



QRG Investments and Holdings Limited

Change Management Policy

Version 3.0

<p>QRG Investments and Holdings Limited</p> <p>Change Management Policy</p> <p>Version 3.0</p> <p>Internal</p>	
---	--

Document Control

S. No.	Type of Information	Document Data
1.	Document Title	QRG Investments and Holdings Limited Change Management Policy
2.	Document Code	QRGIHLCMP
3.	Date of Release	February 14, 2025
4.	Document Superseded	
5.	Document Approvers	Board of Directors

Document Change Approvals

Version No	Revision Date	Nature of Change	Date Approved
1.0	NA	Initial Version	October 22, 2022
1.0	NA	No Change	October 04, 2023
2.0	February 06, 2024	As per RBI Master Directions, Nov,23.	February 06, 2024
3.0	February 06, 2025	Alignment with ISO 27001:2022 and RBI Master direction, Nov'23	February 06, 2025

Table of Contents

1.1	Scope	4
1.2	Responsibility.....	4
1.3	Enforcement.....	4
1.4	Authority	4
1.5	Abbreviations and Definitions.....	4
2.1	Change Management Lifecycle	5
	Figure 1: Change Management Flow.....	6
2.1.1	Development of Change	7
2.1.2	User Acceptance Test	7
2.1.3	Change request creation and categorization	7
	Table 2: Change Types	8
2.1.4	Change request approval.....	9
2.1.5	CAB Approval.....	9
2.1.6	Migration to Production (including Data Migration).....	10
2.1.7	Roll-back plan.....	11
2.2	Emergency Changes.....	11
2.3	Patch Management	11
2.3.1	SAP Patch Management	11
2.4	Guidelines for Audit Trail.....	12
3.	Document Management	12

<p style="text-align: center;">QRG Investments and Holdings Limited Change Management Policy Version 3.0 Internal</p>	
--	---

1. Purpose

This policy intends to set up guidelines for executing and monitoring changes to IT Infrastructure and IT applications. This shall ensure that only authorized changes are implemented and the adverse impact of change-related incidents on service quality and business operations is minimized.

1.1 Scope

The scope of change management Policy covers the changes made to the IT infrastructure and IT applications of QRG Investments and Holdings Limited (“QRGIHL”).

1.2 Responsibility

It is the responsibility of the IT Team/Managed service provider and respective or concerned business/functional team to implement and maintain the guidelines as defined in the change management policy.

1.3 Enforcement

All changes made to the IT infrastructure and IT applications of QRGIHL are covered under this policy. Requests for deviations from this policy must be documented and managed using the approved process. Any requests for deviations from this policy must be approved in accordance with the *Security Exception Management Policy*.

1.4 Authority

The Board of Directors approves and enforces this policy and mandates processes to monitor and ensure compliance to this policy.

1.5 Abbreviations and Definitions

- a) CR: Change Request ;
- b) UAT: User Acceptance Testing ;
- c) ITSM: IT Service Management including all outsourced activities ;
- d) Business Team: Business Team are the drivers of the business. Business Team includes personnel from business divisions such as Finance, Production, Marketing, HR, Procurement etc. ;
- e) Solution Manager: Solution Manager acts as an interface between Business Team and IT Team/Managed service provider ;
- f) CAB: o u t s o u r c e d Change Advisory Board approves changes before moving the Changes developed to the production environment. (Refer section 2.1.5) ;
- g) Team Lead/Designated Employee: Lead of respective IT domain ; provides approval on change request ;
- h) Technical Team: Technical team handles the technical requirements (such

<p>QRG Investments and Holdings Limited Change Management Policy Version 3.0 Internal</p>	
--	---

- i) as Version upgrade, kernel change, etc.) of the system/application; and
SAP BASIS Team: SAP BASIS team shall be responsible for implementing, configuring, and monitoring SAP technical environment.
- j) CIO: Chief Information Officer
- k) CISO: Chief Information Security Officer

2. Policy

Change Management is the process of planning, documenting, coordinating, implementing, and monitoring changes affecting the development, quality / test, and production platform within the QRG IHL environment.

The objectives of the change management processes are to:

- a) Ensure that changes are implemented with minimum disruption to the services IT has committed to its users;
- b) Support the efficient and prompt handling of all changes;
- c) Provide accurate and timely information about all changes;
- d) Ensure all changes are consistent with business and technical plans and strategies;
- e) Ensure that a consistent approach is followed;
- f) any changes to an application system or data are justified by genuine business needs and approvals supported by documentation and subjected to a robust change management process; and
- g) Provide additional functionality and performance enhancements to systems while maintaining an acceptable level of user services.

