Change Management Procedure

Document ID	**CMP.v.1.0.0**
Effective Date	**2023-04-01**

Table of Contents

1. Purpose and Applicability

1.1 This Change Management Procedure (CMP) outlines the essential requirements for planning, organizing, controlling, executing, and monitoring changes that affect technology service delivery, covering all modifications within systems, networks, and environments.

1.2 The objectives of the CMP include establishing best practices for regulatory compliance, enhancing efficiency through automation, improving communication with automated notifications, obtaining necessary approvals for change, mitigating risks from changes, and minimizing impacts on IT and business functions.

1.3 This CMP applies to all software, applications, cloud services, and end-user computing in all the protected environments within the organization.

1.4 This CMP will be reviewed on an annual basis or when significant changes occur in regulations, business models, or technologies.

2. Related Policies and Procedures

2.1. This CMP should be reviewed in conjunction with policies and procedures issued by both the organization and the relevant regulatory bodies, which include, but are not limited to, the following:

a. Bank Negara Malaysia (BNM) Policy Document on Risk Management in Technology (RMiT)
b. Circulations, notices, and memos issued by BNM
c. Information Risk Management Policy
d. Information Operations Management Procedure
e. Information Security Management Procedure

3. Glossary of Key Terms

The following are the definition of key terms in this CMP:

Change Advisory Committee (CAC) is the committee responsible for the approval and assessment of changes.

Types of Change

- **Ad-Hoc Change** indicates a Regular Change process that is initiated on an on-demand basis
- **Hotfix Change** signifies an urgent system modification that is necessary to restore a failed service or address a potential failure that could affect customers, operations, regulatory compliance, reputation, or cause financial losses to the organization
- **Regular Change** denotes a standard change that must undergo the typical change management process, including planning, risk assessment, and authorization

Change Processes

- **Penetration Testing** is a method of testing designed to identify exploitable vulnerabilities within the system
- **Performance Testing** is a technique used to evaluate the system's performance and stability under various loads to determine whether it meets business requirements
- **Regression Testing** is a testing approach aimed at ensuring that the application system continues to operate correctly following any code changes, updates, or enhancements
- **System Development Life Cycle (SDLC)** refers to the methodology used for planning, designing, developing, testing, and deploying an application system or significant modifications to an application system
- **System Integration Testing (SIT)** is the phase of testing where individual units or components are combined and assessed together to identify faults in the integration
- **Unit Testing** is a method of testing that focuses on verifying the functionality of individual components or units of the system, typically at the level of functions or methods, to ensure that each one works as expected in isolation from the rest of the system
- **User Acceptance Testing (UAT)** is a testing method used to verify whether the specified requirements meet the business requirements as identified

4. Overview

All changes go through structured lifecycle of change initiation, analysis, approval, development, deployment, review, and notification, as illustrated in Diagram 1. This approach is essential for ensuring stable and reliable services, reducing incidents related to changes, and maintaining compliance with regulatory standards.

