Safex Group

Change Management Policy

Suresh
01/04/23

S.NO.	TOPIC	PAGE NO.
1	Document Control	3
2	Purpose	4
3	Objective	4
4	Definitions	4
5	Policy Statements 5.1 General Rules 5.2 Change Identification 5.3 Change Review 5.4 Change Assessment 5.5 Responsibility	4
6	Change Management Procedure	8
7	Change Management Roles	8
8	Type of IT Change	9
9	Normal Change Request Procedure 9.1 Initiation & Classification 9.2 Change Request Type 9.3 Nature of Change 9.4 Assessment & Authorization 9.5 Plan & Schedule 9.6 Testing 9.7 Implementation 9.8 Backup & Roll Back	10
10	Emergency Change Request Procedure	15
11	Enforcement	15

Safex Group

Change Management Policy

1. Document Control

S. No.	Type of Information	Document Data
1.	Document Title	Change Management Policy
2.	Document Code	ITCMP01
3.	Date of Release	01-04-2023
4.	Document Version No.	1.1
5.	Document Owner	Safex Group
6.	Document Author(s)	Suresh Yadav (AVP. IT)
7.	Document Approver	Piyush Jindal (Group Director)

Document Update Summary

Version No.	Revision Date	Nature of Changes	Date Approval
1	-		
2			
3			

Suresh
01/04/23

2. Purpose

The purpose of this policy is to establish an organisation wide approach to technical change control. Information technology ('IT') and business functions must manage system changes in a rational and predictable manner. Changes require planning, monitoring, testing and follow-up evaluation to reduce negative impact to the user community and to increase the value of information resources.

3. Objective

The objective of change management policy is to ensure that all changes *(including emergency maintenance and patches)* to IT system components are carried out in a standardised manner in a controlled environment.

4. Definitions

Change	*Change is a modification done on the existing IT systems or components used to deliver IT services.*
Change Request ('CR')	*A form, or screen, used to record details of a request for a change to any components within an infrastructure or to procedures and items associated with the infrastructure.*
IT System Components	*IT system components include applications, databases and servers, network devices, security devices and other IT Infrastructure devices.*
Configuration Management Database	*A configuration management database ('CMDB') is a repository of information containing details of all the components of IT systems.*

5. Policy statement

5.1 General Rules

- All changes shall be documented and authorised as per the approved Change Management Policy.
- All changes shall be carried out by employees with expert knowledge of the particular domain.
- Every change to critical information resources such as: operating systems, computing hardware, networks, and applications is subject to the Change Management Policy.
- Any change that alters the security profile (risk) of the Company should not be instituted without permission from AVP (IT).

- In the event of any disaster situation where some technical failure occurs, personnel should follow their project level business continuity and disaster recovery plan.
- AVP (IT), appointed by Management of Safex Group, will review change requests and to ensure that change reviews and communications are being satisfactorily performed.
- The appointed personnel for change management may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back out plans, the timing of the change will negatively impact a key business process such as year-end accounting, or if adequate resources cannot be readily available. Adequate resources may be a problem on weekends, holidays, or during special events.
- The non-production changes shall not require any testing procedure.
- Change management log must be maintained for all changes *(in excel)*. The log must contain, but is not limited to:

  a. Change ID

  b. Date and time of change completed and change submission

  c. Owner contact information

  d. Nature of the change

  e. Indication of success or failure.

  f. Risk and priority of change.

  g. Change state.

  h. Approval status.

5.2 Change Identification

- All changes done to existing IT systems shall be initiated using a formal Change Request ('CR'). This Change Request ('CR') must contain, but is not limited to:

  a. Description of change

  b. Change requested by, analysed by.

  c. Cost and benefit of the change.

  d. Priority and impact of the change

  e. Risk evaluation.

  f. Reviewer of the change.

  g. Change tested (if required)

  h. Roll back plans (in case the failed changes)

i. Pre-implementation approvals

j. Post-implementation details

- Examples of IT systems related changes which needs adherence to this policy are:
  a. Firewall rule base changes
  b. Configuration changes in core applications.
  c. Patches installation for applications.
  d. Configuration changes in the application, database or web server etc.
- All IT systems and software related changes shall be classified into either:
  a. Standard change
  b. Emergency change or unplanned outage change.
  c. New requirement
  d. Requirement change
  e. Design change
  f. Other
- The Changes shall be classified using the following parameters:
  a. Urgency of the change
  b. Impact of the current issue, which triggered the change
- All classified changes shall be prioritised into Low, Medium, High or Critical based on the change urgency and Impact of the current issue.
- For the purpose of identifying the relevant change management structure, all changes shall be tagged to any of the following based upon the nature of change implementation:
  a. Operational IT configuration changes
  b. Infrastructure related changes
  c. Application related changes
- All "Emergency Changes" shall be documented retrospectively.

