CHANGE MANAGEMENT PROCEDURE

Table of Contents

CHANGE MANAGEMENT PROCEDURE

CHANGE MANAGEMENT PROCEDURE

1. Purpose

The purpose of the Change Management Procedure is to ensure that changes are effected in a rational and predictable manner while carrying out replacement / updating of Information processing facilities at SITS.

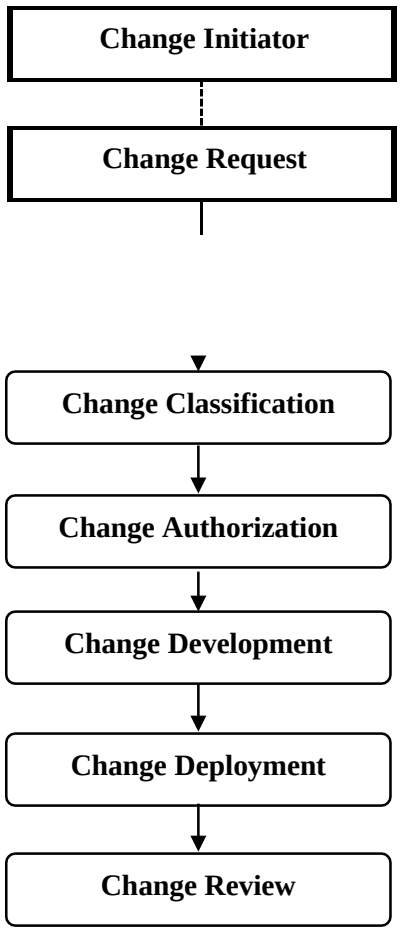
2. Scope

This procedure is applicable whenever a change is effected for any of the Information Processing facilities of SITS across its various locations.

3. Procedure

3.1.1 Change Process

Change Management Process can be graphically represented as a process flow diagram depicting the key tasks needed to be performed in order to successfully deploy a change



Change Management Process Flow Diagram

3.1.2 Change Request

Role Cluster	Type of Change Request
Infrastructure	New systems and improvements to existing systems and infrastructure.
Operations	Changes that affect or improve day-to-day operations of the technology.
Third party	Third-party and supplier-related changes—for example, changes to an outsourced partner system affecting in-house systems.
Release	Changes to the configuration, release and change management systems and processes.
Security	Changes to security processes—for example, authentication or network security improvements.
Support	Changes enabling incident and problem resolution and changes to the help desk system.
Service	Changes driven by new service level requirements, service improvement projects, or business strategy.

Any Change shall be requested through Email or through Change Management Ticket (**Annexure I**), which contains the following information

- The change initiator's name, position, and contact information.
- The change owner's name, position, and contact information.
- Description of the change, that is, a full account of the nature of the change.
- Project or Corporate.
- Project or Support function.
- If the change relates to any incident, incident number and incident description
- Description and identity of any items to be changed.
- Reason for the change.
- Impact analysis.
- Implication of not implementing the change.
- A cost-benefit analysis of the change and budgetary approval, if required.

- Effort and resource required.
- Implementation steps, completion date, actual completion date.
- Location of the release.
- Back-out plan, Time required, Actual Time taken.
- Change verification and approval.

3.1.3 Change Classification

Change shall be classified based on the priority and category of change. Though this is done by the change initiator, the approving authority shall review the same.

Priority	Priority Definition
Emergency	Causing loss of service or severe usability problems to a large number of users, a mission- critical system, or some equally serious problem. Immediate action required. Emergency meetings of the CAB / ISG / SMT may need to be convened. Resources may need to be immediately allocated to deploy such authorized changes.
High	Severely affecting some users or having an impact upon a large number of users. To be given highest priority for change building, testing, and implementation resources.
Medium	No severe impact, but rectification of an incident cannot be deferred until the next scheduled upgrade. For example. To be allocated medium priority for resources.
Low	A change is justified and necessary, but can wait until the next scheduled release or upgrade. To be allocated resources accordingly.

Change priorities needs to be set based on the following definitions:

Change category needs to be set based on the following definitions:

Category	Category Definition
Major	Involves potential impact on the highest percentage of users or a business-critical system. The change may be new technology or a configuration change. It may involve downtime of the network or a service.
Significant	Affects a high percentage of users. The change is a nonstandard change, such as a new product, new users, or network changes, and may involve downtime of the network or a service.
Minor	Affects a smaller percentage of users and risk is less because of the organization’s experience level with the proposed change.