2.1 Change Management Lifecycle

The change management lifecycle includes guidelines to be implemented to control the impact of changes introduced into applications, infrastructure processing business information and supporting IT applications.

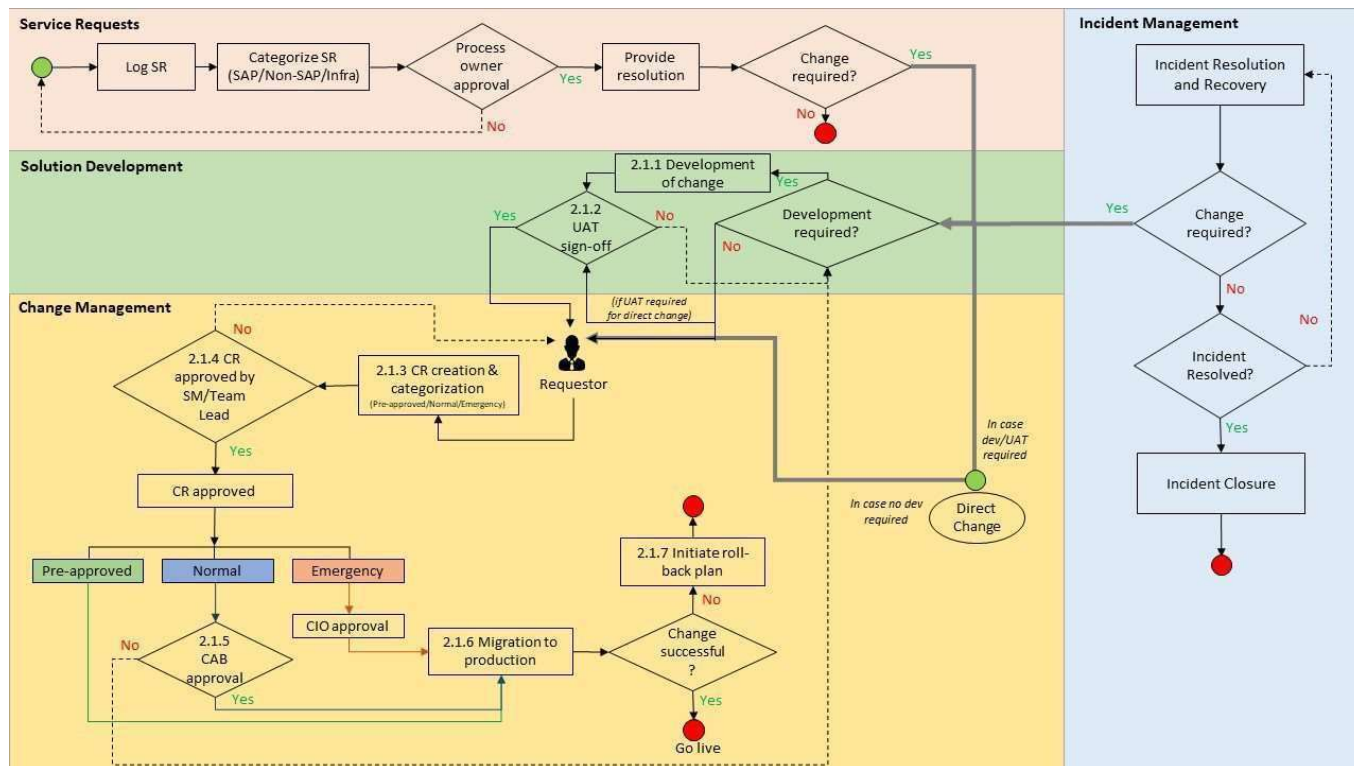


Figure 1: Change Management Flow

A change can be initiated from the below mentioned sources:

- a) **Service Request:** Any service request which requires a change for its resolution ;
- b) **Incident:** Any incident which may require change for its resolution ; and
- c) **Direct change:** A direct change process which may not originate from a service request or an incident, such as patch updates, version upgrade etc.

The activities of the change management lifecycle include:

- a) Development of change ;
- b) User acceptance test (UAT) ;
- c) Change request creation and categorization ;
- d) CR approval ;
- e) CAB approval ;
- f) Migration to production ; and
- g) Roll-back plan.

Post initiation of the change management lifecycle, if the requestor requests for any additional requirements to be incorporated, the enhancements would follow the change

<p style="text-align: center;">QRG Investments and Holdings Limited Change Management Policy Version 3.0 Internal</p>	
--	---

management lifecycle for relevant approvals.

2.1.1 Development of Change

A change may originate from a service request, an incident or could be a direct change. If the change does not require development, it shall be directed to the requestor for CR creation.

