

## CHANGE MANAGEMENT PROCESS

### Document Control Sheet

<b>VERSION</b>	1.0
<b>PROCESS NAME</b>	Change Management Process
<b>PROCESS OWNER</b>	IT Governance & Service Management
<b>STATUS</b>	APPROVED
<b>DATE SIGNED OFF</b>	20-06-2022
<b>REVIEW FREQUENCY</b>	Triennial
<b>CLASSIFICATION</b>	INTERNAL

*\*Review to the document may be made when the organization experiences significant changes or as the need arises within the three-year review cycle.*

## CHANGE MANAGEMENT PROCESS






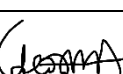
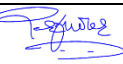

### Version and Update History

Date	Document Version	Document Revision History	Document Author/Reviser
09-06-2022	1.0	Document Creation and review by IT's stakeholders	Information Technology Group

### Distribution List

Name	Version	Date
All staff of IT	1.0	09-06-2022

### Approvals

Date	Document Version	Approver Name and Title	Approver Signature
9-6-2022	1.0	Head IT Governance & Enterprise Architecture	 17/6/2022
		Head Enterprise Infrastructure	 20/6/2022
		Head IT E-Channels Services	 20/6/2022
		Head Enterprise Application	 21/6/2022
		Chief Information Officer / Head, IT	 21/6/2022
		Chief Information Security Officer	 21/6/2022
		Chief Compliance Officer	 19/08/2022
		Chief Operating Officer	 19/08/22

Change Management Process

# CHANGE MANAGEMENT PROCESS

## Contents

1.0	Introduction .....	4
1.1	Purpose .....	4
1.2	Scope .....	4
1.2.1	Out of Scope .....	5
1.3	User .....	5
2.0	Vision, Objectives and Policy .....	5
2.1	Vision .....	5
2.2	Objectives .....	6
2.3	Policy .....	6
3.0	Change Management Process overview .....	8
3.1	Change Types and Categories .....	8
3.1.1	Prioritization .....	11
3.2	Process Flow .....	12
3.3	Process Narrative .....	13
4.0	Roles & Responsibilities .....	15
4.1	Change Management SLA .....	17
4.2	RACI Matrix .....	18
4.3	CAB Meetings .....	18
4.4	Change Schedule .....	19
5.0	Metrics & KPI .....	19
6.0	Supporting Document .....	21
7.0	Appendix .....	21
Inputs	.....	21
Outputs	.....	21
8.0	Appendix B .....	22

# CHANGE MANAGEMENT PROCESS

## 1.0 Introduction

PremiumTrust Bank is a commercial and retail banking organisation within the Federal Republic of Nigeria. PremiumTrust Bank is committed to ensuring the delivery of quality services to our external and internal customers, in support of their goals and objectives.

Consequently, PremiumTrust Bank instituted a program to develop, implement and maintain a Management System in accordance with ISO 20000-1:2018 international standards, to address the needs and expectations of interested parties (internal and external stakeholders), as well as support the bank's strategic priorities.

This is the Change Management Process which describes the standardized methods and procedures used for efficient and prompt handling of all changes, to minimize the impact of change-related incidents upon service quality, and consequently improve the day-to-day operations of the organization.

### 1.1 Purpose

The purpose of this document is to set out the Change Management Process within PremiumTrust Bank. This document describes the vision, objectives and policies, process overview, roles and responsibilities, metrics, and key performance indicators, and supporting documents.

### 1.2 Scope

This covers all PremiumTrust Bank's computing systems and platforms. The primary functional components covered in the Change Management process include:

- ✦ **SDLC** – Changes handled through the formal software development life cycle will be included within this change management program.
- ✦ **Hardware** – Installation, modification, removal or relocation of computing equipment.
- ✦ **Software** – Installation, patching, upgrade or removal of software products including operating systems, access methods, commercial off-the-shelf (COTS) packages, internally developed applications, packages and utilities.
- ✦ **Database** – Changes to databases or files such as additions, reorganizations, and major maintenance.
- ✦ **Application** – Application changes being promoted to production as well as the integration of new application systems and the removal of obsolete elements.
- ✦ **Moves, Adds, Changes and Deletes** – Changes to system configuration.

