal:** any change that is not a standard or emergency change.

On occasion, there may be a need to implement a change sooner than the normal change approval will permit. Some organizations choose to identify these as an **Expedited** change. See **Appendix G** for details on this additional change type.

Change States

Changes should be tracked throughout their life cycle to support proper handling and reporting. The *state* of a change indicates where it is in relation to the life cycle and helps determine what the next step in the process might be. The typical uses of the workflow state values in the ServiceNow base system are:

- **Draft:** default value upon creation.
- **Review:** planning is complete and the change is under peer review prior to submission for approval.
- **Approval:** the change has been submitted for approval.
- **Scheduled:** the change has been approved and is ready for implementation activity.
- **In Progress:** change implementation activities are in progress.
- **Completed:** the change has been implemented.
- **Closed:** the change record is closed and can no longer be updated.
- **Cancelled:** the change has been closed because it is no longer required.

2 Process Roles

Each role is assigned to perform specific tasks within the process. Within a process, there can be more than one individual associated with each role. Additionally, a single individual can assume more than one role within the process, although typically not at the same time. Depending on the structure and maturity of a process, all roles described may not exist in every organization.

The following table describes the typical roles defined for change management.

Role	Description
Process Owner	<p>A senior manager with the ability and authority to ensure the process is rolled out and used by all departments within the IT organization.</p> <p>Responsible for:</p> <ul style="list-style-type: none"> • Defining the overall mission of the process. • Establishing and communicating the process mission, goals, and objectives to all stakeholders. • Resolving any cross-functional (departmental) issues. • Ensuring consistent execution of the process across the organization. • Reporting on the effectiveness of the process to senior management. • Initiating any process improvement initiatives.

Role	Description
Change Manager	Responsible for: <ul style="list-style-type: none"> Managing the day-to-day activities of the process. Gathering and reporting on process metrics. Tracking compliance to the process. Maintaining the change schedule and projected service outage. Facilitating/leading Change Advisory Board (CAB) meetings. Authorizing Standard change templates/models.
Requester	The person raising the change request. A requestor can be anyone in the organization who needs a change to be made or they may submit change requests on behalf of others.
Change Coordinator	<p>There may be different coordinators for each category of change.</p> Responsible for: <ul style="list-style-type: none"> Reviewing RFC(s) to determine approval based on value to the business, potential risk associated with the implementation (or not) of the change, and the benefits expected to be realized. Performing a risk and impact assessment of submitted RFC and seeking additional information, if needed. Creating any additional tasks that must be performed beyond those identified by the Requester. Coordinating the change build, test, and deployment activities, as appropriate. Participating in the change review prior to closure. Providing expert input at the CAB meetings, as needed.
Change Advisory Board (CAB)	<p>The CAB (typically comprised of representatives from all areas of IT, the business, and possibly 3rd party providers or suppliers) supports the assessment, prioritization, authorization, and scheduling of changes.</p> Responsible for: <ul style="list-style-type: none"> Reviewing and approving RFCs. Reviewing the change schedule and providing information to help identify conflicts or resource issues. Reviewing projected service outages. Reviewing unauthorized and failed changes. Reviewing proposed Standard change templates/models.
Implementer(s)	This role may also be referred to as <i>release packaging</i> or <i>deployment</i> practitioner. Responsibilities of this role include the building, testing and physical deployment tasks associated with approved changes that may be assigned to multiple individuals.

2.1 RACI Matrix

ID	Activities	Change Manager	Change Coordinator	Requester	Change Advisory Board	Emergency Change Advisory Board	Implementer(s)
CHG SC	Standard Change						
CHG SC.1	Access ESS portal or service catalog.			A/R			
CHG SC.2	Select appropriate Standard change.			A/R			
CHG SC.3	Provide requested information.			A/R			
CHG SC.4	Submit request.			A/R			I
CHG SC.5	Enter new date for change.			A/R			
CHG SC.6	Perform assigned task(s).			I			A/R
CHG SC.7	Mark task(s) as completed.			I			A/R
CHG SC.8	Document Necessary Correction(s)			A/R			I
CHG SC.9	Review Comments and Remediate			C			A/R
CHG NC	Normal Change						
CHG NC.1	Create new RFC.			A/R			
CHG NC.2	Document change description.			A/R			
CHG NC.3	Associate affected CI(s).			A/R			
CHG NC.4	Document change, test, and back-out plan.			A/R			C
CHG NC.5	Indicate desired or new change date.			A/R			C
CHG NC.6	Submit the request.		I	A/R			
CHG NC.7	Review RFC.	A/C	R	C			
CHG NC.8	Cancel RFC.		A/R	I	I		
CHG NC.9	Assess RFC.	A	R	I			
CHG NC.10	Request Approval	A	A/R	I			
CHG NC.11	Authorize or reject minor change.	A/C	R	I			I
CHG NC.12	Authorize or reject major or significant change.	A/R	C	I	C		I
CHG NC.13	Coordinate change build and test.	A/C	R	C	I		C
CHG NC.14	Schedule deployment.	A/R	R	C	C		C
CHG NC.16	Coordinate deployment.	C	A/R	C	I		C
CHG NC.17	Conduct post-implementation review.	I	A/R	C	I		C
CHG NC.18	Verify and close RFC.	A/R	R	I	I		C

ID	Activities	Change Manager	Change Coordinator	Requester	Change Advisory Board	Emergency Change Advisory Board	Implementer(s)
CHG EC	Emergency Change						
CHG EC.1	Create New RFC			A/R			
CHG EC.2	Enter planned start/end date and time			A/R			C
CHG EC.3	Document Minimal Change, Test, and Back out Plan			A/R			C
CHG EC.4	Request Approval	I	I	A/R			
CHG EC.5	Assess Emergency Change Request	A/R	R	C			C
CHG EC.6	Convene ECAB	A/R	C	C		I	I
CHG EC.7	Authorize or Reject Emergency Change	A/R	I	I		C	I
CHG EC.8	Coordinate Deployment		A/R	C		I	C
CHG EC.9	Conduct Post Implementation Review	I	A/R	C		I	C
CHG EC.10	Review and Close Emergency Change	A/R	R	I		I	I
	R: Responsible, A: Accountable C: Consulted, I: Informed						

