ADIB – Standard

Change Management Standard
STD-ITD-537

Date: 30th November 2023
Version: 13.0

Version Control & Change Management

Version	Issue Date	Details of Change	Reason for change
13.0	November 2023	Standard updated with current practices and the ORM recommendations.	Standard improvement
12.0	November 2022	In Exceptions Added: Significant and application impact changes implementations are not allowed during the freeze period, which extends in between 25th of each month till 2nd of next month. Application owner must obtain CIO approval to execute any implementation during the freeze period, freeze period is not applicable to emergency changes.	To avoid any unforeseen negative impact on bank services during month end.
11.0	October 2022	Change validity should not exceed one year unless a valid justification is provided, and proper assessment is conducted and approved by change manager and	To enhance Governance control and align with best practices.
10.0	30th June 2022	Control is added to ensure "Elevated user access to IT, Generic user Id's etc. were created as part of implementation/migration and remained to be removed from the production environment" Shifted ownership to Head of Technology GRC	To ensure no elevated access is leaked in production environment. To align document change management standard.
9.0	30th January, 2022	Added cloud related controls	Cloud adoption
8.0	Publishing Date	Modified: Replaced "Pre-CAB" to "Change approvers"	To align with Change Management Team Structure
7.0	Publishing Date	Added: - Rollback to be performed as per the rollback plan mentioned in the RFC - Ensuring change entry and exit criteria has been satisfied - There is a roll back plan available for all types of changes, Normal, Significant and Pre-Approved Updated Document owner.	To align with new ORG structure and as per Central Bank Audit requirements
6.0	Publishing Date	Updated "Pre-CAB Committee members" to "Change Approvers" Modified "Review Approval Matrix" and "Approving Authority Matrix"	To ensure faster time to market for agile changes
5.0	Publishing date	Added clarity on Impact and risk Analysis, Update of CAB, ECAB and Pre CAB roles	Revised according to the current practice and audit inputs
4.0	Publishing date	Moved to New template	Moved to new approved template to maintain the uniformity of all documents

| 3.0 | Publishing date | Standard updated with current practices and the change manager recommendations. | Standard improvement |
| 2.1 | Publishing date | Streamlining of complete standard | Process optimization |

Prepared by	Approved by	Reviewed by
IT Governance team	Change Manager Head of IT GRC	IT Governance Manager Cloud Chapter Lead

Document Contents

1   Overview

The objective of this document is to standardize the method for efficient and prompt handling of all changes to minimize the impact of any related incidents arising from the change.

This standard is applicable to all changes to infrastructure, systems, applications, and any other specialized changes in ADIB IT environment.

2   Applicability

All ADIB ITD

3   Standard Owner

Head of Technology GRC

4   Standard Statements

4.1   Definitions and Change Classification

4.1.1   **Change**

A change can be defined as any addition, removal, or modification to any component in the ADIB IT Environment which can have an impact on the IT Service.

4.1.2   Normal Changes shall be further categorized based on Impact and Risk scoring, into the following Change Complexity:
- Major
- Significant
- Minor

The classification of the change priority is based on the Priority matrix in Appendix-C

  4.1.2.1   Any request for change shall be classified as Normal Change which satisfies any of following characteristics (but not limited to):
- New systems (includes Infrastructure, systems, applications, special parameter)
- Proof of Concept changes
- Changes to existing systems such as upgrades / new module / new functionalities etc.
- Which impacts customer or the bank accounting system
- Which requires downtime of the impacted system

  4.1.2.2   **Proof of Concept Changes (POC):** changes primarily conducted on non-Production environment which are conducted during a pre-defined period and will be rolled back once the POC activity is concluded.

4.1.3   Emergency Change

An Emergency Change is an unplanned change, which is tested and implemented, in a very short notice to fix a production / security issue or protect ADIB from an unacceptable risk of failure or degradation of services, lack or loss of functionality. A request for change shall be classified as Emergency Change when:

  4.1.3.1   If the change is not implemented immediately, it could lead to major impact to business such as:
- Unavailability of business-critical systems/applications.
- Affecting high percentage (20% or more) of users.
- Affecting major part of infrastructure.

4.1.4   Pre-approved Change

  4.1.4.1   A request for change shall be classified as Pre-Approved Change when:
- The associated risk is low or at an acceptable level to ADIB ITD.
- There is no service impact (downtime).
- The Pre-approved change procedure is documented, tested, and validated.