# CHANGE MANAGEMENT PROCESS

- ✦ **Schedule Changes** - Requests for creation, deletion, or revision to job schedules, back-up schedules or other regularly scheduled jobs managed by Information Technology department.
- ✦ **Desktop** – Any modification or relocation of desktop equipment and services.
- ✦ **Generic and Miscellaneous Changes** – Any changes that are required to complete tasks associated with normal job requirements.

## 1.2.1 Out of Scope

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

- ✦ Contingency/Disaster Recovery.
- ✦ Changes to non-production elements or resources.
- ✦ Changes made within the daily administrative process. Examples of daily administrative tasks are:
  - Password resets
  - User adds/deletes
  - User modifications
  - Adding, deleting or revising security groups
- ✦ Rebooting machines when there is no change to the configuration of the system
- ✦ Switch Port reset and update for NAC.
- ✦ File permission changes.
- ✦ Add backup targets to the enterprise backup solution.
- ✦ Including Standard Operating Procedures.

## 1.3 User

Users of this document and its content shall be all staff of PremiumTrust Bank

## 2.0 Vision, Objectives and Policy

### 2.1 Vision

The vision of Change Management Process is to control the lifecycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services.

## CHANGE MANAGEMENT PROCESS

### 2.2 Objectives

The objectives to conduct a Change Management Process exercise across the Bank is to ensure that changes to IT services and their associated components are recorded and then evaluated, authorized, prioritized, planned, tested, implemented, documented, and reviewed in a controlled manner to:

- ✦ Provide standardized methods to meet the change management requirements supporting PremiumTrust Bank's operations.
- ✦ Accomplish IT changes in the most efficient manner while minimizing the business impact, costs, risks, change related incidents and problems.
- ✦ Increase the number of changes an organization can absorb without adverse impact
- ✦ Reduce the number of backed-out and failed changes
- ✦ Respond quickly to changing business requirements
- ✦ Enable the business to swiftly address customer dissatisfaction
- ✦ Allow the business to rapidly respond to changing legislation and regulatory needs
- ✦ Minimize the exposure to risk
- ✦ Review and approve the number of changes that can be permitted to be pushed to production within the same change window.

### 2.3 Policy

#### General

- ✦ Formal change management procedures must be utilized for all amendments to IT systems (IT infrastructure) used for live processing.
- ✦ All changes to programs must be reviewed, tested, and properly authorized in a test environment before moving them to the live environment.

#### Change Request Initiation

- ✦ Changes must be initiated by formal requests – Request for Change (RFC)
- ✦ The following items of information must be supplied on a change request for it to be processed and approved.
  - Initiator name and contact details
  - Summary of change
  - Change Description
  - Business Justification
  - Service(s) Affected

## CHANGE MANAGEMENT PROCESS

- Impact
- Urgency
- Roll back Plan
- ✦ Relevant **documentation** should be attached to the change record if required. The list of documentation to be presented to the CAB include but not limited to the following.
  - Test scripts
  - User Acceptance Test
  - Business Requirement Documentation
  - Group Head Approval
  - Risk Assessment
  - Implementation plan
  - Roll back plan
  - Enterprise Architecture Diagram
  - Any other relevant document

### Assessment of Changes

- ✦ Changes must be categorized and prioritized to reduce the impact on live systems.
- ✦ Changes must be assessed from the dual perspective of technical and business risk.
- ✦ This should include the timing of the proposed change and its potential impact on security, capacity, service continuity plans and release management, amongst other areas.
- ✦ Change Initiators must not assess their own changes. The technical assessor must have sufficient technical knowledge to be able to give an informed opinion regarding the change subject.

### Approval, Schedule of Change and Control

- ✦ Appropriate change authorities e.g., Change Advisory Board (CAB), will be responsible for the review and approval of change requests. This will be defined as part of the change management process.
- ✦ Every RFC must be assigned a precise status of Approved, Cancelled, or Represent, after Change authority's review, and requestors must be kept informed about the status of their request.
- ✦ Change Initiators must not approve their own changes. Where possible the assessors of a change should be different to the approver(s).
- ✦ Back-out plans must exist for all approved changes.
- ✦ Approved change must be schedule within defined maintenance windows except for emergency changes.
- ✦ Approved and planned changes must be detailed

## CHANGE MANAGEMENT PROCESS

- ✦ Changes must be tested in accordance with the impact and resource assessment (wherever possible)
- ✦ Test results must be reviewed and approved by owners and IT Quality Assurance before the update is made to the executable program code.
- ✦ Application changes must follow approved solution delivery methodology
- ✦ When changes are implemented, the associated documentation, procedures and related CIs must be updated accordingly, including updating related controls and plans (e.g., continuity plan) if required.

