PremiumTrust Bank

ISMS Roles, Responsibilities and Authorities

Classification: Internal
April 2023
Document Number: PTB/ISMS/ISRRA/C5002

Document Control Sheet

Version and Update History

Date	Document Version	Document Revision History	Document Author/Reviser
April 3, 2023	1.0	Document creation	Information & Cyber Security

Change Control

Change Clause/Frequency
The contents of this document are subject to change control on a twelve (12) months review cycle.

Table of Contents

1. Purpose, scope, and users

This document describes the roles, responsibilities and authorities needed to be identified, communicated, and maintained to manage the Information Security Management System.

2. Information Security Management System Roles

Within the Information Security Management System, there are a number of roles, each with their own responsibilities, which need to be allocated to specific individuals or groups within the organization.

The following roles need to be allocated:

1. Top Management
2. Board
3. PremiumTrust Bank Steering Committee
4. Information Security Manager
5. Internal Auditor
6. ISO Champions
7. Human Resources
8. Legal and Compliance
9. Communications
10. Disaster Recovery Team
11. All Staff

The specific responsibilities and authorities of each of these roles are set out in later sections of this document.

2.1 Specific Roles and Responsibilities

Roles	Responsibilities	Key Skills and Competencies
PremiumTrust Bank Steering Committee/Top Management/Board	• Establish the ISMS policy, objectives and plans. • Communicate the importance of meeting the objectives and the need for continual improvement. • Maintain an awareness of business needs and major changes. • Ensure that customer requirements are determined and are met with the aim of improving customer satisfaction. • Determine and provide resources to plan, implement, monitor, review and improve the information security management system e.g., recruit appropriate staff, manage staff turnover • Manage risks to the organization and services. • Conduct reviews of the information security management system at planned intervals, to ensure continuing suitability, adequacy and effectiveness. • Establish a continual improvement policy with respect to ISMS for PremiumTrust Bank • Ensure that arrangements that involve external organizations having	• Understand the business. • Understand the business need for protection. • Understand the business. 'impact' of violation **Training:** ISO 27001 Executive Awareness

Roles	Responsibilities	Key Skills and Competencies
	access to information systems and services are based on a formal agreement that defines all necessary security requirements.	

Roles	Responsibilities	Key Skills and Competencies
Information Security Management System Manager	• Ensuring that the information security management system conforms to the requirements of the ISO27001:2022 • Reporting on the performance of the information security system. • Manages ISMS as a programme thereby ensuring that security principles are part of the organization's life cycle • Performs risk assessment based on new asset identification • Informs stakeholders about new areas of risk including suggestions from multiple sources. • Monitors the ISMS controls • Manage risks associated with access to the service or systems	• Understand information assets. • Understand Information Security including CIA. • Understand ISO 27001 control requirement. • Ability to interpret policy documents (internal and external) and explain to business 'how to implement or demonstrate compliance. • Access to the ISMS roles and responsibilities document **Training:** ISO27001 Lead Implementer Course

Roles	Responsibilities	Key Skills and Competencies
Internal Audit/Internal Control	• Periodically performs compliance checks to make sure that the relevant parties are performing their assigned duties, and to make sure that other ISMS requirements are being consistently observed. • Conduct internal audit of the ISMS. • Verify the implementation of ISO27001 and ISO22301 controls and independently reporting on the performance of the ISMS to top management.	• Ability to make judgments about the 'intent, implementation and effectiveness'. • Pass a judgment and make a justification of the judgment. **Training:** ISO 27001and ISO 22301 Lead Auditor Course
Team Leads: ISO Champions	• Responsible for allocated ISMS Controls. • Responsible for risk assessments concerning their processes and asset(s). • Ensure that employees are aware of the relevance and importance of their activities and how they contribute to the achievement of the ISMS objectives. • Maintain and review security controls for allocated asset(s). • Ensure the relevant entry in the asset inventory is kept up to date.	• Understand the business need for protection and their information assets including risk assessment. **Training:** • Department training, Induction and continuous awareness.

Roles	Responsibilities	Key Skills and Competencies
	• First point of contact in case of security incidents	
Human Resource Management	• Determine the necessary competencies to ensure the security of information in Premium Trust Bank • Review and manage staff competencies and training needs to enable staff to perform their role effectively. • Participate in the risk profiling of their staff through screening and background checks. • Review the effectiveness of actions taken. • Ensure that employees are aware of the relevance and importance of their activities and how they contribute to the achievement of the ISMS objectives.	• Understand the key business services and the supporting infrastructure need for protection through Risk Assessment **Training:** • Department training, Induction, and continuous awareness. • Attendance to ISO 27001 clauses interpretation sessions