- There is a roll back plan available for all types of changes, Normal, Significant and Pre-Approved (partial / complete or IT Service Continuity Plan).
- Financial requirement for the change shall be included and approved in the respective yearly budget for ADIB ITD
- Pre-approved change shall be valid for a maximum period of 12 months
- Pre-approved change list shall be reviewed on an annual basis by CAB.
- Pre-approved changes need to be approved by CAB.

4.2 Change Management Team Structure

The following shall be the positions for Change Management at ADIB ITD:

4.2.1 **Change Manager**: IT Change Manager, IT-Governance Risk & Compliance

4.2.2 **Release Manager**: Release Manager Representative / IT Release Management Administrator

4.2.3 **Change Approvers**:

- Senior Manager – System Administration, Infrastructure and Operations
- Change Manager
- SME approvers (Network, SecOps, Database, etc.)

4.2.4 **Change Advisory Board (CAB) Committee members:**

- Change Manager
- Senior Manager, Unix & Database Administration
- Head Of Cloud Solutions
- Senior Manager, International Expansions, IT - Demand Management
- Enterprise Architecture Representative
- ORM Representative
- GISD Representative
- Change Requestors
- Relevant SME's

4.2.5 **Emergency Change Advisory Board (ECAB) Committee members:**

- Change Manager
- Head Of Cloud Solutions
- Service Owner Head of department
- Head of QA Chapter

4.3 Change Advisory Board Meeting

4.3.1 All Normal changes shall be reviewed by Change Approvers

4.3.2 All Normal - Minor changes shall proceed to the implementation after the Change Review and Approval

4.3.3 All Significant and Major – Normal changes shall be approved by CAB; In case, downtime is required, additional approval shall be obtained from asset / service owner (business) and CIO or his/her delegate.

4.3.4 Change Advisory Board (CAB) meetings shall be conducted every week.

4.3.5 Proceedings of Change Advisory Board Meeting shall be documented by the Change Manager.

4.3.6 As a part of post CAB communication, the approved changes, and Forward Schedule of Change (FSC) shall be communicated to all the stakeholders, which shall help in planning their activities.

4.4 Change Review

4.4.1 Technical post implementation review shall be conducted by an assigned group member of implementation team to verify that the change was implemented as per the Change Request Form.

4.4.2 Post Implementation Review for all Emergency and Normal Changes shall be performed to confirm that applied changes met the desired outcome & to record lessons learnt, and rollback to be performed as per the rollback plan mentioned in the RFC or the Implementation specification document if required.

4.4.3 Depending on the type of change, the change request shall be reviewed by multiple levels of authorities:
- Requester's Line Manager.
- Change approvers (SME's)
- Change Manager
- CAB.
- ECAB (Emergency Change Advisory Board).

4.4.4 All Requests for Change (RFC) shall be logged in the Change Management tool and assigned to a group / individual for resolution.

4.4.5 All project managers shall follow the Change Management process wherever change in IT systems is required as part of their project.

4.4.6 Once change is registered and reviewed by the Change Coordinator, review and approval of the change shall be done according to the Review Approval Matrix in Appendix D.

4.4.7 All changes shall be assessed for their impact on services and associated risk (refer section 4.11). And ensuring change entry and exit criteria has been satisfied such as IA, IS, FSD, Design Document etc

4.4.8 The proposed change requests shall be reviewed with respect to justification for change, appropriateness of the solution to the reported problem and feasibility.

4.4.9 All non-functional infrastructure changes shall undergo the UAT process (refer section 4.6).

4.4.10 All changes shall be tested in test environment, wherever possible and applicable, and test results shall be attached with change request.

4.4.11 PIR for major changes shall be discussed in CAB. Change Manager in consent with the CAB to take the process improvement initiatives based on PIR observations.

4.4.12 Failed Change: Any change which is not being implemented as planned shall qualify as a failed change.

4.4.13 Changes causing Incidents:

Any change which has resulted in the Severity 1/Severity 2 incident post implementation of the change before closure of the RFC. And the Incident Management process will be triggered and linked to the Change and will follow incident management defined SLA's

4.4.14 DR options in the Change management cycle

4.4.14.1 The DR Options must be considered during the Change Initiation, review, Implementation and Closure phases of the Change request. If an application or infrastructure component does not have a DR plan, non-existence of the DR plan must be justified and later sent for Senior Manager, Unix & Database Administration approval.

