ADIB – Procedure

(ADIB UAE & Subsidiaries)

Technology Risk Management Procedure

PRC-ITD-510

Date: 30th August 2023

Version: 7.0

Version Control & Change Management

Version	Issue Date	Details of Change	Reason for change
7.0	August, 2023	Added reference to ITD processes Change Management and Incident Management.	Risk Management activities for Incidents and Changes are not mentioned in this procedure as they are covered in the Incident and Change Management processes by the respective process owners.
6.0	August, 2022	All sections are aligned with ISO 31000 and ADIB Group Operational Risk Framework & Policy	Alignment with ISO 31000, ADIB Group Operational Risk Framework & Policy and ITD Organization Structure Changes
5.2	December, 2021	Document reviewed and no changed required.	Process annual review
5.1	Publishing Date	Removed reference: Template TML-ITDD-092 Risk Register	ITD Risk Register is integrated into Risk Management Software application (Archer).
5.0	Publishing Date	Republish document	Aligning the process with ORM framework

Prepared by	Approved by	Reviewed by
IT Governance Team	Head of Technology Risk	ITD Governance Manager

Contents

1 Purpose & Scope

The purpose of this to procedure is to outline the process activities for managing Technology Risks in line with the ADIB Group Operational Risk Management Framework & Policy and the ISO 31000 Framework.

This procedure is applicable to all Technology processes and systems managed by ADIB ITD for ADIB UAE and its international sites.
Technology risks related to Information Security are excluded from this procedure as they are managed by the ADIB Group Information Security Department (GISD).

Risk Management activities for Incidents and Changes are covered in ITD Incident Management and Change Management processes by their respective Process Owners. Hence, Technology Incidents and Changes shall not be covered in this procedure to avoid redundancy.

2 Process Owner

Head of Technology Risk

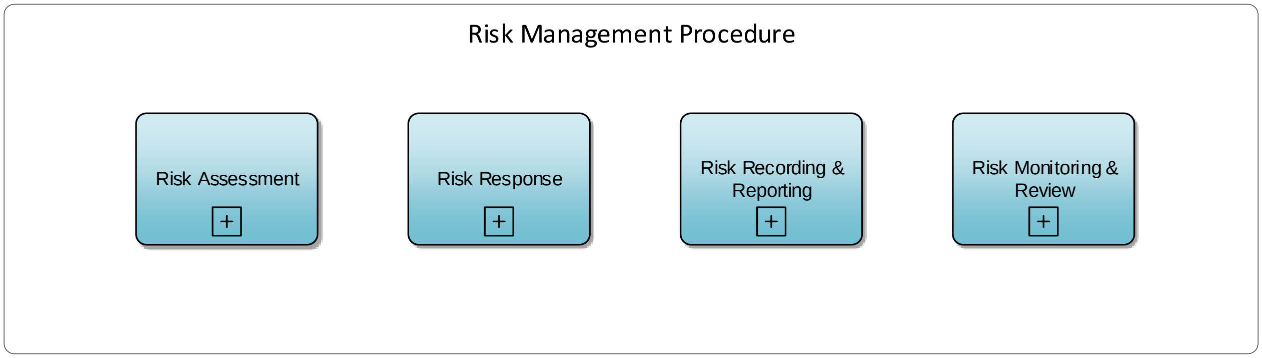
3 Other stakeholders

- CIO
- Head of Technology GRC
- Technology Risk Representative
- Head of Technology Operations
- Head of Technology Reg & Ops Platforms
- Head of Technology Enterprise Architecture
- Head of Technology Digital Banking Platforms
- Head of Technology Enterprise Solutions & Data Platforms
- Head of Technology Retail Banking Platforms
- Head of Technology WBG, Treasury & Risk Platforms
- Head of Digital Factory
- Head of Cloud Center of Excellence

