CYBER SECURITY POLICY
OF
THE BALASORE BHADRAK CENTRAL COOPERATIVE BANK LTD

The Balasore Bhadrak Central Co-operative Bank Ltd
Head Office: O.T. Road, Balasore-756001
Tel. No. 06782- 263022/ 262136 E-mail: ho@bbccb.in

Policy name	Cyber Security Policy
Policy Owner	Balasore Bhadrak Central Cooperative Bank Ltd
Policy issued on	28-11-2023
Policy approved by	Committee of Management of BBCCB

CYBER SECURITY POLICY

1. Introduction

Bank's information systems and the data, these information systems process, are fundamental for its daily operations and effective service provision. The Bank shall implement adequate security policies, procedures and controls to protect confidentially maintain integrity and ensure availability of all information stored, processed and transmitted through its information systems. To build a secure and resilient cyberspace for customer there is a need to have an effective cyber security policy in the Bank.

Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accident man-made or natural and the data exchanged in the cyberspace can be exploited for nefarious proposes. The cyberspace is expected to be more complex in the foreseeable future with increase in networks and devices connected to it.

Use of information technology by the Bank has grown rapidly and is now integral part of the operational strategies of the Bank. It is therefore important to develop policies, procedures and technologies based on the new developments and emerging concerns and fine tune the same as per evolving cyber threats.

The protection of information infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the essence of a secure cyber space. Due to the dynamic nature of cyberspace there is now a need for these actions to be unified under a cyber security policy, with an integrated vision and a set of sustained and coordinated strategies for implementation.

The cyber threat landscape has evolved from one of individual hackers to highly organized groups and advanced cyber-criminal syndicate cyber-attacks are more targeted and sophisticated than ever before. Powerful new malware is capable of stealing confidential data, card information and disabling network infrastructure. Attacks on critical infrastructure, including payment systems, can disable physical machinery cause catastrophic equipment failure and even result substantial financial loss to the Bank. Bank must be prepared to address the various types of threats.

Cyber security policy is an evolving process and it caters to the whole spectrum of people process and technology, it serves as an umbrella framework for defining and guiding the actions related to security of cyberspace.

To combat growing cyber threats and enhancing the resistance of the banking system to address cyber risks, RBI vide its circular no. RBI/2018-19/63/DCBS. CO.PCB. Cir No.1/18.01.000/2018-19 dated 19th October 2018 directed the Bank's as under:

"To put in place a cyber-security Policy elucidating the strategy containing an appropriate approach given the level of complexity of business and acceptable levels of risk duly approved by their Board."

This Cyber Security (CS) Policy has been framed on the basis of stipulated RBI guidelines, information Technology Act and international Standards.

The Cyber Security Policy is distinct from IT Policy and information Security Policy.

2. Ownership

The Board of Management of ***THE BALASORE BHADRAK CENTRAL COOPERATIVE BANK LTD*** is the owner of the policy and ultimately responsible for overall functioning of cyber security in the bank.

3. Cyber Security Scope and Applicability

a. This policy applies to all employees, contractors, consultants and third-party users (internal and external) accessing Bank's information systems from within or outside.

b. This policy covers the usage of all of the Bank's information technology and communication resources, including but not limited to:

I. All computer-related equipment like PCs, workstations, telecom equipment, databases, printers, servers, shared computer resources etc. & all networks & hardware to this equipment is connected.

II. All software including purchased or licensed business software applications, in-house applications, vendor/supplier provided applications. Computer operating systems, firmware and any other software residing on Bank owned equipment.

c. All intellectual property and other data stored on the Bank's system.

4. Policy Framework

a. The Cyber Security Policy is designed as per the cyber security framework defined below. The framework has been built on the basis of the RBI circular to provide a compliance overview for each of the functional areas as outlined in the circular. The Distributed Denial of Services (DDoS), ransom- ware/ crypto ware, destructive malware, business email frauds including spam, phishing etc.

b. Define robust/cyber security framework to ensure adequate cyber

security preparedness for addressing cyber risks, identify the inherent risks and the controls in place to adopt appropriate cyber security framework.

c. Define cyber security measures/controls to ensure protection of Bank's and customer information and to maintain confidentiality integrity and availability of the dataacross the data/information life cycle.

d. To design IT architecture in a manner that it takes care of facilitating the security measures at all times.

e. To respond, resolve and recover from cyber incidents and attacks through timely information sharing, collaboration and action.

