Change Management Procedure

Document Control Information

Document History

The following table tracks information regarding new and revised versions of this document and briefly describes the Changes made.

Date	Version	Status	Author/Contributo	Description
16/4/2020	0.1	Initial Draft	Varadarajan.p	Initial Draft
17/4/2020	1.0	Completed	Varadarajan.p	Completed
19/12/2020	1.01	Reviewed	Mousumi P	Completed
19/04/2022	1.02	Reviewed	Mousumi P	Completed
01/06/2022	2.0	Reviewed	Mousumi P	Completed

Document Review

This section should be created and maintained by the author/ procedure owner.

Version	Name	Metier / Position	Comment (Provide the review scope as necessary)
0.1	Varadarajan.P	Head of Production ITSM	Review comments from GK incorporated
1.0	Varadarajan.P	Head of Production ITSM	Review comments from Amit V incorporated
1.01	Mousumi P	Head of Production ITSM	Review comments from Abirami T incorporated
1.02	Mousumi P	Head of Production ITSM	Review comments from Abirami T incorporated.CMDB and checksum process updated
2.0	Mousumi P	Head of Production ITSM	Review comments from OPC updated and Freeze period details updated

Document Approval

Role	Name	Signature	Date
Head of Production application support	GK	GK	01 June 2022
CTO	Ketan P	KP	20 January 2021
CFO	Amit V	AV	01 June 2022
CIO	Anshuman D	AD	01 June 2022
ITRO	Ajinkya D	AD	19 April 2022

Table of Contents

1. Document Scope

The scope of this document covers policy, process and a level of procedure to explain how the process would be applied to Sharekhan.

2. Change Management Overview

2.1 Change Definition

Change is defined as the addition, modification or removal of a Production or DR computing Environment Configuration Item. This includes all hardware, software and facilities (electricity, moves etc.) that are relevant to the running and support of Production.

*The term “Production” will be used to refer to “Production or DR computing environment” for the remainder of the document.

Note that the following are not part of this process:

- Data and content Changes (e.g. update of data and content on web sites and refresh data applications) if there is no impact on Production
- Unplanned diagnostic debugging of applications, systems and services
- Hardware and software Changes relating to individual PC’s, telephones, printers and individual office suite macros and scripts
- Software development and Changes to test servers that reside upon isolated networks (i.e. have no links to Production)
- Application Configuration Changes – due to the localized nature of these changes and where the validation and control requirements are fulfilled and audited by other means, it is accepted that a Change Record will not be mandatory. However, if the Configuration Change is a manually run script directly on the application or is not carried out via a tool which provides an audit trail, a Change Record is mandatory.

Some examples of application configuration changes include; user permissions on application, email notification configuration for users and batch configuration changes.

The **purpose** of the Change Management Process is to ensure that standardized methods and procedures are used for efficient and prompt handling of all Changes to Production and to ensure overall business risk is mitigated.

The **goal** of the Change Management Process is to respond to changing business requirements whilst maximizing value, reducing incidents and unplanned service disruption and re- work.
The **objective** is to ensure that all Changes are recorded, evaluated authorized planned, tested, implemented, documented and reviewed in a controlled manner.

This is achieved by ensuring all Changes are; appropriately reviewed and authorized, co-ordinate to avoid conflict and managed from a risk perspective.

This process deals with the analysis and co-ordination of Changes and does not cover the execution details of technical tasks related to the implementation of these Changes. It provides a consistent methodology for requesting, classifying, authorizing, tracking and reporting.

Change Management core activities include:

- Planning, controlling and scheduling Change
- Conflict Management
- Communication of major activities
- Management reporting

2.2 Benefits

- Business risk is mitigated
- Reduction of Incidents and service disruption
- Reduction of unauthorized Change
- Increase of successful Change
- Correlation of Incident and Change Records

3. Change Management Policy

3.1 Scope

Sharekhan Change Management using IT Desk

3.2 Policy Statements

- All Changes to Production require a Change Record raised within ITSM Toolset IT Desk.
- All changes must be fully approved prior to implementation except for Restropective change
- Changes performed to fix or prevent a significant Production failure may be recorded after the event. These Change Records must reference a related Incident Ticket where applicable.
- Changes to Production must only be deployed by production facing teams. Therefore Production teams are responsible for creating the Change Record for implementation.
- Non Production teams must request a change to Production via a Service Request.
- Evidence of UAT/Pre testing is considered outside the scope of the Change Management Process
- Change Records must not contain any confidential details such as passwords or client access information etc

3.3 Compliance Criteria

Change Management is a critical part of the Sharekhan management of IT Operational Risk. This process ensures that Changes are implemented effectively and efficiently to meet Sharekhan Business requirements.

This process will be judged as fully compliant when there is evidence of the following controls:

- Changes are correctly recorded and classified to the required standard
- Actions by internal and external audit points are implemented
- Adherence to Sharekhan ITSM Change Management Process

.

3.4 Assurance

- Compliance with this process will be reviewed on a regular basis by IT Governance
- Compliance with this process will be subject to the Sharekhan internal and external audits
- Compliance to this process will be subject to regulatory reviews

