CRESCENT BANK

TRUST BEYOND BANKING.

Risk Assessment Methodology

CRESCENT
BANK
TRUST BEYOND BANKING.

Risk Assessment Methodology

DOCUMENT CLASSIFICATION	Internal
DOCUMENT REF	ISMS-DOC-06-01
VERSION	2
DATED	27 September, 2025
DOCUMENT AUTHOR	Sheheryar Altaf
DOCUMENT OWNER	Ali Khan, ISMS Project Manager

Revision History

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
1	27 September, 2025	Sheheryar Altaf	Initial Draft
2	28 September, 2025	Sheheryar Altaf	Added minor corrections

Distribution

NAME	TITLE
Mr. Ahmed Khan	CEO
Mr. Bilal Qureshi	CFO
Ms. Sara Malik	CISO
Mr. Kamran Pervaiz	Compliance & Audit Head

Approval

NAME	POSITION	SIGNATURE	DATE
Mr. Ahmed Khan	CEO	____________________	28 September, 2025
Mr. Bilal Qureshi	CFO	____________________	29 September, 2025
Ms. Sara Malik	CISO	____________________	30 September, 2025

Contents

Tables

1. Introduction

Crescent Bank manages sensitive customer and financial data. Therefore making information security essential for maintaining trust and meeting regulatory requirements.
This document defines the Risk Assessment Methodology that Crescent Bank will apply to identify, analyze, evaluate, and treat information security risks in a consistent and transparent manner.

To support this, the bank is in the process of establishing an Information Security Management System (ISMS) aligned with the ISO/IEC 27001 standard.

2. Purpose

The purpose of this document is to define the methodology that Crescent Bank will use to identify, analyze, evaluate, and treat information security risks in accordance with ISO/IEC 27001 Clauses 6.1.2 and 6.1.3.

This methodology provides a consistent and structured approach for managing risks within the ISMS, ensuring that information security risks are addressed in a transparent and repeatable manner, and that decisions are aligned with business and regulatory requirements.

3. Objectives

The objectives of this Risk Assessment Methodology are to:

- Provide a consistent process for identifying, analyzing, evaluating, and treating risks.
- Ensure risk decisions align with business and regulatory requirements.
- Support the selection of appropriate controls through the Statement of Applicability.
- Ensure that residual risks are formally reviewed and accepted by management.

4. Scope

This ISMS scope is formally defined and maintained in accordance with Clause 4.3 of ISO/IEC 27001:

Scope Type	Included Elements
1. System Scope	Core banking (Temenos T24), Internet & mobile banking, payment systems, ATMs, POS, servers, databases, network infrastructure, backup & DR systems
2. Physical Scope	HQ (Karachi), critical branches, Data Center & DR site (Islamabad), server rooms, ATM locations, digital banking servers, source code escrow (external provider, Zurich)
3. Organizational Scope	IT, Security, Risk & Compliance, Operations (Retail, Lending, Digital Banking), HR (PII handling),and Financial (sensitive transactions)

5. Roles and Responsibilities

Name	Title	Responsibility in Risk Management	Reports To
Mr. Ahmed Khan	CEO	Oversees risk evaluation at a high level, reviews outcomes against the organization’s risk appetite, and accepts residual risks to ensure alignment with overall business strategy.	—
Mr. Bilal Qureshi	CFO	Allocates budget for risk treatment and ensures cost–benefit alignment in risk management.	CEO
Ms. Sara Malik	CISO	Leads the cybersecurity risk management program, ensuring risks are identified with owners, coordinated with GRC/compliance teams, controls implemented by technical teams, and risk posture reported to the board.	CEO
Mr. Saqib Zulfiqar	Digital Banking Head	Supports the CISO in implementing information security risk management, identifies and owns security risks within the department. Ensures compliance with ISMS requirements.	CEO
Mr. Mubeen Paracha	Retail Banking Head	Supports the CISO in implementing information security risk management, identifies and owns security risks within the department. Ensures compliance with ISMS requirements.	CEO
Mr. Musa Ajmal	Financing Head	Supports the CISO in implementing information security risk management, identifies and owns security risks within the department. Ensures compliance with ISMS requirements.	CEO
Mr. Tariq Umer	Operations Head	Supports the CISO in implementing information security risk management, identifies and owns security risks within the department. Ensures compliance with ISMS requirements.	CEO

Mr. Asim Muneer	HR Head	Identifies risks related to employee data, privacy, and PII, supports implementation of risk treatment measures, and ensures ISMS compliance within the HR department	CEO
Mr. Kamran Pervaiz	Compliance & Audit Head	Ensures regulatory compliance (e.g., SBP guidelines), oversees IS and compliance audits, and supports risk identification, analysis, and mitigation.	CEO
Mr. Abdullah Ali	Data Protection Officer (DPO)	Identifies and analyzes risks related to privacy and data protection across the organization, advises on mitigation with technical teams, and ensures compliance with data protection requirements by monitoring and reporting to senior management	CISO
Mr. Ali Khan	ISMS Project Manager	Coordinates and facilitates the ISMS risk management process, consolidating risks identified by business and asset owners, supporting analysis and evaluation, and ensuring that risk treatment measures are documented, monitored, and implemented by responsible teams	CISO
Ms. Sidra Imran	Technical Lead	Leads ISMS technical controls, coordinates SOC, testing, and incident response, ensures vulnerabilities are remediated, and implements risk treatments approved by management, while residual risk acceptance stays with leadership	ISMS Project Manager