3 Change Management Activity Description

3.1 Process Overview

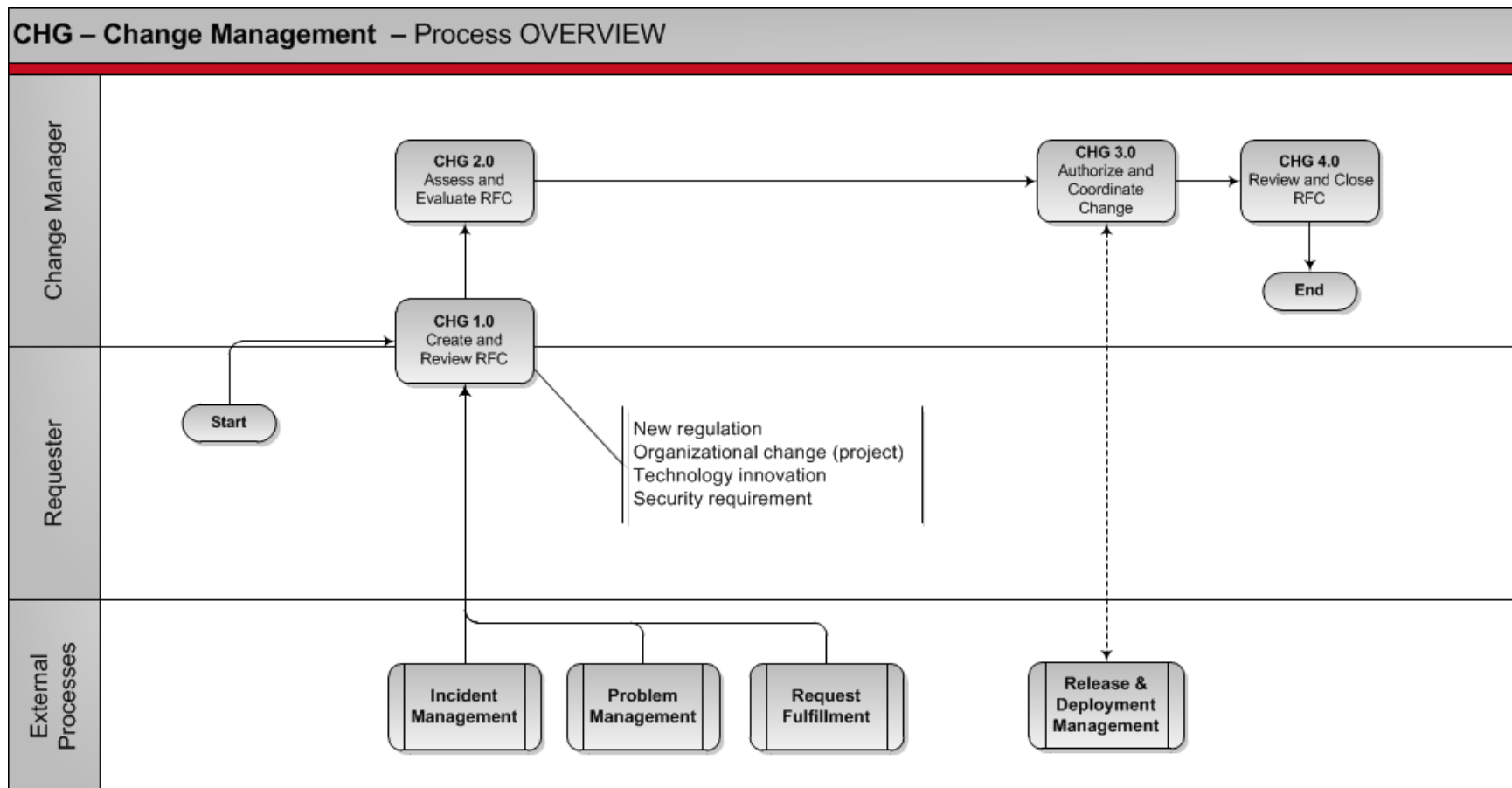


Figure 1.Process Overview

Process Overview Activity Description

ID	Activity	Description
CHG 1.0	Create and Review RFC	During this activity, the RFC is created and all necessary information for its assessment and authorization is captured. Once the information has been captured, the RFC is submitted for review to filter out incomplete, impractical, or duplicate requests.
CHG 2.0	Assess and Evaluate RFC	At this stage, the RFC categorization is validated and detailed risk and impact analysis is performed when necessary. Emergency changes are also identified and the Emergency change procedure initiated.
CHG 3.0	Authorize and Coordinate Change	Necessary approvals must be obtained in order for the change to proceed. For changes requiring build and test, confirmation that the change has undergone and met any testing requirements may be necessary. Once approved, the change is scheduled for implementation. The approved implementation tasks are executed and verified.
CHG 4.0	Review and Close the RFC	Some changes may require a post-implementation review (PIR) to ensure that the change has been implemented successfully and that no unacceptable risks have been identified following the implementation. For minor changes, suitable checks are performed and the change is closed.

CHG Standard Change

	Requester	Implementer(s)
	<pre>graph TD CHG_SC1[CHG SC.1 Access ESS Portal or Service Catalog] --> CHG_SC2[CHG SC.2 Select Appropriate Standard Change] CHG_SC2 -- Draft --> InfoReq{Information Required?} InfoReq -- No --> CHG_SC4[CHG.SC.4 Submit Request] InfoReq -- Yes --> CHG_SC3[CHG SC.3 Provide Requested Information] CHG_SC3 --> CHG_SC4 CHG_SC4 --> Collision{Collision Detector} Collision --> Conflict{Conflict?} Conflict -- Yes --> CHG_SC5[CHG SC.5 Enter New Date for Change] CHG_SC5 --> CHG_SC4 Conflict -- No --> Sched((Scheduled)) Sched --> CHG_SC6[CHG SC.6 Perform Assigned Task(s)] CHG_SC6 --> CHG_SC7[CHG SC.7 Mark Task(s) Completed] CHG_SC7 -.-> Comp((Completed)) Comp -.-> SCComp[Standard Change Completion Notification] SCComp --> CanClose{Request can be closed?} CanClose -- No --> CHG_SC8[CHG SC.8 Document Necessary Correction(s)] CHG_SC8 --> CanClose CanClose -- Yes --> CloseChange[/Close Change/] CloseChange -.-> Closed((Closed))</pre>	
		<pre>graph TD CHG_SC9[CHG SC.9 Review Comments and Remediate] --> CHG_SC6 CHG_SC6 --> CHG_SC7 CHG_SC7 --> CHG_SC9</pre>