Collectively, these objectives provide the foundation for protecting against and preparing for cyber threats (i.e. a proactive approach to cyber security) as well as detecting, responding to and recovering from threats and challenges (i.e. reactive cyber security efforts).

5. Guiding Principle

Bank's approach to cyber security is based on the followingprinciples.

a) Bank has an important responsibility to, safeguard customers confidential information, systems and networks and to ensure their confidentiality, integrity, andavailability. The bank will therefore lead by example in implementing cyber security requirements while building and adopting innovative and new technologies.

b) Individuals are responsible for being aware of threats, adopting best practices, understanding who is collecting their personal information and securing their own information systems and networks.

c) Strong security measures and sound test practices are encouraged to protect personal and private information, unauthorized access or misuse. Bank will derived security procedures from the policy statements and provide the details of necessary actions to achieve the objectives of the policy statement.

6. Policy Statement

The Bank shall strive for the preservation of the Confidentiality, integrity and availability of Bank's information assets pertaining to customer's data, for safe & secure computing environment in order to build adequate trust & confidence in electronic transactions.

7. Objective

a) To safeguard the cyber facing information infrastructure of the Bank various types of cyber threats including, but not limited to Denial of Service (DoS), pursue cyber security policy and initiatives that preserve Bank's values and expectations, consistent with laws and regulations.

b) All the third-party vendors are to be managed as per the information security procedure for third party.

c) Bank will co-ordinate with external agencies during and after the cyber crisis as per the cyber Crises management Plan (CCMP).

d) Head office and Dept. Heads to identify the inherent risk (including the cyber risk) & controls in place for any product/process are lunch of the same and periodically the same is to be reviewed as per the Risk Management Policy of the Bank.

e) An indicative but not exhaustive list of requirements to be put in place by banks to achieve baseline cyber security framework given in the policy. This may be evaluated periodically to integrate risks that arise due to newer threats, products or process.

8. Roles and Responsibilities

➢ CHIEF INFORMATION SECURITY OFFICER

A senior level official (DGM or above) shall be designated Chief Information Security Officer (CISO) of the bank and shall be responsible for articulating and enforcing the policies that the bank uses to protect its information assets apart from coordinating the cyber security related issues/implementation within the organization as well as relevant external agencies.

a) Chief Information Security Officer (CISO) will be primarily responsible for ensuring compliance to various instructions issued on information/cyber security by NABARD/RBI or any other governing body.

b) Chief Information Security Officer (CISO) will be responsible for bringing to the notice of the Board/IT sub-committee of the board about the vulnerabilities and cyber security risk the Bank is exposed to.

c) Chief Information Security Officer (CISO) by virtue of his role, may ensure inter alia, current /emerging cyber threats to business and the Bank's preparedness in these aspects are invariable discussed in such committee(s).

d) Chief Information Security Officer (CISO) shall manage monitor and drive cyber security related projects.

e) Should co-ordinate the activities pertaining to Cyber Security Incident Response Teams within the Bank.

f) Shall develop and get an independent assessment of Cyber Security including its coverage at least on a quarterly basis.

g) Shall have a robust working relationship with Banks Top Management. Chief Information Security Officer (CISO) may be a member of (or invited to) committees on operational risk where IT/IS risk is also discussed.

h) Chief Information Security Officer (CISO) office shall be adequately staffed with technically competent people. If necessary through recruitment of specialist officers commensurate with the business volume, extent of technology adoption andcomplexity.

i) Shall be an invitee to the IT committee and IT steeringcommittee.

➢ BOARD LEVEL IT SUB-COMMITTEE

An Information Technology Sub-Committee at the Board level shall be constituted with the following members:

A.	Chief Executive Officer of the Bank	Chairman
B.	Any 3 (three) members of the Board of Management	Members
C.	Chief Information Security Officer (CISO)	Convener

The IT Sub-Committee of the Board shall meet at least once in a quarter and shall focus on reviewing and assessing the initiatives taken by the I.T. Steering Committee. After which, the committee shall apprise to the Board.

➢ IT STEERING COMMITTEE

An IT Steering Committee shall be formed with at least one representative from the below sections of the Head Office of the Bank:

- IT
- HR
- Legal
- Loans & Advances
- Accounts

Its role is to assist the Executive Management in Implementing IT strategy that has been approved by the IT Sub-committee of the Board.

The IT Steering Committee should apprise/report to the IT Sub-Committee periodically. The Committee should focus on implementation of Bank's IT Policy. Its functions, inter alia include;

a) Defining project priorities and assessing strategies fit for IT Proposals.

b) Reviewing, approving and funding initiatives, after assessing value additions to business process.