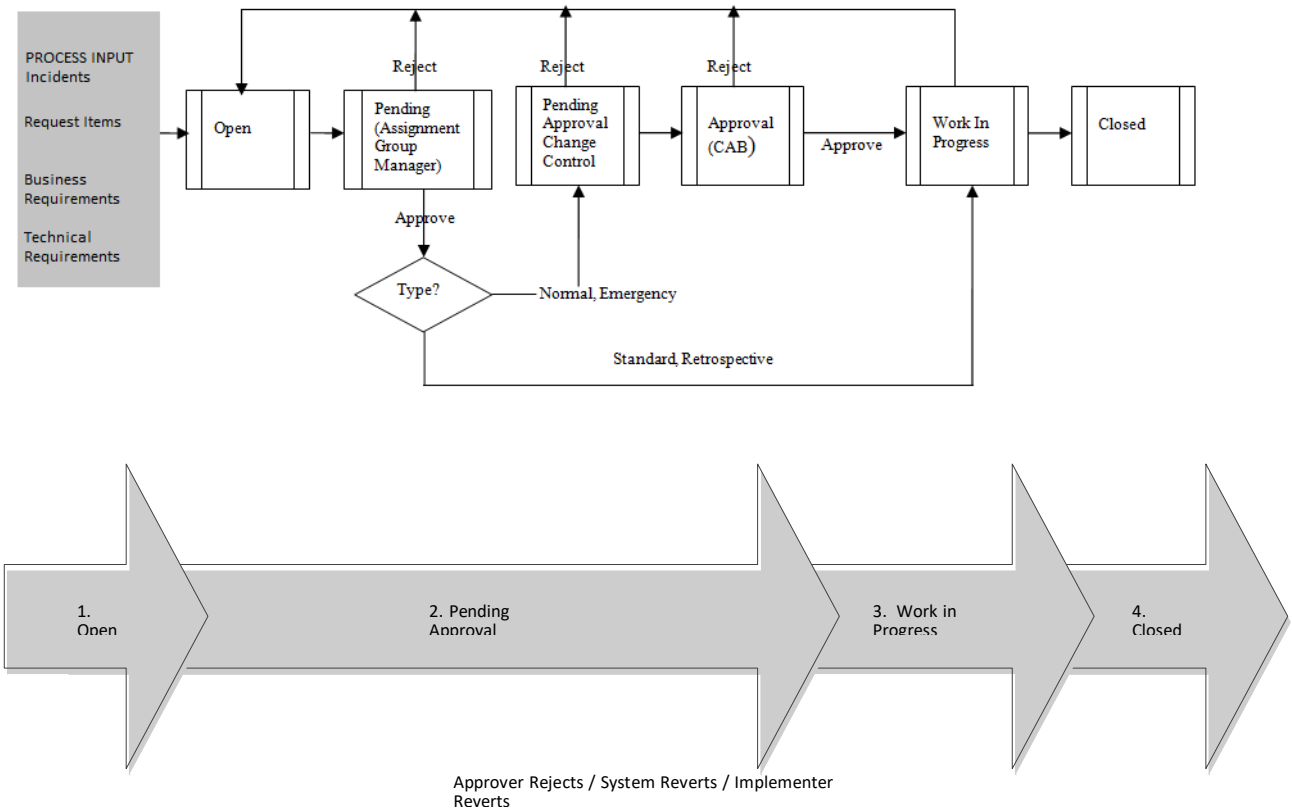
3.5 Segregation of Duties

Segregation of Duties is a global, Sharekhan wide mandate and must be respected by all teams who use the Global Change Management process. If for any operational reasons, there are known Sharekhan recognizes and follows the segregation of Duty principle expectations of BNP Paribas, it must be managed by each IT area and is outside the scope of the Change Management process.

4. Change Management Process

This details the process flow and end-to-end management of Change Records within the Change Management Process.

4.1 Flow Diagram:



4.2 Process Steps

Step	Step details
1	Open (Pending Line Manager Approval) The below points cover the activities during the open state of the workflow: • Record/define the Change details • Assess Impact & Risk • Determine Schedule • Conflict Management • Prepare Implementation and Post Change Test Plans • Identify Stakeholders • Submit Change Record for Approval
2	ITSM validated (pending HOD approval) The below points cover the activities during the pending approval state of the workflow: • Solicit Stakeholder Approvals and record responses • Respond to Approval requests
3	HOD approved (pending implementation) The below points cover the activities during the work in progress state of the workflow: • Implement the Change • Test the result to gauge success
4	Implemented / Work in Progress (pending closure) The below points cover the activities during the closed state of the workflow: • Do the sanity test an check if roll back is required or not.
5	ClosureThe below points cover the activities during the closed state of the workflow: • Indicate the completion of the Change in the Change Record. Notify Stakeholders of outcome • The results (success and failure) are recorded for the changes made • The problem is created in the event of a deployment failure

4.3 Change Reason

Corrective Action	Realigns the Performance of the Project Work with the PM Plan
Preventive Action	Ensures the future performance of the project work is aligned with the PM Plan
Defective Repair	An intentional activity to modify a nonconforming product or Product component
Updates	Changes to formally controlled project documents, plans etc., to reflect modified or additional ideas or Content

4.4 Change Category

Sharekhan IT divided 3 major categories as Application, Infra and Security

4.5 PMO ID and Project Name

Sharekhan approved projects will receive PMO ID and Project Name for future reference

5. Change Types

	Change Request Form			
* Process Steps/Status	1. Open (pending ITSM validation) 2. ITSM validated (pending HOD approval) 3. HOD approved (pending implementation) 4. Implemented / Work in Progress (pending closure) 5. Closed		PMO ID	Project ID (when exists), Not applicable (in case of no project ID)
* Change Reason	Corrective Action/Preventive Action/Defect Repair/Updates		PMO Project Name	Linked to project ID OR Not applicable
* Change Category	Application/Infra/Security			
* Configuration Item (dependent on above)	(Application name) / (server, network, components) / (firewall, W	*	Change Linkage	Not applicable/ITDesk Ticket number (incident/problem/change)
* Change Type	Normal/Emergency/Standard/Retrospective	*	Requested By	Creator
* Affected CI	Implement Team have to fill			
* Affected Locations	Realince/TATA/Lodha/Jolliboard/Ruby/Epire/Playstore/Appstore/others - we need Multi selection and All	*	Implement Team	Text freeformat value
* Request Date	Use Existing (creation date time)	*	Planed End Date	Use Existing (expected implementation end date time)
* Planed Start Date	Use Existing (expected implementation date time)	*	Actual Live/ End Date	duration between "Work Start" & "Work End"
* Justification	clear statement of why the Change needs to be made including the	*	Rollback Plan	Use Existing
* Change Plan	Use Existing Plan of Action	*	Impact	High/Medium/Low
* Risk	High/Medium/Low	*	Post Change Test Plan	a detailed and technical explanation of steps required to ensure the implementation was successful
* Assigned Group	1. ITSM (open) 2. HOD (ITSM validated) 3. Implementor (HOD approved) 4. ITSM (Implemented)	*	Watch List	is driven by a combination of Affected CI's and/or Impacted CI's, Change type and manual intervention.
* Outcome	Successful / Cancelled / Failed		Unauthorized Change	
Post Change Review				

There are four Change Types which are determined based on Risk, Impact, and Urgency (lead time) in the Change Record. Complete Change type calculation logic can be referred to in the appendix.