Figure 2. Standard Change

Standard Change Procedure

ID	Tasks	Procedure	Primary Role	Input	Output
CHG SC.1	Access ESS Portal or Service Catalog	To create a standard change request, access the Employee Self Service portal or the Service Catalog and look for the desired standard change.	Requester	Standard change required	List of authorized Standard Changes on ESS portal or service catalog
CHG SC.2	Select Appropriate Standard Change	Select the desired Standard change from the list of available services/standard changes.	Requester	List of authorized Standard Changes on ESS portal or service catalog	Appropriate Standard change form opened
CHG SC.3	Provide Requested Information	When applicable, provide the requested information in the appropriate field.	Requester	Appropriate Standard change form opened	Requested information provided
CHG SC.4	Submit Request	Click the Submit button to initiate the Standard change. If a specific date has been entered for the execution of the change, the Collision Detector will verify if the requested date is available and is not in conflict with: <ul style="list-style-type: none"> Another change record against the same configuration item (CI). A defined blackout window, where no changes should occur to this CI. A change that is already scheduled for a related (parent/child) CI. 	Requester	Requested information provided	Submitted standard change request Or Identified conflicting date for change implementation
CHG SC.5	Enter New Date for Change	If a conflict has been identified and the change cannot be completed on the initial desired date, provide a new date for the change to be executed.	Requester	Conflicting date for change implementation identified	Standard change request submitted with new valid date

ID	Tasks	Procedure	Primary Role	Input	Output
CHG SC.6	Perform Assigned Task(s)	Perform assigned task(s), as described	Implementer(s)	Assigned predefined task(s) from submitted standard change request OR Corrections or adjustments to be made	Executed task(s) or Corrections
CHG SC.7	Mark Task(s) Completed	Once the task(s) are completed, change the assigned task state to Completed .	Implementer(s)	Executed task(s)	<ul style="list-style-type: none"> Task(s) marked as completed Standard Change Completion Notification sent to Requester
CHG SC.8	Document Necessary Correction(s)	If the Change has not been completed properly, document what needs to be corrected or adjusted in the request form	Requester	Standard Change Completion Notification sent to Requester	Documented Reason(s) for rejection of the Change
CHG SC.9	Review Comments and Remediate	Review comments provided by Requester and make necessary correction or adjustments.	Implementer(s)	Documented Reason(s) for rejection of the Change	<ul style="list-style-type: none"> Corrections or adjustments to be made

