The Muslim Co-Operative Bank Ltd.

Information Security Management System Organization Chart

Document Control

Reference Number	Version	Approval Date	Nature of changes
PR-01	1.0	18/10/2022	1. Initial Policies

Table of Contents

1. INTRODUCTION

To manage the Information Security needs within The Muslim Co-operative Bank Ltd. management framework has been established. This will initiate and control the implementation of an Information Security Management System (ISMS) within the Bank Organization.

This document provides a clear management directive on the creation, management and functioning of the Information Security Committee (ISC) within the Bank. This document also mentions the roles and responsibilities of the various teams at The Muslim Co-operative Bank Ltd.

2. SCOPE

This document is limited to the services which are under the scope of the ISMS. Any changes in this document or other ISMS related documents would require approval from the ISC.

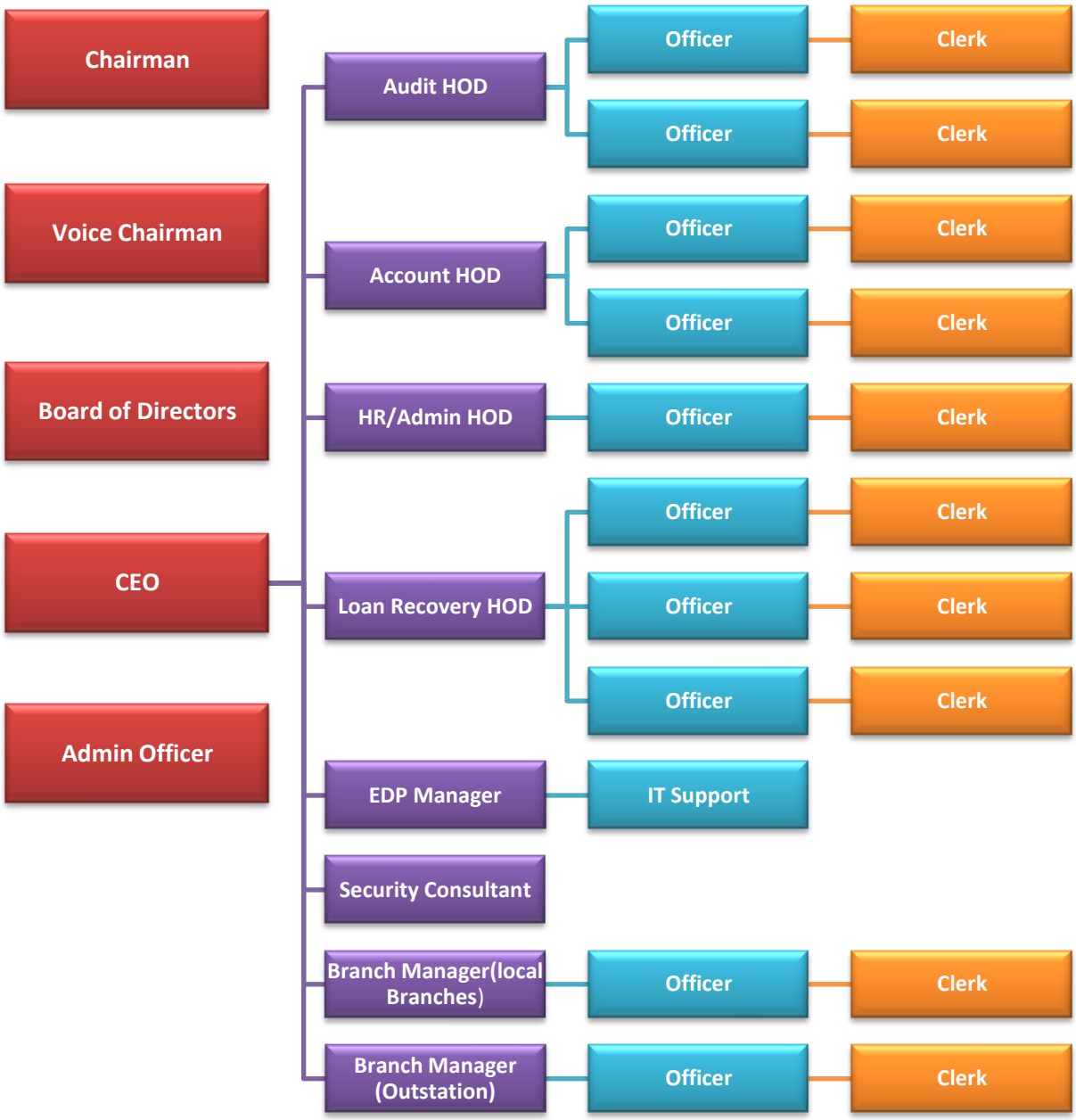
3. DEFINITION

An organizational chart is a diagram that visually conveys a bank's internal structure by detailing the roles, responsibilities, and relationships between individuals within an entity. Organizational charts either broadly depict an enterprise Bank-wide or drill down to a specific department or unit.

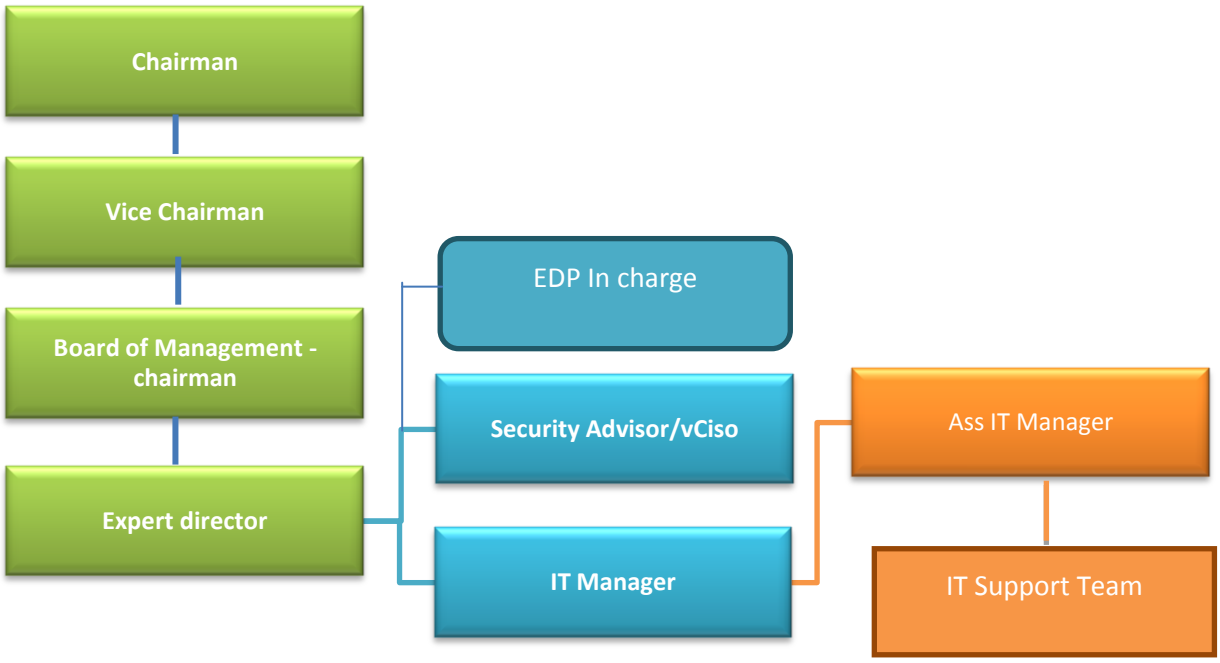
Organizational charts are alternatively referred to as "org charts" or "organization charts."

4. THE ORGANIZATION

4.1. Overall Organization Structure



4.2. IT and ISC Organization Structure



4.3. Information Security Committee

This committee chaired by the Chairman.