Change ticket management including the mandatory information /documentation to be included,

- Reason behind the Change. (Is it on account of any enhancement or fixing an issue?)
- Operational Instruction is needed
- What is the downtime required for this Change.
- Have we done UAT testing and Functional testing.
- Attach approval from HOD and Head of IT Production that they are okay for this change and they have checked the UAT reports.
- Test acceptance

- Incident Number if related to the incident
- Reasons for the urgent issues
- If there is requirement of business team to be informed and if yes then you have concurrence from them.
- If there is requirement of any other team to be informed and if yes then you have concurrence from them.
- POA need to be communicated with all the impacting teams in detail.
- Rollback plan need to be mentioned in detail. For rollback, kindly let us know the time line.
- For all changes we need to inform business teams as well just after the roll out and after completion of successful sanity test.
- Incase the sanity test fails the change should be rolled back and thus need for change related communication to the business team will not be required in that case

5.1 Normal

- Normal Changes are routine planned Changes which are raised conforming to policy lead times.
- Low Risk Changes require 24hrs+ to achieve Normal Classification (except low risk/low impact see standard)
- Med Risk Changes require 48hrs+ to achieve Normal Classification High Risk Changes require 72hrs+ to achieve Normal classification Less than the above will result in an Emergency classification
- Normal Changes follow the full Change workflow.
- 2 days Maximum processing times for Normal changes

5.2 Emergency

- Emergency Changes may only be requested when driven by specific scenarios including a significant Incident, imminent service outage or in order to meet regulatory requirements. Justification for Emergency Changes should be defined in terms of Quantitative Cost (i.e. Money, time) Market Reputation or Regulatory Compliance where possible.
- Raised with less than policy lead time for Normal Changes.
- Emergency Changes follow the full Change workflow.

- Emergency Change Advisory Board (ECAB) a sub-set of the Change Advisory Board who makes decisions about high impact Emergency Changes. Membership of the ECAB may be decided at the time a meeting is called, and depends on the nature of the Emergency Change
- 2 Hrs Maximum processing times for Emergency changes except Android 1 day and iOS 3 days for Google and App store approval process

- UAT test acceptance document and the apporval of the business team, CIO and three HOD is mandatory for the emergency change.

- Emergency change completes the full change work flow within 2 hours that includes the complete testing and approval and if all the above procedures gets compted in 2 hours then its an emergency or else it is not considered as an emergency change.

- The approval for the emergency changes are taken formally in black and white within two hours from the business team, CIO and three HOD is mandatory for the emergency change before implementing the change.

5.3 Standard

- Standard Changes are Low Risk Low Impact Changes which have no effect outside of a single silo / domain.
- No specified lead times.
- Standard Changes only require approval from the HOD and Head of IT production of the assignment group. Change Records will not engage Change Control and/or CAB approval.
- 3 days Maximum processing times for Standard changes

5.4 Retrospective

- Changes performed to fix or prevent a significant Production Incident may be recorded after the event. Justification must include clear reason for the urgency of the implementation.
- These Change Records will be categorized as Retrospective Changes which must reference a related Incident Ticket if applicable.
- Unauthorized Changes made must be submitted as Retrospective to log the event which will be recorded as policy violation.
- Retrospective Change Records must be submitted within 72hrs of change implementation.
- Retrospective Changes only require approval from the respetive HOD and Head of IT production of the assignment group. Change Records will not engage Change Control and/or CAB approval.
- Retrospective Change Records must be submitted,approved within 5 business days of submission.

6. Change Record Fundamentals

The following defines the key elements of the Change process which are used to build the Change Record.

6.1 Scope

- **Configuration Item (CI)** - This is an asset, service component or other item that is or will be under a state of Change. These typically include IT services, hardware, software, buildings, and formal documentation such as process documentation and service level agreements
- **Affected CIs** – this identifies the collection of CI's which will be in a state of Change.
- **Affected Locations** – this identifies the locations which will be affected as a result of the changes. it should match affected locations

6.2 Schedule

- **Planned** – duration between "Planned Start Date" & "Planned End Date" represents proposed implementation schedule during which affected CI's will be in the state of Change. When recording the implementation schedule include sufficient time for contingency plan.
- If due to unforeseen circumstances the implementation exceeds the planned schedule, follow the contingencies documented in the Change plan. When dealing with an overrun, the focus is always to minimize the overall risk to production. Refer to your local operational procedures for further details.
- Changes made outside of planned schedule will be considered as unauthorized (see Unauthorized Change section)

- **Actual** – duration between "Work Start" & "Work End" represents the actual implementation schedule during which the affected CI's were in a state of Change.

6.3 Risk

Risk is defined as a possible event that could cause harm or loss, or affect the ability to achieve objectives. A Risk is measured by the probability of a threat, the vulnerability of the CI to that threat, and the adverse impact it would have if it occurred.

Risk measurement comprises of the following elements:

- **Risk level** - can be selected manually as well as being influenced by Risk Assessment and/or Risk Conditions.
- The matrix below - an intersection of Adverse Impact and Likelihood of Occurrence – can be used to help rank Change risk level of **Low, Moderate or High:**

	Adverse Impact Resulting from Change		
Likelihood of Adverse Impact Occurring	**High**	**Medium**	**Low**
Very Likely	**High**	**High**	**Moderate**
Likely	**High**	**Moderate**	**Moderate**
Unlikely	**Moderate**	**Moderate**	**Low**

- **Risk Assessment** - Change Management can define a set of questions to calculate the level of risk based on scenarios within the environment.
- **Risk Conditions** - Change Management can define risk conditions to calculate the level of risk based on attributes within the Change Record.
- Further guidelines can be found in the Appendices section “Risk Information”.