4.4.14.2 Compliance Self Attestation including but not limited to removal of any elevated access, generic user Id's done by PM and checked in CAB phase by Change Manager and verified in technical post implementation review.

4.4.14.3 If the DR plan exists, it must be ensured in the later phases of change management that the change implementation is replicated in the respective DR plan and has to be approved by DR Manager before closing the change.

4.4.15 Change validity should not exceed one year unless a valid justification is provided, and proper assessment is conducted and approved by change manager.

4.5 Approval

4.5.1 All Normal Major Changes shall be approved by CAB and Head of Technology GRC & Head Technology Operations

4.5.2 Approval for Emergency changes shall be taken from minimum of 2 ECAB members (2 different IT streams) on phone or email; at least 1 email Approval is required. Change ticket shall be raised retrospectively, and necessary approval evidence shall be obtained post implementation of emergency change on next working day. All necessary change records shall be maintained.

4.6 Exception

4.6.1 For change implementation cases which require bypassing any usual step and / or control in the change management process, such as approvals on the ITSM tools, the respective Change Coordinator shall get the approval for the exception from the respective ADIB business unit, the related risk should be assessed and delt with as per ORM escalation Matrix and to be added to the RFC attachment section.

4.6.2 Any deviation to standard change management process/procedure shall be documented/ attached to change request along-with associated risks and shall be approved.

4.6.3 Significant and application impact changes implementations are not allowed during the freeze period, which extends in between 25th of each month till 2nd of next month.

4.6.4 Application owner must obtain CIO approval to execute any implementation during the freeze period. Freeze period is not applicable to emergency changes.

4.7 Pre-approved changes

4.7.1 The following shall be the key elements of a pre-approved change:

4.7.1.1 The change follows an established path / procedure.

4.7.1.2 There is a defined trigger to initiate the Request for Change.

4.7.1.3 The tasks are well known, documented, and proven.

4.7.1.4 Approval to implement has already been given in advance and accepted solution to a specific set of requirements is available.

4.7.1.5 Approval is effectively given in advance.

4.7.1.6 Budgetary approval is within the control of the change requester.

4.7.1.7 The Risk, Cost and Impact is usually low and well understood.

4.7.2   The list of all pre-approved changes shall be approved by CAB.

4.7.3   A list of pre-approved changes shall be maintained in the IT Service Management system. Any inclusions and exclusions shall be authorized by CAB.

4.7.4   All pre-approved changes shall be raised as a pre-approved change in IT Service Management System.

4.7.5   Records of all pre-approved changes shall be maintained in IT Service Management System.

4.8   Cloud Changes

Cloud changes are the changes in which select CI is tagged as Cloud. Below is the high-level flow for cloud related changes:

S.N.	Phase	Ownership and transition to next phase	Approval Level 1	Approval Level 2	Approval Level 3
1	Change Logging	Change Initiator needs to select the Cloud CI while submitting the change.			
2	Change Review	Change Coordinator. If review approvals are secured before planned start date, then change will move automatically.	Change Coordinator	1. Cloud Operations Team. (Cloud Management Team can select the option if requires involvement from Cloud COE) 2. Other Reviews based on selected tasks like Network, Security etc.	Cloud COE Team (If Support requires by Cloud COE team is selected) If change needs to be performed by CSP, Cloud COE Team should align with CSP and get the required inputs like - change schedule, impact assessment, risk assessment etc. and provide approval on change based on that.
3	Change Approval	Automatic after approvals	1. Head of IOP (Only for Minor Changes) 2. Change Manager		
4	Change Implementation	1. Tasks will get assigned to Cloud Operations Team & Cloud COE Team. 2. For Major and Significant Changes, tasks will be created after CAB approval. 3. If CSP involvement is required then task should be closed	CAB Approval (For Major and Significant Changes)		

S.N.	Phase	Ownership and transition to next phase	Approval Level 1	Approval Level 2	Approval Level 3
		after the CSP confirmation only. 4. Once Tasks are closed, change coordinator needs to submit change for closure.			
5	Change Closure	Change Coordinator will close the change			

For application related changes in which cloud CIs are involved, it will follow the application change process and additional approvals and tasks will be included as per above flows.

For Emergency changes in which cloud CIs are involved, it will follow the emergency change process and additional approvals and tasks will be included as per above flows.

4.9   Change Request Categories

Please refer to Appendix B for Change Request categories.