3.3 Normal Change

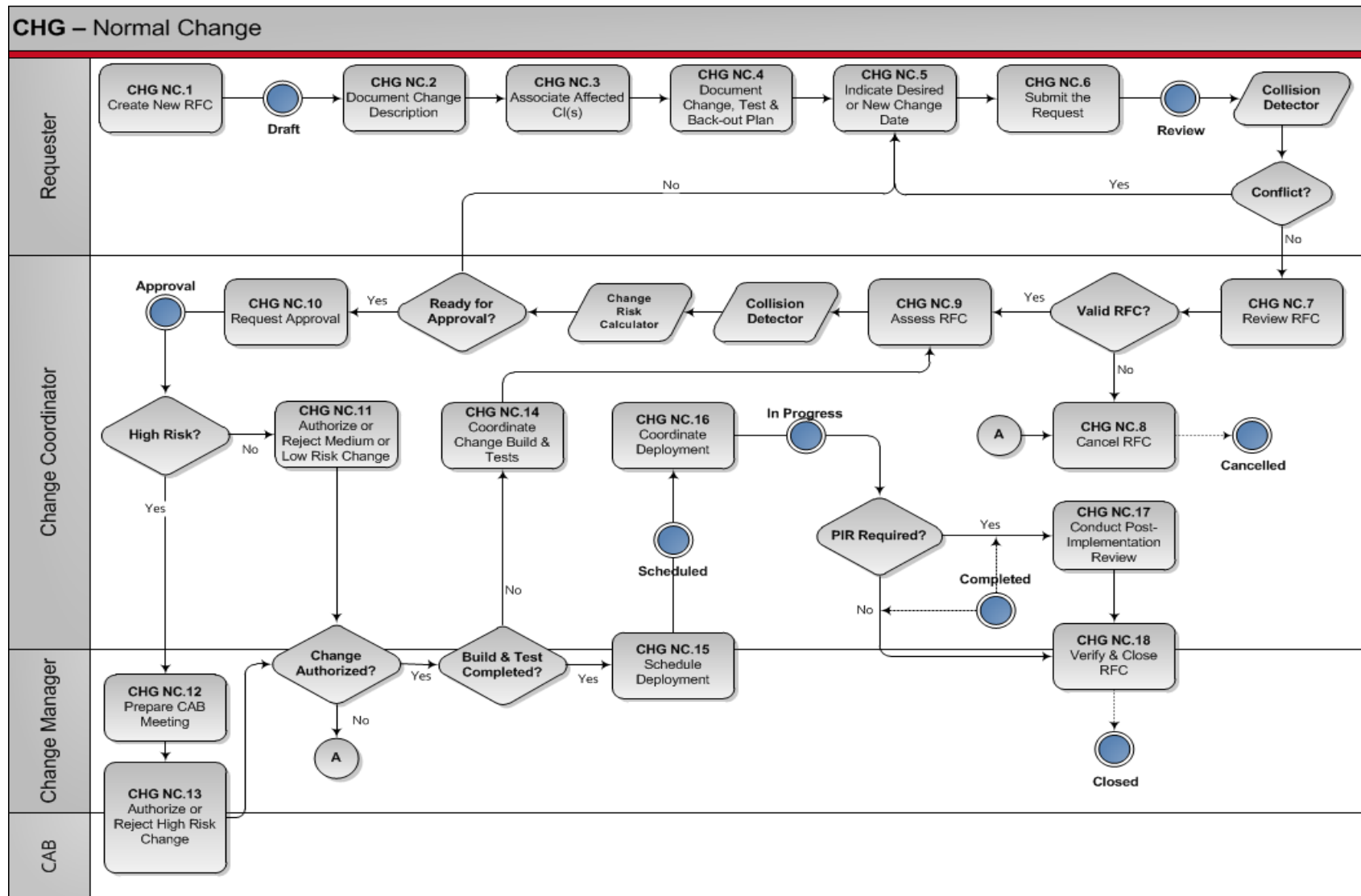


Figure 3.Normal Change

Normal Change Procedure

ID	Tasks	Procedure	Primary Role	Input	Output
CHG NC.1	Create New Request for Change (RFC)	From the Change application, click Create New to open the Change Request form.	Requester	<ul style="list-style-type: none"> Incident Problem Project 	Opened Change Request form
CHG NC.2	Document Change Description	Provide a summary of the required change in the Short description field and a detailed description of the change including the reason(s) for the change in the Description field.	Requester	Opened Change Request form	RFC form documented with change description
CHG NC.3	Associate Affected CI(s)	In the Affected CIs section, indicate which CI(s) will be impacted by the change.	Requester	RFC form documented with change summary and detailed description	RFC form documented with change description and associated CI(s)
CHG NC.4	Document Change, Test, and Back out Plan	Document the Change plan, Test plan, and Back-out plan.	Requester	RFC form documented with change description and associated CI(s)	RFC form documented with change description, associated CI(s), Change plan, Test plan, and Back-out plan
CHG NC.5	Indicate Desired or New Change Date	<p>In the Schedule section, indicate the Planned start date and Planned end date of the change.</p> <p>If the Conflict Checker has identified a date conflict with:</p> <ul style="list-style-type: none"> Another change record against the same configuration item (CI). A defined blackout window, where 	Requester	RFC form documented with change description, associated CI(s), Change plan, Test plan and Back out plan	RFC form ready to be submitted

ID	Tasks	Procedure	Primary Role	Input	Output
		<p>no changes should occur to the associated CI(s).</p> <ul style="list-style-type: none"> A parent/child related CI for which a Change is already scheduled. <p>Provide a new <i>Planned start date</i> and <i>Planned end date</i> for the change to be executed.</p>			
CHG NC.6	Submit the Request	Click the Submit button to submit the change request for review.	Requester	RFC form ready to be submitted	Draft RFC submitted for review
CHG NC.7	Review RFC	<p>Open the submitted RFC and review its content to ensure that it is:</p> <ul style="list-style-type: none"> Complete Practical Necessary Unique and does not repeat RFCs that have already been accepted, rejected or that are still under consideration 	Change Coordinator	Draft RFC submitted for review	Valid RFC Or Invalid RFC
CHG NC.8	Cancel RFC	If the RFC does not meet the above requirements, cancel the RFC and inform the requester of the reason(s) for the rejection.	Change Coordinator	Invalid RFC	Cancelled RFC
CHG NC.9	Assess RFC	<ul style="list-style-type: none"> Verify that the calculated risk level is appropriate for the change and that the business impact is well documented. See Appendix D for information on risk assessment techniques. Ensure that the Change, Back-out, 	Change Coordinator	Valid RFC Or Documented change build and test results (CHG NC.13)	Valid RFC with accurate risk land impact documented

ID	Tasks	Procedure	Primary Role	Input	Output
		<p>and Test plans are documented properly</p> <p>Or</p> <p>Once the Change build and tests are completed and documented, validate the initial RFC categorization, risk, and impact levels, and adjust if necessary</p>			
CHG NC.10	Request Approval	The RFC is submitted for approval/authorization.	Change Coordinator	Valid RFC with accurate risk and impact documented	RFC submitted for approval
CHG NC.11	Authorize or Reject Medium or Low Risk Change	The Change Coordinator approves or rejects medium or low risk change.	Change Coordinator	Medium or Low Risk RFC submitted for approval	Authorized or Rejected Medium or Low Risk RFC
CHG NC.12	Prepare CAB Meeting	<p>Prepare a CAB meeting agenda. A typical CAB agenda contains:</p> <ul style="list-style-type: none"> • RFCs to be assessed by the CAB • Outstanding changes • Failed, backed-out, and identified unauthorized changes • Change calendar • Emergency changes implemented since last CAB meeting <p>Distribute the CAB meeting agenda to all CAB members and required SMEs.</p> <p>SME approvers can be:</p> <ul style="list-style-type: none"> • Customers • User group representatives 	Change Manager	High Risk Changes to be Authorized	<p>Formal CAB meeting invitation</p> <p>And</p> <p>CAB meeting agenda with list of High Risk changes to be authorized sent to CAB members and SMEs</p>

ID	Tasks	Procedure	Primary Role	Input	Output
		<ul style="list-style-type: none"> Service owners Application developers Specialists/technical consultants Services and operations staff Third-party representatives 			
CHG NC.13	Authorize or Reject High-Risk Change	The CAB recommends approval or rejection of high risk change.	Change Manager/CAB	Formal CAB meeting invitation And CAB meeting agenda with list of High Risk changes to be approved sent to CAB members and SMEs	RFC authorized for build and test Or RFC authorized for deployment Or RFC Rejected
CHG NC.14	Coordinate Change Build and Test	Ensure that required tasks for building the change have been assigned to appropriate technical groups. Validate that the change is thoroughly tested and that the test results are documented.	Change Coordinator	RFC authorized for build and test	Documented test results
CHG NC.15	Schedule Deployment	<ul style="list-style-type: none"> Verify that the requested implementation date does not conflict with other changes, maintenance windows, or blackout periods. Adjust the schedule if necessary. Update the change calendar. See Appendix E for information on techniques to assess potential schedule conflicts. 	Change Coordinator/ Change Manager	RFC authorized for deployment	RFC scheduled for implementation

ID	Tasks	Procedure	Primary Role	Input	Output
CHG NC.16	Coordinate Deployment	<p>Ensure the change is deployed as defined in the approved execution plan and that all tasks are updated properly.</p> <p>In the event that the deployment cannot be completed successfully, the back-out plan is executed.</p>	Change Coordinator	Scheduled deployment	<p>Change completed successfully</p> <p>Or</p> <p>Change completed with issues</p> <p>Or</p> <p>Change completed unsuccessfully</p>
CHG NC.17	Conduct Post-implementation Review (PIR)	<p>Conduct a PIR if justified by change management process policies. Examine how the change was handled throughout its entire life cycle, and whether it produced the desired results.</p> <p>Document opportunities to improve the implementation of similar changes in the future and assign action items accordingly.</p>	Change Coordinator	Change implementation requiring PIR	Documented PIR
CHG NC.18	Verify and Close the RFC	<p>Ensure that all the necessary implementation information has been captured.</p> <p>Depending on the result of the implementation, select the appropriate closure code and close the RFC.</p> <p>Note: The RFC can only be closed after all associated tasks have been closed.</p>	Change Coordinator/ Change Manager	<p>Change completed successfully</p> <p>Or</p> <p>Change completed with issues</p> <p>Or</p> <p>Change completed unsuccessfully</p>	Closed RFC