4 RACI

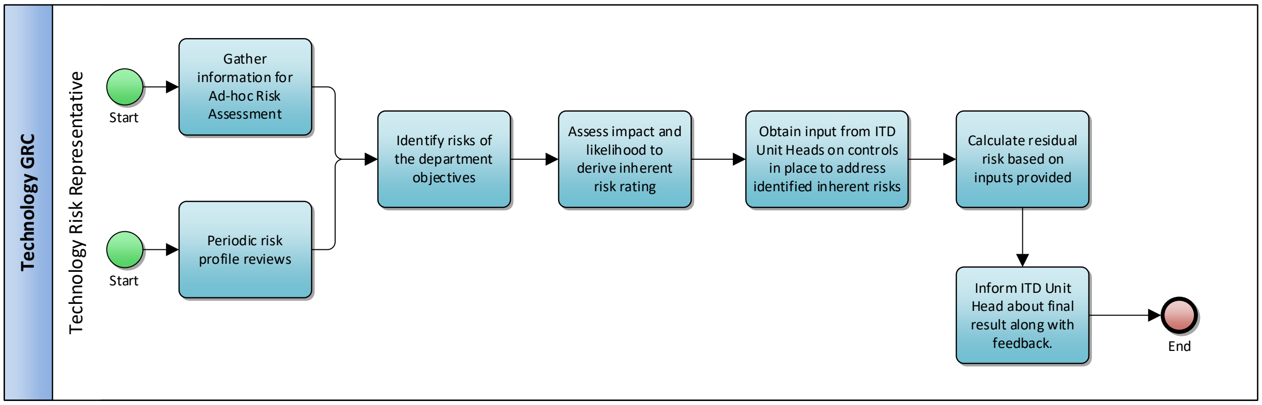
Roles / Activity	Technology Risk Representative	ITD Dept Technical Lead/SMEs	ITD Department/Unit Head	Head of Technology Risk	Head of Technology GRC	CIO
Risk Assessment (Identification, Analysis, Evaluation)	R	R	R	A, C	I	I
Risk Response	C	R	A	C	C, I	C, I
Risk Recording & Reporting	R	R	R	A, R	I	I
Risk Monitoring & Review	R	C	I, C	A	I	I

5 Risk Management Procedure – High Level



6 Detailed Process Description and Workflows

6.1 Risk Assessment (Identification, Analysis, Evaluation)

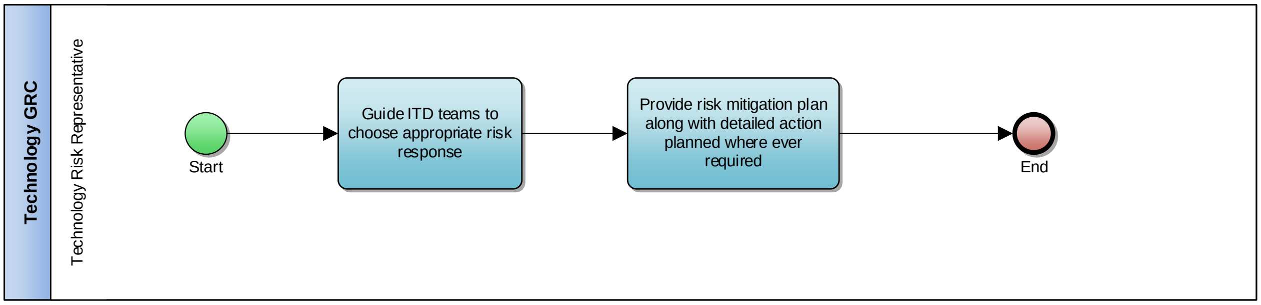

Technology GRC
Technology Risk Representative
Start
Gather information for Ad-hoc Risk Assessment
Start
Periodic risk profile reviews
Identify risks of the department objectives
Assess impact and likelihood to derive inherent risk rating
Obtain input from ITD Unit Heads on controls in place to address identified inherent risks
Calculate residual risk based on inputs provided
Inform ITD Unit Head about final result along with feedback.
End

Sr. No.	Process Step Description	Responsibility	Document (STD, SOP, FORM, CL, TML WI) / Tool Reference
1.	Gather the below information as part of Risk Planning: **Ad-hoc Risk Assessment** 1. Scope of the assessment 2. Exclusions 3. Objective(s) of the assessed scope 4. Objective of the risk assessment – such as but not limited to: a. To support decision making - decide between competing technology options/objectives/systems/vendors/services b. Identify & assess specific category(s) of risk(s) in Technology production environment/processes, in response to emerging technology trends/opportunities, new technology threats etc.	Technology Risk Representative	ITD Process Portal

Sr. No.	Process Step Description	Responsibility	Document (STD, SOP, FORM, CL, TML WI) / Tool Reference
	c. New technology systems /processes/roles/organization structure d. Major changes on existing production technology systems/processes/roles/organization structure etc.) 5. Historical issues/incidents and trending data related to the scope. 6. International standards/control frameworks/expert opinions & ratings related to the scope. **Periodic Risk Profile Reviews of Technology Departments** 1. Department Objectives 2. Department Organization structure 3. Department Processes & Practices 4. Tools & Technologies Used by the Department 5. Business systems/services supported by the Department. 6. Third party vendor dependencies 7. Applicable Regulations 8. Related historical data – incidents, external & internal audit findings. 9. Related emerging threats to the Department objectives. 10. Related trending data, expert opinions on emerging technology processes, systems 11. International standards/control frameworks related to the Department processes, organization structure and tools.		
2.	Identify risks to the Department Objectives from the below risk sources through brainstorming and interview sessions with Department Owner, Department Technical SMEs\Leads and include external SMEs wherever required. 1. People risks. 2. Process risks 3. Risks from Technology/Tools used by the Department. 4. External sources/events (external frauds, vendors, natural disasters, emerging trends, threats etc.) 5. Regulatory Risks	Technology Risk Representative	
3.	Assess Impact and likelihood of the identified risks to derive inherent risk rating.	Technology Risk Representative	ADIB Group Operational Risk Framework & Policy
4.	Provide inputs on existing controls/ compensating controls in place to address the identified inherent risks.	ITD Department/Unit Head and ITD Department	