4.10   Impact and Risk Assessment of Changes

- All changes shall be assessed for their risk and impact, with respect to proposed change to the asset / service, downtime, implementation, and any impact to other dependent assets / services.
- Impact analysis examines the proposed change to identify potential consequences of change and to estimate the effort associated with implementing the change.
- Risk assessment examines the proposed change to identify factors that negatively affect the business, prevent users from fulfilling their roles, and control the change to eliminate or improve such factors.
- Impact analysis and risk assessment shall be calculated based on standardized questionnaire utilizing weighted scoring in Appendix C.
- Based on risk assessment, Priority shall be decided for the implementation of the change.
- Change Impact and Risk assessment shall be defined as follows:

Risk Index Rating:		Impact Index Rating:	
Rating	Risk Scoring	Rating	Impact Scoring
High	17 – 24	High	25 -40
Medium	9 – 16	Medium	13 – 24
Low	1 – 8	Low	1 -12

Note: - Impact and risk scoring shall be calculated based on standardized questionnaire utilizing weighted scoring in Appendix C

4.11   Change Complexity Determination

Change complexity shall be determined based on the following Matrix

Change Complexity	Risk-High	Risk-Medium	Risk-Low
Impact-High	Major	Major	Significant
Impact-Medium	Major	Significant	Significant
Impact-Low	Significant	Minor	Minor

4.12   Change Priority

Change priority is automatically determined by the change management system based on the following Matrix:

Priority	Impact – Multiple Business Groups / Enterprise	Impact – One Business Group / Site	Impact - Multiple Users	Impact – None or Single User
Urgency-Very High	Critical	Critical	High	Medium
Urgency-High	High	High	High	Medium
Urgency-Medium	Medium	Medium	Medium	Low
Urgency-Low	Low	Low	Low	Low

- The Change Approvers and CAB committee and other associated teams/committee shall give preference to critical and high priority changes while approving the change requests.

4.13   Change Deployment Testing

- Changes shall be tested in a test environment wherever possible, with respect to quality, security and to ensure the fulfilment of the requirements and test results shall be attached in change request, wherever possible.
- The following shall be considered for infrastructure changes in case test environment is not available:
  - If the IT system on which the change is to be carried out (such as a server) is available in development environment, then test the change in development.
  - If the IT system on which the change is to be carried out (such as network/ security device) is available in DR environment, then test the change in DR environment.
  - In case of routers / switches first test the change on non- critical routers/ switches.
  - In case change request require bulk roll out then first carry out the change on required sample systems.
- The following changes shall initiate the UAT for testing the change, before the change is implemented in the production environment:
  - Code Changes.
  - Major Software Enhancements.
  - Software Error / Bug fixes.
  - Software Functional Changes.
  - End-to-End Testing is required for changes; and
  - Changes that have an enterprise level impact.
    a. Non-functional infrastructure changes such as: New laptop models
    b. New PCs models
    c. Systems which effect large group of end users (DLP, IP Phones, Video Conferencing, Citrix portals, PAM, PCs/Laptops Images

4.14 Notifications

▪ Notification for change request status shall be automated through the Change Management Tool (Service Now) according to the table in Appendix F.

4.15 Status Code

▪ The status of each change request shall be updated in the Change Management tool () according to the table in Appendix G.

5 Appendix

5.1 Appendix A – Roles and Responsibilities

The responsibilities of various roles in Change Management Process are listed as follows:

Roles	Responsibilities
Change Requester	- Provide detail description of Change through appropriate form (RFC) - Know what Changes they can request - If required, provide additional information in Change review and assessment phase - Obtain appropriate approvals (Business units & IT) before submitting RFC - Where relevant, ensure that the key risks related to significant changes are assessed and within the appetite and/or escalated/accepted as per ORM escalation matrix
Change Coordinator (Team Leads shall perform role of Change Coordinator).	- Reviews the RFC for completeness of information. - Ensure appropriate approvals (Business units & IT) are obtained before submitting RFC - Reject invalid RFC. - Assess the complexity of Change - Creates change tasks for building, testing, and implementing a change. - Coordinates the review phase of the change. - Liaise with all necessary parties to coordinate Change building, testing and implementation, in accordance with schedules. - Review all outstanding Change Requests awaiting consideration or awaiting action - Analyze Change records to determine any trends or apparent problems that could occur - Communicate the status of the Change to various service support and process managers - Facilitate the Change Manager in preparing the necessary reports - Verifies that the change passed the test criteria. - Update Change & Release Manager about the necessity of Release Record during Assessment and Planning phase - Coordinates all activities in case the Emergency Change process is triggered. - Communicate and take approval for downtime from the respective system owner.
Change Analyst	Involved in Change Review to deliver input to the Change Coordinator when assessing the Change