### Review, Evaluation and Reporting

- ✦ The success of changes will be reviewed at an appropriate time after their implementation to judge their success or otherwise. The review will be about:
  - the change met the required objectives, standards, and functionality
  - users and customers are happy with the results
  - the change was implemented as per the planned resources, agreed schedules and anticipated costs
  - there are related incidents or problems since the change was implemented
  - There were unexpected side effects
  - There are opportunities to improve the next similar change
- ✦ The Change Manager may obtain feedback from the originator of the change request which will then be considered as part of the review.
- ✦ Unsuccessful changes shall be reviewed, and further actions agreed
- ✦ Statistics will be collated on change management for input to the regular IT service report and the Change Advisory Board.

### 3.0 Change Management Process overview

#### 3.1 Change Types and Categories

Presented in the table below are three types of change including:

- ✦ Standard,
- ✦ Emergency
- ✦ Normal.



## CHANGE MANAGEMENT PROCESS

Type	Description
Standard Change	<p>Standard change refers to a pre-authorized or pre-approved change that is low risk, relatively common and follows a procedure or work instruction. Standard change shall meet the following descriptions:</p> <ul style="list-style-type: none"> <li>• Logged and approved by the Requester's Head of Unit and CIO and Change Manager notified.</li> <li>• Defined trigger to initiate RFC</li> <li>• Tasks are well known, documented, and proven</li> <li>• Budgetary approval within control of change requestor</li> <li>• Risk usually low always well understood</li> <li>• E.g., could be triggered by Request Fulfilment process</li> </ul>
Emergency change	<p>Emergency change, a change that must be implemented as soon as possible, for example to resolve a major incident or implement a security patch. Emergency changes would basically fall under these categories</p> <ol style="list-style-type: none"> <li>Changes which are urgently required to resolve a major incident or problem.</li> <li>To fix a fault in a business-critical system</li> <li>It requires Different authorizations (ECAB)</li> <li>It requires Retrospective documentation.</li> <li>Changes required to avoid an imminent service failure or resolve failures.</li> </ol> <p>These will be fast-tracked through the CM Process and given additional resource where required.</p> <p><b>Note</b> that a failure in forward planning to log a normal change in enough time to obtain approval does not constitute an emergency change and will not be treated as such</p>

## CHANGE MANAGEMENT PROCESS

Normal change	<p>Any service change that is not a standard change or an emergency change. These are changes, which can be further categorized into <b>minor or major</b> based on risk and impact. Normal changes are:</p> <ol style="list-style-type: none"> <li>Changes that must follow the complete change management process; require a full range of assessment and authorizations to ensure completeness and the least possible disruption in service.</li> <li>Changes that must be reviewed and approved by the appropriate change authorities on the change management portal.</li> </ol>
---------------	---

Depending on the level of costs, resource requirements and risks involved, and on the scope and relationship to other changes, (Normal) changes are further categorized into:

- ✦ Minor
- ✦ Major,

This categorization is used to assign appropriate change authority.

Category	Description	Change Authority
Minor Change	Changes with low impact and require few resources to implement. Change is of <b>Low Impact, Low Risk.</b>	Change Manager
Major Change	<p>Changes that have significant impact on services and the customer are regarded as major change and shall go through: Design and Transition of New or Changed Services process in addition, the following changes shall go through design and transition:</p> <ol style="list-style-type: none"> <li>the removal or decommissioning of a service</li> <li>the transfer of a service from one vendor to another vendor.</li> </ol> <p>It should be noted that the above should be managed as a project.</p>	Subject to the change approval process on the change portal

