ESTD: 1919 Phone:0836-2353249

THE ARYA VAISHYA CO-OPERATIVE BANK LTD.

Registered office; Hosur, Hubli-580 021.

Email : avcbankltd@gmail.com

(CORE BANKING BANK)

INFORMATION SECURITY POLICY

Introduction

THE Financial Sector is getting increasingly interconnected and complex. Acquisition, processing and use of vast amounts of customer data apart from banks' own business information has brought to light the vulnerabilities in information systems that can lead to compromise of confidentiality, integrity and availability of information. This brings into focus the need for effective Information Security Governance in banks to protect themselves and their customers adequately and appropriately. The Guidelines from the RBI Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds have also reiterated the urgency for putting in place a robust information security framework in banks. This document is a contribution in that direction.

Definition

“Information security governance is a subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, manages risks appropriately, usesorganisational resources responsibly, and monitors the success or failure of the enterprise security programme” - ISACA.

Essentials for IS Governance

Effective Information Security Governance in Banks calls for a variety of efforts and initiatives across the entire spectrum of the Organizational Structure. Notable among them are: Board level direction and active involvement in Information Security Top Management support for prompt resolution of Information Security Issues Integration between Business and Information Security Alignment of Information Security mechanisms with Organizational Goals and Objectives Information Security planning and assessment of new technologies before deployment. Ownership and accountability, at all levels – controlling offices as well as field operations – for planning, implementing, monitoring, reporting on and improving Information Security.

Information Security Governance

Critical Success Factors

The Critical Success Factors which would facilitate the attainment of satisfactory levels of Information Security Assurance within the bank are: Appropriate placement of Information Security within the Organizational Structure Consistent message and conviction from the Board and the Top Management vis-a-vis Information security policy perspectives Adequate and appropriate employee education and awareness on information asset protection Continuous and consistent enforcement of information security polices and standards Ability and willingness to justify the cost of Information Security initiatives Constantly raising the bar with regard to Best Practices and Metrics being adopted in ensuring and improving Information Security.

Managerial Focus

This document focusses on the managerial aspects of Information Security and not on the technical side.

Internal Organization

Objective: To manage information security within the organization.

Management commitment to information security

Control: Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

Information security coordination

Control: Information security activities shall be co- ordinated by representatives from different parts of the organization with relevant roles and job functions.

Allocation of information security responsibilities

Control: All information security responsibilities shall be clearly defined.

Information Security: Core Principles

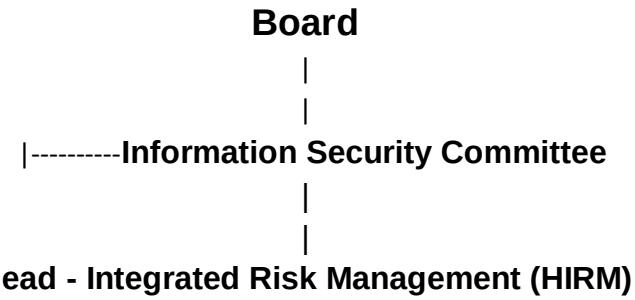
- There must be a robust governance framework in place to ensure top management involvement and oversight in Information Security on a regular basis.
- Information security must be a dynamic and ongoing process aimed at continuous improvement.
- The principle of Defence in Depth may be adopted to protect critical assets by providing them with a layered security.
- Information security must focus on business and provide value and quality to its stakeholders. Information security risks and costs are the joint responsibility of Business and IT.
- Information security should be part of everyone's responsibility and hence to be embedded in staff roles and job descriptions. Information security function must have a dedicated, skilled, experienced & adequately staffed team.
- All IT and Business Changes, including new initiatives must be subjected to a thorough and robust risk management process with a clear focus on protecting classified information and critical business applications.
- Information security must be part of the design architecture of any product and service. Information security risk management must be based on Business Impact Assessment and evaluate current and future threats and develop a long term roadmap for effective protection of all information assets.
- Information Security Programme must encompass the Business Continuity Management and Disaster Recovery Plans of the Bank.
- Information security team must act in a professional and ethical manner to foster a positive security culture within the Bank. The Information Security Committee must have an effective oversight to review and monitor the Information Security Programme of the Bank.
- Information security function must provide timely and accurate metrics on performance with regard to Information Security. Information security governance must comply with relevant legal and regulatory requirements.
- Policies and controls must account for business context.