Roles	Responsibilities
	• Builds, tests, and implements changes based on the change tasks. • Executes the backup plan if required. • After implementation, evaluates the change handling and closes the Change • Verifies the change tasks created by Change Coordinator for building, testing, and implementing a Change
Change Implementer (Same as Change Analyst)	• Carryout the tasks as assigned by Change Coordinator • Report on the completion / failure of the assigned task to Change Coordinator • Perform testing or co-ordinate with testing team and review the test results

Change Manager (Process Owner)	• Coordinate with IT Governance to perform the following:
	  ○ Ensures uniform deployment of the process
	  ○ Reviews effectiveness and efficiency of the process
	  ○ Monitors the process for ensuring compliance
	  ○ Periodically reviews changes in Post Implementation
	  ○ Review and determines and executes Follow-up actions
	• Ensures that new services are added, and outdated services are removed from Change catalogue (Pre-approved and Standard change list)
	• Ensures that the process is defined, documented, maintained, and communicated at all levels within the organization and to vendors
	• Ensures that changes are presented for approvals to appropriate approval groups based on change category and change approval matrix.
	• Establishes and communicates the process roles and responsibilities
	• Establishes and communicates the process, service levels, and process performance metrics
	• Provides adequate process training within organization
	• Conduct CAB as per schedule every week by communicating all stakeholders and ensure their availability during CAB and collating data required for CAB meeting.
	• Obtain CAB approval for Implementation change
	• Document proceedings of CAB and actions, decisions to be communicated to the stakeholders / pre-identified notification receiving members list

CAB Committee:	• Reviews the RFC for Business and Technical Impacts • Verify the Change Schedules before approving Changes • Approve or deny Change when requested
ECAB Committee:	• Review and approve all Emergency Changes

IT Governance	• Coordinate with Change Manager to complete the following:
	  ○ Reviews effectiveness and efficiency of the process
	  ○

5.2 Appendix B – Change Categories

The Change Request Categories shall be defined in Service Management Tool as follows:

Category	Subcategory
Application	New Application
	New Module/Function
	Architecture
	Patch Update
	Functional Enhancement
	Performance Enhancement
	License Update
	Bug-Fix
	Maintenance
	Decommission
	Data Change
	Interface
	Security
Infrastructure	New Build
	Bug Fix
	Maintenance
	Architecture
	Capacity
	Security
	Performance Enhancement
	Patch Update
	Upgrade
	Hardware
	Decommission
	Non- Production

5.3 Appendix C – Impact and Risk Ratings:

Impact Analysis Questionnaire and Weights:

Question	Answer	Weight
Financial Impact?	No	1
	Yes	4
Functional (Business Process) Impact (Significant Process change, control design change, control waivers, etc....)?	No	1
	Yes	4
Down Time Required?	No	1
	Less than 30 Mins	2
	30 Min to 1 Hours	3

Question	Answer	Weight
	More than 1 hour	4
No. of Systems Impacted?	None	1
	One System Impacted	2
	Two or more Systems impacted	4
Users Affected?	None or Single User	1
	Specific Users	2
	One Business Group /Site	3
	Multiple Business Groups / Enterprise	4
Integrations / Interfaces Impacted?	No Integrations Impacted	1
	One Integration Impacted	2
	Two or more integrations impacted	4
GL creation?	No	1
	Yes	4
Impact on Core Banking systems?	No	1
	Yes	4
Impact on Channels?	No	1
	Yes	4
Impact on Middleware?	No	1
	Yes	4

Risk Analysis Questionnaire:

Risk Questions	Answer	Weight
Application Criticality?	Low	1
	Medium	2
	High	4
Implementation Complexity	Minor (Parameter Change)	1
	Medium (one Module Configuration)	2
	Major (System Level)	4
No. of Implementation Groups Involved?	2 Group or less	1
	3 Groups	2
	4 or More Groups	4
Manual Activities involved?	No	1
	Yes	4
Roll back / Recovery plan in place?	Yes - Full Recovery Plan	1
	Yes - Partial Recovery Plan	2
	No	4
Change for Locations?	One	1
	Two	2
	Global	4