## CHANGE MANAGEMENT PROCESS

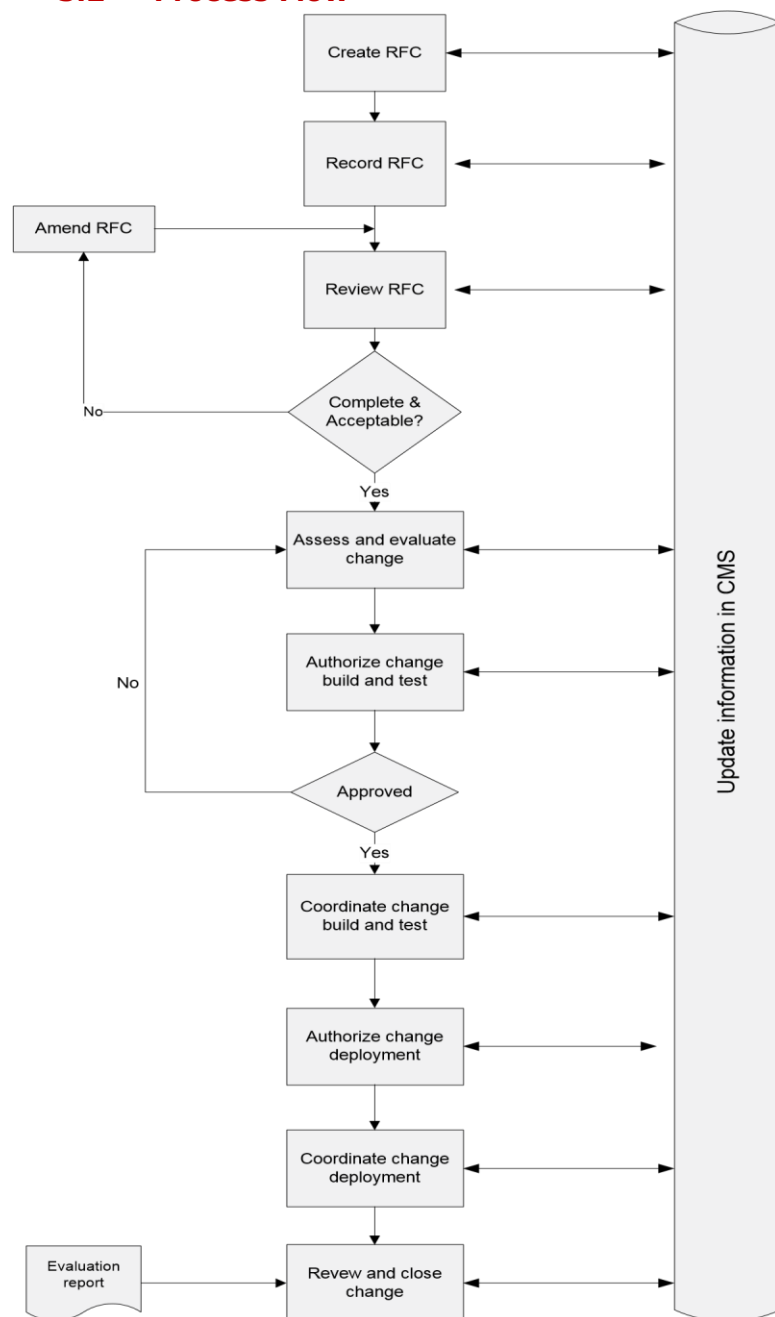
### 3.1.1 Prioritization

Based on **impact** and **urgency** (how long implementation can afford to be delayed), changes will be prioritized to establish the order in which they will be considered.

Priority	Description
Immediate	Fixing identified errors that put lives at risk, causing significant loss of revenue, Inability to deliver public facing services or requires immediate action (Emergency changes).
High	Fixing identified errors that are severely affecting some key users or impacting a large number of users such as implementing enhancement that support new business initiatives (e.g. new or enhance service), meet legislative or other requirements, respond to short term opportunities.
Medium	Fixing identified errors that have no severe impact, but cannot wait until next scheduled release or upgrade, such as, implementing improvements that maintains business viability or supports planned initiatives.
Low	Fixing identified errors that can wait until the next scheduled release or upgrade, improvements in a service functionality, or add new facilities

# CHANGE MANAGEMENT PROCESS

## 3.2 Process Flow



Change Management Process

## CHANGE MANAGEMENT PROCESS

### 3.3 Process Narrative

The following steps are carried out in the change management process.