Strategies for Implementation

- The Information Security Committee at the top management level should be responsible for overall governance of the Information Security Programme of the Bank and will report to the Board.
- A Working Group on Information Security should be set up in the Bank, which shall have representatives from business, operations, audit, IT, vigilance, physical security / admin etc.
- This Working Group should meet on a regular basis to discuss implementation issues pertaining to information security.
- The Information Security Risk Management shall cover risk identification, assessment, remediation and acceptance of residual risk. Education and Awareness efforts shall be continued on a regular basis to keep the rank and file abreast of their roles and responsibilities vis-à-vis the expectations from the Information Security Policy.
- Information Security should be a regular component in training programmes offered within the Bank.
- Customer Education on Information Security, especially in Electronic Banking and delivery channels, must be accorded due prominence.
- Regular, multi-pronged efforts must be made to inculcate best practices and common minimum standards among customers to provide security to their electronic transactions.
- Appropriate tools and channels may be utilized for this purpose. Security Implications of the Business Continuity and Disaster Recovery Policies must be approved and periodically reviewed by the Board.
- Information Security function must be adequately staffed, trained, equipped and motivated to maintain the Bank's Security Posture at expected levels.
- Banks information system shall be regularly subjected to regular information security testing commensurate with their exposure (criticality and threats) level.
- The information security programme (design, implementation & execution) should be reviewed and tested by the Bank's IT audit.
- The IT audit strategy should be aligned with information security strategy for the areas of implementation and execution.

- The information security enforcement strategy should be comprehensive and should cover the complete lifecycle of Data, Applications, Technology, Infrastructure, People, Products andServices.
- The Information security programme shall be tested on an ongoing basis for compliance to applicable regulations.
- Bank should not only have security strategy but also ability to execute strategy and ability to measure execution.

Organization Chart for IS Governance



Information Security Committee

The role of the Information Security committee is to devise strategies and policies for the protection of all assets of the bank (including information, applications, infrastructure and people). The committee will also provide guidance and direction on the Security Implications of the business continuity and disaster recovery plans.

Responsibilities:

- Develop and facilitate implementation of information security policies, standards and procedures to ensure that all identified risks are managed within the bank's risk appetite.
- Create an information security and risk management structure covering the entire bank, with clearly defined roles and responsibilities.
- Create and follow a risk assessment process that is consistent across the bank to identify, evaluate key risks and approve control measures and mitigationstrategies.

- Regularly monitor the information security and riskmanagement processes and corrective actions toensure compliance with regulatory requirements.
- Ensure that the Information Security Team isappropriately skilled and adequately staffed.
- Regularly present reports to the Board and invite feedback on the information securitymanagement processes.

Head – Integrated Risk Management (HIRM)

The Head of Integrated Risk Management will be a senior level official of the rank of Manger/AGM/CEO. The HIRM is responsible for all Risk Management functions in the Bank, like Credit Risk, Market Risk, and Operational Risk. Information Security will be one of the most critical components of Operational Risk that has to be looked after by the HIRM. He is the senior-most executive in the Information Security function in the bank and provides the required leadership and support for this across the bank, with the full backing and commitment from the Board.

Responsibilities*(in the Information Security Governance domain):*

- Information Security Governance
- Information Security Policy and Strategy
- Information Security Risk Assessment, Management and Monitoring
- Security Aspects and Implications of Business Continuity Planning in the Bank.
- Allocation of adequate resources for Information Security Management.

Sd/-
General Manager

Sd/-
Chairman

Approved in the meeting of the Board of Directors held on 30-05-2024