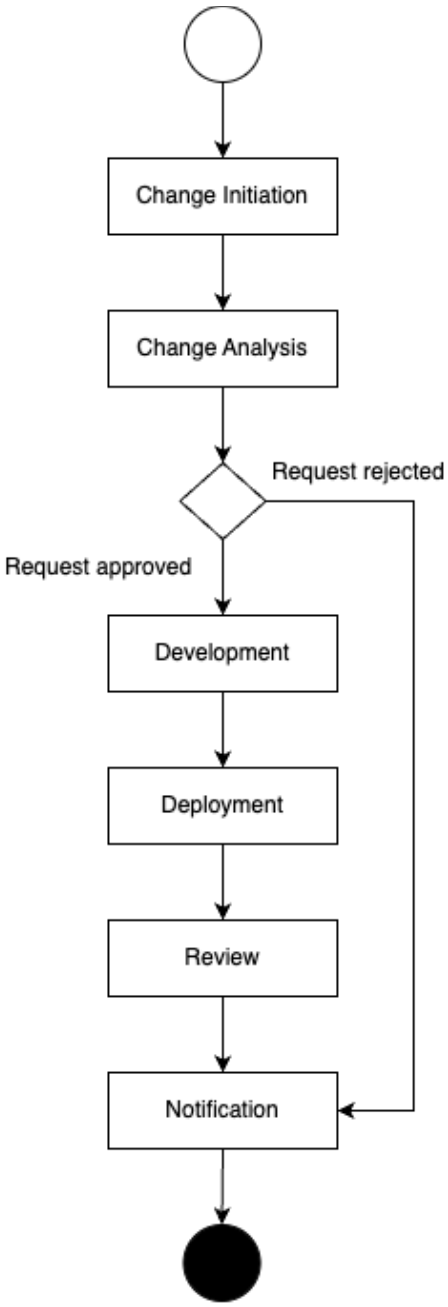

Diagram 1: Overview of change management lifecycle

5. Roles and Responsibilities

Role	Responsibilities
Change Requester: Business Owner, Product Owner, Platform Owner, Application Owner	• Major driver of a change through the entire change request flow • Initiate a change request with all the relevant requirements and impact analysis • Lead post change implementation review and notification
Functional Unit Head	• Review the completeness of each change request initiated by its unit • Approve a change request for submission to CAC
Software Engineering	• Design of system/application specifications based on requirements provided in a change request • Develop system/application according to established application development guidelines • Implement unit testing to ensure completeness and correctness of application functionalities according to requirements • Prepare system/application releases for deployment • Collaborate with change requester, Cybersecurity Engineering, and QA Engineering teams to address all critical bugs and vulnerabilities found throughout the testing processes
Cybersecurity Engineering	• Evaluate the associated cybersecurity risks based on the requirements specified in a change request • Collaborate with change requester and Software Engineering teams to design mitigations for cybersecurity risks identified • Conduct penetration testing to discover potential vulnerabilities in system/application • Collaborate with change requester and Software Engineering teams to address all critical vulnerabilities found throughout the testing process
Quality Assurance (QA)	• Conduct SIT and regression testing to ensure the completeness

Engineering	and correctness of application functionalities according to requirements • Collaborate with change requester to conduct all necessary UATs • Prepare test results and test report signoffs
Change Advisory Committee (CAC)	• Review the completeness and correctness of information submitted in a change request • Advise the strategy of each requested change: scope, timeline, resources, and dependencies • Approve/reject each change request • Committee members include o Respective Head of Business Department o Respective Head of Technology Department o Respective Head of Functional Units • Committee will be chaired by the CTO or an equivalent delegation
Chief Information Security Officer (CISO), Risk Officer	• Conduct independent review of all technology risks related to a critical change • Advise on risk mitigation strategies • Report critical risks to the relevant committees

6. Categories of Changes and Handling

All changes will be categorised into one of the following categories:

Category	Description
CAT01	• Mandatory changes required by regulatory requirements and/or critical business functions • All hotfixes will be categorized as CAT01 change
CAT02	• Changes for introducing new changes or enhancing existing business and operation efficiencies
CAT03	• Pure UI/UX changes that do not alter any business/operation functionalities

All changes are required to go through the Change Management Process described in Section 7.

7. Change Management Process

The following diagram illustrates the end-to-end flow of the change management process