3.4 Emergency Change

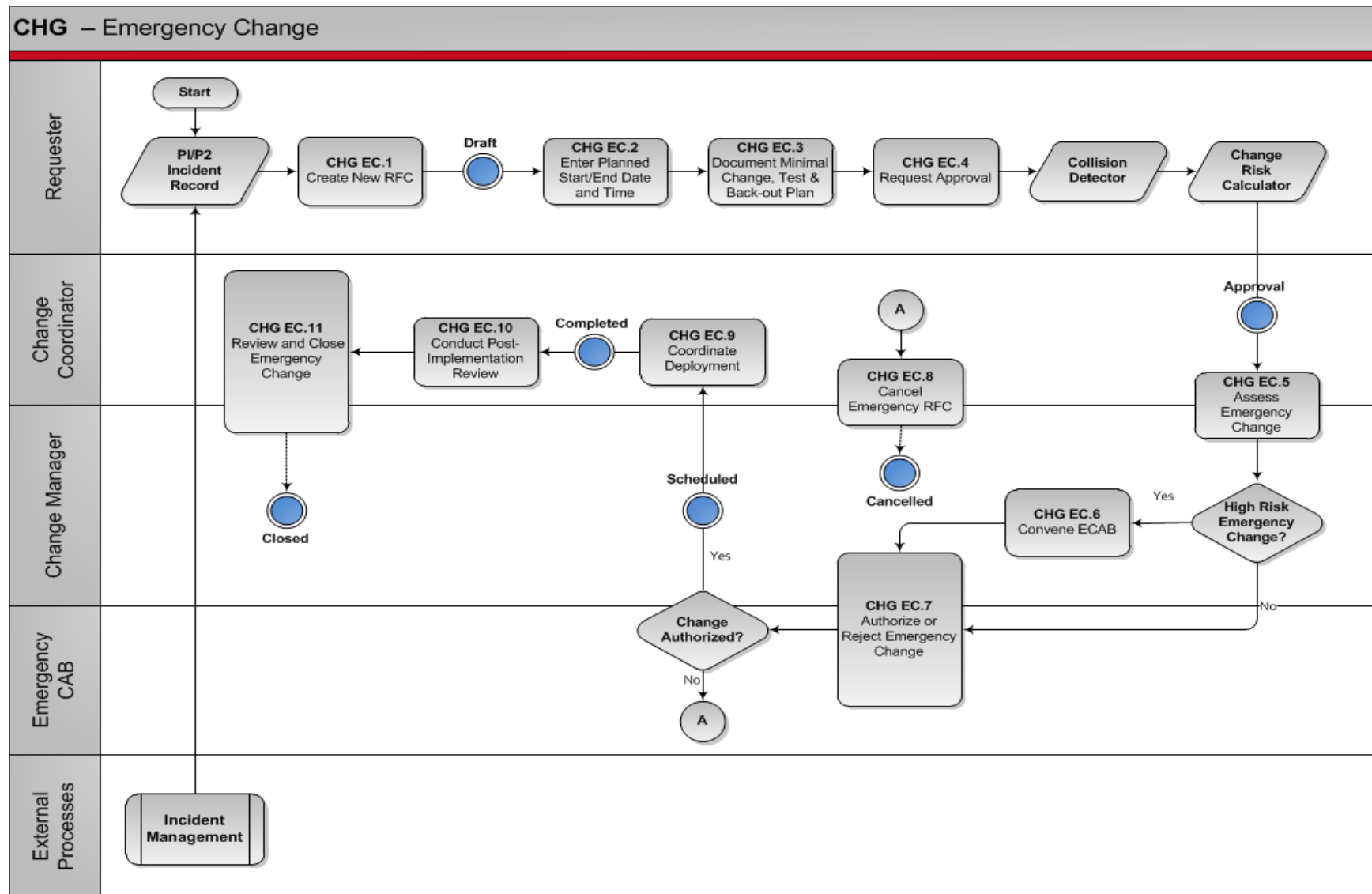


Figure 4. Emergency Change

Emergency Change Procedure

ID	Tasks	Procedure	Primary Role	Input	Output
CHG EC.1	Create New Emergency Change (RFC)	<ul style="list-style-type: none"> From a Priority 1 or 2 Incident, click “Create Change” do open the Change Request form. Review the information transferred from the Incident record in the Description field and ensure it provides a detailed description of the change. 	Requester	Priority 1 Incident Or Priority 2 Incident	Opened Emergency Change Request form containing all information from originating P1/P2 Incident record.
CHG EC.2	Enter Planned Start/End Date and Time	<ul style="list-style-type: none"> Enter the Planned Start Date and Time Enter the Planned End Date and Time 	Requester	Opened Change Request form	RFC form documented with change description and Planned Start/End date and time
CHG EC.3	Document Minimal Change, Test, and Back out Plan	Provide a minimal description for the Change plan, Test plan, and Back-out plan.	Requester	RFC form documented with change description and associated CI(s) and originating P1/P2 Incident record	RFC form documented with minimal Change plan, Test plan, and Back-out plan
CHG EC.4	Request Approval	Click the “Request Approval” button to submit the Emergency Change Request to Change Management for approval.	Requester	RFC form documented with Minimal Change plan, Test plan, and Back-out plan	Emergency Change submitted for approval