If the change requires a development, the technical team / solution manager/Managed service provider / Outsourced development agency team shall develop a change in the development environment. On successful development, the technical team / solution manager/ /Managed service provider / Outsourced development team or individual who developed the change(s) will release for UAT .

2.1.2 User Acceptance Test

Once the system testing is successful in development or test environment, the client server shall be made available for the user to perform user acceptance testing (if applicable). A detailed UAT results along with the sign-off and other relevant documentation (if applicable), are to be updated/attached in the ITSM tool of managed service provider.

- i. The workgroup owner (business user or IT personnel) / technical team/solution manager/managed service provider/outsourced development team shall test the changes in the quality environment (if applicable)and provide their approvals on the change request form ;
- ii. If the UAT results are not satisfactory, then the technical team/solution manager/Managed service provider / Outsourced development agency team will enhance the change as per requestors' requirement ; and
- iii. If the UAT results are satisfactory, the workgroup owner (business user or IT personnel) / technical team/solution manager/Managed service provider / Outsourced development agency team will provide their go-ahead

2.1.3 Change request creation and categorization

All changes shall be logged in the ITSM tool provided by the Managed service provider irrespective of their source. A change record shall be created for every change to track and log necessary information to take appropriate actions including the identification of stakeholders.

- a) A change request shall record complete information about the following, (but not limited to);

<p align="center">QRG Investments and Holdings Limited Change Management Policy Version 3.0 Internal</p>	
---	---

- i. The nature of change (business/technical/both) ;
- ii. Type of changes;

SAP	All changes and enhancements deployed for SAP application
IT infrastructure	All changes and enhancements deployed on IT infrastructure

Table 2: Change Types

- iii. Resource requirement (people/infrastructure) ;
 - iv. Proposed timeline of the changes ;
 - v. Change advisory board (CAB) involvement, if required ;
 - vi. Change impact (High/Medium/Low) ;
 - vii. UAT requirements (if applicable) ; and
 - viii. Documentation for roll-back plan.(if applicable)
- b) Change category shall be assigned as per table below to ensure effective and efficient change management:

Change category	Impact	SM / team lead approval	UAT sign-off	CAB approval	Remarks
Normal changes – A change which has medium to high level impact; and is complex in nature and/or may require downtime for implementation.	Medium to high impact	Yes	Yes	Yes	<ul style="list-style-type: none"> Request shall be submitted on tool/mail, prior to implementation. All the manual change requests shall be logged in ITSM Tool, to be tracked to closure. CAB approval from must be taken prior to implementation

Pre-approved change – A change which has minimal impact and/or repetitive in nature and does not require downtime.	Low impact	Not mandatory	Yes	Not mandatory	<ul style="list-style-type: none"> Request shall be submitted on tool/mail, prior to implementation. All the manual change requests shall be logged in ITSM Tool, to be tracked to closure.
Emergency change- A change which requires an immediate action, basis the criticality of business or high priority incident and/or may require downtime on immediate basis.	High impact	Yes	Yes	Not mandatory	<ul style="list-style-type: none"> Request should be submitted by the change requestor. Emergency change shall be approved by the CIO / CISO If required, CAB approval can be taken post deployment of change in production

Table 3: Change Category

2.1.4 Change request approval

Once the change request is created by the requestor, it goes for approval to the solution manager / team lead/Managed service provider for their approval. The solution manager / team lead/Managed service provider shall then provide his/her approval on the CR form and forward the CR for CAB approval if required. If the CR is rejected by the solution manager / team lead, it will be redirected to the requestor to make relevant updates.

If the change does not require CAB approval (in case of emergency and pre- approved changes), the change shall directly be deployed in the production environment.

2.1.5 CAB Approval

Migration of a new/existing infrastructure and/or IT applications from development environment to production environment will require a CAB approval, depending upon the category of change. The CAB approval must be taken for all normal changes prior to deployment in production. (Refer table 2).

<p align="center">QRG Investments and Holdings Limited Change Management Policy Version 3.0 Internal</p>	
---	---

The CAB shall meet at least on weekly basis to approve changes before migration of change to production. The CAB shall include following personnel:

- a) At least 1 personnel from IT infra team of Managed Service provider ;
- b) At least 1 personnel from applications team of managed service provider ;
- c) At least 1 personnel from functional team ;
- d) IT security team/ Managed service provider member, if required;

However, depending upon the criticality of the changes, additional members may be added for specific cases.

The change types which require CAB approval have been mentioned in Table Number 3. The Change advisory board (CAB) shall:

- a) Review UAT signoffs ;
- b) Provide clarification or additional support to the change requestors as may be required ;
- c) Review and approve change requests ;
- d) Provide feedback and advice with respect to recommendations to change requests; and
- e) Discuss in case any unethical procedures are being followed for change management.

