CRESCENT BANK

TRUST BEYOND BANKING.

Gap Assessment Report

CRESCENT
BANK
TRUST BEYOND BANKING

Gap Assessment Report

DOCUMENT CLASSIFICATION	Internal
DOCUMENT REF	ISMS-REP-01
VERSION	1
DATED	3 September, 2025
DOCUMENT AUTHOR	Sheheryar Altaf
DOCUMENT OWNER	Ali Khan, ISMS Project Manager

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
1	3 September, 2025	Sheheryar Altaf	Initial Draft
2	4 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	____________________	3 September, 2025
Mr. Bilal Qureshi	CFO	____________________	4 September, 2025
Ms. Sara Malik	CISO	____________________	5 September, 2025

Contents

1. Purpose

The purpose of this gap assessment is to evaluate the organization’s current Information Security Management System (ISMS) against the requirements of ISO 27001, including clauses 4–10 and Annex A controls. The assessment identifies gaps, provides a roadmap for remediation, and helps the organization prepare for ISO 27001 certification.

2. Objectives

The objectives of this gap assessment are to identify gaps in the organization’s ISMS against ISO 27001 requirements, determine the compliance status for each clause, assess the overall level of compliance, provide clear recommendations to rectify the gaps, and establish a roadmap to achieve readiness for ISO 27001 certification.

3. Executive Summary

This gap assessment evaluates Crescent Bank’s current Information Security Management System in relation to ISO 27001 requirements, including Clauses 4 to 10 and Annex A controls. The assessment shows that the bank has strengths such as a clear ISMS context, a documented scope, and well-defined objectives. There are, however, areas that need improvement, including the information security policy, leadership involvement, risk assessment and treatment, internal audits, and management of nonconformities. Focusing on these areas will help Crescent Bank strengthen its security practices, meet ISO 27001 requirements, and prepare effectively for certification.

4. Scope

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

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. Assessment Methodology

The gap assessment was carried out through:

1. **Document Review**: Examined ISMS policies, procedures, and records.
2. **Stakeholder Interviews**: Engaged key staff to validate practices.
3. **Observation**: Verified physical and technical controls.
4. **Control Evaluation**: Compared existing practices with ISO/IEC 27001 clauses (4–10) and Annex A and with the following State Bank ETGRM

5.1 Assessment Criteria

The evaluation of ISO/IEC 27001 clauses (4–10) and Annex A controls was conducted using the following compliance scale:

- **Compliant :** The requirement is fully implemented and aligns with ISO 27001 standards.
- **Partially Compliant :** The requirement is implemented to some extent; however, certain elements are incomplete or require improvement.
- **Non-Compliant :** The requirement has not been implemented or is entirely absent.

6. Detailed Findings

Clause	Requirements	Evidence	Findings	Compliance status	Recommendations
Clause 4: Context of the Organization					
Organization context & Scope	The organization has defined its context and documented ISMS scope aligned with objectives and business needs	Context and scope document , Business objectives , Meeting minutes	Requirements of Clause 4.1 addressed.	**Compliant**	Documents are complete, but require periodic review and updates in line with business changes
Interested parties	The organization shall determine the interested parties relevant to the ISMS, their requirements, and how these requirements affect the ISMS.	Stakeholder register, MoUs/SLAs, Regulatory license (e.g., SBP), IS policy, meeting minutes.	Required licenses are in place, but MoUs/SLAs are outdated (2+ years) and IS policy is missing.	**Partially Compliant**	MoUs/SLAs should be updated and create an information security policy.
ISMS establishment	Organization shall establish, maintain, and continually improve an ISMS in line with ISO 27001 requirements	PID document, scope document and hierarchy of organization document.	Organization has addressed the requirements of Clause 4.4	**Compliant**	Make sure the ISMS is regularly aligned with business and information security goals.

Clause 5 : Leadership					
Leadership & commitment	Top management shall demonstrate leadership and commitment to the ISMS.	Management review minutes, resource allocation, role assignments, and evidence of leadership participation	Resources are allocated, but there is a shortage of resources, and leadership participation is negligible.	**Partially Compliant**	Resources should be increased for the ISMS, and participation should be improved, as this gives a positive signal.
Information security policy & roles and responsibility	Top management shall establish, approve, and communicate an information security policy and assign roles aligned with organizational needs	Approved Information Security Policy document, management review minutes, communication records and hierarchical structure	The information security policy is missing, and Structure was not provided initially.	**Non - Compliant**	Develop, approve, and communicate an information security policy aligned with business and security needs.

Clause 6: **Planning**					
Risk assessment & treatment	Risks shall be identified, analyzed, evaluated, and recorded in a risk register; SoA and Risk Treatment Plan must be established and maintained.	Risk Register, Statement of Applicability, Risk Treatment Plan, risk-based funding records, meeting minutes, staff awareness records	Risk assessment and treatment procedures are not defined; Risk Register and Statement of Applicability (SoA) are missing	**Non-Compliant**	Clause 6 should be followed, as risk assessment and treatment are at the core of risk management.
Security objectives	Information security objectives shall be measurable, assigned to responsible personnel and to be communicated to relevant employees.	Documented information security objectives, PID , meeting minutes, responsibility assignments, and records of employee awareness and communication.	IS objectives and scope are defined, PID shows timelines/deliverables, but employee awareness needs improvement.	**Compliant**	Maintain objectives and scope per Clause 6 and improve employee awareness and communication

Clause 7: Support					
Competence, Awareness & Communication	Employees shall be competent, trained, and aware of ISMS policies, objectives, and responsibilities, with communication provided as needed according to their role.	Training and awareness session records, Financial Allocation document, and communication documents	Training and communication do not meet Clause 7 requirements.	**Partially Compliant**	Enhance employee training and improve awareness and communication for third-party vendors.
Documentation	All ISMS documents required by ISO 27001 shall be prepared, approved, maintained, and made accessible to relevant personnel.	IS Policy, SoA, Risk Register, Risk Treatment Plan, objectives, procedures, internal audit reports, and meeting minutes	Risk register, treatment plan and internal audit have not been performed or are not at par with the ISMS standard	**Partially Compliant**	Perform risk assessment and treatment, create the SoA, and conduct internal audits.