5.3 Change Review

- All standard changes shall be further categorised into Major or Minor.
- The following parameters shall be used to decide the category:
  a. Downtime involved in the change

b. Impact of the current issue

- All "Standard Major Change & Standard Minor Change" shall be discussed, reviewed and approved by the Group Director along with key stakeholders related to the particular change.
- All "Emergency Changes" shall be discussed, reviewed and approved by the Group Director.

5.4 Change Assessment

- All approved changes shall be implemented through one of the following ways:
  a. Change implementation as per the current CR
  b. Change implementation links to an existing CR in the current scheduled changes
- All changes shall be reviewed, assessed and approved based upon a business, quality and security requirement.
- All changes shall be approved or rejected by the Group Director as an outcome of the review and assessment.
- **Entry criteria**
  a. Any existing or change to CI's that offer services are defined or revised
  b. This policy is applied to all points related to the Standard Requirements
- **Exit criteria**
  a. When existing or new or change to change initiator's that offer services are defined or revised, they are approved and baselined as per the Standard Requirements
  b. Change criteria defined within the policy having an impact on services provided.

The Safex Group chairs the CAB (Change Advisory Board) to evaluate and approve or disapprove the change. The change implementer ensures that the change is tested, properly implemented or rolled back.

5.5 Responsibility

Document/ Procedure Responsibility	Department(s)/ Process(es)/ Function(s)	Designation
Preparation	IT departments/ process/ functions	IT Managers, Senior Manager IT
Review	All departments/ process/ functions	AVP (IT)
Approval	Management review committee	Group Director

6. Change Management Procedure

The IT change management process typically consists of different procedures:

Request for change review: Change coordinators use this procedure when they are dealing with requests for change.

Change planning: Change coordinators and specialists employ this process to prepare the implementation plans for changes.

Change approval: The change manager and approvers *(e.g., service owners)* follow this procedure to approve planned changes. The members of CAB (Change Advisory Board) have the right to approve or reject the request for change.

Change implementation: Tech teams use this process to implement infrastructure changes.

Change closure: Tech teams follow this procedure when they perform production tests after changes have been implemented, and change coordinators employ it when they close out changes.

7. Change Management Roles

ROLE	DESCRIPTION
Change Initiator	The change initiator recognizes and identifies the need for change. *(Your change initiator should be someone who works directly with support services tools. Members of your team who provide support services to customers may be best suited for this position due to their frequent interaction with the system.)*
Change Coordinator	Assesses requests for change that originate from incident management, problem management, release management, or continuity management. The change coordinator registers change as needed to handle requests for change or receives change requests from other change initiators; prepares implementation plans by creating tasks; and monitors the progress of changes.
Change Manager	Is generally needed in mid-sized and larger organisations. If your IT department is part of a larger company, you will need to pick one or multiple persons to perform the role of change manager. These individuals are responsible for managing change procedures, receiving and prioritising change requests, evaluating the risk level associated with requests, and keeping thorough records of the outcome of each change.
Approver	The approver decides whether to approve or reject changes.
Change Implementation Team	The change implementation team consists of the engineers who are responsible for actually making changes.

8. Types of IT Changes

There are different types of change requests, or change classes, that are typically managed in different ways:

• **Standard changes** are changes to a service or to the IT infrastructure where the implementation process and the risks are known upfront. These changes are managed according to policies that the

organisation already has in place. Since these changes are subject to established policies and procedures, they are the easiest to prioritise and implement, and often don't require approval from a risk management perspective.

Examples:

a. New User ID creation, email ID creation, access card, issuance of laptop to users
b. Normal maintenance items and provisioning that are documented in the service statement or SLA
c. Changes that have an established process, carry limited risk, and are documented in the service statement or SLA
d. Non-enterprise changes
e. Changes that are performed daily for end users

• **Normal changes** are those that must go through the change process before being approved and implemented. If they are determined to be high-risk, the Group Director must decide whether they will be implemented.

Examples:

a. Desktop related issues, which needs hardware to be replaced
b. Planned link outages, during which we need to change over to alternate/back up.
c. Code/software upgrades
d. Hardware upgrades
e. Major service-impacting reconfigurations (e.g., security event)
f. Maintenance activity that is not defined in service statements or service level agreements

• **Emergency changes** arise when an unexpected error or threat occurs, such as when a flaw in the infrastructure related to services needs to be addressed immediately. A security threat is another example of an emergency situation that requires changes to be made immediately. It is a compulsive change that has to be on top priority without which the impact can be catastrophic. For instance, in case of a contingency such as natural disasters, terrorist attacks, new virus attacks that cannot be currently handled by the existing antivirus / malware / firewall.

Examples:

a. Operational activities, such as repair, that are not optional
b. Disaster
c. Critical fix
d. Rollback
e. Restart process

9. Normal Change Request Procedure

9.1 Initiation & Classification

The following section documents the activities involved in initiating and classifying a standard change request.