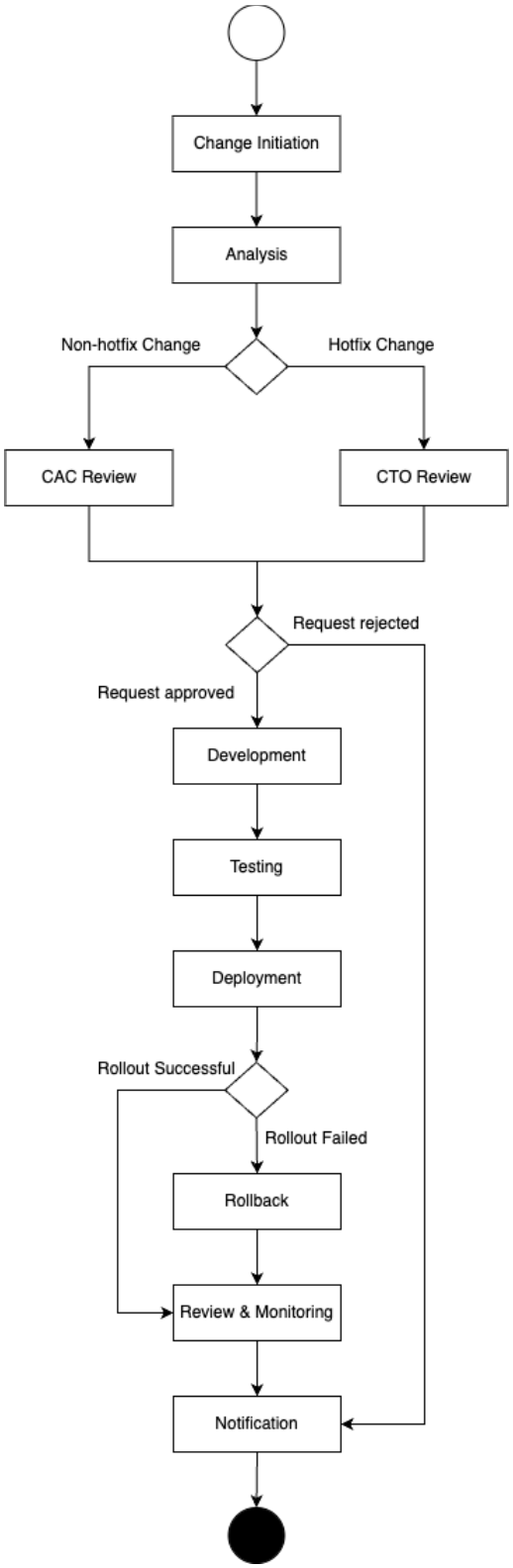

Diagram 2: Change Management Process

7.1 Change Initiation

a. The change requestor raises a change request that includes the following information, as applicable:
    i. Description of the change
    ii. Business/Operation/Technology justification for the change
    iii. Required testing and the corresponding signoffs
    iv. Risk and impact analysis, which includes but is not limited to:
        a. Impact on the relevant business functions
        b. Impact on the target application and its dependencies
        c. Required resources: time, cost, and human capital
        d. Consequences if the change is not implemented
        e. Workaround or mitigation plan for each identified risk
        f. Deployment and rollout plans
        g. Rollback strategy

7.2 Change Request Analysis

a. Functional unit head(s) will review the completeness and correctness of information included in change request before it is submitted to the relevant change approval parties

7.3 Change Request Approval

a. Change request will be reviewed and approved by the corresponding parties according to the types of change:
    i. Non-hotfix Changes
        - Mandatory approval by the CAC
    ii. Hotfix Changes
        - Mandatory approval by the CTO or an equivalent delegation
        - Notification to the CAC once change request is approved

7.4 Change Development

a. The respective development team(s) will proceed with the design and development of change according to the established application development guidelines

7.5 Testing

a. Functional and security testing will be conducted by both the QA Engineering and Cybersecurity Engineering teams
b. All critical bugs and vulnerabilities found during the tests must be addressed
c. Test results, test acceptance and the corresponding signoffs will be documented

7.6 Change Deployment

a. Preparation of release by the respective engineering teams
b. Deployment of the release to production environment according to the approved deployment schedule as part the change request
c. Continuously monitor the rollout of the new release

7.7 Rollback

a. Initiate rollback to the target release version identified in the approved rollback plan as part of the change request
b. Continuously monitor the rollback

7.8 Post-Deployment Review & Monitoring

a. Change requester will continue to monitor the performance of the new release on production environment
b. Change requester will lead the review of the change management process to identify potential areas of improvement for the continuous enhancement of the change management process

7.9 Post-Deployment Notification

a. Change requester will provide a notification report to CAC and the relevant functional units after the completion of a change