Step	Description	Who
Create RFC	<ul style="list-style-type: none"> <li>Raise a Request for Change (RFC) or <b>Change proposal</b></li> <li>Create a Change record within the Change Management system detailing all the required information</li> </ul>	Change Initiator
Record RFC	<ul style="list-style-type: none"> <li>Create a Change record within the change portal system detailing all the required information</li> </ul>	Change Manager
Review RFC for completeness	<ul style="list-style-type: none"> <li>The change request needs to be checked that all the required information has been entered. The change should be referred or rejected if it is:               <ol style="list-style-type: none"> <li>Totally impractical</li> <li>A duplicate change request.</li> <li>Incomplete</li> <li>Check for BRDs and UAT duly signed by ISSC and the business owners</li> <li>Check for approvals of the Initiator's head of department</li> <li>Check for appropriately tested Roll-back plan.</li> </ol> </li> </ul>	Change Manager
Assess and evaluate change	<ul style="list-style-type: none"> <li>Assess implications of the proposed change from a business and a technical point of view.</li> <li>Assess and evaluate change based on impact and risk.</li> <li>This should include the timing and impact on security, capacity, service continuity plans and release management, amongst other areas</li> <li>Assess and evaluate, determine change category based on impact and risk.</li> <li>Consider potential impact of failed change on services and service assets/CIs. Prioritize change.</li> </ul>	Change Manager

## CHANGE MANAGEMENT PROCESS

Step	Description	Who
Authorize Change build and test	<ul style="list-style-type: none"> <li>Obtain formal authorization from a change authority</li> <li>Approve if OK, Reject if not. Refer to change manger or initiator if more information required</li> </ul>	Change Authority
Coordinate change build and test	<ul style="list-style-type: none"> <li><b>Schedule</b> authorized change</li> <li>Formally pass authorized change to the relevant technical groups for building (work order)</li> <li>Coordinate building and testing activities</li> <li>Change that is part of a release is coordinated by <i>Release and deployment process</i></li> </ul>	Change Manager
Authorize Change deployment	<ul style="list-style-type: none"> <li>Evaluate the design, build and testing of the change for related risks and to ensure it meets requirements.</li> <li>Approve if OK, or refer to change manger or builder if more work is required</li> </ul>	Subject to the Change Authority on the change Portal
Coordinate Change deployment	<ul style="list-style-type: none"> <li>Coordinate deployment activities</li> <li>Deployment should be scheduled when least impact on live services is likely</li> <li>Make the change on the date and time scheduled. Test to ensure it has worked successfully</li> <li>Remove the change if unsuccessful (Roll-back change)</li> <li>Deploying a release is part of the release and deployment process</li> </ul>	Change Manager
Review and close change	<ul style="list-style-type: none"> <li><b>Evaluate change</b> for performance and absence of unaccepted risks.</li> <li>Review the change records to ensure that no related incidents or problems have arisen since the change was made</li> <li>Close with a status of successful or Unsuccessful</li> </ul>	IT Governance/IT Change Manager
Update CMS (CMDB)	<ul style="list-style-type: none"> <li>Update change and configuration information in CMS from initiation to closure</li> </ul>	Change Manager/Configuration Manager

### Change Management Process

## CHANGE MANAGEMENT PROCESS

### 4.0 Roles & Responsibilities

Role	Responsibilities
Change Initiator/Change Implementer	<ul style="list-style-type: none"> <li>Responsible for identifying the need for a change and providing the required information to allow the change request to be assessed</li> <li>Get relevant approvals from all stakeholders and attach in the RFC</li> <li>Works with the change builder/ developer or vendor to define the exact requirements of the change</li> <li>May be involved in user acceptance testing of the change once built</li> <li>Creates the items necessary for the change (e.g., new or revised software programs)</li> <li>Performs system testing and liaises with the change originator to perform UAT</li> <li>Plans the details of the change, tests it prior and post implementation</li> <li>Provides feedback to the change manager on the status of the change</li> </ul>
Change Management Team defined on the Portal / IT Governance Team	<ul style="list-style-type: none"> <li>Owner of the change management process</li> <li>Reviews every RFC for the relevant attachments and stakeholders' concurrences</li> <li>Responsible for identifying improvements to the process and ensuring it is adequately resourced</li> <li>Provides information regarding the success rates of the process</li> <li>Chairs the Change Advisory Board meetings and coordinates its activities</li> </ul>