➢ INFORMATION SECURITY COMMITTEE

Since IT/Cyber security affects all aspects of an organization, in order to consider/cyber security, an **Information Security Committee** of executives shall be formed.

The Chief Information Security Officer (CISO) shall be the Member Secretary of the Committee.

The Information Security Committee may include, among others,

- The Chief Executive Officer (CEO) and
- Two senior Management officials well versed in the subject.

The Committee shall meet at least once on a quarterly basis. Major responsibilities of the Information Securities Committee, inter alia include:

a) Developing and facilitating the implementation of information security policies, standards and procedures to ensure that all identified Risk are managed within a Bank's Risk appetite.

b) Supporting the Development and implementation of the Bank's information security management program.

➢ INFORMATION TECHNOLOGY CELL

a) To provide IT products support and services to the divisions and functions in accordance with the cyber security requirements of the Bank.

b) Provide alternative solutions on industry practice to satisfy increased protection requirements.

c) Provide relevant support to other on meeting cyber securityobjectives and plans.

d) Provide periodic metrics to evaluate the cyber security posture of the Bank on a quarterly basis.

e) Coordinate all activities necessary for compliance to the cyber security policy

f) Oversee the execution of the cyber security planning at the functional level

g) Maintain and update the relevant document.

9. Implementation Approach

Successful implementation of the Cyber Security Policy requires continuous commitment, governance and action by various stake holders who are collectively responsible for the Bank's approach to cyber security. Bank shall develop and maintain or hire professional cyber security workforce. Bank has implemented various controls/measures to address various cyber security threats in addition to this, Bank will adopt new innovative cyber security technology and solutions as required from time to time to protect ban information assets.

a) Cyber Crisis Management Plan of the Bank should cover effective measure prevent cyber-attacks and to promptly detect any cyber intrusion so as to respond / recover / and contain the fall out.

b) Respective Officers /Management of IT Dept. Controlling Cyber facing applications must take following steps to make progress against the Cyber Security Objective.

c) Identify & Safeguard Bank's Cyber facing information Infrastructure.

i. Identify & prepare a list of the Cyber facing information infrastructure Assess the threat to Cyber facing information infrastructure.

ii. Identify the Gap and the cyber security controls

iii. Implement cyber security controls / standards or suggestmanagement action plan to mitigate risk.

iv. Analyse cyber security trends and threats to provide timelyreports to management

v. Always make the use of trustworthy technology productsand services

vi. Continuously monitor the security posture of cyber facing IT& information infrastructure.

d) Respond, resolve and recover from cyber incidents:

In case the cyber facing infrastructure, the asset owner suspects any incidents then:

i. Do the preliminary assessment of the incident

ii. If any cyber-attack is observed, report the matter immediately to the competent authority in accordance with the Bank's cyber crisis Management plan.

iii. Take immediate remedial steps to stop/reduce the cyber infections within cyber facing information infrastructure as per CCMP.

iv. Take action to correct and recover from cyber security incidents and system failures

v. Establish mechanisms and procedures to facilitate timely information sharing and action among stakeholders as per the CCMP.

vi. Enhance and maintain situational awareness capabilities.

vii. Establish and continuously enhance incident response capabilities

viii. Ensure preparedness by conducting cyber security exercisesand drills.

10. Cyber Security Awareness Training

a) Bank shall take the steps to enhance cyber security awareness amongst the staff using trainings, posters, mails etc. on continuous basis.

b) Staff of IT Dept. Handling cyber facing applications must take periodic trainings to make themselves aware of new cyber threats and measures.

11. Reporting and Performance Measurement

a. Performance of Cyber Security implemented by the Bank should be monitored continuously and based on the assessment future cyber security requirements should be identified.

b. Regular assessment should be carried out for identifying potential threats in cyber security.

c. Quarterly report about the Cyber Security Incident should be put before the Board and return thereof should be to be submitted to RBI on due date.

12. Policy Review and Approval

This policy document shall be reviewed at least annually by the information Security Department or in events of any significant changes in the existing Information Security environment (internal/external) affecting policies and procedures. The policy owner must be responsible to make the changes to the policy document and to get approved from the Board.

13. Compliance

a. The Bank expects all employees to comply with the policies. Violation or any attempted violation of the cyber security policy shall result in disciplinary action to be taken by the Bank as per the extant guidelines. Disciplinary action shall be consistent with the severity of the incident as determined by an investigation.

b. Violations, if any, of the cyber security policy must be reported to the respective department head and the HEAD OF IT.

c. While the Bank would like to respect privacy of its employees, it reserves the right to audit and / or monitor the activities of its employees and information stored, processed transmitted or handled by the employees using Bank's information systems.