6.4 Impact

Impact measurement is composed of the following elements:

- **Impact Level** - is a measure of the disruption caused to the CI and/or Services during the Change implementation.
- High – (Outage)
- Medium – (Degradation)
- Low – (No Impact)
- **Impact Description** - is an explanation or elaboration of the selected Impact level which provides additional relevant information
- **Impacted CIs** - this identifies the collection of CI’s which may experience the impact of Change.

6.5 Documentation

- **Justification** – is a clear statement of why the Change needs to be made including the reason for urgency if appropriate.
- **Change Plan** – a detailed and technical explanation of steps required to implement the Change.
- **Post Change Test Plan** - a detailed and technical explanation of steps required to ensure the implementation was successful.
- **Attachments/Document links** - Once the change is approved, any supporting information provided by an external URL link or attachment must not be modified where it significantly alters the scope of the change.

6.6 Communication

- **Approvers** – are driven by a combination of Affected CI’s, Change type and manual intervention.
- **Watch List** - is driven by a combination of Affected CI’s and/or Impacted CI’s, Change type and manual intervention.
- **Automatic notification** – Individuals or groups defined in “Requested By” , “”Assignment Group and “Assigned To” fields receive automatic notification during different states of the Change Record life cycle.

6.7 Change Linkage

- **Related Changes** – a related Change Record.
- **Requested Items** – a Service Catalogue Request Item related to the Change Record.
- **Incidents Pending Change** – an Incident Ticket which will be resolved by the Change Record
- **Incidents caused by Change** – an Incident Record caused by the Change Record
- **Problems** – a Problem Ticket related to the Change Record
- **Problem Task** – a Problem Task related to the Change Record

- **Enhancements** – Enhancement Record which will be implemented via the Change Record
- **Defects** – Defect Record which will be resolved via the Change Record
- **External References** – related links not covered in existing fields in the Change Record

6.8 Conflict Management

Conflict management is employed automatically and manually during the entire lifecycle of the Change.

- **Conflicts** – this lists conflict records which are automatically identified in conjunction with configuration item/schedule, blackout schedules and maintenance schedules.
- Manual conflict management is assisted by referral to various information sources such as events calendars.
- **The Advanced Notification Calendar (ANC)** is the recognized point for Sharekhan Change Management teams to record major activities to assist with conflict management. Refer to Events Calendars section for further details.

6.9 Post Change Review

In addition to standard post-tests which should occur after the implementation of any Change, a formal 'Post Change Review' should be considered for use in the event of a failed change or one that causes an Incident (where no other formal procedure is used – e.g. PIR as part of the Incident process).

6.10 Unauthorized Change

Unauthorized change to Production is prohibited. Where this occurs escalation will be made to senior management and this may lead to disciplinary action.

Any of the following will be considered as unauthorized:

- A Production Change made without a corresponding Change Record
- A Change Record that is not fully approved when implemented
- An implementation begins prior to the scheduled window start date/time or continues after the scheduled end date/time
- An implementation that goes beyond the original approved scope

Please refer to Incident Related Changes section whereby the above may be considered exempt.

6.11 Incident related Changes

Emergency & Retrospective Changes may be raised for the following scenarios:

- To fix a Production failure (driven by the Incident Management Process) where an Incident reference is available.
- As a proactive measure to prevent a Production Incident.

In the event of a Production failure, support teams are authorized to make Changes to the Production environment, only if the Change is necessary to ensure the continued operation and availability of key systems and services. These Changes may be required to take place either during or outside of normal business hours. If this is required, the support teams involved MUST first have Management authority (for application Changes the CTO will approve and for infrastructure changes CFO will approve) to proceed. Evidence of this management approval will be required via email or directly in the Change Record. . An Incident reference should also be related where applicable. Once the go ahead has been received, the Change should be implemented at the agreed time.

It is also the responsibility of the support team to ensure that all relevant staff are notified of the Change; this includes any business or IT users who may be impacted by the Change, both locally and globally. This can be carried out in conjunction with the Change Management team and Application Production Support managers.

In this scenario, a Change Record can be submitted prior to or after the implementation. Where the Change is raised retrospectively it is recommended that this is done within 24hrs of implementation to ensure there is an up-to-date record of all Changes that have occurred.

If time permits and/or in the event of a proactive measure, the Change Management team will put the Change up for approval and expedite the approval process

6.12 Process Inputs

- Incidents
- Problems
- Service catalogue request items
- Business or technical requirements
- Evidenace of Approval

6.13 Process Output

- Change Record
- Forward schedule of Change
- Change Review Meeting and minutes
- Evidenace of Approval
- Adjusted Configuration Items
- Stakeholder communication
- Optimized risk
- Reporting

6.14 Target Audiences

- Sharekhan Application, Infrastructure and Security IT Teams
- Sharekhan Business Users/Functions

7.1 Checksum Validation

Checksum is a calculated value that is used to determine the interigity of data.For every applicatoion related change it is must to have a checksum validation number. The checksum number will be provided by the ADM team which is a code that ADM Team has used to run the or test the application in UAT.The checksum number will be added in the change ticket. The production team will not deploy any application change without the checksum number. The production team will first run the checksum code in cmd and confirm and then they will deploy the change. Incase if there is a mismatch in the checksuum number then the production team will not deploy the change and a new checksum will be provoded by the ADM team for the production team to deploy the same.

7.2 CMDB validation

BMC application architectural verification or review will now be mandatory while raising the change request. Below steps needs to be followed to verify and update the hostname and connected hostname details in the change form using the BMC tool.

The change requestor while raising any chage will have to verify the possible impacted server/ application based on the architectural work flow using the BMC tool and for that one has to use the following steps –

In sharekhan network open the url : https://10.12.30.53/ui/ login with the default user id and password (the mentioned BMC url opens only in sharekhan network, that is either in office network or through vpn).

Once logged in type the required host name in search box of the home page and validate.After validating it in BMC tool search box, copy and paste the host name in the column name BMC_ASSETNAME in the change form in ITDesk.