6. Risk Assessment Approach

Crescent Bank will adopt an asset-based approach, identifying risks associated with critical information assets. A qualitative assessment method will be applied, with risks rated against predefined likelihood and impact criteria (Low, Medium, High). The results will be recorded in a risk register and illustrated through a risk heat map to support informed management decisions.

This methodology ensures a consistent and repeatable process, aligned with ISO/IEC 27001:2022 Clause 6.1.2, and tailored to the Bank's size, regulatory environment, and operational context.

6.1 Risk Appetite and Tolerance

Crescent Bank maintains a low tolerance for information security risks due to its regulatory obligations and the criticality of banking operations.

1. High Risks (Score 16–25): Not acceptable; must be treated or mitigated.
2. Medium Risks (Score 9–15): Normally require mitigation; acceptance is allowed only with strong justification and formal approval from senior management.
3. Low Risks (Score 1–8): May be accepted by the relevant risk owners if consistent with business objectives.

This framework ensures that risk decisions remain consistent with the Bank's conservative risk appetite and its commitment to safeguarding information assets and regulatory compliance.

7. Risk Identification Process

Risks will be identified by business owners, department managers, and employees, based on their knowledge of processes and assets. Risk sources may include internal and external factors, such as information assets, threats, vulnerabilities, legal/regulatory obligations, past incidents, and audit findings.

Identification techniques include workshops, judgment, review of past incidents, threat intelligence, and structured meetings. All identified risks will be documented and placed in the risk register as input for analysis and evaluation.

9. Risk Analysis Process

Risks identified by business/asset owners will be analyzed using an asset-based, qualitative approach. Each risk will be assessed for likelihood and impact, using predefined criteria tailored to the Bank's context. Likelihood is rated on a 1–5 scale, from Rare (1) to Almost Certain (5), reflecting the probability of occurrence.

Impact is also rated 1–5, considering multiple dimensions such as operational disruption, financial loss, reputational damage, and legal/regulatory consequences. An average score is calculated across these dimensions to determine the overall impact. The risk score is obtained by multiplying Likelihood × Impact, and risks are categorized as Low (1–5), Medium (6–14), or High (15–25). Likelihood is generally a single rating but may be averaged if multiple reviewers provide different scores.

The results are documented in the risk register and visualized in a risk heat map, giving management a clear view of risk exposure and supporting informed decision-making. This approach ensures a consistent, repeatable, and ISO 27001:2022 Clause 6.1.2–aligned process tailored to the Bank's operational context.

8. Risk Evaluation Process

Business owners evaluate risks within their departments, applying the Bank's defined risk appetite and criteria. Senior management evaluates medium and high risks, and formally approves acceptance decisions documented in the risk register

Low risks (1–5): May be accepted by the risk owner if aligned with objectives.

- **Medium risks (6–14):** Reviewed with senior management; mitigation required unless justified for acceptance.
- **High risks (15–25):** Not acceptable; must be treated, transferred, or avoided.

This process ensures that risk decisions are consistent, transparent, and aligned with the Bank's business and regulatory obligations.

9. Risk Treatment Process

Once risks are evaluated, senior management assigns treatment actions to the appropriate business owners, managers, or technical teams. Risk treatment is not limited to technical controls; it may also include administrative or organizational measures, contractual arrangements with third parties, or strategic decisions such as avoiding certain activities. Residual risks may be formally accepted with proper approval. The objective is to ensure risks are reduced to a level consistent with the Bank's defined risk appetite and regulatory obligations.

10. Risk acceptance

Risk acceptance occurs when management chooses to retain a risk because it is within the Bank's risk appetite or further controls are not feasible or cost-effective. Low risks may be accepted by owners if aligned with objectives, while medium or high risks require formal senior management approval. All accepted risks must be documented, justified, and periodically reviewed.

11. Link to SoA

Risks selected for treatment shall be mapped to appropriate Annex A controls (or other necessary controls). These controls and justifications will be documented in the Statement of Applicability (SoA) to demonstrate traceability and compliance with ISO/IEC 27001

12. Review & Update

The Risk Assessment Methodology will be reviewed at least every 6 months, and earlier if significant business, regulatory, or technological changes occur. The review ensures that risk criteria, risk appetite, and processes remain appropriate and aligned with the Bank's objectives and ISO/IEC 27001 requirements. Updates shall be approved by senior management, and the latest version communicated to relevant stakeholders.