5.4 Appendix D – Review Approval Matrix

Task Group	Task	Change-Coordinator	CSA	Database	Network	Server	Storage	Security
Application	Application Deployment	✔	✔					
	Patch/Update	✔	✔					
	Decommission	✔	✔					
	Software Installation	✔	✔					
	Version upgrade	✔	✔					
	Configuration/Parameter change	✔						
	Data Change	✔						
	New Interface	✔	✔					
	License Configuration	✔	✔					
	Reports Enhancement	✔						
	Access Permission Changes	✔						
	Task Not Required	✔						
database	Configuration	✔		✔				
	Data	✔		✔				
	Decommission	✔		✔				
	Installation	✔	✔	✔				
	Patch Release	✔	✔	✔				
	Backup / Restore	✔		✔				
	Security	✔		✔				
	Access Control							

Task Group	Task	Change-Coordinator	CSA	Database	Network	Server	Storage	Security
Network	Configuration	✔			✔			
	Data	✔			✔			
	Decommission	✔			✔			
	Firewall Communications	✔			✔			
	Firewall Security	✔			✔			
	Hardware	✔			✔			
	New Installation	✔	✔		✔			
	System Software	✔			✔			
	Upgrade	✔	✔		✔			
	Voice	✔			✔			
	Access Control	✔						
Server	Bug fix	✔				✔		
	Configuration	✔				✔		
	Decommission	✔				✔		
	Hardware	✔				✔		
	New Build	✔	✔			✔		
	Patch Release	✔	✔			✔		
	Upgrade	✔	✔			✔		
	Access Control	✔						
	Operating System Changes	✔				✔		
Storage	Configuration	✔					✔	
	Hardware	✔					✔	
	Size	✔					✔	

Task Group	Task	Change-Coordinator	CSA	Database	Network	Server	Storage	Security
	Upgrade	✓	✓				✓	
	New Installation	✓	✓				✓	
	Access Control	✓					✓	
	Configuration	✓						✓
	Firewall Communications	✓						✓
Security	New Installation	✓	✓					✓
	Upgrade	✓	✓					✓
	Access control	✓						✓
Application-->New Application	Any	✓						
Infrastructure--> Non-Production	Any	✓						

ADIB مصرف أبوظبي الإسلامي

5.5 Appendix E - Approving Authority Matrix:

Change Category	Implementation Group	Change Complexity	Change Approval						Release Review (Only for Denial or Phase changed Releases)	Release Implementation	Release Closure			Change Implementation CAB (Normal Change)	Change Implementation ECAB (Emergency Change)	
			DRB Approval	CSA Infra Approval	Application Owner	Release Manager	Senior Manager, Unix & Database Administration	Change Manager	Release Manager	CSA	Release Manager	ICD	Sharia	FCD	Change Manager	Head of IT Governance Risk & Compliance	Head of Technology & Communication Services
Application	Application	Major			✔	✔	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
		Significant			✔	✔	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
		Minor			✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✘	✘	✘
Infrastructure	database	Major			✘	✘	✘	✔							✔	✔	✔
		Significant			✘	✘	✘	✔							✔	✔	✔
		Minor			✘	✘	✔	✔							✘	✘	✘
	Network	Major			✘	✘	✘	✔							✔	✔	✔
		Significant			✘	✘	✘	✔							✔	✔	✔

ADIB مصرف أبوظبي الإسلامي

| Dept./ Unit: | ITD / GRC | Issue Date: | 19th Feb, 2019 |
| Standard: | STD-ITD-537 Change Management Standard | Version: | 5.0 |

Change Category	Implementation Group	Change Complexity	Change Approval						Release Review (Only for Denial or Phase changed Releases)	Release Implementation	Release Closure				Change Implementation CAB (Normal Change)	Change Implementation ECAB (Emergency Change)	
			DRB Approval	CSA Infra Approval	Application Owner	Release Manager	Senior Manager, Unix & Database Administration	Change Manager	Release Manager	CSA	Release Manager	ICD	Sharia	FCD	Change Manager	Head of IT Governance Risk & Compliance	Head of Technology & Communication Services
		Minor			✗	✗	✓	✓							✗	✗	✗
	Server	Major			✗	✗	✗	✓							✓	✓	✓
		Significant			✗	✗	✗	✓							✓	✓	✓
		Minor			✗	✗	✓	✓							✗	✗	✗
	Storage	Major			✗	✗	✗	✓							✓	✓	✓
		Significant			✗	✗	✗	✓							✓	✓	✓
		Minor			✗	✗	✓	✓							✗	✗	✗
	Security	Major			✗	✗	✗	✓							✓	✓	✓
		Significant			✗	✗	✗	✓							✓	✓	✓
		Minor			✗	✗	✓	✓							✗	✗	✗