Once the host name is pasted in then BMC_ASSETNAME column, go back to BMC and search and copy the connected asst. In order to do that go back to BMC tool search page then - go to search> hostname > Host > Report > Observed communcation host > then select All > Action > Export as csv > Open csv file > Copy all name (Host name)) and paste the connected assets in the column BMC_ASSETNAME_CONNECTED in the change form in ITDesk.

8. Roles and Responsibilities

8.1 Roles & Description

The Roles and Description for Change Management within BNP Paribas are defined below. Occasionally one individual may hold more than one role, but in such cases the responsibilities remain the same

Role	Description
Requester	The Requester is the person who requires the Change to be made ("Requested By") on the Change Record. Where applicable they should ensure they chase outstanding approvals (and highlight any issues to Change Management). Perform Post Implementation testing Where required.
Implementer	The Implementer is a member of the Assignment Group ("Assigned To") on the Change Record. They define the change, solicit approval, implement the change and perform Post Implementation testing once in Production. Where applicable they should ensure they chase outstanding approvals (and highlight any issues to Change Management).
Change Management	Change Management manages the lifecycle of Changes ensuring that process standards are followed. They have the most holistic overview of the Change landscape. They are the single point of contact for questions related to the execution of the Change Management Process. Change control is a subgroup of Change Management. Their approval groups derive from Review Groups of the Affected CI. Their review is primarily focused on scope, conflicts, schedule risk and Impact and overall quality of the change.
Approver	Approvers are automatically or manually added to Change Records because they have a vested interest in the Change. The interest may be based on their support or management of Affected CI's or work supporting the Change. **CAB** – CAB consists of all other Approvers, comprised of the below categories: Affected CI Review Groups – The Review Groups on all Affected CIs Affected CI Support Group Line Managers(s) – applied if different from the Assignment Group Line Manager. Change Task Assignment Group Line Manager(s) - where tasks are present the Line Manager of the task's Assignment Group is applied to be aware of the resource requirement. Manually added – additional approval may be added where Appropriate.
Change Process Owner / IT Service Management	Process Owner is the ultimate authority on the process definition, they ensure the process supports the company's policies, represent and promote the process to the business, IT leadership and other process owners, continuously verify the process is still fit for purpose and use and finally, manage any and all exceptions that may occur.
IT Support Manager	Domain Head within APS or Infra teams.

8.2 Change RACI Matrix table

Responsible	R
Accountable	A
Consulted	C
Informed	I

	Requester	Implementer	ITSM	Head of Production
• Record/define the Change details				
o Define scope of Change by way of CI/Affected CI	R	C	A	I
o Ensure co-ordination of all tasks as part of the C implementation, is clearly defined within the Change Record.	R	C	A	I
• Prepare Change, Back-out & Post Change Test plans				
o Ensure that sufficient supporting documentation, such as Change plans, Post Change Test plan (Testing by the Requester should be considered as part of any post implementation testing required) and Back-out plans,	R	C	A	I
Have been tested and included in the Change Record.	R	C	A	I
• Identify Stakeholders				
o Where necessary, manually add Approvers and watchers.	A	C	R	I
Assess Impact & Risk				
Consider risk conditions and assessments; revise impact and risk values as needed.	R	C	A	I
• Determine Schedule				
o Schedule the Change with adequate lead time to	R	C	A	I
Allow for stakeholder review and response.				
o Ensure Change window is wide enough implementation, testing, and back-out if needed.	C	A	R	I
• Conflict Management				
o Execute/review conflict checks within IT Desk	C	A	R	I
o Manual checks with other changes calendars including ANC	C	A	R	I
o Resolve schedule conflicts	A	C	R	I
• Submit Change Record for Approval				
o Complete all details in Change Record with accuracy and completeness	R	C	A	I
Solicit approvals, address queries promptly, record responses				
o Chase Approvers (where applicable)	R	C	A	I
o Ensure queries related to the Change Record are addressed promptly	R	C	A	I
o Certify that scope and risk selections are accurate and that pre-tests have been completed by the requester.	R	C	A	I
• Respond to Approval requests				
o Review and validate the Change Record promptly; raise any questions/concerns; approve/reject	A	C	R	I

o Validate stakeholders in Approvers and watchers; add or remove as needed	A	C	R	I
o Check that the scope, risk, and impact of the Change is correct	A	C	R	I
o Check the quality of the Change, Post Change Test and Back-out plans	A	C	R	I
o Check the Change window is wide enough for implementation, testing and back-out if needed	A	C	R	I
• Implement the Change				
o Confirm Change Record is approved before starting Change plan	A	C	R	I
o Follow the Change plans to implement the Change	A	R	C	I
o Respect the Change window	A	R	C	I
o Ensure that all associated documentation updates have been published.	C	A	R	I
• Test the result to gauge success				
o Follow the Post Change Test Plans to confirm successful completion of implementation	R	C	A	I
• Back-out if required				
The Back-out plans to reverse the Production Change decision	A	C	R	I
o Follow the Back-out plans to reverse the Production Change.	A	R	C	I
• Indicate the completion of the Change in the Change Record				
o Complete the Change Record promptly using the correct completion code.	C	R	A	I
• Input				
o Assist / provide input into Post Change Reviews	C	R	A	I
• Operation				
o Produce defined reports, including those required for controls related to the Change Management process.	R	A	C	I
o Maintain an overall visibility on Change Records processed through IT Desk (via reports, spot checks, etc.)	C	A	R	I
o Chair Change review meetings, with all actions taken and distributed to the relevant teams; provide the agenda and minutes.	A	C	R	I
o Participate in Internal Round Table (IRT) meetings.	C	A	R	I
o Where established, assist with the communication of significant events, such as freeze periods, core infrastructure maintenance, BCP exercises, key business activities	A	C	R	I
o Process enforcement	A	C	R	I
• Ownership				
o Overall design	A	C	R	I
o Ensuring the process delivers business value	A	C	R	I
o Ensures compliance with any and all related Policies	A	C	R	I
o Process role definitions	A	C	R	I
o Identification of Critical Success Factors and Key Performance Indicators	A	C	R	I
o Process advocacy and ensuring proper training is conducted	A	C	R	I
o Process integration with other processes	A	C	R	I
o Continual Process Improvement efforts	A	C	R	I