Category	Category Definition
Standard	Affects the smallest percentage of users and has a set release process.

3.1.4 Change Authorization

3.1.4.1 Authorizing Network/Server minor changes

Minor changes in the Network/Server shall be authorized by Director of MIS /HSG

3.1.4.2 Authorizing Changes affecting a group

Changes pertaining to a group shall be authorized by Project Manager and IT Manager.

3.1.4.3 Authorizing Changes affecting NAME OF THE FUNCTION

3.1.4.4 Change Advisory Board (CAB)

CAB typically consists of:

- Change manager
- Client or business manager representing the client.
- User managers or user group representatives.
- Experts/technical consultants.
- Security expert.

Depending on the nature of the change, CAB can additionally include:

- Network infrastructure representative.
- Applications developers/maintainers.
- IT Services staff (System Administrator).
- Contractor or third parties' representatives as required (for example, in outsourcing situations).

3.1.5 Change Development

After an RFC has been approved (using the appropriate path based on its priority and category), it moves into the change development phase. This phase is concerned with the steps necessary to plan the change, develop the deliverables of the change (for example, developing new code or configuring new hardware), and the handover to the release management process for the deployment of the change into the operational environment. Also during this phase, the criteria for deploying the change into operations shall be identified.

3.1.6 Change Deployment

Changes are deployed into operation only after the CAB or the change owner (as appointed by the CAB) ensures that the criteria for functional deployment (as identified during the change development phase) are met. The deployment criteria need to be mentioned in the implementation plan.

In order to determine whether the deployed change has been effective and has achieved the desired results, it is necessary to monitor the changes in the operational environment. For a small change, this may consist of checking on the desired functionality. For larger changes, it might require the monitoring of network and server information, performance data, event logs, or response times.

3.1.6.1 Roll out (To include change implementation plan)

If the change has not met the objectives, then a decision needs to be made about what, if anything should be done. If the change is affecting users or parts of the IT infrastructure adversely, a decision might be made to back out the change and remove it from the production environment.

In such cases, the issues involved in conducting the back-out should be evaluated, including:

- The amount of effort required to perform the back-out.
- The effect it might have on other (either planned or already deployed) changes.
- The possibility that users are already using the changed system, although not to the best effect, and removing some functionality that the users have become used to may be worse than leaving it as it is.

3.1.7 Change review

Following a successful release and deployment into the operational or, as in the case of a standard change, just a deployment into operation review process must be conducted to establish whether the change has had the desired effect and has met the requirements from the original request for change.

3.1.8 Change Communication

3.1.8.1 Change plan notification

Change owner is primarily responsible to ensure that communication with respect to the status of the RFC. The change owner shall provide project status feedback to the change manager and identify any problems as they arise. The change owner presents all formal updates and proposals to the CAB after the CAB approves the RFC for passage through the various phases. Also the change owner shall intimate the change plan to all the relevant stakeholders as identified in the impact analysis of the RFC along with the impacted areas of the service.

3.1.8.2 Change completion notification to all stakeholders

Once the change development is completed and deployed as described in the section 3.1.5, change owner shall intimate all the relevant stakeholders about the change deployment. All the stakeholders shall then give a formal signoff on the change deployment using the RFC form (Approval information).

4. Executive Owner

The MIS Department/CISO will be responsible for implementing and executing the policy mentioned in this document as well as the procedures in the related documents. The execution will be monitored and reviewed by the Chief Information Security Officer/Director of MIS.

5. Roles and Responsibilities

6.

Roles	Responsibilities
Department Head	Responsible for Executing & Implementing the procedure in this document and associated documents across SITS
COO	Overall Responsibility for ensuring the implementation of this Policy.

Definitions

COO	Chief Operating Officer
IT Department	Head of IT Department in SITS

Maintenance & Update Trigger

CISO / Director of IT will be the Owner of this Policy. Any changes, modifications required shall be forwarded to the Information Security Group comprising of the DISOs / Department Heads. CISO shall make the final recommendation to the Senior Management Team for their approval.

Measurement

- Number of Change Request made.
- Number of Change Request Approved.
- Number of Change Request Rejected.
- Number of Change Request Successfully Executed.
- Number of Change Request failed.
- Number of Emergency Changes Effected.