## CHANGE MANAGEMENT PROCESS

Role	Responsibilities
	<ul style="list-style-type: none"> <li>Facilitate the CAB meetings and co-ordinates its activities</li> <li>Reviews and approves or rejects Minor changes based on the information provided</li> <li>Runs the process on a day-to-day basis</li> <li>Performs the initial check and classification of changes</li> <li>Maintains the change schedule and ensures that all changes are in the correct status</li> <li>Assist and work with the configuration Manager in updating changes made to CIs because of implemented change request.</li> </ul>
Change Advisory Board	<ul style="list-style-type: none"> <li>This is a committee made up of IT unit heads, Compliance, Risk and Business units responsible for assessing and prioritizing every change request, changes can only be implemented by the concurrence of the CAB.</li> <li>Every change request (RFC) must be assessed for impact and resource requirements, roll back strategy and the Configuration Item (CI) to be affected before being considered for approval by the Change Advisory Board (CAB).</li> <li>The Chairman of the CAB shall be nominated by the members of the CAB. The members of the board shall be constituted of staff whose roles are as contained below. Other members may be inducted to the board as deemed necessary by the management of IT services or as recommended by the board.</li> <li>To be nominated by the CAB – Chairman CAB</li> <li>Head, Operational Risk</li> <li>Chief Information Security Officer</li> <li>Head, IT Channels Services</li> <li>Head, Project Management</li> </ul>

Change Management Process



## CHANGE MANAGEMENT PROCESS

Role	Responsibilities
	<ul style="list-style-type: none"> <li>• Head, Enterprise Application Services</li> <li>• Head, IT Service Management</li> <li>• Head, Infrastructure Management</li> <li>• Head, IT Governance</li> <li>• GH, E-business</li> <li>• GH, Compliance</li> <li>• Customer Engagement and Experience Centre Nominee</li> <li>• Operation Directorate Nominee</li> </ul>

### 4.1 Change Management SLA

Task	Responsibilities	Timeline
Initiation	Change Initiator	<24 Hours before CAB meeting
Review	Change Manager	1 Day
Planning	Change Manager	1 Day
Review Implementation Plan	CAB & Change Manager	1 Hour per Change
Approve Implementation Plan/Change Request	CAB	1 Day (Subject to the number of RFC reviewed)

## CHANGE MANAGEMENT PROCESS

### 4.2 RACI Matrix

The table below clarifies the responsibilities at each step using the RACI method.

R= Responsible      A= Accountable      C= Consulted      I= Informed

S/N	Step	Change Initiator	Change Manager	CAB	Change Implementer
1	Raise change request	A/R	I	I	I
2	Record RFC	I	A/R		I
3	Classify and Review RFC for completeness	C	R	A	I
4	Amend RFC	A/R	C	I	I
5	Assess and evaluate change	I	R	A	I
6	Authorize Change build and test	I	R	R/A	I
7	Coordinate change build and test	I	R	A	C
8	Authorize Change deployment	I	R	R/A	C
9	Coordinate Change deployment	I	R	A	C
10	Schedule Change	I	R	A	I
11	Prepare and Test Change	A/R	I	I	A/R
12	Implement Change	I	I	A	R
13	Roll Back Change	I	I	A	R
14	Review and close change	I/R/A	R	I	I/R/A
15	Update change and configuration information	I	R/A	I	I

### 4.3 CAB Meetings

The volume and classification of changes will be reviewed during the first few weeks of operation of the Change Management process to help to decide the most appropriate frequency of full CAB meetings.

- The frequency of CAB meetings would be communicated to all staff of IT services. In events where CAB meetings cannot hold at pre-defined periods, a new date would be communicated to staff in advance to this meeting.
- Changes to be reviewed at CAB meeting must be logged on the request for change portal.

