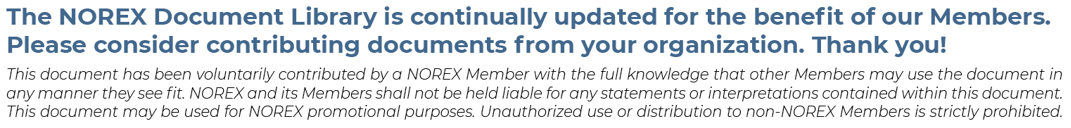


**GLOBAL IT CHANGE MANAGEMENT PROCESS**

This document describes a globally consistent IT change management process based on ITIL best practices.

18 Pages 50-407



**Global IT Change Management**

**Process**

**Table of Contents**

Table of Contents 2

About this document 3

Summary of changes 3

Chapter 1. Executive Summary 4

Chapter 2. Scope & Definitions 5

2.1. Scope 5

2.2. Out of Scope 5

2.3. Definitions 5

Chapter 3. Change Management Process 8

3.1. Standard Change 8

3.2. Normal Change 8

3.3. Emergency Change 9

3.4. Risk Assessment Calculator 10

3.5. Post Implementation Review 10

Chapter 4. Required Change Documentation 11

Chapter 5. Change Scheduling 12

5.1. Standard Maintenance Windows 12

5.2. Change Request Calendar 12

5.3. Change Freeze 13

5.4. Exception tab 13

Chapter 6. Roles & Responsibilities 13

6.1. Change Requester 13

6.2. Change Implementer 13

6.3. Change Approvers (Manager, CI Owner, Business and CAB approvals) 14

6.4. UAT Approvers 14

6.5. PIR Approvers 14

6.6. Global Change Manager 14

6.7. Global ITSM Process Owner 14

Chapter 7. GCAB Membership and Meetings 15

7.1. GCAB Membership and Participation 15

7.2. Function of the GCAB 15

7.3. CAB Member Expectations 15

7.4. Emergency CAB (E-CAB) 15

Chapter 8. Metrics, Reports and Meetings 15

Appendix 1: STANDARD CHANGE MANAGEMENT PROCESS 16

Appendix 2: NORMAL CHANGE MANAGEMENT PROCESS 16

Appendix 3: EMERGENCY CHANGE MANAGEMENT PROCESS 17

Appendix 4 - RACI CHART 17

Appendix 5: UAT / OAT and PIT TEMPLATE LINKS 18

Appendix 6: RISK ASSESSMENT MATRIX 18

Appendix 7: PROCESS UPDATES COMMUNICATION PLAN 18

**About this document**

This document describes a globally consistent IT Change Management Process for [ORG]. It is based on Information Technology Infrastructure Library (ITIL) best practices. Ensuring effective change management within the company’s production IT environment is extremely important in providing quality delivery of IT services as well as achieving Sarbanes-Oxley compliance. The intent of this process is to ensure effective management of change while reducing risk.

**Summary of changes**

This section records the history of significant changes to this document. Only the most significant changes are described here.

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Description of change** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Where significant changes are made to this document, the version number will be incremented by 1.0.

Where changes are made for clarity and reading ease only and no change is made to the meaning or intention of this document, the version number will be increased by 0.1.

**Chapter 1. Executive Summary**

The purpose of Change Management is to allow [ORG] IT function to respond to changing business and IT needs while maximizing service value, reducing incidents, disruption, and re-work. Change Management achieves this by having standardized methods and procedures for the efficient and effective handling of all changes. Following the guidelines outlined in this process will ensure all information technology changes satisfy Sarbanes-Oxley (SOX) corporate governance audit requirements. The goals of Change Management are:

* Establish a globally standard process and tool for managing changes
* Right-size the approval requirements based on the level of risk
* Ensure appropriate communications regarding changes based on the level of risk
* Capture metrics and lessons learned to continuously improve the Change Management process
* Ensure compliance with SOX requirements

Key components of the process include:

1. **Accurate Documentation:** Identify the information relevant to a specific change that needs to be collected throughout the change management process
2. **Formal, Defined Approval and Oversight 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 obtain the highest level of success
3. **Post-Implementation Review (PIR):** All emergency, and failed changes including process failures, will require a PIR to be conducted to capture lessons learned and reduce the future likelihood of failed / emergency changes