9.Meetings and Controls

9.1Meetings

Meeting Description (Owner)	**Attendees** (Representation required from the following teams)	**Agenda**
Weekly Meeting	ITSM Management, Requestor, implementer, Production Team, IT Support Team and the Executive committee as approver	To review and approve the changes
OPC Bi Monthly APS Risk and Controls Review meeting (OPC)	ITSM Management, OPC team Governance team	Review quality of sample Change tickets
Monthly KPI Meeting	ITG-CIO, CEO, CFO, CTO, ITRO, Head of Production, Head of Infra	Review change KPI
Bi yearly Process Review for Continuous Service Improvement (Service Management)	ITSM Management	Review Change process
Yearly Process Review (Service Management)	ITSM Management	Review of Continuous Service Improvement and process is current and validated

9.2 Procedure Risks & Controls

The following defines the Risks and Controls applicable to the Change Management Process.

Please refer to Formal Level 2 Group Controls Sharekhan by BNP Paribas Group and Formal Level 1 Internal Controls as defined by OPC and Governance - see Appendix Formal Controls section.

9.3 Key Risks

The Key Risks related to the Process are:

Team	Lib Risk Ref	Library Risk Description
Change Management	ITRSK00155	Risk that local Audit requirements and recommendations impacting Change Management are not reported/managed centrally, impacting the Efficiency and compliance of Change Management to meet the businesses requirements and expectations.
Change Management	ITRSK00158	Risk of lack of awareness, knowledge and training of the CMIM processes and tooling by the user base, impacting the Integrity, Efficiency and Effectiveness of the processes, tooling and data to support operations and therefore the business.
Change Management	ITRSK00183	Risk of Change being implemented with inappropriate, inadequate or incomplete approvals being obtained, impacting the integrity, efficiency and/or availability of Production systems used to support the business.
Change Management	ITRSK00182	Risk of inadequate quality control on the content and accuracy of Change tickets impacting the integrity and availability of Production systems used to support the business.
Change Management	ITRSK00169	Risk that Changes are implemented without formal testing and/or appropriate sign-off that impact the confidentiality, availability or integrity of systems/data resulting in an Incident and a subsequent loss to the business.
Change Management	ITRSK00157	Risk of lack of management of conflicting Changes across sites and territories, impacting the efficiency, reliability and available of Production systems to support the business

9.4 Controls

Formal Level 2 Group Controls and Formal Internal Controls as defined by OPC BNP Paribas Group

This document is consistent and compliant with the L2 controls mandated by BNP Paribas Group as well as the reporting L1 Controls formulated by OPC at point of publication of document. These are included in the appendices as reference, see Appendix Formal Controls section.

9.5 Controls – Internal Service Management Operational Controls:

Control Checks	
1	All Change Records which are implemented without full approval to be reviewed.
2	All Change Records which caused P1 / P2 Incidents to be reviewed (Post Change Review)
3	Conflict management is exercised and recorded
4	Regular review meetings which are appropriately attended, minute and distributed
5	Changes are periodically reviewed to validate Change type and state is suitable

9.6 Freeze Periods

A freeze period is a period of time where specific restrictions are introduced within the Change process. Typically, Changes that match a particular criteria will be disallowed or will require a higher level of approval during the period.

Blackout schedules, risk conditions and event calendars can all be utilized to assist with establishing freeze periods.

We have agreed on freeze period for continoues 2 weeks towards the end of the year keeping in mind market behaviour, people availability. Information about the change freeze period will be circulated at least a month in advance

Ad-hoc freeze periods may be requested due to particular business or market conditions/events which may create market volatility or which necessitate extra vigilance to achieve a stable Production environment. See Freeze Period Information in Appendices section for further details.

Year-End Change Freeze Periods EXAMPLE

Change Records already submitted in IT Desk for implementation during the freeze period are currently being assessed for risk and impact to Finance.

Year-End Change Freeze

The Year End Change Freeze commence for continoues 2 weeks towards the end of the year and it will be either during Diwali or at the end of the year depending on market behaviour, people availability. Information about the change freeze period will be circulated at least a month in advance including the management.

Due to the need for increased vigilance and stability required over the year-end period, a more extensive Freeze is in place leading up to Year end. This is a hard freeze which covers ALL Production Changes.

9.7 Freeze Details

- The only exceptions to the Change freeze will be those which are Business Critical prior to Year End or those that fit the standard definition of a Break/Fix (emergency) where intervention is required to recover or prevent a system failure. These will follow the normal process for implementation
- Any Changes raised that directly impact or could potentially impact the availability of systems will be closely examined and subject to senior management approval.
- Low risk / low impact (Standard) Changes will not be possible within the freeze period, these will be escalated to High Risk & will be evaluated using the same process.
- Changes to the Escalation contacts may occur leading up to the Freeze and will therefore, be communicated.
- Should a Change impact multiple business/organization areas then a representative from each area will be required to approve.
- When submitting your Change Record please ensure that the maximum amount of relevant information is included to enable Sharekhan Change Management to make an accurate assessment of Risk and Impact.
- Change Records already submitted for implementation during the freeze period are currently being assessed for risk and impact to the Business.
- During freeze period it is manadotory to take approval CIO, Head of of IT Production and HOD for every change.

10 Supporting Tools

The following tools and systems are used as part of the process:

- ITSM Toolset IT Desk is used to manage Application and Infrastructure Incidents, Problems, Changes and Requests. It is a web based tool available on a global basis through the intranet https://itdesk.sharekhan.com/
- Events Calendar – see Events Calendars section

10.2 Events Calendars

Events calendars are used to log and schedule activities taking place within and/or relating to Production.

10.3 Advanced Notification Calendar

The Advanced Notification Calendar (ANC) in weekly CAB meeting we present and discuss about all upcomig changes and then minutes report is sent with those changes for all stakehoders.