The other committee members will be the

Sr. No.	Name	Roles
1	Dr P.A Inamdar	Chairman
2	Shri S.A Inamdar	Vice-Chairman

3	Shri Sadik Lukde	Expert Director
4	Shri Mohamad Zafar Khan	Expert Director
5	Shri Mohamad Shahid	Managing Director (In Charge)
6	Shri Azim Shaikh	IT Manager
7	Shri Gulam Sarwar	IT Officer
8	Amol Aher	Security consultant/vCiso

To maintain a balance between business interests and best-fit security, the ISC will also have a representative from the Service Providers. Together these members will function as one team.

5. ROLES & RESPONSIBILITIES

The roles and responsibilities of the Information Security Organisation members are as follows

Roles	Responsibilities
Board of Directors	Approve the Information Security Policies and support its implementation.
Information Security Committee (ISC)	The Director's shall be the chairman of the ISC. The ISC shall have representation from the following Departments • CEO • IT Manager • CISO Members from Internal Audit, HR, Legal, Finance and other departments should be called for the ISC meeting on need basis The ISC roles and responsibilities shall be as follows : • Developing and facilitating the implementation of information security policies, and procedures to ensure that all identified risks are managed within a bank's risk appetite. • Approving and monitoring major information security projects and the status of information security plans and budgets, establishing priorities, approving procedures. • Supporting the development and implementation of a bank-wide information security management program. • Reviewing the position of security incidents and various information security

Roles	Responsibilities
	assessments and monitoring activities across the bank • Reviewing the status of security awareness programs • Assessing new developments or issues relating to information security • Requirement for generating effective metrics for measuring the performance of security control • Reporting to the Board of Directors on information security activities. • Conducting regular ISC meetings (at least quarterly) and maintenance of meeting minutes.
Information Security Officer	• Establishing, implementing, monitoring, reviewing, maintaining and improving Information Security Management System (ISMS). • Reviewing the security policies/procedures and suggesting improvements • Coordinating the ISC meetings. • Providing consultative inputs to the ISC on security requirements. • Coordinating information Security initiatives in the organization. • Driving and monitoring the ISC directives in the organization. • Updating ISC about IS initiatives, issues and incidents. • Facilitating and conducting risk assessments of Information Assets used and recommend mitigation controls. • Promote security awareness amongst employees, customers and partners.
IT Security Function	The IT Security is responsible for the execution of Information Risk policies, framework, guidelines and control processes The responsibilities of IT Security includes, but not limited to: • Enable Information Security controls • Define IT security procedures and guidelines in line with the IS Policies • Provide Security Architecture • Implement and monitor operational effectiveness of mandatory IT controls • Analysis of Security incidences, both internal and external and arriving at Lessons learned
IT Director	• Develop and maintain this policy. • Review and approve any exceptions to the requirements of this policy. • Take proactive steps to reinforce compliance of all stakeholders with this policy.
Business Heads	• Heads of Business Units are ultimately responsible for managing information risk in their respective business as part of their wider risk management responsibilities • Nominate Asset owner • Providing resources and support to the Asset Owners for information security implementation in the business unit
Supervisors or Department Representative	• Support all employees in the understanding of the requirements of this policy. • Immediately assess and report to the IT service desk any non-compliance instance with this policy.
Contract Administrators	• Ensure that the responsibilities and security obligations of each party to the contractual relationship are outlined in the contract executed between the organizations and the contractor/sub-contractor.

