CRESCENT
BANK

TRUST BEYOND BANKING

ISMS Project Initiation Document

CRESCENT BANK
TRUST BEYOND BANKING

ISMS Project Initiation Document

DOCUMENT CLASSIFICATION	Internal
DOCUMENT REF	ISMS-DOC-00-1
VERSION	1
DATED	24 August 2025
DOCUMENT AUTHOR	Sheheryar Altaf
DOCUMENT OWNER	Ali Khan / ISMS Project Manager

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
1	24 August 2025	Sheheryar Altaf	Initial Draft

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		27 August 2025
Mr. Bilal Qureshi	CFO		26 August 2025
Ms. Sara Malik	CISO		25 August 2025

Contents

Tables

1 Background

The International Standard for Information Security, ISO/IEC 27001, is a globally recognized standard that defines requirements for an Information Security Management System (ISMS)—a structured framework to ensure the confidentiality, integrity, and availability (CIA) of an organization's information assets. ISO/IEC 27001 was first published in 2005, updated in 2013, and evolved from the earlier British Standard, BS 7799.

2 Objectives and benefits

2.1 Project objectives

The objectives of this ISMS Project are as follows:

1. To achieve certification to the International standard for information security, ISO/IEC 27001 within a 6-7 month timeframe
2. To establish a more proactive information security framework within Crescent Bank in line with business requirements
3. To implement best practice in information security so that the organization's information assets are better protected
4. To increase the awareness of Crescent Bank staff of information security issues

Achievement of ISO/IEC 27001 certification will require Crescent Bank to invest time and money into the initial implementation project and the ongoing maintenance of the processes involved.

2.2 Anticipated benefits

However, from the shared experience of previous implementations in other organizations of similar size it would be reasonable to anticipate the following major areas of benefit:

- Significantly reduces risk of data loss, harm, or reputational damage.
- Provides assurance to customers, staff, board, and suppliers that their data is secure.
- Enables participation in tenders requiring ISO 27001 certification.
- Demonstrates the bank's commitment to information security and compliance with regulations (e.g., SBP ETGRM).
- Supports continuous improvement of information security controls, helping prevent incidents before they occur.
- Streamlines processes, reduces chaos, and gives clear direction and strategy for decision-making.
- Improves management of security breaches, minimizing business impact.

Steps will be taken where possible to quantify the achievement of the project against these anticipated benefits.

3 Scope, dependencies, constraints and assumptions

3.1 Scope

In Scope:
The ISMS implementation covers the management of information security across all Crescent Bank systems, including employee PCs, ATMs, data center servers, networks, digital banking servers, and CCTV recordings. It includes physical locations such as the data center, head office in Karachi, all branches, ATMs, teller areas, and approval areas for loans and cash. Organizational units in scope include HR, Finance, Retail, Digital Banking, Audit and Compliance, and Credit departments.

Out of Scope:
Any systems, locations, or organizational units not listed above or not related to Information Security are explicitly excluded from the ISMS project

3.2 Project dependencies

This project has the following inter-dependencies with other projects either planned or in progress within the organization:

PROJECT	NATURE OF DEPENDENCY
Completion of ATM upgrades	ISMS controls can only be applied after ATMs are upgraded
Key staff availability for project tasks and reviews.	Project tasks and reviews cannot proceed without key staff participation
Data center relocation or server upgrades	Security configurations and ISMS processes require the new infrastructure

Table 1: Project dependencies

3.3 Constraints

The following constraints are applied to this project:

- The project must be achieved within the stated timescale.
- Existing technology and IT systems may limit the implementation of certain security controls.
- The project must comply with regulatory requirements (e.g., SBP, ETGRM).

3.4 Assumptions

In preparing this project initiation document, it is assumed that:

- Business managers are willing and available to participate in regular ISMS review meetings where appropriate
- Enough financial resources are available when required for any necessary expenditure recommended by the project
- Enough human resource is available to progress the project in a timely fashion.

4 Project organization and authorities

4.1 Project organization

The project will be overseen by a project board which will have primary responsibility for the governance of the project and the achievement of its objectives.

4.1.1 Project board

The project board will consist of:

ROLE	NAME	TITLE
Project Sponsor	**Mr. Bilal Qureshi**	CFO
Project Manager	**Mr. Ali Khan**	IS Manager
Senior Supplier	**Ms.Zunaira**	External Supplier
Senior Advisor	**Ms. Sara Malik**	CISO

Table 2: Project board

4.1.2 Project team

The Project Team will be responsible for producing the required deliverables and supporting project activities

5 Project resources

The following resources will be allocated to the project by top management.