ID	Tasks	Procedure	Primary Role	Input	Output
CHG EC.5	Assess Emergency Change Request	<ul style="list-style-type: none"> Verify that the calculated risk level is appropriate for the change and that the business impact is well documented. See Appendix D for information on risk assessment techniques. Ensure that the Change, Back-out, and Test plans are documented properly 	Change Manager/ Change Coordinator	Emergency Change submitted for approval	Emergency Change ready to be Authorized
CHG EC.6	Convene ECAB	For a High Risk Emergency Change, convene the ECAB members, to obtain proper authorization.	Change Manager	High Risk Emergency Change ready to be authorized	ECAB session in progress
CHG EC.7	Authorize or Reject Emergency Change	The ECAB recommends approval or rejection of High Risk Emergency Change Change Manager/Coordinator is responsible to authorize or reject Low or Medium Risk Emergency Change.	ECAB Change Manager/Change Coordinator	Emergency Change ready to be authorized	Authorized or Rejected Emergency Change
CHG EC.8	Cancel Emergency Change	If the Emergency Change is rejected, cancel the RFC and inform the requester of the reason(s) for the rejection.	Change Coordinator/ Change Manager	Rejected Emergency Change	Cancelled RFC
CHG EC.9	Coordinate Deployment	<p>Ensure the change is deployed as defined in the approved execution plan and that all tasks are updated properly.</p> <p>In the event that the deployment cannot be completed successfully, the back-out plan is executed.</p>	Change Coordinator	Authorized Emergency Change	<p>Change completed successfully</p> <p>Or</p> <p>Change completed with issues</p> <p>Or</p> <p>Change completed unsuccessfully</p>
CHG EC.10	Conduct Post Implementat ion Review	Conduct a PIR if justified by change management process policies. Examine how the change was handled throughout its entire life cycle, and whether it produced the desired results.	Change Coordinator	Change implementation requiring PIR	Documented PIR

ID	Tasks	Procedure	Primary Role	Input	Output
		Document opportunities to improve the implementation of similar changes in the future and assign action items accordingly.			
CHG EC.11	Review and Close Emergency Change	<p>Ensure that all the necessary implementation information has been captured.</p> <p>Depending on the result of the implementation, select the appropriate closure code and close the RFC.</p> <p>Note: The RFC can only be closed after all associated tasks have been closed.</p>	Change Coordinator/ Change Manager	<p>Change completed successfully</p> <p>Or</p> <p>Change completed with issues</p> <p>Or</p> <p>Change completed unsuccessfully</p>	Closed Emergency Change

4 Process Control

4.1 KPIs

KPIs are best represented as trend lines and tracked over time. They provide information on the effectiveness of the process and the impact of continuous improvement efforts.

KPI/Metric	Purpose
Number/percent of changes completed by Type.	Measure of process efficiency. Look for opportunities to increase percentage of Standard changes and lower percentage of Emergency changes.
Number/percent of changes completed by state (such as Successful or Unsuccessful).	Measure of the effectiveness of the change management process.
Number/percent of completed changes that caused incidents.	Measure of negative impact to IT service quality.

4.2 Operational Data

Active changes that require visibility, oversight, and possible management intervention are best tracked on a dashboard or homepage that is monitored by the Change Manager.

Item	Purpose
Forward schedule of changes.	Ability to see a calendar view of all changes that have been approved for implementation.
List of changes awaiting CAB or ECAB approval.	Provides view of work in progress.
List of changes awaiting post implementation review.	Provides view of work in progress.
List of changes that caused incidents.	Provides quick view of changes that need investigation to determine if process improvements are needed.


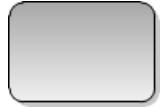





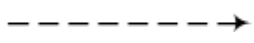

4.3 Reports and Homepages

There are numerous default reports available in ServiceNow that can be used to generate charts, can be published to a URL, or can be scheduled to be run and distributed at regular intervals. Users can also create custom reports. See [Creating Reports](#) in the ServiceNow Wiki for more detail on this capability.

In addition to reports, each user can create a personal homepage and add gauges containing up-to-the-minute information about the current status of records that exist in ServiceNow tables. See [Customizing Homepages](#) in the ServiceNow Wiki for details.

Appendices

Appendix A: Diagram Convention

Symbol	Description
	Process start or end point: Represents the starting and ending point of the process.
	Process activity or task: Presents an activity or task that needs to be accomplished to produce a specific outcome.
	Predefined external process or organization: Indicates a contribution from an external process or organization.
	Decision: Indicates that a question needs to be answered in order to identify the following activity or task in the process. The answers are indicated on the different connectors attached to the decision box. Every answer is linked to an associated activity or task.
	System Action or Function: Indicates that an action is being performed in the system as an output of the previous activity and an input to the next.
	Off-page reference: Indicates a reference to another diagram within the same process. The number of the referenced diagram is indicated in the shape.
	On-page reference: Indicates a link to another activity within the same diagram.
	Association: Indicates an association or a relation between the connected, processes, tasks, or activities. May be represented by a dotted or dashed line.
	Sequence flow: Shows the order in which the activities are performed. Represented by a solid line and arrowhead.

Appendix B: Glossary of Terms and Acronyms

Term	Acronym	Definition
Alert		A notification that a threshold has been reached, something has changed, or a failure has occurred. Alerts are often created and managed by system management tools and are managed by the event management process.
Assessment		Inspection and analysis to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency and effectiveness targets are being met.
Attribute		A piece of information about a configuration item. Examples are name, location, version number, and cost. Attributes of CIs are recorded in the configuration management database (CMDB).
Back-out		An activity that restores a service or other configuration item to a previous baseline. Back-out is used as a form of remediation when a change or release is not successful.
Baseline		<p>(ITIL <i>Continual Service Improvement</i>) (ITIL <i>Service Transition</i>) A snapshot that is used as a reference point. Many snapshots may be taken and recorded over time but only some will be used as baselines. For example:</p> <ul style="list-style-type: none"> ▪ An ITSM baseline can be used as a starting point to measure the effect of a service improvement plan ▪ A performance baseline can be used to measure changes in performance over the lifetime of an IT service ▪ A configuration baseline can be used as part of a back-out plan to enable the IT infrastructure to be restored to a known configuration if a change or release fails.
Category		A named group of things that have something in common. Categories are used to group similar things together.
Change		The addition, modification, or removal of anything that could have an effect on IT services.
Change Advisory Board	CAB	A group of people who support the assessment, prioritization, authorization, and scheduling of changes. A change advisory board is usually made up of representatives from all areas within the IT service provider, the business, and third parties such as suppliers.
Change Management	CHG	The process responsible for controlling the life cycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services.
Change Record		A record containing the details of a change. Each change record

