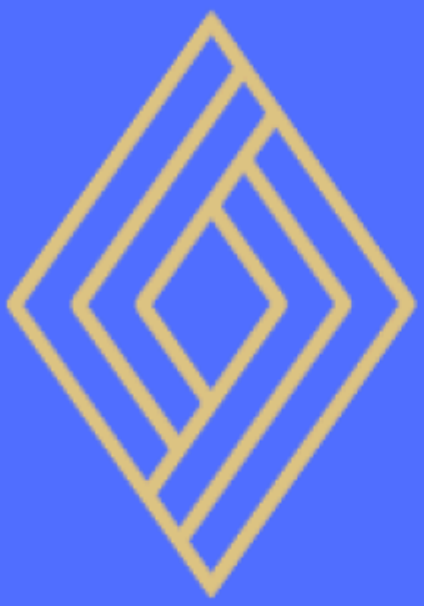

CRESCENT BANK

TRUST BEYOND BANKING.

Information Security Context, Requirements and Scope

Information Security Context, Requirements and Scope

DOCUMENT CLASSIFICATION	Internal
DOCUMENT REF	ISMS-DOC-04-1
VERSION	1
DATED	27 August, 2025
DOCUMENT AUTHOR	Sheheryar Altaf
DOCUMENT OWNER	Ali Khan, ISMS Project Manager

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
1	26 August, 2025	Sheheryar Altaf	Initial Draft
2	27 August, 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 August, 2025
Mr. Bilal Qureshi	CFO	_____	29 August, 2025
Ms. Sara Malik	CISO	_____	30 August, 2025

Contents

Figures

Tables

1. Introduction

Crescent Bank is committed to safeguarding its business information and has established an Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2022.

This document outlines the bank's operating environment, the internal and external factors that influence it, and the potential consequences of information security breaches. It covers:

1. The organizational context
2. Relevant internal and external issues
3. Interested parties and their information security requirements
4. The scope, boundaries, and applicability of the ISMS

2. Organizational context

The organizational context of Crescent Bank is set out in the following sections. Given the fast-moving nature of the business and the markets in which it operates the context will change over time. This document will be reviewed on an annual basis and any significant changes incorporated. The ISMS will also be updated to cater for the implications of such changes.

2.1. Functions

Crescent Bank consists of the following organizational functions:

1. Finance and Accounting
2. Human Resources
3. Operations
4. Project Management
5. Risk and Compliance
6. Information Technology
7. Retail Banking

An organization chart is shown below:

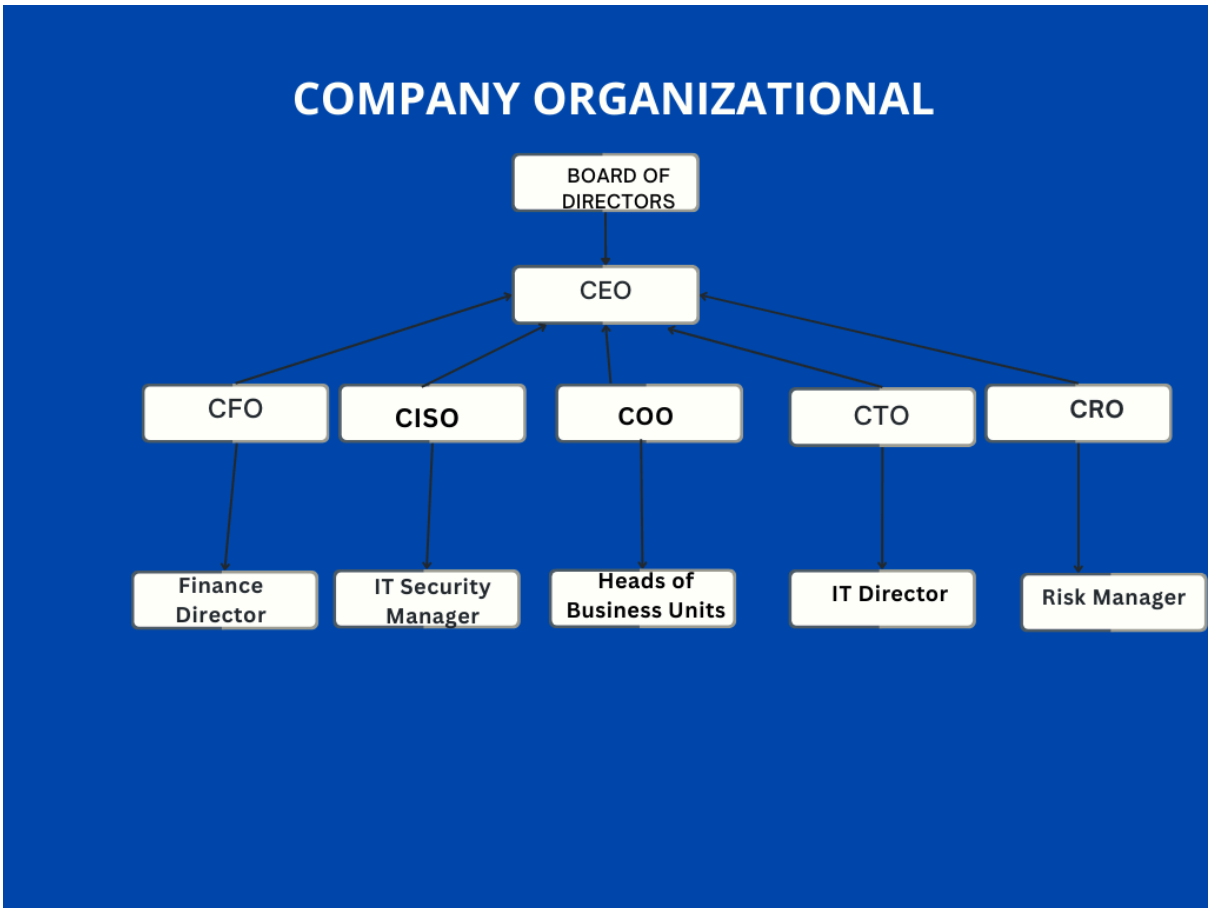

Figure 1: Organization chart

2.2. Organizational Functions and Locations:

1. **Board of Directors / Executive Management:** Corporate Headquarters, Karachi
2. **Finance and Accounting:** Corporate Headquarters, Karachi
3. **Human Resources:** Corporate Headquarters, Karachi
4. **Information Technology / Risk & Compliance:** Corporate Headquarters, Karachi
5. **Retail Banking / Operations:** Branches nationwide (7 branches across Pakistan)
6. **Data Centers:** Primary data center at Corporate HQ,
7. **Disaster Recovery:** Disaster Recovery site at Islamabad
8. **Physical escrow:** Held at SafeX, Zurich, Switzerland

2.3. Services

1. **Retail Banking**: Branches and ATMs managing deposits, withdrawals, and customer PII.
2. **Lending & Financing**: Loans and credit services with sensitive financial data.
3. **Digital Banking**: Online/mobile banking, cards, e-wallets. High-risk and high-priority for ISMS
4. **Payments & Settlements**: Clearing, transfers, and bill/merchant payments under SBP oversight.

   Note: Lending and digital banking are revenue-critical and most at risk; all services handling PII/financial data are regulated, and disruptions impact continuity.

2.4. Major Partnerships & Supply chains

1. **PTCL Cloud** – Cloud hosting & DR (ISB/KHI/LHR); supports digital banking & DR site; 3+ yrs; PII encrypted; SBP & PCI-DSS compliant.

2. **KPMG Pakistan** – Compliance auditor (ISO 27001, PCI DSS, SBP); core banking audits & reporting; 5 yrs; limited/anonymized PII; Big Four advisor.

3. **Temenos T24** – Core banking platform (Geneva HQ, KHI support); retail, lending, Islamic finance; 7 yrs; PII in accounts & transactions; trusted global solution.

The ISMS scope includes outsourced dependencies such as cloud hosting, audit services, and critical vendor software that support core banking and digital operations.

2.5. Objectives and policies

Information Security objectives are established to protect critical assets, ensure regulatory compliance (SBP/ETGRM), maintain business continuity, and mitigate cyber risks.

2.6. Business policies

Policies have been set by the organization in a variety of areas and these must be taken into account during the information security planning process to ensure that they are met. The main relevant policies are:

1. Information Security Policy
2. IT Access Control Policy
3. Internet Acceptable Use Policy
4. InfoSec Risk Management Policy

2.7. Legal and Regulatory Requirements

The bank must comply with SBP (State Bank of Pakistan) Information Security Regulations and the Enterprise Technology Governance and Risk Management (ETGRM) issued by SBP.