Clause 8: Operation					
Operational planning & control	ISMS processes and controls shall be implemented in operations and aligned with policies, objectives, and risk treatment plans	Operational logs, implemented procedures, change/incident records, and internal audit evidence showing ISMS controls in practice	The organization has logs and screenshots in the file system, but no incident records are in place, and audits, implementation, and remediation are missing.	**Partially Compliant**	Implement incident records, ensure operational logs are backed up, and perform audits and remediation in line with Clause 8
Clause 9 : Performance Evaluation					
Monitoring, measurement, analysis & evaluation	ISMS processes, controls, and objectives shall be monitored and evaluated using defined metrics, with results recorded and acted upon	Logs, screenshots, metrics, responsibility records, reports, and corrective actions reports.	Logs and screenshots exist, but frequency, dashboard, and audit methods are lacking.	**Partially Compliant**	Logs and screenshots shall be stored per defined mechanisms and frequencies, with roles assigned.
Internal Audit & Management review	Conduct internal audits to assess ISMS and have management periodically review performance, risks	Audit reports, checklists, corrective actions, review minutes, metrics	No process exists for internal audits management reviews	**Non - Compliant**	An internal audit mechanism should be in place to review the ISMS at defined intervals.

Clause 10: **Improvement**					
Nonconformity & corrective action	Residual risks and all nonconformities shall be identified and addressed through corrective actions in line with ISMS processes.	Nonconformity reports, corrective action records, meeting minutes, control effectiveness reviews, and awareness/communication records.	There is no system in place to address non-conformities in accordance with the clause	**Non - Compliant**	Nonconformities reports should be taken seriously, and steps should be taken to address them on a priority basis
Continual improvement	The ISMS shall be continually improved based on audits, monitoring, nonconformities, and business or risk changes	Corrective action records, audit follow-ups, management review minutes, updated policies, and KPI trends showing ISMS improvements	While certain improvements to the mechanism have been made, an effective risk mitigation system has not been established	**Partially Compliant**	The ISMS requires continuous improvement and adaptation.

7. Gap Analysis Summary

Clause	Compliant	Partially Compliant	Non - Compliant
Clause 4-10	3	7	4

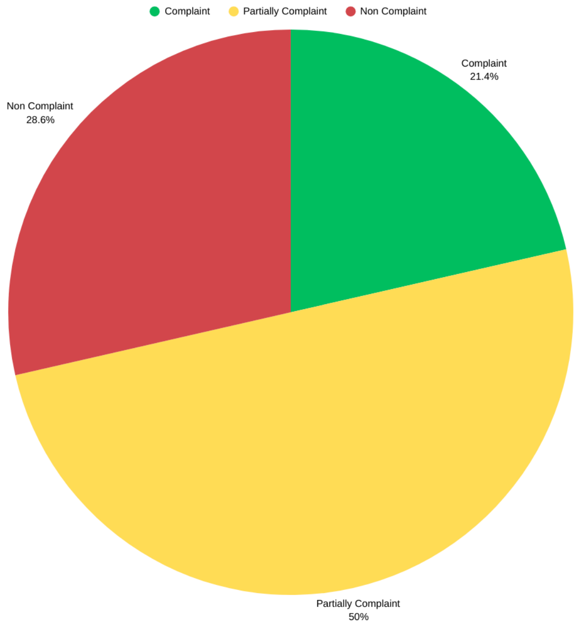
8. Recommendations / Remediation Plan

Priority	Clause	Action item	Action Required
High	5.2 : IS policy	Management establishes and shares the security policy.	Define and share a security policy aligned with business needs
High	6 : Risk assessment & treatment	Risks must be identified, analyzed, recorded in a Risk Register, with a SoA and Risk Treatment Plan maintained.	Follow Clause 6 requirements, as risk assessment and treatment are core to risk management.
High	9.2 : Internal Audit	An internal audit mechanism should be in place, should review the ISMS at defined intervals	Conduct internal audits to assess ISMS compliance and have management periodically review performance, risks
High	10.1 : Nonconformity & corrective action	Residual risks and nonconformities must be identified and corrected per ISMS processes.	Non-conformities should be prioritized and addressed properly regularly

9. Conclusion

The gap assessment has identified key focus areas where Crescent Bank needs to strengthen its ISMS to achieve ISO 27001 certification. By developing a comprehensive information security policy, demonstrating leadership commitment, implementing robust risk management, and establishing a structured internal audit program, the organization can enhance its security posture, ensure compliance, and successfully attain certification.

10. Appendices


Complaint
Partially Complaint
Non Complaint
Complaint 21.4%
Non Complaint 28.6%
Partially Complaint 50%