Term	Acronym	Definition
		documents the life cycle of a single change. A change record is created for every request for change.
Change Request		See Request for Change.
CI Type		A category that is used to classify configuration items. The CI type identifies the required attributes and relationships for a configuration record. Common CI types include hardware, document, and user.
Classification		The act of assigning a category to something. Classification is used to ensure consistent management and reporting. CIs, incidents, problems, and changes are usually classified.
Closed		The final status in the life cycle of an incident, problem, or change. When the status is closed, no further action is taken.
Closure		The act of changing the status of an incident, problem, or change to closed.
Configuration Item	CI	Any component or other service asset that needs to be managed in order to deliver an IT service. Information about each configuration item is recorded in a configuration record within the configuration management system and is maintained throughout its life cycle by service asset and configuration management.
Configuration Management Database	CMDB	A database used to store configuration records throughout their life cycle. The configuration management system maintains one or more CMDBs. Each CMDB stores attributes of CIs and relationships with other CIs.
Configuration Management System	CMS	A set of tools, data, and information that is used to support service asset and configuration management. The CMS is part of an overall service knowledge management and includes tools for collecting, storing, managing, updating, analyzing, and presenting data about all configuration items and their relationships. The CMS also includes information about incidents, problems, known errors, changes, and releases. It may contain data about employees, suppliers, locations, business units, customers, and users. The CMS is maintained by service asset and configuration management and is used by all IT service management processes.
Configuration Record		A record containing the details of a configuration item. Each configuration record documents the life cycle of a single configuration item.
Continual Service Improvement	CSI	Ensures that services are aligned with changing business needs by identifying and implementing improvements to IT services that support business processes. The performance of the IT service provider is continually measured and improvements are made to processes, IT services, and IT infrastructure in order to increase efficiency,

Term	Acronym	Definition
		effectiveness, and cost effectiveness.
Customer		Someone who buys goods or services. The customer of an IT service provider is the person or group who defines and agrees to the service level targets. The term is also sometimes used informally to mean user, for example, 'This is a customer-focused organization.'
Diagnosis		A stage in the incident and problem life cycles. The purpose of diagnosis is to identify a workaround for an incident or the root cause of a problem.
Effectiveness		A measure of whether the objectives of a process, service, or activity have been achieved. An effective process or activity is one that achieves its agreed objectives. <i>See also</i> Key Performance Indicator.
Efficiency		A measure of whether the right amount of resource has been used to deliver a process, service, or activity.
Emergency Change		A change that must be introduced as soon as possible, for example to resolve a major incident or implement a security patch. The change management process normally has a specific procedure for handling emergency changes.
Employee Self Service	ESS	A module in ServiceNow that allows users to make requests, view articles, log incidents, and search the knowledge base through a user-friendly website called the Employee Self-Service Portal (ESS Portal).
Event		A change of state that has significance for the management of an IT service or other configuration item. The term is also used to mean an alert or notification created by any IT service, configuration item, or monitoring tool.
Impact		A measure of the effect of an incident, problem, or change on business processes. Impact is often based on how service levels will be affected. Impact and urgency are used to assign priority.
Incident		An unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet affected service is also an incident.
Key Performance Indicator	KPI	A metric that is used to help manage an IT service, process, plan, project, or other activity. Many metrics may be measured, but only the most important of these are defined as key performance indicators and used to actively manage and report on the process, IT service, or activity. They should be selected to ensure that efficiency, effectiveness, and cost effectiveness are all managed.
Known Error	KE	A problem that has a documented root cause and a workaround. Known errors are created and managed throughout their life cycle by problem management. Development groups or suppliers may also

Term	Acronym	Definition
		identify known errors.
Major Incident		The highest category of impact for an incident. A major incident results in significant disruption to the business.
Metric		Something that is measured and reported to help manage a process, IT service, or activity.
Policy		Formally documented management expectations and intentions. Policies are used to direct decisions and to ensure consistent development and implementation of processes, standards, roles, activities, IT infrastructure, and so on.
Post-implementation Review	PIR	A review that takes place after a change or a project has been implemented. It determines if the change or project was successful and identifies opportunities for improvement.
Priority		A category used to identify the relative importance of an incident, problem, or change. Priority is based on impact and urgency, and is used to identify required times for actions to be taken. For example, the SLA may state that priority 2 incidents must be resolved within 12 hours.
Problem		A cause of one or more incidents. The cause is not usually known at the time a problem record is created. The problem management process is responsible for further investigation.
RACI	RACI	A model used to help define roles and responsibilities. RACI stands for responsible, accountable, consulted, and informed.
Release		One or more changes to in IT service that are built, tested, and deployed together. A single release may include changes to hardware, software, documentation, process, and other components.
Request for Change	RFC	A formal detailed proposal for a change to be made. The term is often misused to mean change record or the change itself.
Restore		Taking action to return an IT service to the users after repair and recovery from an incident. This is the primary objective of incident management.
Risk		A possible event that could cause harm or loss or affect the ability to achieve objectives. A risk is measured by the probability of a threat, the vulnerability of the asset to that threat, and the impact it would have if it occurred.
Role		A set of responsibilities, activities, and authorities assigned to a person or team. A role is defined in a process or function. One person or team may have multiple roles. For example, a single person may carry out the role of configuration manager and change manager.

Term	Acronym	Definition
Root Cause		The underlying or original cause of an incident or problem.
Root Cause Analysis	RCA	An activity that identifies the root cause of an incident or problem. Root cause analysis typically concentrates on IT infrastructure failures.
Service		A means of delivering value to customers by facilitating the outcomes customers want to achieve without the ownership of specific costs and risks.
Service Desk		The single point of contact between the service provider and the users. A typical service desk manages incidents and service requests, and also handles communication with the users.
Service Level		Measured and reported achievement against one or more service level targets.
Service Level Agreement	SLA	An agreement between an IT service provider and a customer. A service level agreement describes the IT service; documents service level targets, and specifies the responsibilities of the IT service provider and the customer.
Service Request		A formal request from a user for something to be provided, for example, a request for information or advice; to reset a password; or to install a workstation for a new user.
Stakeholder		A person who has an interest in an organization, project, or IT service. Stakeholders may be interested in the activities, targets, resources, or deliverables. Stakeholders may include customers, partners, employees, shareholders, owners, or others.
User		A person who uses the IT service on a day-to-day basis. Users are distinct from customers, as some customers do not use the IT service directly.
Workaround		Reducing or eliminating the impact of an incident or problem for which a full resolution is not yet available, for example, by restarting a failed configuration item. Workarounds for problems are documented in known error records. Workarounds for incidents that do not have associated problem records are documented in the incident record.