Roles	Responsibilities
Human Resources	• HR is responsible for disciplinary procedures were required following a breach of security policy or misuse of IT facilities. • Present each new employee or contractor with the relevant organizations' IT and Security Policies, upon the first day of commencing work with organizations. • Support all employees in the understanding of the requirements of this policy.
Information Asset Owner	Information asset owners shall be allocated to each information asset and shall ensure that security processes associated with these assets are established. For data and IT systems, they are called as application owners. The asset owner or the application owner is usually the business owner. Each application should have an application owner (asset owner) who will typically be part of the concerned business function that uses the application. Responsibilities would include, but not be limited to: • Assigning initial information classification and periodically reviewing the classification to ensure it still meets business needs under the guidance of the Information security Management Department (ISMD). • Ensuring security controls are in place, as recommended by ISMD; • Reviewing and ensuring currency of the access rights associated with information assets they own; • Determining access criteria and backup requirements for the information assets/applications they own. An information asset owner may delegate authority for the operation and protection of assets under their responsibility to an asset custodian. However, it will remain the responsibility of the asset owner to accept risk and to take appropriate steps to ensure that delegated authority is being responsibly applied
Asset Custodian	• An asset custodian shall be a member of the information technology team • A custodian shall typically, but not necessarily be confined to, assist the owner in the identification of control mechanisms, ensuring their development/purchase, implementation, maintenance and effective operation, reporting issues that affect the information asset in the operational environment to the owner • Together with the business owner, a custodian shall develop and maintain an information asset inventory including Confidentiality, Integrity and Availability ratings in such a way that the relationship between business process and IT component is documented and known by both parties • A business owner shall not relinquish accountability for risk management of the owned asset by a delegation of responsibility
User Manager	The user manager is the immediate manager or supervisor of an employee. He has the ultimate responsibility for all user IDs and information assets owned by bank employees. In the case of nonemployee individuals such as contractors, consultants, etc., this manager is responsible for the activity and for the bank assets used by these individuals. He/she is usually the manager responsible for hiring the outside contractor.

Roles	Responsibilities
	All Managers are responsible for ensuring that their staff is aware of information security policies, and for encouraging compliance with those policies, and for defining roles and responsibilities to support segregation of duties as directed by this policy
All users (Employees and contractors, Visitors and or Volunteers)	• End Users are responsible for the following with regard to information security: • Responsible and accountable for activities associated with an assigned account, as well as assigned equipment and removable media; • Protect the secrecy of passwords and Business Information. • Report known or suspected security incidents Employees and third party staff: Employees and Third-Party Staff are responsible for making themselves aware of information security issues and responsibilities, for complying with policy, and for reporting security incidents of which they become aware.
Technology Infrastructure Service Providers	• Infrastructure services shall be provided by strategic outsourced partners with Service Level Agreements. The service providers are custodians of IT assets on behalf of The Muslim Co-operative Bank Ltd. and are responsible for the implementation and operation of the infrastructure as appropriate to meet the Confidentiality, Integrity and Availability ratings specified by The Muslim Co-operative Bank Ltd. • Develop Standard Operating Procedures (SOP's), Security Guidelines for the assets managed. • Manage IT assets as per The Muslim Co-operative Bank Ltd. approved policies and procedures.
Application Developers	Application systems (including both business applications and generic supporting software, e.g. middle-ware, databases) may be developed and maintained by an internal IT function or by a third party. These parties are responsible for ensuring that systems are developed and maintained, incorporating user requirements and information security requirements that are in adherence to The Muslim Co-operative Bank Ltd. Policies for Information Risk. They are also responsible, in conjunction with the provider of the underlying technology infrastructure, for ensuring that information risk is adequately managed in development and test environments and report to The Muslim Co-operative Bank Ltd. IT Security.
IT Help Desks, Computer Incident Response Teams	IT Help Desks, Computer Incident Response Teams or equivalent functions are responsible for recognizing potential misuse incidents and passing them on to Risk Management/Internal Audit.
Legal Department	The Legal Department is responsible for drafting and approval of confidentiality and legal agreements.
Operations, Security Operations Functions, and Design functions	Operations, Security Operations Functions, and Design functions where appropriate are responsible for the resourcing and operation of Computer Incident Response procedures.