2.8. Key Information Assets

1. **Customer & Financial Data:** Account details, transactions, PII.
2. **IT Infrastructure:** Servers, databases, core banking systems.
3. **Payment & Transaction Systems:** ATMs, POS, online/mobile banking platforms.
4. **Physical Facilities:** Data center and Disaster Recovery site.
5. **Third-Party Services:** Cloud providers, critical software vendors.

3. Internal and external issues

There are a number of internal and external issues that are relevant to the purpose of Crescent Bank and that affect the ability of the ISMS to achieve its intended outcome(s).

3.1. Internal issues

With regard to the Crescent Bank business itself, there are a number of relevant internal issues which are:

1. **Governance & Structure**:There is no dedicated Information Security Officer; security is managed on a part-time basis.
2. **Policies & Standards:** Password policy outdated (last reviewed in 2019).
3. **Resources**: Limited cybersecurity budget; reliance on legacy tools.
4. **People & Culture**: Only 30% of staff attended the last security awareness training.
5. **Preparedness**: Incident response plan exists but has never been tested.

These general internal issues will be considered in more detail as part of the risk assessment process.

3.2. External issues

Crescent Bank operates in a dynamic environment with several external challenges, including:

1. **Political:** Policy changes, regulatory shifts, and regional instability.
2. **Economic:** Inflation, interest rate fluctuations, low customer demand, and strong competition.
3. **Social:** Changing demographics and rising expectations for secure digital banking.
4. **Technological:** Rapid innovation, reliance on fintech solutions, and AI-driven automation.
5. **Legal/Regulatory:** Compliance with SBP and data protection requirements.
6. **Environmental:** Climate change, natural disasters, and sustainability pressures.

These issues will be analyzed further during the risk assessment process.

4. Interested parties and their requirements

This section of the document sets out the interested parties that are relevant to the ISMS and their requirements. It also summarises the applicable legal and regulatory requirements to which the organization subscribes.

4.1. Interested parties

Interested Party	Requirements / Expectations
Shareholders / Investors	Financial return, strong reputation, secure operations.
Regulatory Bodies	Full legal compliance, secure banking practices
Customers	Confidentiality, integrity, availability, secure and reliable services.
Employees	Safe workplace, job security, clear security policies and awareness.
Board of Directors	Compliance, effective governance, controlled risks

4.2. Potential impact of an information security incident

In general terms the potential impact of an inability to perform normal business processes will be shown may affect one or more of the following areas:

1. Loss of revenue or business opportunities.
2. Risk to health/safety.
3. Reputational damage and loss of customer trust.
4. Breach of legal/contractual obligations and penalties.

4.3. Information security objectives

Based on the requirements and issues set out in this document, the following major objectives are set for information security:

1. Ensure compliance with laws and safety standards.
2. Maintain shareholder and customer confidence.
3. Protect PII and service continuity.
4. Minimize revenue loss.

5. Scope of the ISMS

5.1 Inclusions

The ISMS scope of Crescent Bank is based on internal/external issues, interested party requirements, and legal, regulatory, and contractual obligations.It covers critical systems, functions, and locations handling sensitive information.

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 (SafeX, Zurich)
3. Organizational Scope	IT / Security / Risk & Compliance, Operations (Retail, Lending, Digital Banking), HR (PII handling), Finance (sensitive transactions)

5.2 Exclusions

The following areas are specifically excluded from the scope of the ISMS:

1. **Personal Employee Devices:**
   Not used for official work; no impact on sensitive data or ISMS objectives.
2. **Non-Critical Servers / Test Systems:**
   Do not handle sensitive information; excluded from ISMS coverage.
3. **Systems for Awareness Messages / Non-Business Functions:**
   Only support general communication; no effect on information security.
4. **Employee Lounges / Eating Areas / Common Rooms:**
   No sensitive data stored or processed; irrelevant to ISMS.
5. **Marketing or Cultural Teams:**
   Do not handle critical info; outside ISMS-relevant processes.
6. **General Admin Functions / Non-ISMS Departments:**
   No effect on confidentiality, integrity, or availability of sensitive data.

NOTE: Other Non-Critical Elements:
Any component not affecting information security is excluded to maintain focus