14. Exceptions

a. Approval for exceptions or deviations from the policies, wherever warranted, must be provided by IT Committee for High Risk items and HEAD OF IT information Security Department for Medium and Low Risk items.

b. Exceptions must not be universal but must be agreed on a case by case basis, upon official request made by the information asset owner. These may arise, for example because of local circumstances, conditions or legal reason existing at any point of time. Exceptions to the cyber security policy may have been allowed at the time of execution/updating or on ad-hoc basis if needed.

c. All exceptions during implementation must be submitted by the concerned stakeholder to HEAD OF IT or any other official of the information security team. All the exceptions are to be raised as per the Bank's cyber security policyexception form, The Bank's HEAD OF IT. This request must be approved by the User Department Head / information asset owner.

d. The information Security Department must review all exceptions, as the case may be every year for validity and continuity. The summary of high severity exceptions allowed should be reported to IT committee on a quarterly basis.

15. Inquiries

Any inquiries relating to policy to the application of this policyshould be referred to the Chief Information Security Officer.

16. Cyber Security Domains

1. Inventory Management of IT Assets

   a. The Bank should maintain an up-to-date inventory of IT assets. IT assets include systems and network, including disaster recovery systems and networks with their supporting facilities but limited to information, software, physical, service and people indicating their criticality.

   b. Ensure confidentiality, integrity and availability of information, an information classification scheme designed by the Bank should be adhered to.

c. The Bank should secure information accessible by the internal teams, external agency and partners through approved methods, including information in electronic form, information in physical form and information during transit.

d. Any remote administration connections authorized by the Bank should use strong authentication (typically two- factor authentication) as well as corresponding encryption methods (such as ssh, ssl and vpn) to secure communication traversing the network.

e. Bank should ascertain the risk related to critical information stored, transmitted, processed and accessed.

2. Preventing Access of unauthorized software

a. The Bank should maintain central inventory of all software(s).

b. Bank should develop mechanism to control installation of unauthorized software in the Bank.

c. Bank should track use of authorized / unauthorized software (if any) in the Bank.

d. Bank should define procedures for granting and approving exceptions which at minimum should cover justification of exceptions, duration of exception and authority for approving.

e. Bank shall white list authorized application/software/ libraries etc.

3. Environmental Controls

a. A cyber risk profile based on activities at various locations such as Administrative offices, branches, data center and disaster recovery site, should be documented and maintained which help risk based decision and implementation of cyber security controls.

b. The Bank should ensure that physical access to information processing areas and their supporting infrastructure (communications, power, and environmental) are controlled to prevent, detect, and minimize the effects of unintended access to these areas (e.g., unauthorized information access, or disruption of information processing itself).

c. Bank should monitor compromises of environmental controls relating to temperature, water, smoke, access alarms, service availability alerts (power supply, telecommunication, servers), access logs, etc.

d. The Bank shall evaluate the cyber security risks and take up cyber insurance of an appropriate value from time to time. The need will be assessed on a yearly basis.

4. Network Management and Security

a. Network security architecture should be documented at Bank level. Network security architecture should be updated as and when there are major changes in Bank's environment or at least annually.

b. Security architecture and standard security management principles should be applied in network devices configuration, vulnerability and patch management and change in routing table or setting of network devices.

c. Access to network's device should be restricted to only Bank's authorized network staff and appropriate access control mechanism that support individual accountability and access restriction.

d. Bank should define standard operating procedures for all major IT activities.

e. Bank should ensure that certain, events are logged and these logs are collected using various types of log collection software and infrastructure.

f. A central repository for the log collection should be established which would be used to generate alerts, based on established parameters.

g. Bank should install network security devices, such as firewalls as well as intrusion detection and prevention systems, to protect its IT infrastructure from security exposures originating from internal and external source.

h. Bank should periodically conduct configuration review of network components.

i. Bank shall deploy mechanism to detect and remedy any unusual activities in systems, servers, network devices and endpoints.

j. Bank shall implement solutions to automate network discovery and management.