- The change process begins with the creation of a CR by the change requestor.
- All the change requests should be raised using formal procedure.
- The change requester should provide the following details in the CR:

a. Requestor name
b. Change description
c. Change type
d. Change reason
e. Affected services
f. Change urgency
g. Impact of the current issues *(for which the change is requested)*

- The change requester should state the change urgency and impact of the current issue wisely.
- A unique CR ID must be assigned to every change request.

9.2 Change Request Type

The change requests should be generally classified into 2 types, standard and emergency.

Change requests are classified as 'Emergency' if the change urgency or impact of the current issue were rated as critical or high.

Change requests are classified as 'Standard' if the change urgency or impact of the current issue were rated as Medium or Low.

9.3 Nature of Change

It is necessary to identify the nature of the change and assign the change request to the relevant personnel. The nature of change has to be categorised into any of the following:

Nature of Change	Guideline
IT operations change	Any CR related to core applications.

IT infrastructure change	Any CR related to servers, data centre, backup, active directory, e-mail etc
IT security change	Any CR related to network, firewall, antivirus security etc

9.4 Assessment and Authorization

- Upon prioritising the change request, AVP (IT) should identify the configuration items ('CI') on which the changes are going to be implemented.
- The identified configuration items details should be updated in the CR.
- By referring to the configuration management database ('CMDB') AVP (IT) should identify the other configuration items that will be impacted by the change.
- The AVP (IT) shall include subject matter experts ('SME'), business owners, users in the discussion during the assessment. SME's, business owners and users should also authorise the change.
- The risk and impact assessment should be done from the following perspectives,

a. What are the risks if change is not implemented?

b. What are the risks if change is implemented?

c. What are the impacts if change is not implemented?

d. What are the impacts if change is implemented?

- The Risk and Impact assessment should be done considering the following aspects, but not limited to

a. Risks

- ✓ Financial loss
- ✓ Legal implication
- ✓ Reputation loss
- ✓ Operational disrupt

b. Impacts

- ✓ Impact on dependent services or configuration items
- ✓ Impact on the number of users, services affected during the time change.
- ✓ Impact on SLA
- ✓ Impact on security
- ✓ Impact on functionality and performance
- ✓ Impact on other changes planned

- Update the CR with the risk and impact assessment details.

- After assessment is done, categorise the CR into either Major or Minor, based on 2 factors, namely downtime of the service while implementing the change and the impact on the number of users, services affected during the change implementation.
- Categorise the CR using the matrix given in Appendix- A, table- 4
- Based on the assessment and categorization, AVP (IT) shall update the details and approve the CR.
- If the change request is categorised as major, upon AVP (IT) approval, submit the change for Group Director approval.
- If the outcome of the discussion is to not approve a CR, update the details in the tool and close the CR.

9.5 Plan & Schedule

- Approver should coordinate with the implementation team to prepare the implementation plan and schedule and upload the details in the excel/ automated tool.
- The approved IT systems related changes shall be scheduled for implementation based upon their priorities.
- An implementation plan shall be prepared in the system for all approved change request with the following key details:

a. Date & Time of implementing the change

b. Resource requirements

c. Downtime requirements

d. Testing Steps

e. Data Backup Steps

f. Implementation Steps

g. Roll back steps

- The change requester shall be notified about the updates wherever required in the process.
- The Implementation team should try to schedule the implementation during the change window. This is to avoid any disruptions to the employees.
- If any disruption or downtime to service is expected during the implementation, accordingly the IT team should be notified to send the disruption or downtime notification should be sent to all the relevant parties.

9.6 Testing

- The test cases should be executed as per the test plan. The test plan should consider, at a minimum, the following:

a. Testing to ensure that the change can be implemented and run as required
b. Testing of the back-out procedures
c. Testing the functionality of the final system
d. Success criteria
e. Work instructions and operating procedures *(if applicable)*

- The following should be considered as part of the test phase, as relevant:

a. Unit testing
b. Stress testing
c. Integration testing
d. Security testing
e. Functional testing

- After the tests, the results are checked to identify success and failures. This is done based on the success criteria defined in the test plan.
- If the tests succeed, then the testing team should provide a sign off for the change implementation.
- If the tests were unsuccessful, AVP (IT) should be notified, the root cause should be identified, and the relevant corrective action should be taken.
- If the tests were unsuccessful even after the corrective action, update the details and close the CR.
- Once complete, the results of the tests conducted should be updated in the CR.
- All proposed changes shall be tested on a test system before implementing it in the live production environment.
- Any failure during the implementation and testing of IT systems related changes shall be analysed for root cause of failure and appropriate corrective actions shall be undertaken.