There are three types of changes as described below. Standard and Normal changes must be implemented during the standard maintenance windows defined in section 4.1:

|  |  |  |  |
| --- | --- | --- | --- |
| **Type of Change** | **Change Definition** | **Submission lead times** | **Approvals & Notifications** |
| **Standard Changes** | A low risk, frequently occurring, routine change that is performed using a Standard change template, that has been pre-approved by the Global Change Advisory Board (GCAB) | 1 Business Day | Assignment Group Manager |
| **Normal Change: Requires explicit approvals and is further classified into low, moderate and high risk. See section 3.5 for the Risk Calculator** | | | |
| **Normal -Low Risk Change** | Change being performed is contained to an environment related to a specific business unit or country and is:  - a non-critical tier 3 services / application (or)  - very minor in nature with no change to user experience (or)  - no detrimental business impact if the change fails | 1 Business Day | Assignment Group Manager  CI Group Approvers |
| **Normal -Moderate Risk Change** | * - change being performed may impact a Tier 2 application (or) * - impacts more than one critical location or Business unit (or) * - the implementation may impact the user experience | 1 Week | Assignment Group Manager, CI Group Approvers, GCAB Review |
| **Normal -High Risk Change** | * change being performed may impact a Tier 1 application (or) * impacts multiple locations or business units (or) * implements significant changes to the user experience (or) * failure of the change may cause significant business impact (or) * a history of success has not been established | A minimum of 2 Weeks GCAB notice | Assignment Group Manager, CI Group Approvers  In Person GCAB Review Meeting |
| **Emergency Changes** | A change to resolve an outage, a pending outage, or to address an immediate security or regulatory issue. The change is often recorded after the implementation has been completed | Immediate | Explicit approval of immediate manager and subsequent Emergency CAB (E-CAB) review and approval |
| **\*Business and UAT Approval is mandatory for all application / software changes.**  **\*\*GCAB Approvers will be included on Moderate and High Risk globally impacting changes** | | | |

**Chapter 2. Scope & Definitions**

**2.1. Definition of a Change**

**Change**: A change is defined as the addition, modification or removal of a production IT Service or an associated service component / documentation that may result in a new or changed status of one or more Configuration Item (CI). Simply stated a change is any task or action that can alter the organization's IT production environment.

**2.2. In Scope for IT Change Management**

By default, all items or activities that are included in the definition of a Change are considered in-scope for the IT Change Management Process. It does not matter who in the organization performs the Change, if it meets the definition of a Change, it must follow the IT Change Management Process.

**Examples of Changes in scope:**

* Deployments / removals of hardware in production.
* Software, code, and / or configuration updates to applications or hardware that modify or alter the function, business process, or performance of that service or system.
* Updates from the vendor to software-as-a-service (SaaS) applications.
* Bulk loads of data by IT of 50 records or more in North America or 500 records or more in EMEA.

**2.3. Out of Scope**

Items or activities that do not meet the definition of a Change above, would not be required to follow the IT Change Management Process.

**Examples of items or activities out of scope**:

* Service Requests (access management activities, password resets, user account setup or modification, new report creation, web or database content updates, etc.)
* Single user IT Support / Incident Management for desktop / laptops and local applications
* Business transactions carried out in systems performed by business users as part of the normal course of business.
* Mass data loads performed by business end users as part of the normal course of business, following business process controls

**2.4. Change Exemptions**

For items or activities that may meet or are unclear if they meet the definition of Change, the Change Exemption process exists to provide clarity to specific situations, circumstances, or activities.

To propose a Change Exemption, a ServiceNow Request must be submitted to request approval from CAB and for future tracking purpose. Approved Change Exemptions will be documented in SharePoint, Global IT Change Management folder.

**Examples:**

* Changes to non-production applications or infrastructure.
* Windows Upgrades,
* Monthly scheduled maintenance
* Non-data center site cabling
* Changes to individual PCs settings, user preferences, etc.

**Change Exemption Review Process**

* If an item or activities categorized as a Change Exemption causes any major incident (P1, P2, P3) the Change Exemption will be removed be removed until reviewed potentially re-approved by the CAB.
* Change Exemptions will be reviewed annually and re-approved by the CAB.
* No Change Exemptions will be approved for in scope SOX applications.