5. Secure Configuration

a. Document and apply baseline security requirements/ configurations to all categories of devices (end- points/workstations, mobile devices, operating systems, databases, applications, network devices, security devices, security

systems, etc.), throughout the lifecycle (from conception to deployment) and carry out reviews periodically

b. Periodically evaluate critical device (such as firewall, network switches, security devices, etc.) configurations and patch levels for all systems in the bank's network including in Data Centers, in third party hosted sites, shared-infrastructure locations.

c. The Bank should document minimum baseline security standards (MBSS) for IT platforms.

d. The MBSS should be tested before any major release on an IT platform.

e. The MBSS should be reviewed at least once annually and before major upgrade.

6. Anti-Virus and Patch Management

a. Follow a documented risk-based strategy for inventorying IT components that need to be patched, identification of patches and applying patches so as to minimize the number of vulnerable systems and the time window of vulnerability/exposure.

b. Implement and update antivirus protection for all servers and applicable end points preferably through a centralized system

c. Put in place systems and processes to identify, track, manage and monitor the status of patches to operating system and application software running at end-user devices directly connected to the internet and in respect of Server operating Systems/ Databases/Applications/ Middleware, etc.

d. Changes to business applications, supporting technology, service-components and facilities should be managed using robust configuration management processes, configuration baseline that ensure integrity of any changes thereto

e. Periodically conduct VA/PT of internet facing web/mobile applications, servers & network components throughout their lifecycle (pre-implementation, post Implementation, after changes etc.)

f. Periodically conduct Application security testing of web/mobile applications throughout -their lifecycle (ore-implementation, post implementation, after changes) in environment closely resembling or replica of production environment.

g. As a threat mitigation strategy, identify the root cause of incident and apply necessary patches to plug the vulnerabilities.

h. For further details, Information Security Procedure for Change management is to be followed.

i. The Bank should implement security controls to provide robust defense against the Installation spread and execution of malicious code at multiple points in the enterprise

j. Mechanisms such as-web security, anti-malware and continuous monitoring to detect advanced threats such as ransom ware, cyber extortion, data destruction, DDOS should be implemented.

k. Anti-Virus should be installed on all end points, servers and centrally, managed for policy configuration management, virus definition updates.

l. The Bank should implement and maintain preventive, detective and corrective measures across the enterprise to protect information systems and technology from malware.

m. Anti-Malware packages for operating systems should be deployed and definitions should be periodically updated.

n. Malware protection should be installed on all web- gateways, exchange servers and centrally managed for policy implementation.

o. The Bank should implement white listing of internet websites/systems.

p. Bank should have threat intelligent mechanism that collect & analyses threat related information from different internal and external sources.

q. Based on the analyze threat intelligence. Bank should share inferences and intelligence to regulatory bodies like RBI, IDRBT, and CERT-ln.

r. The Bank shall deploy mechanisms to deep scan network packets including secure {HTTPS, etc.) Traffic passing through the web / internet gateway.

s. Mechanisms to manage events related to phishing/rouge applications should be implemented.

7. User Access Control and Management

a. Provide secure access to the bank's assets/ services from within/outside bank's network by protecting data/ information at and in-transit.

b. Carefully protect customer access credentials such as logon user id, authentication information and tokens, access profiles, etc. against leakage/attacks

c. Disallow administrative rights on end-user workstations/PCs/laptops and provide access rights on a need to know basis and for specific duration when it is required following an established process.

d. Implement appropriate (e.g. centralized) systems and controls to allow, manage, log and monitor privileged/supervisor/administrative access to critical systems (servers/OS/DB, applications, network devices etc.)

e. Implement controls to minimize invalid logon counts, deactivate dormant accounts.

f. Monitor any abnormal change in pattern of logon.

g. Implement measures to control installation of software on PCs/laptops, etc.

h. Implement controls for remote management/wiping/locking of mobile devices including laptops, etc.

i. Implement measures to control use of VBA/macros in office documents, control permissible attachment types in email systems

j. For details, Information Security Procedure for Logical access is to be followed.

8. Secure Mail and Messaging System

a. Implement effective systems and procedures to ensure that e-mails are used as an efficient mode of business communication.

b. Ensure that e-mail service and operations remain secure, efficient while communicating within intranet as well as through internet.

c. Email specific server controls should be documented.

d. Security of email communication should be enhanced by use of disclaimer, hashes or encryption.

e. The Bank should control permissible attachment types in email systems.