9.7 Implementation

- Before the change implementation, the data should be backed up properly.
- If the implementation succeeds, then the implementation team should update the details in the CR and CMDB.
- If the implementation were unsuccessful, the Implementation team should inform AVP (IT), execute the roll back plan and update the CR.
- All IT systems related changes shall be implemented by the implementation team(s) composed of system administrators, database administrators, developers, network administrators, as may be applicable.

- All changes to the IT systems shall be released in the production, only after successful results during testing.
- Any deviation from the initial planned steps during implementation shall be documented by the concerned administrator for record purpose.
- Any failure during the implementation of changes and releases shall be analysed for root cause of failure and appropriate corrective actions shall be undertaken.
- Concerned administrators shall maintain all records related to implementation and testing of IT systems related changes.

9.8 Back Up & Roll Back

- All critical changes to the production IT systems shall be supported by adequate back up plans to ensure successful recovery of data in case of any failure.
- All critical production IT systems shall be backed up as per the defined back up schedule before implementation of the change.
- If the backup of data doesn't match with the current state of data in the production systems, a complete backup of the production systems shall be taken before the change.
- All changes and releases to the production IT systems shall be supported with a detailed roll back plan to ensure successful system roll back in case of a failure.
- Change implementation team shall verify the integrity of the IT system after successful roll back of data
- Concerned administrators shall maintain records of all such roll backs of production IT systems and any failure during the roll back shall be analysed for its root cause.
- All IT and non-IT processing systems shall be monitored for their effective operation after successful implementation of changes.
- AVP (IT) shall ensure the changes made to the configuration items are properly updated in the CMDB.

IT systems are subject to formal change control processes. Such processes provide a managed and orderly method by which changes are requested, tested, approved, communicated prior to implementation *(if possible)*, and logged. Attributes of a formal change control process/ procedure include:

- Assignment of a technical change manager or change control team
- Written change requests submitted for all changes, both scheduled and unscheduled.
- Change requests receive formal approval before proceeding with the change.
- A testing plan is required to include IT and business representatives where appropriate.
- A change log is maintained for all changes. The log should contain, but is not limited to:

a. Date of submission and date of change

b. Owner and custodian contact information
c. Nature of the change
d. Indication of success or failure

10. Emergency Change Request Procedure

All the change requests that were classified as Emergency should follow the below mentioned procedure steps:

- Prioritisation, categorization of CR does not apply to emergency CR, since the confirmed emergency CR will always have the change urgency 'Critical' or 'High'.
- All the Emergency CR should be approved by both AVP (IT) and the Group Director.
- Scheduling of change implementation also does not apply to emergency change, instead the change should be implemented at the earliest.
- The Emergency change request shall be approved based on the impact and risk assessment done by the CAB.
- Approved emergency CR should be submitted to the implementation team for the preparation of implementation and roll back plan.
- There will be no testing involved in the emergency CR.
- The Emergency CR shall be updated retrospectively after the implementation of the change.

11. Enforcement

Policy violations

- Violation of the Policy will result in corrective action from the management. Disciplinary action will be initiated consistent with the severity of the incident as determined by the investigation, and may include, but not limited to:

a. Loss of access privileges to information assets
b. Termination of employment or contract
c. Other actions deemed appropriate by Management

- Violation of the policy shall be reported to the **IT Head**.

Table-1 **Change Urgency**

Rating	Value	Guidelines
Critical	4	Immediate and sustained response involving all IT resources is required.
High	3	Immediate action required from assigned resources only
Medium	2	Moderate urgency , Work can be scheduled
Low	1	No urgency; work can be scheduled

Table-2 **Impact of Issue**

Rating	Value	Guidelines
Critical	4	Critically Business impact - 1. Operations cannot continue from the same location 2. Immediate impact on reputation 3. legal/ regulatory/ compliance actions may be initiated against the organisation
High	3	Major operational impact- 1.Critical business operations are also affected 2. Continuation of this incident may result in loss of reputation/ legal or regulatory implications.
Medium	2	Minor operational impacts Only noncritical business operations are affected No financial /legal/regulatory impact;
Low	1	No or minor impact on operations; No financial /legal/regulatory impact;

Table- 3 **Prioritization Matrix**

Below table shows the possible combination of priority ratings derived using parameters 'change urgency' and 'Impact of current issue'.

Impact of Current Issue / Change Urgency	Critical 4	High 3	Medium 2	Low 1

Critical	4	16	12	8	4
High	3	12	9	6	3
Medium	2	8	6	4	2
Low	1	4	3	2	1

Priority = Change Urgency X Impact of the Current Issue,

The priority should be assigned 'Critical' if the priority value derived is either 12 or 16,
The priority should be assigned 'High' if the priority value derived is 9,
The priority should be assigned 'Medium' if the priority value derived is either 4 or 6 or 8,
The priority should be assigned 'Low' if the priority value derived is either 1 or 2 or 3.

Sukhi
01/04/23