**2.5. Definitions**

* **Approver:** A member of the Approval Groups for the platform or service being changed or affected. Responsible for assuring the total quality of all requests including all documentation requirements. Has the authority to approve or reject changes.
* **Approval Group:** Group of individuals authorized and responsible for the review and approval of Change Requests.
* **Back Out Plan:** A contingency plan of step-by-step instructions with defined success criteria (with sufficient detail to allow an individual with similar skills to execute the plan and is understood by all approvers) to minimize any disruption of service if a change implementation does not go as planned.
* **Backed Out Change:** If a change was not completed and backed out, all parties impacted by the unsuccessful completion of the change must be notified. A backed out Change Request must be closed as an Unsuccessful change and updated to reflect issues requiring the back out.
* **Black Out Window** (*also referred to as a financial freeze):* Windows in change calendar when no change should be deployed, or certain specific types of changes should not be deployed.
* **Bulk Adds, Updates, Deletes:** When a data update or change is performed via a direct system / data base manipulation that bypasses established online end user GUI interface for the sake of speed of execution. It can be risky bypassing established and tested online end user GUI interfaces functionality hence a Change Request is required. Loading bad data in applications that are driven by configuration data can result in making it inoperable. Similarly, adding or removing user accounts in bulk, may lead to business disruption with users unable to access required IT services. To mitigate these risks, it’s important to follow good Change Management practices. For example:
* Load data in the test environment where applicable, and confirm that the result is as expected
* Schedule the load when the application is not in use by the business (in case the result is not as expected so that it can be restored from backup)
* Back up the application’s production data or database
* Upload the Bulk changes
* Validate that the result is as expected or restore from backup
* **Business Approver:** Person who confirms that the proper testing and validation has occurred and is ready to proceed into production.
* **Business Hours Change:** Implementing new technology, setup, or take down of non-critical sites and third party-initiated changes that are low risk and have no business impact.
* **Business Impact Analysis:** is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a accident, emergency or disaster.
* **Change Advisory Board (CAB):** A team whose goal is to provide cross-functional visibility to all normal change requests, to assist the change management team in the assessment and prioritization, and to ultimately approve or deny change requests.
* **Change**: A change is defined as the addition, modification or removal of a production IT Service or an associated service component / documentation that may result in a new or changed status of one or more Configuration Item (CI). Simply stated a change is any task or action that can alter the organization's IT production environment.
* **Change Management:** The process of requesting, analysing, developing, approving, implementing, and reviewing a planned or unplanned change within the IT infrastructure. Start the Change Management process as soon as the customer, business or IT management authorizes the planning of the change, which typically should be well in advance of the minimum lead time.
* **Communication Plan**: Information designed to inform the impacted teams of the event timing and to provide a description of the included updates and their benefits.
* **Configuration Items (CI)**: A configuration item is any component or service asset that needs to be managed to deliver an IT service. Within [ORG] all production IT devices, systems, applications, business services, or other significant components of the infrastructure are defined as CIs.
* **Configuration Management Database (CMDB):** A database that holds Information about each CI within the defined scope and is maintained throughout its lifecycle under change management process.
* **Emergency CAB**: A subset of the CAB that is responsible for changes that are considered emergency change.
* **Emergency Change** (Break / Fix): A change required to immediately restore service or to avoid an outage where no other workaround is available. A change that must be implemented as soon as possible, for example to resolve a major incident or implement a security patch.
* **Implementation:** The enactment of a change to a platform, service or facility.
* **Implementation Plan**: A step-by-step set of instructions detailing information on how the proposed change will be implemented and tested. Level of detail must be sufficient for a person with similar skill to execute the implementation successfully and be understood by all reviewers / approvers.
* **Implementer**: The person / assignee or group of individuals who perform implementation of a change activity. If the Implementer does not have Change Management system access, it is the responsibility of change owner to close the Change Request with success / failure detail.
* **Lead Time**: The required amount of time between when a Change Request is submitted and the change start date / time.
* **Maintenance Windows**: A maintenance window is a defined period during which planned outages and routine changes to production services and systems may occur. The purpose of defining standard maintenance windows is to allow clients of the service to prepare for possible disruption or changes.
* **Normal Change**: A Normal Change is planned and submitted within defined submission lead times and requires explicit approval from Assignment Group Managers, CI approval group, Business Owners and UAT Approver (for application / software releases), and Global CAB as relevant. Normal Changes are further categorized into low, moderate or high risk. Please refer to the Risk Assessment Calculator below for determining the level of risk
* **Opened By (Change Owner):** The IT staff member submitting and owning the Change Request.
* **Operational Testing** **(OAT):** Testing done by infrastructure before the solution is released or deployed when no UAT testing can be performed.
* **Out of Scope:** A pre-defined subset of changes that have been identified as having no impact or outside the scope of the Change Management process. They require the submission of a Request for Change for tracking and recordkeeping purposes
* **Post Implementation Review (PIR):** A review that is conducted when a change implementation has not been successful.
* **Post Implementation Testing (PIT):** is a form of testing which is used to verify the success of a deployment into a production environment and ensure that it is operational.
* **Post Implementation Testing Approver / PIT Approver:** Personresponsible for validating that the system functions as expected after a change is implemented and providing evidence of the testing results.
* **Requested By (Change Requestor):**  Person requesting a corrective action, preventative action or defect repair to the production environment.
* **Risk Assessment:** A matrix of the level of risk for each aspect of a change scope, impact, complexity, severity, users, and location.
* **Standard Change:** A pre-authorized change that is low risk, relatively common and follows a specified procedure or work instruction. A standard change is one that is frequently implemented, has repeatable implementation steps, and has a proven history of success.
* **Successful Change:** A change is considered successful if it was completed as planned within the agreed change window without having to implement a back out plan.
* **Urgent Change:** An expedited change that does not follow the prescribed submission lead time but is implemented during standard maintenance windows. It follows the same approval process defined for Normal Changes.
* **User Acceptance Testing (UAT):** The process of verifying that the solution works for the business unit or user.
* **User Acceptance Testing Approver / UAT Approver:** Person responsible for validating accuracy of testing and providing evidence of testing results.
* **Unsuccessful Change:** A change is considered unsuccessful if it needed to be backed out or exceeds planned change window (or retrospectively causes an Incident to occur upon or after implementation).