**Change Management Process**

## CHANGE MANAGEMENT PROCESS

- Changes to be assessed cannot be logged when the meeting is ongoing. The changes being reviewed at meeting must be logged at least twenty-four hours to the commencement of the meeting.
- CAB members would be unanimous in agreements reached and where members are unable to reach a decision, the initiator shall be responsible with fulfilling the CAB's exceptions raised during the CAN session.
- CAB meeting would be chaired by the change manager or delegated to a CAB member if he/she is unavailable.
- Minutes of the CAB meeting showing the concurrence of all stakeholders involved shall be maintained and documented by the Change Manager.

CAB members are expected to attend CAB meetings. Members are expected to send in representatives should they be unavailable during meeting times.

### 4.4 Change Schedule

The Change Manager is responsible for issuing the change schedule monthly. This will set out details of the changes to be implemented monthly and will form the basis for planning the deployment of releases. The following information will be included:

- + Date and time of implementation
- + Change number
- + Change description
- + Systems and users impacted
- + Expected duration of change

It is anticipated that this information will also be made available on the Intranet or Service desk tool.

### 5.0 Metrics & KPI

The following KPIs will be used on a regular basis to evidence the successful operation of the change management process:

## CHANGE MANAGEMENT PROCESS

S/N	Metrics	KPI
1.	Number of changes per month that are known to have circumvented the change management process	$\leq 0\%$
2.	Number of emergency changes raised per month	$\leq 5\%$
3.	Percentage changes implemented successfully on first attempt	$\geq 95\%$
4.	Percentage of changes for which the expected benefits are realised	$\geq 95\%$
5.	Changes performed during business hours	$\leq 5\%$
6.	Reduction in the change request backlog	$\leq 15\%$
7.	% Of change approved but not implemented	$= 100$

The following reports will also be produced by the Change Manager on a regular basis and reviewed as part of the CAB meetings to identify trends and possible process improvements:

- Number of changes raised and closed by week/month.
- Breakdown of categories of change requests raised i.e., Normal, Emergency and Major
- Average time to process a change request of each category.
- Percentage successful change requests
- Sources of change requests e.g., business area
- Types of change requests e.g., server, network or by business application

Requirements for further reports will be reviewed on a regular basis by the IT GRC team. Identified improvements will be input to the Service Improvement Plan.

## CHANGE MANAGEMENT PROCESS

### 6.0 Supporting Document

Reference	Document's Name
Change Approval Authority	Change Approval Authority
ISO/IEC 20000-1: 2018 Service Management System Requirements	Document of external origin

### 7.0 Appendix

#### Inputs

Input	From
Change, RFCs, Change proposal	Service Desk, Technical Team, Customer
Projected Service Outage	Technical Team, Supplier
Assets and CIs details (baseline)	Configuration management process (CMDB)
Release, deployment, Test, and back-out plans	Release and deployment process, Change implementer
Change plan, Test and Evaluation reports	Change implementer, Release, and deployment process

#### Outputs

Output	To
Rejected or Approved RFCs/proposal	Change initiator
Major Changes	Design and transition of new or changed services
New or changed services, CIs, assets	Configuration management process (CMDB)
Updated Change Schedule	Service desk, Release, and deployment process
Change decisions, actions, records, and reports	Stakeholders, Service Desk, Change initiator

### 8.0 Appendix B

#### Developing a Roll-back Plan

Development of the Roll-back plan is essential to ensuring effective recovery in the event of a failed change. The Roll-back plan shall be based on the technical impact analysis and the implementation plan. The Change implementer needs to document the change Roll-back plan in detail, which can be used if the implementation of the change is not successful.

This plan shall document the timing at which the Roll-back plan should be invoked – i.e., at what stage is the change implementation considered unsuccessful. High level information on the details of the change Roll-back plan should be documented in the request for change portal.

The change Roll-back plan should be tested, and the results validated in the test environment.

#### Testing

All changes will undergo some level of testing depending on the complexity of the change. Once the change is built, configured, and integrated in the development environment, the change is moved to the Test/QA environment. This phase focuses on conducting testing and quality assurance to ensure reliability and performance of all components. Tester should document testing done and the results of the test.

Tester should test for:

- ✦ Performance
- ✦ Security
- ✦ Functionality
- ✦ Testing of the Roll-back plan