9. Removable Media

a. By default, access to removable media, drives {USB ports, CD / DVD ROM drives, floppy drives) should be disabled.

b. Critical and sensitive information stored in removable media should be sanitized before disposal. Removable media should be disposed of securely and safely when no longer required.

c. Bank should deploy governing mechanism for use of personally owned and official mobile devices.

d. Bank should deploy mechanism to scan removable media for malwares, before granting any read /write access.

e. Bank should implement centralized policies through active directory or endpoint management systems to restrict use of removable media.

f. Exceptions for granting write access to removable media should be granted after approval of HEAD OF IT and regular recertification process should be established, tracked and documented.

10. User \ Employee \ Management Awareness

a. The Bank should deploy mechanism to protect data at rest and in transmit by implementing secure access controls to the Bank's network.

b. The Bank should deploy mechanism in place to protect customer access credentials against data leakages.

c. The Bank should provide access rights on a need to know basis for specific duration.

d. Users should not be granted administrative rights on end-user workstations /laptops.

e. The Bank should implement centralized authentication and authorization system for accessing IT assets including but not limited to applications, operating systems, databases, network and security devices/systems, point of connectivity.

f. The Bank should enforce strong password policy for all critical assets.

g. The Bank should implement appropriate systems and controls to log and monitor administrative access to critical systems.

h. The Bank should implement controls to minimize invalid logon counts and deactivate dormant accounts.

i. The Bank should deploy measures to control installation of software on end user devices.

j. The Bank should deploy controls to restrict use of VBA/Macros in office documents.

k. The Bank shall deploy controls to monitor abnormal changes in pattern of logon.

11. Customer Education and Awareness

a. Customer education and awareness program should be designed and implemented.

b. Customers should be encouraged to report any phishing mails/websites, etc.

c. Customers shall be educated on the downside risks involved in sharing of their login credentials to any third party and the consequences arising of such situations.

d. Communication medium such as E-mail, SMS, banner, advertisements, Audio-Visual at branch offices should be used to improve customer cyber security awareness.

12. Backup and Restoration

a. Periodic back up of the important data should be taken and store this data 'off line' (i.e., transferring important files to a storage device that can be detached from a computer/system after copying all the files).

13. Vendor and Outsourcing Risk Management

a. Banks shall carefully evaluate the need for outsourcing critical processes and selection of vendor/partner based on comprehensive risk assessment

b. Among others, banks shall regularly conduct effective due diligence, oversight and management of third party vendors/service providers & partners.

c. Establish appropriate framework, policies and procedures supported by baseline system security configuration standards to evaluate, assess, approve, review, control and monitor the risks and materiality of all its vendor/outsourcing activities shall be put in place

d. Banks shall ensure and demonstrate that the service provider adheres to all regulatory and legal requirements of the country. Banks may necessarily enter into agreement with the service provider that amongst others provides for right of audit by the bank and inspection by the regulators of the country.

e. Reserve Bank of India shall have access to all information resources (online/in person) that are consumed by banks, to be made accessible to RBI officials by the banks when sought, though the infrastructure /enabling resources may not physically be located in the premises of banks

f. Further, bank has to adhere to the legal and regulatory requirements relating to geographical location of infrastructure and movement of data out of borders.

g. Banks shall thoroughly satisfy about the credentials of vendor/third-party personnel accessing and managing the bank's critical assets.

h. Background checks, non-disclosure and security policy compliance agreements shall be mandated for all third party service providers.

14. Vulnerability Assessment and Penetration Testing

a. The Bank should periodically conduct vulnerability assessment and penetration testing (VA/PT) for all the critical systems.

b. Vulnerabilities identified should be remediated in a timely manner.

c. Penetration testing of public facing systems and critical applications should be carried out by professionally qualified teams.

d. Concerned Asset owners/team leaders should ensure that necessary remedial measures are implemented to close the findings detected by penetration testing.

e. VA/PT findings and follow up actions should be closely monitored by senior management as well as Information Security/ IT audit team.

f. The Bank should periodically & actively participate in external cyber drills.

15. Risk Based Transaction Monitoring

a. Fraud Risk Management System (FRMS) should be deployed by Bank across each delivery channel for monitoring risk based transactions.

b. Continuous surveillance should be used to monitor and detect fraudulent or large transactions in the Bank.

c. Immediate notifications through alternate channels like E-mail and SMS are provided to customers on transactions executed by customer across various means i.e. online, cheque, ATM.

d. For transaction above tolerance limit Call Back Verification (CBV) control shall be implemented.