**Chapter 3. Change Management Process**

Change Requests must be created within ServiceNow, which is [ORG]’s selected technology platform for IT Service Management.

**3.1.** **Standard Change**

The process to implement a Standard change is described below:

To request approval of a new standard template, the Change Requestor will need to submit a new standard change template proposal available in ServiceNow. All requests for new additions to the Standard Change Library (templates) are processed and approved through the GCAB.

The process to implement a standard change is as described below:

* The Change Requester submits the standard change request via the ServiceNow tool for the Assignment Group Manager’s approval including the completed UAT / OAT template and the PIT Template (Plan).
* The change needs to be submitted at least 1 business day in advance of the change implementation
* The change is built, tested and deployed as outlined in the Standard Change Template
* If the change is successful, the Change Implementer updates the CMDB (if necessary) and closes the Change Request ticket
* If the change is unsuccessful, the Change Implementer executes the back-out plan as applicable, completes the Post Implementation Review (PIR) and submits the PIR for approval (Director or above). This approval closes the change record
* Failed standard changes are reviewed at the next GCAB and the Change Manager and / or GCAB will determine if the Standard Change Template should be removed from the Standard Change Library. Also, if the PIR identifies any actions, such as missing steps, the CAB must ensure the Standard Template is appropriately updated

Please refer to [Appendix 1](#_Appendix_1_–) for the Standard Change Process Flow swim lane.

**3.2. Normal Change**

The process to implement a normal change is as described below:

* Ensure appropriate sponsorship discussions have occurred with relevant stakeholders / leadership prior to initiating the change process within ServiceNow
* The Change Requester submits the change request, identifying whether the change is Low, Moderate or High risk based on the Risk Assessment
* Change request is routed to the relevant approval groups based on the selected CI(s) and Risk level
  + **Low Risk Changes:**
    - A change is defined as low risk if it’s contained within a single country / business unit or impacts a non-critical tier 3 service / application. A very minor change with no change to user experience / no detrimental impact if the change fails.
    - Needs to be submitted for approval at least 1 business day in advance of implementing the change
    - Requires approvals from the Assignment Group Manager and the CI approval group, Business Owners and UAT Approver (for application / software releases)
  + **Moderate Risk Changes:**
    - A change is defined as Moderate Risk, if it impacts more than one country / business unit, impacts a Tier 2 application (or) the implementation may impact the user experience
    - Needs to be submitted for approval at least 1 week in advance of implementing the change
    - Requires approvals from the Assignment Group Manager, CI approval group, Business Owners and UAT Approvers (for application / software releases), and GCAB for global CIs
  + **High Risk Changes:**
    - A change is defined as High Risk, if it impacts multiple countries / business units, impacts a Tier 1 application or implements significant changes to the user experience / failure of the change may cause significant business impact or a history of success has not been established
    - Needs to be submitted for GCAB approval at least 2 weeks in advance of implementing the change
    - Requires approvals from the Assignment Group Manager, CI approval group, Business Owners and UAT Approver (for application / software releases), and GCAB
* All change types require the completed UAT / OAT template and the PIT Template (Plan) to be attached for approvals.
* When all approvals are obtained, the Change Implementer proceeds to deploy the change according to the approved schedule. If all approvals are not obtained, the change cannot be implemented and will either need to be cancelled or rescheduled
* If a change is rejected, the Change Requester will be notified of the reasons for rejection and the change is reset back to a “New Change” status. The change will need to be resubmitted after the corrections have been made
* The Change Implementer updates the Change Record after the change is deployed
  + Ensures the FINAL PIT Template is completed and attached
  + If the change is successful, the Change Implementer updates the CMDB as necessary or closes the Change Request.
  + If the change is unsuccessful the Change Implementer executes the back-out plan, completes the PIR and submits for approval (Director or above).
  + In some cases where the change exceeds the allocated change window but there is no business impact, the Change Implementer, in discussions with the Business / Assignment Group Manager, may decide to proceed with the change despite being outside the scheduled window.
* The VP or above approval on the PIR will close the change ticket
* The Change Manager validates the PIR record and provides feedback where necessary

Please refer to [Appendix 2](#_Appendix_2_–) for the Normal Change Process Flow swim lane.