Roles	Responsibilities
Operations	Operations within each of the major organization units are responsible for managing and operating the technology and network infrastructure in accordance with these policies.
Procurement and Business Units	Procurement and Business Units are responsible for ensuring that appropriate contracts and non-disclosure agreements are put in place, and ensuring that staff and contractors are issued with relevant security-related information. They are also responsible for ensuring that cloud-based services are risk assessed and security reviewed.
Internal Audit Functions	Internal Audit Functions are responsible for managing investigations into cases of suspected misuse of technology facilities.
System Designer Functions	System Designer Functions within each of the major organization units are responsible for ensuring that systems and networks are developed and implemented in accordance with policy.

5.1. Directors

The Directors (Top Management) demonstrates leadership and commitment with respect to the information security management system (ISMS) by:

- Endorsing the information security policies.
- Supporting the enforcement of approved policies through the Information Technology, Human Resources, External Affairs, and Health Safety & Environment initiatives.
- Providing appropriate and adequate infrastructure, processes and resources in order to facilitate implementation of the policies.
- Communicating the importance of effective ISMS within the organization.
- Conducting management reviews on a periodic basis.
- Promoting the continual improvement of the ISMS.

5.2. Chief Information Security Officer (CISO)

- Plan, implement and maintain an information security management system.
- Coordinate with the senior management on the identification, development, secure handling and management of entity-wide information assets.
- Plan, develop and maintain an organization-wide information security risk assessment methodology in coordination with the higher management in the entity.
- Ensure that appropriate operational controls are selected and implemented according to the results of the risk assessment.
- Develop the required policies, and procedures, based on the results of the risk assessment.

- Ensure organization-wide compliance to the information security management system and periodically report the effective performance of the ISMS performance to the information security steering committee.
- Plan and conduct periodic information security awareness, education and training for entity's staff and applicable external parties.
- Regularly assess different components of the IT network, including applications to measure the effectiveness of a stated control or group of controls and to ensure that the component is compliant with published policies.
- Facilitate regular internal and external audits of the ISMS.

5.3. Head of Departments

Head of departments shall support ISMS implementation through the following:

- Drive implementation within their teams.
- Assist the CISO during an investigation, assessment, and risk mitigation involving Information Technology (IT) resources.
- Report and encourage team members to report security weaknesses or incidents within the Bank.
- Ensures that any information processing work has segregation of duties well established in the internal roles such that there is no opportunity of fraud, if applicable to the team or the process.

5.4. Information Security Committee (ISC)

The (ISC) is an advisory body providing guidance to the Bank with regards to the implementation of the ISMS. The ISC would

- Ensure the objectives of the ISMS are aligned with the overall strategy of DPE.
- Supervise, review and ensure the implementation of ISMS and its controls across the organization.
- Promote information security culture within the organization.
- Ensure that information security is designed in all business processes technology projects, systems and services.
- Ensure that adequate resources are provided to implement, support, and operate the ISMS.
- Review
    - The status of actions from previous management reviews.
    - Changes in external and internal issues that are relevant to the information security management system.
    - Feedback on the information security performance, including trends in;
        - Nonconformities and corrective actions.

        - Monitoring and measurement results.
        - Audit results.
        - Fulfilment of information security objectives.
    - Feedback from interested parties.
    - Results of risk assessment and status of a risk treatment plan.
    - Opportunities for continual improvement.
- Maintain Minutes of Meeting (MOM) documents as evidence of the results of management reviews.

5.5. Users

Following are the responsibilities of all users with access to Bank information:

- Maintain the security of the information they have access to.
- Follow the requirements of the Acceptable Usage Policy.
- Report security weakness/incidents to the IT Help Desk.

5.6. Auditor

The audit process department has the following responsibilities:

- Carry out periodic compliance checks using various testing methodologies/tools to assess the level of compliance with respect to the information security policies, procedures and other relevant documentation by all parties concerned, report the deviations, and provide recommendations for ensuring compliance.
- Report audit findings to ISC, recommend preventive and corrective action.

6. DOCUMENT HISTORY

As per the document, control Sheet.

*** End of Document ***