16. Incident Response arid Cyber Crisis Management

a. Bank should adhere to incident response procedures to respond consistently to attacks, minimize all loss, leakage or disruption during an attack.

b. Learning's from information security incidents should be documented and communicated to stakeholders. This information shall be used in improving the processes and systems to reduce recurrence and/or future impact of the security incident.

c. Employees and third parties shall report any observed or suspected information security weaknesses in systems or services through proper communication channels.

d. Bank should develop recovery strategies to ensure critical application systems are resumed within the agreed Recovery Time Objectives (RTO).

e. Management responsibilities should be assigned to ensure a quick, effective, and orderly response to information and cyber security incidents.

f. For information security incident that involves legal action (either civil or criminal), evidence should be collected, retained, and presented as per laws to conform to the rules laid down in the relevant jurisdiction(s).

g. Contacts with relevant authorities such as law enforcement agencies, regulatory bodies and national nodal agencies should be maintained.

h. The Bank should have process for collecting and sharing of threat information from local, national or international sources following legally accepted/defined means/processes.

i. Advance cyber security incident like containing ransom ware/cyber extortion, data destruction, DDOS, etc. should follow cyber crisis management plan.

j. Cyber-attacks should be controlled by implementing security controls like shielding, quarantining the affected devices/systems.

k. Policy for aligning, Incident Response and Digital forensics to reduce the business downtime/ to bounce back to normalcy should be in place.

17. Forensics

a. The Bank should conduct preliminary investigation and evidence gathering and involve external forensics service on case to case basis

b. The Bank should have a forensic risk evaluation criterion to decide on incidents that qualify for forensics.

c. Security function must coordinate legal, HR.

d. Digital evidence related to information security incidents should be collected, stored and processed to facilitate necessary forensic investigation as per the applicable laws and regulations.

e. The Bank should periodically and actively participate in external cyber drills.

17 CYBER CRISIS MANAGEMENT

Cyber crisis management plan that includes identification, validation, activation, response, recovery and containment of cyber crisis should be documented, implemented and reviewed at least annually.

Type of Threats

1. Hacktivists; these are individuals or groups who seek to disrupt systems and networks for a variety of motives, including notoriety, financial gain, or political agendas. They connect across borders to overwhelm targeted websites and access sensitive information. They may seek to harm their enemies by either shaming them or disabling their services. Hacktivists typically launch distributed denial of service (DDoS) attacks, deface websites, access sensitive government data, and publish the personal information of high- ranking persons and business leaders.

2. Advanced Persistent Threats (APT}: These occur when malicious actors use complex and unique malware to quietly gain access to proprietary or personal information and sensitive government information. They may also use customized solutions to take advantage of insiders, social engineering, network hardware, and third-party software to cause various malfunctions, destroy data, and disable networks.

3. Cyber Crime Syndicates: These organizations seek account information to make fraudulent transactions or to siphon money, information theft is also common, and as cyber criminals will sell sensitive corporate information to unauthorized individuals or groups. Cyber criminals leverage various methods to achieve their objectives, such as distributing massive amounts of e-mails while posing as banks or other authorities to obtain customer identification and financial information. They may also use large-scale DDoS attacks to overwhelm Internet dependent enterprises.

4. Malicious Insiders: These are trusted individuals who are motivated to compromise the confidentiality, integrity, or availability of an organization's information and information systems. Their motives may include financial gain, revenge, or ideology. Insiders do not need to infiltrate perimeter network defenses because they have trusted access to Information and information systems and can use various methods to damage or destroy government and business systems.

5. Root kit: is a collection of tools that are used to obtain administrator-level access to a computer or a network of computers. A root kit could be installed on any computer by a cybercriminal exploiting a vulnerability or security hole in a legitimate application on the computer and may contain spyware that monitors and records keystrokes.

6. Botnet: also called a "zombie army" is a collection of software robots, or bots, that run automated tasks over the Internet. It is a group of computers connected to the Internet that have been compromised by a hacker using a computer virus or Trojan horse. An individual computer in the group is known as a "zombie" computer.

   The botnet is under the command of a "bot herder" or a "bot master," usually to perform nefarious activities by running programs such as worms, Trojan horses, or backdoors. This could include distributing spam to the email contact addresses on each zombie computer, for example. If the botnet is sufficiently big in number, it could be used to access a targeted website simultaneously in what's known as a denial-of-service (DoS) attack. The goal of a DoS attack is to bring down a web server by overloading it with access requests.

7. Trojan horse: Users can infect their computers with Trojan horse software simply by downloading an application they, thought was legitimate but was in fact malicious. Once inside the computer of a user, a Trojan horse can do anything from recording his/her passwords by logging keystrokes (known as a keystroke logger) to hijacking the webcam to watch and record his/her every move.