**3.3. Emergency Change**

An Emergency Change is implemented to resolve an outage or a pending outage or to address a security or regulatory issue. A verbal approval must be obtained from the Assignment Group Director (or delegate) and the impacted stakeholder(s). The change is documented after the implementation has been completed and approved by the Emergency CAB (E-CAB). The process to implement an Emergency Change is as described below:

* The Change Requester determines that an Emergency Change is required (change needed to fix the Incident)
* The Change Requester immediately contacts the Assignment Group Director (or delegate) and the impacted stakeholder(s) to obtain a verbal approval to implement the change
* If the change is not approved, then the Change Requester shall follow the Normal Change process.
* If the change is approved, the Change Requestor contacts the Change Implementer who proceeds to immediately build, test (If possible) and implement the change
* The Change Requester submits an Emergency Change Record in Service Now (within 24 hours of Implementation) and submits to the E-CAB for formal approval
* The Change Implementor, updates CMDB CIs as relevant. All changes to CI’s are validated and approved by the Assignment Group Managers
* Attach completed UAT / OAT template and the PIT Template FINAL
* The Change Implementor completes the PIR and submits for approval (IT Director or above).
* If the change is unsuccessful, the Change Implementer executes the back-out plan (if required), completes the PIR and submits for approval (Director or above).
* Once PIR is approved, the Change is routed to the E-CAB for final approval. E-CAB will follow-up to ensure relevant actions are followed through, and other feedback provided as needed. This approval will close the change ticket
* Please refer [to Appendix 3](#_Appendix_3_–) for the Emergency Change Process Flow swim lane.

**3.4. Risk Assessment Calculator**

Risk score is a calculated number that reflects the severity of a risk by ranking factors. Risk probability characterizes the chance that a certain event may occur. Risk impacts can affect more than one project objective. These are referred to as risk categories and are assessed independently through the matrix below.

Graphical user interface, application

Description automatically generated

For full calculator details please refer to **Appendix 6**.

**3.5. Post Implementation Review**

All Unsuccessful and Emergency Changes require a mandatory Post Implementation Review within ServiceNow which covers the following:

* Emergency Changes:
  + Reason for an emergency and what can be done to reduce the future likelihood of the emergency
  + If it’s a recurring emergency is there a problem ticket created to address root cause
* Unsuccessful Changes:
  + What was the impact to the Business?
  + Root Cause: Why was the change unsuccessful?
    - *Process failure or Business Impacting Change?*
    - *Was the testing lacking? If yes, what is the improvement plan?*
    - *Was there a proper allocation of time / resources to implement the change?*
    - *Did the backout plan function correctly for unsuccessful changes?*
  + What were the lessons learned?
  + What are the Action items or action / steps being taken to ensure this does not re-occur?

Prior to closing an approved Emergency Change or if the sub-state selected is “unsuccessful” the following PIR Steps in the Change Record will become mandatory:

**Post Implementation Review Completion Steps**

* Required PIR info must be filled in and submitted for approval to Assignment Group Director or delegate in their absence
* The PIR will be routed to the Assignment Group Director for approval
* Upon approval, the PIR task will be closed
* Ongoing audits of the PIR’s will be conducted by the Change Manager to ensure the spirit of the PIR is being adhered to and actions tracked and completed in a timely manner by the Assignment Group Director

All Emergency changes must be closed within 48 hours of completion.

**Chapter 4. Required Change Documentation**

All Change Requests require a detailed accounting of all services, functions and locations impacted or potentially impacted by the change implementation, and the degree to which their functionality will be affected or interrupted. Also describe any change or impact to the user experience. It is also important to ensure the appropriate change category is selected by the Change Requestor. Depending on category selection additional workflow approvals are required.

* Communication Plan

If an IT Change has a change to User Experience both the User Community and the IT Service Desk must be informed, and as necessary trained on these Changes. Plan must include:

• Who are the impacted Users?

• What is the impact?

• What is the training method?

• When and how will notification(s) be sent out?

* Implementation Plan
* Business Impact Analysis
* Backout Plan
* Post Implementation Test Plan
* UAT / OAT Template
* PIT Template (Plan and Final)

**User Acceptance Testing / Operational Acceptance Testing (UAT / OAT):**

Wherever possible, acceptance testing must be performed, and results must be attached to the Change Request for all Changes (Changes to Code, Configuration, Bulk Data / Access, Reports, etc.). End-to-end test scenarios should be documented before testing starts with pass criteria, master data needs, test resource assignments, sequencing, etc.

For Application / Software changes, UAT Approval is required prior to Implementation and must be triggered by the Change Requestor (in ServiceNow). The UAT approver must ensure that the test scenarios documented in the attached Global UAT Testing template, are relevant to the change being performed. The UAT approval, is an indication that the test scenarios and pass criteria have been verified and are applicable / relevant to the CI and Change in scope.