If the CAB rejects a change request, the CR is assigned to solution manager team / technical team/Managed service provider /Outsourced development agency to rework on the change.

2.1.6 Migration to Production (including Data Migration)

A change shall be migrated to production post relevant approvals (wherever applicable) and testing, to minimize the impact of a change.

- a) Pre-approved changes directly move to production post approval from Change Advisory Board (CAB);
- b) Emergency changes move to production post approval of CIO /CISO ;
- c) For normal changes, post CAB approval, changes shall be migrated to production environment:
 - i. Post CAB approval, the request goes to Production / SAP – Basis team/Managed service provider for moving the changes into production; and
 - ii. The Production / SAP Basis team/Managed service provider shall migrate the changes to the Production environment and confirm to the technical team/solution manager team about successful migration, who shall then inform the same to the workgroup owner (business user or IT personnel).
- d) Relevant information security controls should be in place to protect data or information throughout its life cycle to maintain confidentiality, integrity and availability.

<p align="center">QRG Investments and Holdings Limited Change Management Policy Version 3.0 Internal</p>	
---	---

2.1.7 Roll-back plan

Roll-back procedures shall be documented at the stage of CR creation, prior to deployment of change in production. A roll-plan shall be initiated with necessary approvals if the change does not give desired results or if the change has an unforeseen impact. Approvals from business head and IT head/Managed service provider, if required, shall be taken as applicable.

2.2 Emergency Changes

An emergency change shall relate to the immediate or imminent resolution of a known or potential production problem where outage of a system, application, network, or other service component has occurred or potentially will occur. An emergency change is required to be implemented immediately to maintain the continuity of services.

- a. In case of the need for an emergency change, request shall be submitted by the change requestor along with approval of CISO/ CIO before change implementation ;
- b. CISO/ CIO approval is mandatory for all emergency changes. Approval for emergency changes can be taken over e-mail, SMS or on the ITSM tool. If verbal approval is taken, the change requestor shall send an email to all solution manager and head of IT/CIO to acknowledge the approval ; and
- c. Testing shall be carried out in the quality environment even for emergency changes to ensure that the availability, accuracy and integrity of live data and systems are not impacted.

2.3 Patch Management

Patches shall be routed through either a normal or direct change and shall follow the change management process. (Refer Figure 1)

2.3.1 SAP Patch Management

SAP patch management follows the regular SAP change management process except for some changes as described below:

- The change requestor here would be the IT personnel responsible for SAP. Since, this would be a request from IT department or directly from SAP, the same must be documented in the ITSM tool which will contain all the details & descriptions/number of patches ;
- The BASIS administrator shall apply and migrate the patches/notes into development environment for testing ;
- It shall then be tested by the various module coordinators in the IT Team/Managed service provider;
- After successful testing, the patches are applied in quality environment ;
- Testing shall be done by all module coordinators for standalone and integrated testing ;
- After successful testing in quality, patches are applied in production environment ;

<p align="center">QRG Investments and Holdings Limited Change Management Policy Version 3.0 Internal</p>	
---	---

- The BASIS administrator shall inform the requester about the details of the patch, affected modules and downtime required for implementing the patch in the production environment.
- Once the patch is applied, the BASIS administrator shall inform all the stakeholders about the successful implementation of the patch in production environment; and
- Roll-back procedures shall be initiated with necessary approvals if the changes do not give desired results or if the changes have unforeseen effects. The required approvals from business head and IT head, if required shall be taken as applicable.

2.4 Guidelines for Audit Trail

- Every IT application which can access or affect critical or sensitive information, shall have necessary audit and system logging capability and should provide audit trails.
- The audit trails shall satisfy business requirements apart from regulatory and legal requirements. The audit trails must be detailed enough to facilitate the conduct of audit, serve as forensic evidence when required and assist in dispute resolution, including for non-repudiation purposes.
- Mechanisms should be put in place for regularly monitoring the audit trails and system logs to detect any unauthorized activity.

3. Document Management

- Any amendment to this policy/ procedure or issue of any guidance or circular etc. under this policy/ procedure has to be incorporated in the policy on an ongoing basis by the Management.
- This policy will be reviewed atleast every year by Board/ Committee.
- Any amendment to this policy/ procedure or issue of any guidance or circular etc. under this policy/ procedure has to be incorporated in the policy on an ongoing basis by the Management.
- This procedure replaces any other procedure issued earlier by the Company to the extent specifically covered here. This policy should be followed both in letter and spirit.
- The Company is committed to continuously reviewing and updating policies and procedures-based on the Company's risk assessment and incorporating any regulatory requirement as maybe required.
- Any amendment to this procedure or issue of any guidance or circular etc. under this procedure has to be approved in writing by the approving authority.