8. Spam: is electronic junk email. The amount of spam has now reached to about 90 billion messages a day.

   Email addresses are collected from chat rooms, websites, and news groups and by Trojans which harvest users' address books. SPIM is spam sent via instant messaging systems such as Yahoo! Messenger, MSN Messenger and ICQ. Its Danger level is Low but Prevalence is Extremely High.

   Spam can clog a personal mailbox, overload mail servers and impact network performance. On the other hand, efforts to control spam such as by using spam filters run the risk of filtering out legitimate email messages. Perhaps the real danger of spam is not so much in being a recipient of it as inadvertently becoming a transmitter of it. Spammers frequently take control of computers and use them to distribute spam, perhaps the use of a botnet. Once a user's computer is compromised, their personal information may also be illegally acquired.

9. SQL Injection: Such attack involves the alteration of SQL statements that are used within a web application through the use of attacker-supplied data. Insufficient input validation and improper construction of SQL statements in web applications can expose them to SQL injection attacks. SQL injection is such a prevalent and potentially destructive attack that this has become the number one threat to web applications.

10. Authentication Bypass: This attack allows an attacker to log on to an application, potentially with administrative privileges, without supplying a valid username and password.

11. Information Disclosure: This attack allows an attacker to obtain, either directly or indirectly, sensitive information in a database.

    a. Compromised Data Integrity: This attack involves the alteration of the contents of a database. An attacker could use this attack to deface a web page or more likely to insert malicious content into otherwise innocuous web pages.

    b. Compromised Availability of data; this attack allows an attacker to delete information with the intent to cause harm or delete log or audit information in a database.

    c. Remote Command Execution: Performing command execution through a database can allow an attacker to compromise the host operating system. These attacks often leverage an existing, predefined stored procedure for host operating system command execution.

12. Ransomware: is a type of malware that prevents or limits users from accessing their system, either by socking the system's screen or by locking the users' files unless a ransom is paid. More modern ransom ware families, collectively categorized as Crypto - ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key.

13. Website defacement: is an attack on a website that changes the visual appearance of the site or a webpage. These are typically the work of system crackers, who break into a web server and replace the hosted website with one of their own.

14. Spoofing: is an attack situation in which one person or program successfully masquerades as another by falsifying data, thereby gaining an illegitimate advantage. E-mail spoofing is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source. The email often contains malicious software as attachment which will be used to get unauthorized access to the user's computer.

15. Session Hijacking: Sometimes also known as cookie hijacking is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system. Once the user's session has been accessed the attacker can masquerade as that user and do anything the user is authorized to do on the computer.

16. Man in the Middle Attack: It is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. Online banking and e-commerce sites are frequently the target of such attacks. The attacker can capture login credentials and other sensitive data from the user's computer with this type of attacks.

18. CONTROL MEASURES IMPLEMENTED IN BANK:

1. Use and maintain updated anti-virus software - Anti-virus software recognizes and protects our computer against most known viruses. Anti-virus software is maintained up-to-date with latest version, patches & updated definition on ail the Desktops and Servers and monitored.

2. Keep our operating system and application software up-to-date:- Bank deployed security patches on all endpoints, as soon as they become available, to eliminate exploitable vulnerabilities (i.e. zero day vulnerabilities) or known problems.

3. Regular Backup: - Execution of daily backups of all critical systems and periodically execute an "offline" backup of critical files to removable media in accordance with Data Retention Policy and IS Procedure for Data Backup.

4. Blocking of removable media devices: - Prevention or limitation of all removable media devices on systems to limit the spread or introduction of malicious Software and possible exfiltration of data, except where there is a valid business need for use.

5. Restricting account privileges: - All daily operations are executed using standard user accounts unless administrative privileges are required for that specific function. Configuration of all standard user accounts to prevent the execution and installation of any unknown or unauthorized software. Both standard and administrative accounts have access only to services required for nominal daily duties, enforcing the concept of separation of duties.

19. VULNERABILITY INDEX OF CYBER SECURITY FRAMEWORK (VICS):

Bank must take half-yearly review of the Vulnerability Index of Cyber Security Framework (VICS) and fill up the four part questionnaires as follows.

i. Basics of Cyber Security Framework

ii. Strength of Policy Framework

iii. Vendor Management

iv. Cyber Crisis Management Plan

After filling up the VICS questionnaires, the IT Cell shall review any shortcomings and work with the IS auditor and the IT Steering Committee to rectify the deficiencies and update the Board level IT Committee.