* Business owns UAT scope.
* Test resources should be assigned based on their ownership or SME’s of a process
* End to end scenarios are created that match a typical business ‘day in the life’.
  + User Stories maybe used as a starting point
  + Defects should be logged for issues identified and retested once fix is ready
* Tester access must be assigned based on the business role / function, ensuring right permissions have been granted
* All scenarios using the change request Category Application / Software must provide evidence of success using screen captures on the ‘Screenshots or error’ page. Such screen captures MUST include the time and date stamp located at the bottom right corner of the tester’s computer. Screen captures missing this time / date stamp cannot be accepted as evidence. Change requests using the Category Infrastructure must provide screen print evidence where applicable.

For Infrastructure / Security changes that are not directly business facing, OAT should be carried out by IT prior to deploying the change whenever possible (Mass loads, security firewall changes, etc.). IT Owns the testing scope including test cases and acceptance criteria.

Please refer [to Appendix 5](#_Appendix_5_–) for the UAT / OAT Template link.

**Post Implementation Testing (PIT):** PIT must be carried out for ALL changes immediately after deployment of any change to production. The specific PIT date must be included in the PIT plan. If the PIT cannot be completed immediately after deployment, a date must be agreed upon by the business along with a notation of the business reason at the time the PIT plan is created.

PIT is the last line of defense to safeguard production and should be carried out both by IT (to validate the system is operational and error free) and Business (to validate all the required changes / data loads have moved correctly and without errors) All changes must clearly document a comprehensive PIT Plan under the planning section of the Change Request. PIT Plan and Final must be attached to the Change. PIT should follow the same or similar validation test as performed during UAT, keeping the following in mind:

* Include most important and critical steps that allow maximum functionality coverage
* Include steps to test new features as well as major existing features
* Verify major impact areas
* Include any critical bugs that were found in test environment
* DO NOT overwrite the PIT Plan
* All scenarios using the change request Category Application / Software must provide evidence of success using screen captures on the ‘Screenshots or error’ page. Such screen captures MUST include the time and date stamp located at the bottom right corner of the tester’s computer. Screen captures missing this time / date stamp cannot be accepted as evidence. Change requests using the Category Infrastructure must provide screen print evidence where applicable.
* PIT is required for changes not implemented or rolled back and must include the reason PIT can't be performed.

The completion of the Post Implementation Task by the Change Implementor, is an indication that all the PIT scenarios have been carried out and with successful results by the relevant testers.

Please refer [to Appendix 5](#_Appendix_5_–) for the PIT Template link.

**Chapter 5. Change Scheduling**

**5.1. Maintenance Windows**

Maintenance windows are a predetermined period during which [ORG] and partnering organizations can reasonably perform proactive maintenance and enhancements to production environments.

The following maintenance windows specified should be used for all changes unless mitigating circumstances require alternate scheduling (an Emergency Change or Business Hours Change). See Section 2.3 Definitions for the definition of a Business Hours Change.

**Global Maintenance Window**

|  |  |  |
| --- | --- | --- |
| **Type of Change** | **Day of the Week** | **Time of Day** |
| Standard & Normal  Low / Moderate Risk Change | Monday  Tuesday  Wednesday  Thursday | 7 PM Monday thru 4 AM Tuesday  7 PM Tuesday thru 4 AM Wednesday  7 PM Wednesday thru 4 AM Thursday  7PM Thursday thru 4 AM Friday  Local Time |
| Standard & Normal  Low / Moderate / High Risk Change | Friday - Monday | 7 PM Friday thru 4 AM Monday  Local Time |

**5.2. Change Request Calendar**

All business events and approved changes are displayed in the [ORG]’s IT Change Calendar, which is available within ServiceNow Change Calendar. Change Requesters and Change Implementers should review the change calendars to identify any potential conflicts prior to picking a change implementation date.

**5.3. Change Freeze**

No normal or urgent changes to **financial systems / services** should occur during the Financial System Change Freeze unless it’s an emergency. The Global Year End Change freeze applies to Financial systems, critical Tier 1 / 2 services, and major project deployments. Exceptions require approval from executive leadership and the Emergency CAB

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Event** | **Duration** | **Event Start** | **Event End** | **Applies To** |
| Global Monthly Financial System Change Freeze | 10 Business Days | Ongoing - 1st (5) business days and Last (5) business days of the month | | All Non-Emergency Changes to SOX Financial Applications (including up and down stream impacts) |
| Global Quarterly Financial System Change Freeze | 14 Business Days | Ongoing - Last (7) business days of the quarter ending and 1st (7) business days of next quarter beginning | | All Non-Emergency Changes to SOX Financial Applications (including up and down stream impacts) |
| Global Year End Change Freeze | 20  Business Days | Starting  Ongoing: Last 10 Business days in December | Through  First 10 Business days in January | All Non-Emergency Changes to SOX Financial Applications (including up and down stream impacts) |

**5.4. Exception tab**

Changes during a change freeze require completion of the exception tab. The completed tab needs to be approved by executive leadership (VP or above) and submitted via the change approval workflow in ServiceNow to the Emergency CAB for consideration. The exception tab addresses the following concerns

• Business & Security risk (risk of implementing now vs. waiting until after the change freeze)

• Impact on production services (up and down stream) and customers

• Complexity of the proposed change

• Who has reviewed the plan and any new or modified code?