Changes and activities which should feature on the calendar include:

- BCP/DR Activities including Data Centre Power Down and Isolation Tests
- Major releases and application upgrades
- Major infrastructure upgrades
- Building power downs
- Generator and UPS maintenance
- Freeze periods
- Special business/market requirements/events, extended business working

Updating of the ANC is controlled by Sharekhan Change Management & is reviewed in the weekly meeting along with other teams. Within this forum (and outside of it) it is agreed which activities should be entered.In case of conflict of planned changes, the executive commiitee (CEO, CTO, CFO) wil decide the priority of changes according to business requirments..

10.4 BCM/SCM/DR events schedules on the ANC

1. BCM Team should discuss the BCM/DR activity and intended date with their local Change Management (CM) Team. The BCM team needs to be clear on the scope and requirements of their exercise and detail this. It will be discussed whether the exercise is considered an event or Change.
2. Local CM team will review local Change schedule, review the ANC, and discuss with CM teams (including who control the ANC) in respect of the scheduling and any conflicts.
3. If the date is agreed the Local CM team will advise the BCM Team to submit a Change Record in IT Desk.
4. If there is a conflict this will be arbitrated with involvement from Local CM, CM and for Sharekhan BCM related events and IT exercises.
5. CM will update the ANC with the BCM activity
6. BCM will communicate the agreed date and activity.
7. If any reschedule is required, all teams must be kept informed (BCM, local CM team).
8. Dates for BCM/DR activities **should not** generally be communicated outside of the Sharekhan community until the date has been recorded on the ANC.

- It is understood that BCM/IT relationships may differ in each region. Therefore the coordination with Change Management and the creation of the Change Record may be administered by another IT team.
- CM may add the entry provisionally (TBC) as the communication & conflict discussions can often take some time to complete. This then allows all stakeholders to see that the date/activity is in discussion.

10.5 APS, Security & Infra Events Calendar

It is strongly recommended that Security, Infra & APS areas will own and manage their own internal calendars to provide a yearly view of their release schedule.

Where required, any major activities should be co-ordinate with Change Management and the ANC

11 Appendices

11.2 Request for Change Process

The following guidelines incorporate the 2 policy statements below:

- Non Production teams must request a Change Request via IT Desk.
- Evidence of UAT/Pre testing is considered with in the scope of the Change Management Process

11.3 Process explained:

1) APS, Security and Infra (Implementing team) will create Change Request to create a Change Record ONLY when the following has been provided within the Change Request:

- Reason behind the Change
- What is the downtime required for this Change.
- Have we done UAT testing and Functional testing?
- Attach approval from HOD that they are okay for this change and they have checked the UAT reports.
- If there is requirement of business team to be informed and if yes then you have concurrence from them.
- If there is requirement of any other team to be informed and if yes then you have concurrence from them.
- POA need to be communicated with all the impacting teams in detail.
- Rollback plan need to be mentioned in detail. For rollback, kindly let us know the time line.

2) This will create a Change Record with a Requested Items link, which links the IT Desk Request to the Change Record.

3) Depending on which Change Request option is taken will depend on which fields are copied/mapped to the Change Record.

4) The Implementer adjusts any fields on the change record as required and submits it for approval.

11.4 Risk Information guidelines

All Production Changes involve some level of risk. Risk is reduced when stakeholders cooperate to identify and assess these risks. When making a Change it is important to consider not only the risks to the Configuration Item in scope but also risks to other systems. Change Management tools, such as the Risk Matrix below, help facilitate this cooperation and communicate the overall risk in a meaningful way.

Identifying and assessing the potential negative impacts, and the likelihood that that they will occur, is both difficult and subjective. Therefore, the things that stakeholders need to consider when making such assessments are:

- Nature of the Change
- Is this is a “critical” system?
- How many users?
- How many locations?
- How Complex is the change?
- Timing/Schedule
- How close is the Change to a business/market event?
- Will key stakeholders be readily available for support or troubleshooting
- How tight is the schedule?
- Personnel involved
- Are the key stakeholders experienced with this type of Change?

11.5 Consider the following:

1. In addition to an assessment of the potential impact on the environment being changed and any related environments that could be impacted; the Risk Evaluation should consider the confidence of the implementing team and their ability to perform the Change successfully. The level of experience, skill and availability of the resource/s must be considered to determine if there is potentially a higher negative impact to Production.

2. A Change to a firewall or network component may be very simple, but the impact on security, business processing and/or the availability of systems might be very high if an error occurred during the Change, or indeed if the Change did not go ahead. The skill/experience levels of the resource/s would mean that they are less likely to make a mistake, quicker to recognize and assess a mistake if it occurred and better equipped to recover from the mistake.

3. The process of releasing a Change to an application into Production may be considered low risk, since the process is carried out regularly and routinely. However, the nature of the bundled Changes to the application might mean that there is a higher risk of functional impact to business processing.

4. A Change to a non-active component of a service which is used for resilience is less likely to have a high impact to security, business processing and/or the availability of systems.

11.6 Risk Matrix

A risk rating is a simple and useful tool for communicating overall risk. The matrix below - an intersection of Impact and Likelihood of Occurrence – should be used to help rank Change risk level of **Low, Moderate or High:**

	Adverse Impact Resulting from Change		
Likelihood of Adverse Impact Occurring	**High**	**Medium**	**Low**
Very Likely	**High**	**High**	**Moderate**
Likely	**High**	**Moderate**	**Moderate**
Unlikely	**Moderate**	**Moderate**	**Low**

11.7 Change Type Calculations

Change types are calculated as per three variables:

Risk – An estimation of how dangerous or safe it is to make this change.*

Impact – A measure of the disruption caused to the CI and/or Services during the Change implementation.*
High=Outage, Medium=Degradation, and Low=No Impact.