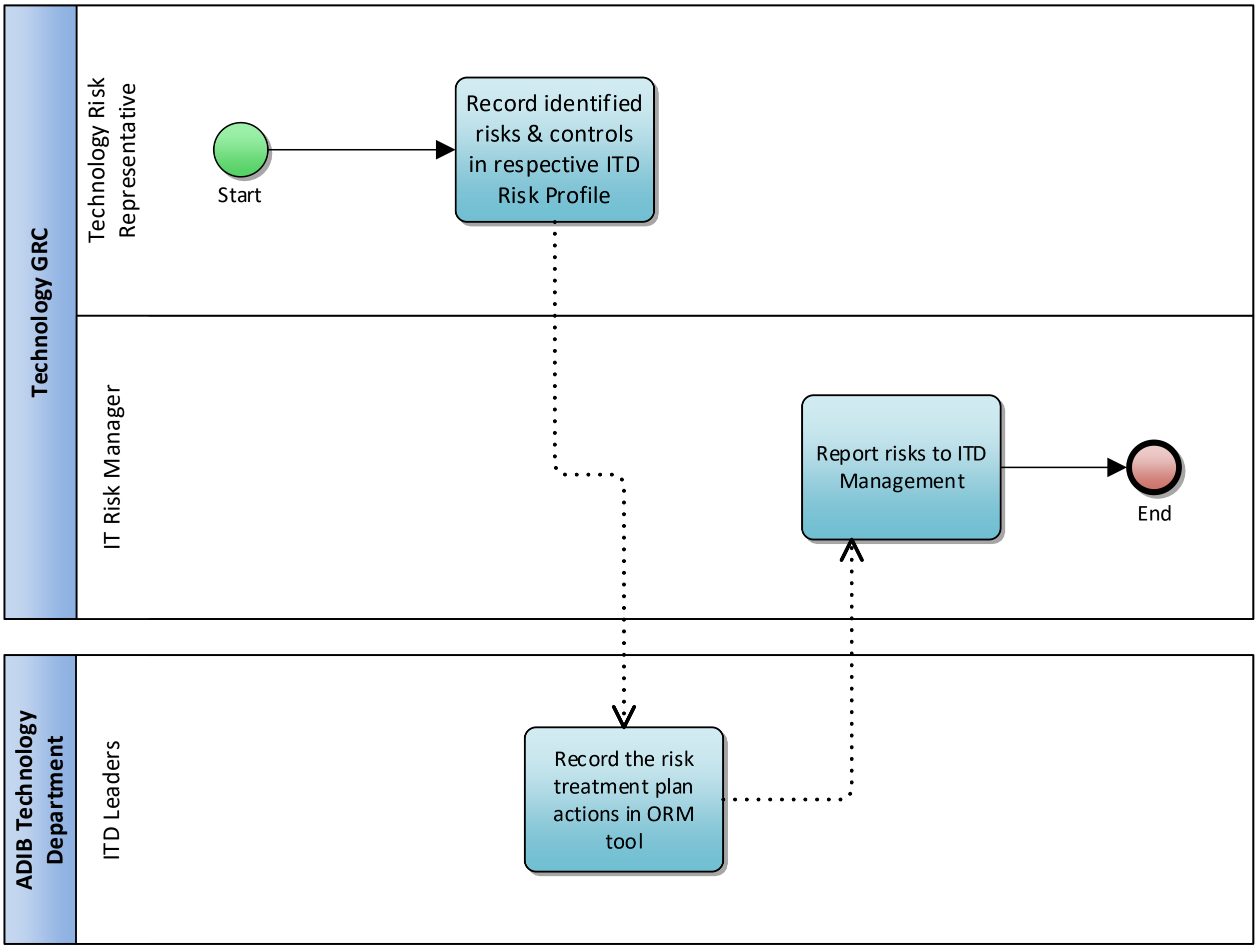
Sr. No.	Process Step Description	Responsibility	Document (STD, SOP, FORM, CL, TML WI) / Tool Reference
		Technical Lead/SMEs	
5.	Calculate residual risk based on the control inputs provided above	Technology Risk Representative	ADIB Group Operational Risk Framework & Policy
6.	Inform ITD Department/Unit Head on the final results of the Risk Assessment along with feedback of recommended mitigation actions, wherever required, to reduce the residual risk to be within the ADIB Risk Appetite.	Technology Risk Representative	ADIB Group Operational Risk Framework & Policy