• How was the change tested and ease of backout?

**Chapter 6. Roles & Responsibilities**

Roles associated with the Change Management process are not intended to correspond with organizational job titles. In some cases, many persons might share a single role; and in other cases, a single person may assume many roles. Responsibilities may be delegated but does not remove responsibility from the individual accountable for a specific action.

**6.1. Change Requester**

The Change Requester is the person submitting and owning the Change Request. The Change Requester is usually an IT staff member. Their responsibilities include:

* Secures appropriate IT and Business approvals prior to initiating the change management process
* Completes the ServiceNow Change Request, in collaboration with the Change Implementer and ensures that the change is fully approved prior to implementing the change
* Ensure Change Requests are executed in the approved Maintenance Windows
* Ensure the change is fully tested, and relevant UAT and Business approvers are added to the Change Request
* Identify resources required to implement the change and verify availability on the planned change date and time (including DBAs, Infrastructure, UAT testers, Post Implementation testers etc.)
* Communicates status of the change back to the business or project team

**6.2. Change Implementer**

The Change Implementer / Assignee implements and monitors the change (Requester and Implementer can be same person). The Implementer’s responsibilities include:

* Assisting the Change Requester with change request ticket documentation as necessary
* Creation of the implementation plan, test plan and backout plan
* Ensure all the relevant approvals, including the UAT approval and documentation is recorded in the Change Request prior to deploying the Change
* Deploy the Change
* Ensure Post Implementation testing is completed immediately after deployment
* Ensure Change Request is completed and closed within the approved Maintenance Window
* Execute the back out plan if required and complete the PIR for Unsuccessful and Emergency Changes

**6.3. Change Approvers (Manager, CI Owner, Business and CAB approvals)**

* Thoroughly Review the Change Request prior to approval. Have relevant discussions with team members to clarify questions before approving the Change:
  + Confirm the Change is being implemented during approved maintenance windows
  + Review all the items in the Planning Section
  + Ensure Risk Assessment has been completed accurately
  + Ensure all required documentation is attached to the change record

**6.4. UAT Approvers**

* Complete the UAT testing and update the Global UAT test template with testing results
* Attach the UAT template to the Change Request
* Provide UAT approval within the Change Request as proof that the testing was successful; and the testing scenarios documented in the UAT template are comprehensive with the right results.

**6.5. PIR Approvers**

* Review the PIR thoroughly and conduct relevant discussions with the team members on the lessons learned and action outcomes
* Approve PIR’s in a timely manner (within 48 hours of Change implementation)
* Where a root cause is not known, or a permanent fix not applied, ensure a Problem Record is created and assigned to a team member with due dates
* Ensure all the documented actions are assigned to team members and completion tracked

**6.6. Global Change Manager**

The Change Manager is responsible for functional implementation and operation of the Change Management Process and its activities. The Change Manager’s responsibilities include:

* Educate IT staff on the Change Management process
* Propose and implement improvements to the Change Management process
* Create and communicate Change Management Metrics
* Chair the GCAB meeting
* Validate the type and risk of the change and escalate approval delay issues
* Ensure PIRs are conducted per the policy and actions effectively tracked
* Ongoing auditing of Changes to ensure process adherence and drive improvements
* If an unauthorized change is discovered, escalate to IT Leadership

**6.7. Global ITSM Process Owner**

The Process Owner is accountable for the success and strategic development of the Change Management Process.

**Chapter 7. GCAB Membership and Meetings**

**7.1. GCAB Membership and Participation**

The Global Change Advisory Board (GCAB) is engaged to assess all High & Moderate Risk changes and to pre-approve the use of Standard Changes Templates. Its primary purpose is to mitigate risk to the Organization by evaluating change requests from the perspective of business and end-user impact.

The GCAB includes permanent representation from all IT teams responsible for providing and supporting [ORG]’s IT services. The success of this CAB is dependent upon the contributions of its members who represent these teams. Regular GCAB meeting attendance should generally be restricted to this primary GCAB member, with other team members attending as necessary.