Change Category	Implementation Group	Change Complexity	Change Approval						Release Review (Only for Denial or Phase changed Releases)	Release Implementation		Release Closure			Change Implementation CAB (Normal Change)	Change Implementation ECAB (Emergency Change)	
			DRB Approval	CSA Infra Approval	Application Owner	Release Manager	Senior Manager, Unix & Database Administration	Change Manager	Release Manager	CSA	Release Manager	ICD	Sharia	FCD	Change Manager	Head of IT Governance Risk & Compliance	Head of Technology & Communication Services
Application-->New Application	Any	Any	✓	✗	✗	✓	✗	✗	✗	✗	✓	✗	✗	✗	✓	✓	✓
Infrastructure-->Non-Production	Any	Any	✗	✓	✗	✗	✗	✓	▢	▢					✗	✗	✗

5.6 Appendix F - Notification Matrix:

Notification	Target Audience
▪ Change in status of Change Request ▪ Any update in Change Request ▪ Request for additional information ▪ Any change escalation	Change Coordinator and Change Requestor
▪ Change in status of Change Request ▪ Any update in Change Request ▪ Any change escalation ▪ Any approval given for change ▪ When task is assigned	Change Implementer(s)
▪ Notification for change approval	CAB
▪ Change in status of Change Request ▪ Any change escalation ▪ Notification for change approval	Change Manager

5.7 Appendix G - Change Request Status Codes:

Status Code	Description
Approval Status Codes	
Pending	Pending for approval from Change Approvers/ CAB
Approved	Approved by Change Approvers / CAB
Rejected	Rejected by Change Approvers / CAB
Closure Status Codes	
Successful	Change completed successfully
Completed with Problem	Change completed successfully but with problems (i.e. extended Change window not factored before change)
Failed	Change failed and triggered an incident
Roll-back	Change failed and roll-back implemented to restore services
Rejected	Change Request is rejected by Change Approvers / CAB
Withdrawn	Change Request is withdrawn by the Requester
Cancelled	Change Request is cancelled

5.8 Appendix H – References

Doc. Ref. No.	Name	Type of Document (Policy / Standard)
IMSM-ITD-001	Integrated Management System Manual	Manual

5.9   Appendix I – Email Notification for Production changes

System/Application Name:

Name: (name of the changed for example firewall upgrade)

Executive Summary: (A brief summarized paragraph on the subject change. This paragraph is intended to be read by ADIB Senior Management/Leaders) - to be reviewed by department head

System Criticality: (High, Medium, Low)

Scope:

Benefits:

Implementation steps:

Implementation duration date/time:

*Impact Rating (Enterprise, Site/Dept., Multiple Users, User) - to be reviewed by department head

*Impact Rating (High, Medium, Low) - to be reviewed by department head

Impact on other systems and Interfaces:

Down time:

QA and UAT completed (YES/NO, if no Why):

Infrastructure, support, new-laptops models, new PC's, models and non-application systems which affect the end users experience such as DLP, IP Phones, Video conferencing, Citrix portals, PAM, PC/Laptops images/Hardware, etc.) shall be tested under the QA function supervision and sign off.

Business approval received (YES/NO, if no Why):

Involved teams: (internal, external and business)

Readiness and test plans:

Rollback plan: (detailed task list with timing) – If roll back is decided, explicit approval is needed prior to the rollback.

Communication: to whom to communicate (before, during and after the implementation)

Risk: In case there is risk associated with the change, which approved it.

Rollback verifier: (person or vendor verified the role back plan and timing)

Included in external reporting (Critical Severity-1 Application Changes**) (Yes/No)? (To be filled by the department Head)**

For new services mention the following: -

- **Service IT owner:** *Manage the service from IT perspective/coordinating with business/end user and vendor.*
- **Service implementer:** *IT unit implementing the solution (technical capabilities).*
- **Service operator:** *Daily operation, respond to end user calls, BaU.*
- **Service support:** *Resolve service issues.*
- **Service monitor:** *Ensure the service is functioning as intended and alerts are investigated.*