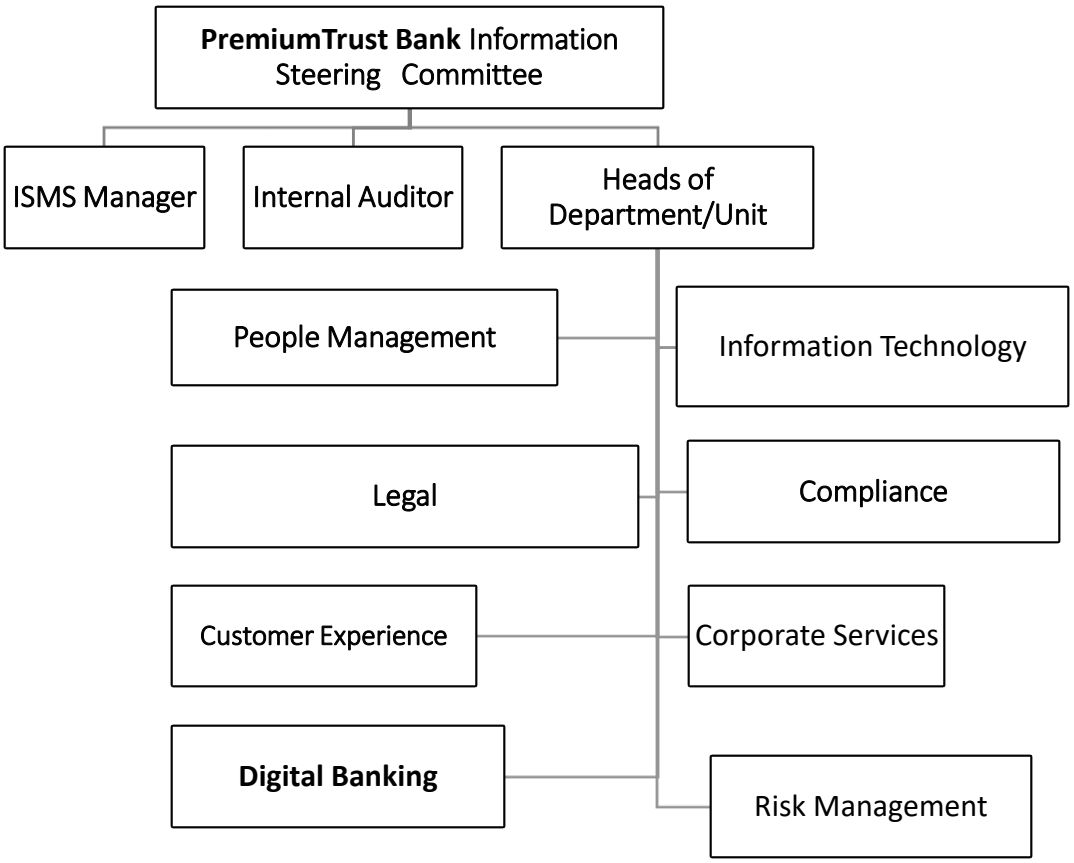
Roles	Responsibilities	Key Skills and Competencies
	• Maintain education, training, skills, and experience records. • Ensure internal communication amongst interested parties and employees within Premium Trust Bank • Ensure welfare of staff and visitors within Premium Trust Bank premises	
Legal and Compliance	• Identify all legal, regulatory, and contractual requirements. • Follow up on compliance. • Report any infraction to management and follow up on closure.	**Training:** • Mandatory attendance to ISO 27001 • clause interpretation sessions
Communications	• Ensure external communication with customers, partner entities, local community, and other interested parties, including the media. • Facilitating structured communication with appropriate authorities and ensuring the interoperability of multiple • responding organizations and personnel, where appropriate.	• Understand the key business services and the supporting infrastructure need for protection and continuity through Business Impact Analysis and Risk Assessment • Understand the business 'impact' of violation. • Understand the process flow of crisis management. **Training**: Department training,

Roles	Responsibilities	Key Skills and Competencies
		Induction, and continuous awareness.
Disaster Recovery Team	• Recovering servers, operating systems, and any other components upon which the applications are based. • Restoration of applications and data from and liaison with external network suppliers. • Setup and configuration of the business applications once they have been restored to the server hardware. This will involve liaison with third party application support services.	• Understand backup and recovery procedures. • Be able to perform system administration roles on a variety of operating systems. **Training:** • Department training, Disaster recovery planning and crisis management, Induction and continuous ISMS awareness.

Roles	Responsibilities	Key Skills and Competencies
Evacuation Team (Fire Marshalls)	• The overall success of the fire administration process and in case of a "real" disaster, they are responsible for ensuring the personnel are evacuated effectively within a specified period of time. • Ensuring that all personnel are evacuated within their physical area, including areas such as toilets, and handicapped personnel. • Keeping watch and documenting the time it takes for all the personnel inside the office to be evacuated. • Manage the muster points in preparedness for disaster and take the roll call after evacuation. • Relocating key personnel to the alternative premise/location	• Understand basic fire drill and evacuation procedures. • Be able to operate basic fire equipment. **Training:** • Environmental and health safety basic training • Department training, Induction, and continuous awareness on the ISMS.

Roles	Responsibilities	Key Skills and Competencies
Incident Management Team – Gold	• Give strategic direction and responsibility for decision making. • Final authority to activate Business. Continuity plan and Disaster Recovery Procedures (BCP/DRP). • Decision to implement the plan. • Confirm alternate site availability. • Approve all actions not pre-planned i.e. emergency actions. • Approve major equipment purchases. • Resolve issues of priority. • Identify problem areas. • Prepare crisis management plan which works best during emergency situations	• Understand the business and operation process and procedures. Department training, Induction and continuous ISMS awareness.
Incident Management Team – Silver	• Attends the site of the incident as quickly as possible. • Assesses the extent and impact of the incident. • Acts as interface with the board and other high-level stakeholders • Responsible for ensuring internal communications are effective.	• Understand the business and operation process and procedures **Training:** • Department training, Induction and continuous ISMS awareness.

Roles	Responsibilities	Key Skills and Competencies
	• Liaises with emergency services such as police, fire and medical. • Contributes to decision-making based on knowledge of business operations, products, and services. • Advises on what must be done to ensure compliance with relevant laws and regulatory frameworks	
All Users (Staff, Vendors, Contractors)	• Ensure they are aware of and comply with all information security policies of the organization relevant to their business role • Report any actual or potential security breaches. • Contribute to risk assessment where required	• Ability to comply with end user compliance requirements **Training:** Department training, Induction, and continuous awareness.


PremiumTrust Bank Information Steering Committee
ISMS Manager
Internal Auditor
Heads of Department/Unit
People Management
Information Technology
Legal
Compliance
Customer Experience
Corporate Services
Digital Banking
Risk Management