**7.2. Function of the GCAB**

* Regularly scheduled weekly meetings
* Review and approval of Moderate and High-Risk changes and other changes as necessary
* Review all Unsuccessful and Emergency Changes
* Assist with comprehensive service impact analysis
* Post Implementation Reviews (PIRs) for critical or failed changes
* Ensure complete and accurate documentation of change requests

**Important:** The GCAB is neither a forum nor a substitute for project planning and resource coordination.

**7.3. CAB Member Expectations**

* Have a solid understanding of the Global Change Management Process
* Read the Change thoroughly before approving
* Commit to attendance (or have a designated alternate attend in your place)
* Actively participate in GCAB discussion
* Be empowered to make decisions on behalf of [ORG] IT & Business
* Communicate to your team relevant information from GCAB meetings discussions
* Act as a Change Management advocate and resource within your team

**7.4. Emergency CAB (E-CAB)**

Emergency changes are reviewed post change by a separate Emergency CAB (E-CAB). The purpose of the E-CAB is to review emergency changes to verify they followed process and were applicable for situation.

**Chapter 8. Metrics, Reports and Meetings**

[ORG] IT will focus on a few select Key Performance Indicators (KPIs) to measure the success and efficiency of the Change Management process. As the Change Management process matures, the KPIs may change to focus on different areas that need improvement.

* Number of changes implemented by type, team
* Reduction in the number and percentage of urgent and emergency changes
* Reduction in the number of failed changes (technical failures and process failures)
* Number of changes backed-out, together with the reasons (e.g., incorrect assessment, bad build)
* Number / percentage of changes where approval exceeded the lead time
* Number of Incidents and Major Incidents resulting from Change
* Open changes past scheduled deployment date
* Number of RFCs rejected

A reporting pack including all the KPIs above will be shared and reviewed at the ITSM Process Governance forums. The purpose of this meeting is to ensure consistent adherence to process, identify lessons learned, ensure post implementation reviews are being effectively conducted and reduce the likelihood of urgent, emergency and failed changes.

**Appendix 1: STANDARD CHANGE MANAGEMENT PROCESS**

Diagram

Description automatically generated

**Appendix 2: NORMAL CHANGE MANAGEMENT PROCESS**

Diagram

Description automatically generated

Note: Application / Software releases require Business and UAT approval. Within Service Now, please select the change category “Application / Software” which will force both approvals via the tool.

**Appendix 3: EMERGENCY CHANGE MANAGEMENT PROCESS**

Diagram

Description automatically generated

**Appendix 4 - RACI CHART**

|  |  |
| --- | --- |
| **Obligation** | **Role Description** |
| **R**esponsible | Responsible to perform the assigned task |
| **A**ccountable (only 1 person) | Accountable to make certain work is assigned and performed |
| **C**onsulted | Consulted about how to perform the task appropriately |
| **I**nformed | Informed about key events regarding the task |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ALL CHANGES** | **Change Requestor** | **Change Implementer** | **Change Approver (s)** | **Change Manager** | **GCAB** | **Senior Leadership** | **Stakeholders** | **Project Manager** |
| Approval / Removal of Standard Templates | R | I | C | A | R |  | I | I |
| Create a Change in ServiceNow for approval\* | R / A | R | I | C | C | C | C / I | C / I |
| Review and Approve a Change in ServiceNow | C / I | C / I | R / A | C | R | R / I | R / I | I |
| Build, Test, Deploy and Verify the Change | C / I | R / A | I | C |  |  | R / I | I |
| Execute Back-out Plan | I | R / A | I | C |  | I | I | I |
| Post-Implementation Review | R | R | I | A / C |  | I | I | I |
| Close Change in ServiceNow | I | R / A | I | C |  | I | I | I |
| Update CMDB |  | R / A |  | C |  |  |  |  |
| Create Change Proposal including impact analysis and obtain approvals | R / A | C | C | C | C | C | C | I |
| Review & provide feedback on High-Risk Change Proposal | R | R | R | R | R | A / R | C | I |
| Communication of Changes | R / A | C | C | C | C | C | C | I |

\*For emergency changes the change can be created after the change has been implemented with verbal approval from immediate manager. The SN Change Requests require e-CAB approvals.

**Appendix 5: UAT / OAT and PIT TEMPLATE LINKS**

UAT / OAT TEMPLATE

PIT TEMPLATE

**Appendix 6: RISK ASSESSMENT MATRIX**

Graphical user interface, application

Description automatically generated

**Appendix 7: PROCESS UPDATES COMMUNICATION PLAN**

* Understand the ask or request
* Present to Global CAB for approval and socialization
* Officially update the SRC Global IT Change Management Process
* Provide updates to Functional CABs for local training / support
* Formal communication outward to ALL IT and / or Business
* Utilize IT User Survey for on-going continuous improvement