Source: ITIL® glossary and abbreviations

© Crown copyright 2011. All rights reserved. Material is reproduced with the permission of the Cabinet Office under delegated authority from the Controller of HMSO.
ITIL® is a registered trade mark of the Cabinet Office

Appendix C: Standard Change Guidelines

Standard Changes for Process Efficiency

A Standard change type is one for which approval has been granted in advance (typically by the Change Manager), and is usually low risk, routinely performed, and has been implemented without incident in the past; that is, has a good track record. Standard changes follow a fast-path through the process and may or may not require scheduling. A change process with unnecessary levels of administration and oversight may be viewed as overly bureaucratic and therefore subject to resistance. Therefore, Standard changes should be identified early when building the change management process to promote efficiency and buy-in.

Standard Change Models

Standard changes are often managed and controlled through the use of change models. A change model is a pre-defined sequence of steps that must be taken to execute a change in an agreed and accepted manner. ServiceNow provides the ability to create change models with template functionality. These templates are constructed so that much of the information about the change is already pre-filled. Values for items such as the planned start and end date and time, requester, and possibly the affected CIs need to be provided. See [Creating a Template](#) in the ServiceNow Wiki for more information on how to build templates for standard changes.

Initiating a Standard Change from the Service Catalog

Standard changes are frequently used to fulfill service requests initiated from the service catalog. In these cases, the service catalog can be used to request changes through a record producer. Record producers appear in the service catalog like catalog items, but when submitted, they create a change record with the information provided either by the user or by a template. See [Record Producer](#) in the ServiceNow Wiki for more information on how to use this feature to generate a standard change from a service request.

Appendix D: Risk Assessment

It is a best practice to use a risk-based assessment when evaluating a change. This approach helps identify factors that may disrupt the business or impede the delivery of services. Different approaches can be taken to assess and manage risks and each organization must determine the approach it will use. The following list details the various approaches that are supported by ServiceNow. The approaches are listed in order of complexity, starting with the most simple:

1. Manually select the risk value from a pre-defined list (for example, Low, Moderate, High, Very High).
2. Use a simple matrix that determines risk based on impact and probability, where:
 - **Impact** is the effect that a negative outcome would have on business.
 - **Probability** is the likelihood that a negative outcome will occur.

Risk is generated from impact and probability according to the following table.

	Probability High	Probability Medium	Probability Low
Impact High	Risk 1	Risk 2	Risk 3
Impact Medium	Risk 2	Risk 3	Risk 4
Impact Low	Risk 3	Risk 4	Risk 5

3. The ServiceNow Change Risk Assessment plugin provides a flexible way to capture information from the end user to determine risk. Libraries of questions can be used to derive the risk of a change based on criteria contained within the change record. For example, a different set of questions could be set for a hardware change versus a software change. The assessment uses a weighted score approach for each question and the overall score for an assessment is evaluated against thresholds to determine the risk of the change. See [Change Risk Assessment](#) in the ServiceNow Wiki for information on how to use this plugin.
4. In addition to manually evaluating risk, it is possible to *automatically establish the risk of the change based on the CI* that is identified in the change record. The Change Risk Calculator plugin enables dynamic calculations of the risk and impact of a change and bundles some best practice risk calculations that use CI attributes and time measures. See [Best Practice - Change Risk Calculator](#) in the ServiceNow Wiki for information on how to use this plugin.

Appendix E: Scheduling Assessment

The Change Management Collision Detector plugin provides the ability to detect whether planned changes conflict with other changes or have other scheduling issues. When the Collision Detector is run, any issues that are detected are added to the **Conflicts** related list at the bottom of the Change Request form with an explanation of the issues detected. See [Collision Detector](#) in the ServiceNow Wiki for more information on how to use the Collision Detector plugin to identify scheduling conflicts for a change.

Activating the Change Management Collision Detector plugin automatically enables the [Maintenance Schedules](#) plugin if it is not already active. Depending upon the conflict properties that are selected, this enables the Collision Detector to identify:

- Conflicts with the maintenance schedule of the *selected CI* in the change record.
- Conflicts with the maintenance schedules of any child or parent CIs or any affected CIs that may be listed in the change record.
- Conflicts with any blackout schedules (times during which changes cannot be scheduled) that have been created.

Appendix F: Emergency Change Guidelines

Emergency Change Description

The 'emergency' change procedure is reserved for changes intended to repair an error in an IT service that is negatively impacting the business to a high degree, whereas changes that are intended to introduce immediately required business improvements are handled as 'normal' changes with the highest urgency. The number of emergency changes proposed should be kept to an absolute minimum because they are generally more disruptive and prone to failure. However, when an emergency change is necessary, measures should be taken to ensure the change is designed carefully and properly tested prior to its implementation.

Emergency Change Authorization

There might not be sufficient time to convene all the CAB members when an emergency change arises. In this case, authorization is provided by the emergency CAB (ECAB). Membership of the ECAB may be decided at the time a meeting is called and depends on the nature of the emergency change. While not all emergency changes will require the involvement of the Change Manager or the ECAB, it is essential that the Change Management process policy clearly defines the required levels of authorization and delegated authority to ensure appropriate decisions are made in any conceivable circumstance.

Late or Retroactive Change

It may not be possible to update all Change Management records at the time that urgent actions are being completed. However, it is essential that temporary records are made during such periods, and that all records are completed retroactively, at the earliest possible opportunity. An agreed time for completion of these updates should be documented in the Change Management process policy.

Essentially, the emergency change procedure will follow the normal change procedure except that:

- Approval will be given by the ECAB rather than waiting for a CAB meeting
- Testing may be reduced, or in extreme cases forgone completely, if considered a necessary risk to deliver the change immediately
- Documentation, i.e. updating the change record and configuration data, may be deferred, typically until normal working hours.

Appendix G: Expedited Change Guidelines

While ITIL describes three different types of service change (Standard, Emergency and Normal), many organizations manage a fourth type of change, often referred to as 'Expedited'. An expedited change is basically a normal change that must be implemented sooner than originally planned and therefore must bypass the normal approval process due to lack of lead-time. These types of changes can be easily identified because the 'planned start date' will be earlier than the lead-time required for the normal change approval process (including CAB review). Expedited changes are usually the result of an unexpected shift in business need, poor planning, or both. In any event, an expedited change will require a separate approval process to be defined. Expedited changes should be monitored and reviewed by the Change Manager to identify opportunities for process improvement or additional staff Change Management process awareness and education.