6.2 Risk Response


Technology GRC
Technology Risk Representative
Start
Guide ITD teams to choose appropriate risk response
Provide risk mitigation plan along with detailed action planned where ever required
End

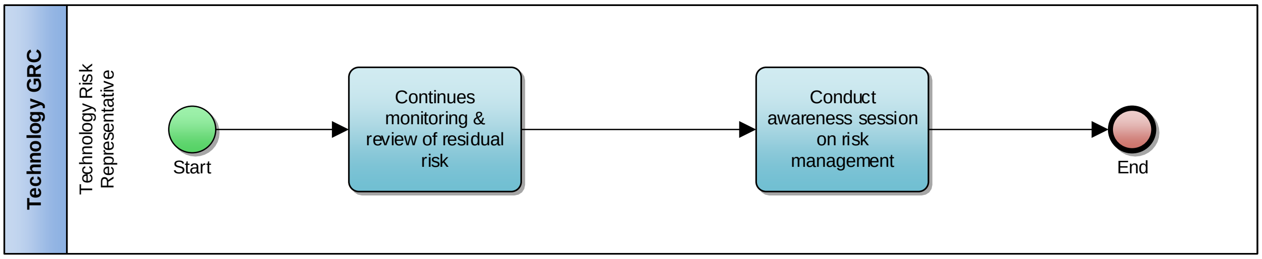
Sr. No.	Process Step Description	Responsibility	Document (STD, SOP, FORM, CL, TML WI) / Tool Reference
1.	Guide the ITD team to choose the appropriate risk response to ensure the residual risk is within ADIB's Risk Appetite	Technology Risk Representative	ADIB Group Operational Risk Framework & Policy
2.	Provide the risk mitigation plan wherever required along with detailed action plans and timelines for implementing them.	ITD Department/Unit Head	

6.3 Risk Recording & Reporting


Technology GRC
Technology Risk Representative
Start
Record identified risks & controls in respective ITD Risk Profile
IT Risk Manager
Report risks to ITD Management
End
ADIB Technology Department
ITD Leaders
Record the risk treatment plan actions in ORM tool

Sr. No.	Process Step Description	Responsibility	Document (STD, SOP, FORM, CL, TML WI) / Tool Reference
1.	Record the identified risks and controls in the respective ITD Risk Profile	Technology Risk Representative	ADIB ORM System
2.	Record the risk treatment plan actions	ITD Unit Head	ADIB ORM System
3.	Risks are reported to ITD Management	Head of Technology Risk	BRCC

6.4 Risk Monitoring & Review


Technology GRC
Technology Risk Representative
Start
Continues monitoring & review of residual risk
Conduct awareness session on risk management
End

Sr. No.	Process Step Description	Responsibility	Document (STD, SOP, FORM, CL, TML WI) / Tool Reference
1.	Continuous monitoring and review of residual risk is performed via: 1. RCSA 2. KRI 3. Risk Profile Reviews 4. Internal Control Assurance Reviews 5. Internal and External Audits 6. Technology Incidents	Technology Risk Representative	
2.	Conduct awareness sessions on Risk Management as per annual awareness plan	Technology Risk Representative	

7 Key Performance Indicator (KPI)

Sr. No.	Key Performance Indicators	Target	Frequency	Reporting to whom	Source	Formula
1	Perform risk assessments for ITD units as per plan	100%	Annual	Head of Technology Risk Management	Manual	(Number of Assessments performed / Number of Assessments planned) * 100

8 Risks and Controls

Risk	Controls	**Reference** (section number in the procedure)
Unawareness around risk management procedure among ITD Units.	Awareness around risk management procedure with relevant stakeholders	6.4 Awareness session

9 Key Risk Indicator (KRI)

Metric Name	Calculation Method
Outdated Risk Profiles	Count of ITD Departments where Risk Profiles were not reviewed in a calendar year

Metric Name	Calculation Method
Risks from New Systems and Major Changes	Count of new systems and/or major changes deployed without Technology Risk Assessments

10 Appendices

Appendix 1: References

Name	Type of Document (Policy / Standard)
Group ORM Framework and Policy	Policy
ISO 31000	International Standard

Appendix 2: Acronyms

Abbreviation	Acronym
ADIB	Abu Dhabi Islamic Bank
ITDD	Information Technology Division
KPI	Key Performance Indicators
RR	Risk Register