Urgency (lead time)

*see Change Record Fundamentals section & Risk Information Guidelines (appendix) for further details.

for further details

Lead Time	Urgency
< 0 Hrs	1 - Critical
0 to 24 hrs	2 - High
24 to 48 hrs	3 - Moderate
48 to 72 hrs	4 - Low
72Hrs +	5 - Very Low
Lead Time	Time difference between Planned Start Time & $now

Calculation

Risk	Impact	Urgency	Change Type
Low	3 - Low	5 - Very Low	Standard
Low	3 - Low	4 - Low	Standard
Low	3 - Low	3 - Moderate	Standard
Low	3 - Low	2 - High	Standard
Low	3 - Low	1 - Critical	Retrospective
Low	2 - Medium	5 - Very Low	Normal
Low	2 - Medium	4 - Low	Normal
Low	2 - Medium	3 - Moderate	Normal
Low	2 - Medium	2 - High	Emergency
Low	2 - Medium	1 - Critical	Retrospective
Low	1 - High	5 - Very Low	Normal
Low	1 - High	4 - Low	Normal
Low	1 - High	3 - Moderate	Normal
Low	1 - High	2 - High	Emergency
Low	1 - High	1 - Critical	Retrospective
Moderate	3 - Low	5 - Very Low	Normal
Moderate	3 - Low	4 - Low	Normal
Moderate	3 - Low	3 - Moderate	Emergency
Moderate	3 - Low	2 - High	Emergency
Moderate	3 - Low	1 - Critical	Retrospective
Moderate	2 - Medium	5 - Very Low	Normal
Moderate	2 - Medium	4 - Low	Normal
Moderate	2 - Medium	3 - Moderate	Emergency
Moderate	2 - Medium	2 - High	Emergency
Moderate	2 - Medium	1 - Critical	Retrospective
Moderate	1 - High	5 - Very Low	Normal
Moderate	1 - High	4 - Low	Normal
Moderate	1 - High	3 - Moderate	Emergency
Moderate	1 - High	2 - High	Emergency
Moderate	1 - High	1 - Critical	Retrospective
High	3 - Low	5 - Very Low	Normal
High	3 - Low	4 - Low	Emergency
High	3 - Low	3 - Moderate	Emergency
High	3 - Low	2 - High	Emergency
High	3 - Low	1 - Critical	Retrospective
High	2 - Medium	5 - Very Low	Normal
High	2 - Medium	4 - Low	Emergency
High	2 - Medium	3 - Moderate	Emergency
High	2 - Medium	2 - High	Emergency
High	2 - Medium	1 - Critical	Retrospective
High	1 - High	5 - Very Low	Normal
High	1 - High	4 - Low	Emergency
High	1 - High	3 - Moderate	Emergency
High	1 - High	2 - High	Emergency
High	1 - High	1 - Critical	Retrospective

11.8 Change Checklists

These Checklists are designed to assist Change Creators and Approvers in ensuring that thought and consideration has been applied in the information provided, when raising and approving a Change Record. These lists are not final and conclusive and therefore may be added to by Change Management.

11.9 Change Checklist for Change Implementer

- Is this Change being carried out during agreed maintenance windows (where established).
- Has communication been carried out to all affected parties?
- Is there enough time to recover in the event of major issues during the Change, before the Business could be impacted?
- Are there pre-implementation conditions required in the Change plan?
- Back-out must be considered, clearly documented and explicit within the Change Record.
- Is the Start and End time of the Change reasonable (including contingency/Back-out)?
- Has a thorough impact analysis been performed?
- Is there sufficient notice given (Lead Time) for the Change?
- Have Tasks been created for all teams involved / required to implement and test the Change?
- Have you confirmed those resources implementing the Change and do they have all the information required to do this?
- Is there any impact of dependency on services or applications or with other changes.

11.10 Change Checklist for Change Management

- Is this Change being carried out during agreed maintenance windows (where established).
- Are the Affected CI's / Impacted CI's lists accurate and complete?
- Does the Impact Description clearly state the expected impact to users/services? Is user communication required – and if so, has this been carried out?
- Has sufficient supporting documentation been provided (Change, Post Change Test/Back-out plans and scripts)?
- Do additional stakeholders (Approvers, Approval groups, Watch list) need to be added to the Change to ensure that all affected parties review the implementation?
- Are other regions affected by this change? If so apply appropriate ITSM/Change Management approval group to enable them to add additional local approval if required.
- Are there scheduling conflicts which need to be escalated?
- Have Tasks been created for all teams involved / required to implement and test the Change?
- Is there any impact of dependency on services or applications or with other changes.

11.11 Change Checklist for Change Approver

- Are resources available for implementation / testing of Change?
- Are there scheduling conflicts which need to be considered?
- Is the scope of the Change specified correctly?
- Has the quality of the Change, Post Change Test and Back-out plans/scripts been validated /checked?
- Is the Impact & risk assessment provided, accurate and clearly identified?
- Is there any impact of dependency on services or applications or with other changes.

12 Formal Controls

12.2 Sharekhan IT OPC List of Group Standard Level 2 Controls

Mapping Group Control	Control	Managerial Verification point
ITG0021 / Rule 57	#0021 - System of processes to manage IT Production	Each deployment must be validated before actual deployment, according to the rules established by the Operational change management process.
ITG0021 / Rule 60	#0021 - System of processes to manage IT Production	All operational changes in IT Production scope must be declared and recorded.
ITG0021 / Rule 61	#0021 - System of processes to manage IT Production	Changes are classified into at least three categories: • Normal-type change. Change is scheduled enough in advance to comply with the cycle and time frames assumed in impact analyses as well as preparation and information actions.
ITG0021 / Rule 62	#0021 - System of processes to manage IT Production	Some changes can be automatically approved. Criteria for automatic approval must be defined. A Change Advisory Board (CAB) must validate other changes before deployment. The CAB bases its decision on information contained in the change ticket. The CAB's acceptance criteria must be documented. Each change ticket must contain the following information: • Service impacts • Risks • Evidence of release tests • Rollback procedure
ITG0021 / Rule 70	#0021 - System of processes to manage IT Production	Each entity must designate a single process owner per process with the assignments and responsibilities set out below.
ITG0021 / Rule 71	#0021 - System of processes to manage IT Production	Each entity must designate a single for the entitle, with the assignments and responsibilities set out below.

13 Acronym

- BCM- Business continuity Management
- SCM- Security continuity Management
- DR – Disaster Recovery