5.1 Human resources

The following people will be available to the project for the periods specified:

NAME	ROLE	PERIOD AVAILABLE	COMMITMENT
Mr. Ali Khan	Project Manager	7 months	5 days per week
Ms . Sidra Imran	Technical Lead	7 months	6 days per week

Table 3: Human resources

5.2 Technical resources

The following technical resources will be allocated to the project:

RESOURCE	PURPOSE	PROVIDED BY
Server capacity	Support ISMS tools and monitoring applications	Service Delivery team
SIEM tool	Log collection, correlation, and incident monitoring	Security Operations
Backup system	Ensure business continuity and data recovery	IT Operations

Table 4: Technical resources

5.3 Information resources

Information resources allocated to the project are as follows:

RESOURCE	PURPOSE	PROVIDED BY
Security Incident database	Analysis of risk areas	Help desk
Asset spreadsheet	Identification of information assets	Finance team

Table 5: Information resources

5.4 Financial resources

The following financial resources are available to the project.

RESOURCE	AMOUNT	AVAILABILITY
Capital budget	PKR 15,000,000	FY 2024 – FY2025
Revenue Budget	PKR 8,000,000 p.a.	Ongoing

Table 6: Financial resources

6 Timescales and milestones

The planned timescale of the project is to deliver the ISMS by 15/2/26

Within the overall timescale of the project it is envisaged that the following milestones will be achieved:

MILESTONE	TIMEFRAME
Project Initiation	25 August 2025
Gap Assessment	31 August 2025
Risk assessment completed	15 September 2025
Management system in place	30 September 2025
All required controls in place	15 October 2025
First management review completed	15 November 2025
Internal audit completed	15 December 2025
Stage One Review	15 January 2026
Stage Two Audit	15 February 2026

Table 7: Milestones

Progress against these milestones will be tracked as part of project reporting and reviewed at project board meetings

7 Project communication

7.1 Project progress reporting

Internal:

- Weekly highlight reports emailed to project board detailing progress, upcoming tasks, issues, risks, and ISO/IEC 27001 conformance.

- Monthly meetings with management to review milestones, decisions, and resource requirements.

External:

- Periodic updates to external suppliers/consultants via email or scheduled calls regarding project progress, deliverables, and dependencies.

8 Deliverables

The following major deliverables will be created as part of this project:

REF	DELIVERABLE	DESCRIPTION
1	Information Security Management System PID	A formal document that defines the project's scope, organization, resources, constraints, and key deliverables
2	ISO 27001 Gap Assessment	Assesses current situation and identifies gaps against ISO 27001
3	Information security policy	Defining the policy of the organization with respect to key aspects of information security
4	Statement of Applicability	Statement of which of the reference requirements of ISO27001 are applicable to Crescent Bank
5	Procedures and controls to address risk	An appropriate set of documentation to ensure that identified risks are addressed and treated satisfactorily
6	Risk Assessment and Treatment Process	How risk assessment and treatment is performed
7	Risk Assessment report(s)	Results of risk assessment using the defined process
8	Risk Treatment Plan(s)	What will be done about the identified risks
9	Information security records	Minutes of meetings, reviews, visitor books and other information security-related records
10	Training and awareness programs	Combination of formal training for key staff and briefings for all other staff
11	Audit reports	From internal and external audits
12	ISO/IEC 27001 Certificate	Evidence of certification to the ISO/IEC 27001 standard from a Registered Certification Body

Table 8: Deliverables

This list is in addition to deliverables produced as part of the management of the project, e.g. project plans, progress reports.

9 Initial project risk assessment

At this stage in the project, the following potential risks have been identified:

RISK	IMPACT	LIKELIHOOD	SCORE	INITIAL TREATMENT
Staff not trained properly	High	Low	**MEDIUM**	Involve staff in the project; encourage development via appropriate training
Market conditions affecting bank (economic instability)	Medium	Medium	**MEDIUM**	Align project costs with available budget; secure top management commitment despite external pressures.
Outdated security technology	Medium	High	**HIGH**	Prioritize upgrade of critical security tools; include technology refresh in project budget.
Insufficient resources	High	Medium	**HIGH**	Monitor progress against plan; raise issues to Project Sponsor if appropriate; delay project if required
Non-compliance with regulatory requirements (e.g., SBP)	High	Medium	**HIGH**	Engage compliance/legal teams; align ISMS policies with SBP regulations; regular compliance reviews

Table 9: Project risk assessment

The treatment actions identified above will be taken by the project manager in order to address these risks.