भारतीय रिज़र्व बैंक

RESERVE BANK OF INDIA

www.rbi.org.in

Annex to Circular on Cyber Security Framework in Banks

Annex 1

Baseline Cyber Security and Resilience Requirements

An indicative but not exhaustive list of requirements to be put in place by banks to achieve baseline cyber-security/resilience is given. This may be evaluated periodically to integrate risks that arise due to newer threats, products or processes. Important security controls for effective cyber security as may be articulated by CERT-In also may be referred. Some of the key points to be kept in mind are:

a. In view of the growing technology adoption and potential threats, the role of IT Sub-committee may be reviewed; Board level involvement and guidance would set the right tone at the top.
b. It is important to endeavour to stay ahead of the adversary.
c. Cyber Security Operations Centre should have the capacity to monitor various logs / incidents in real time / near real time.
d. It is important to keep the vigil and to constantly remain alert.
e. While hardware devices and software applications may provide security, it is important to configure them appropriately.
f. Human resources are the key and ensure that they are provided with appropriate training. Communicate the security policy of the bank periodically.

Baseline Controls

1) Inventory Management of Business IT Assets

1.1 Maintain an up-to-date inventory of Assets, including business data/information including customer data/information, business applications, supporting IT infrastructure and facilities – hardware/software/network devices, key personnel, services, etc. indicating their business criticality. The banks may have their own framework/criteria for identifying critical assets.

1.2 Classify data/information based on information classification/sensitivity criteria of the bank

1.3 Appropriately manage and provide protection within and outside organisation borders/network taking into consideration how the data/information are stored, transmitted, processed, accessed and put to use within/outside the bank's network, and level of risk they are exposed to depending on the sensitivity of the data/information.

2) Preventing execution of unauthorised software

2.1 Maintain an up-to-date and preferably centralised inventory of authorised/unauthorised software(s). Consider implementing whitelisting of authorised applications / software/libraries, etc.

2.2 Have mechanism to centrally/otherwise control installation of software/applications on end-user PCs, laptops, workstations, servers, mobile devices, etc. and mechanism to block /prevent and identify installation and running of unauthorised software/applications on such devices/systems.

2.3 Continuously monitor the release of patches by various vendors / OEMs, advisories issued by CERT-in and other similar agencies and expeditiously apply the security patches as per the patch management policy of the bank. If a patch/series of patches is/are released by the OEM/manufacturer/vendor for protection against well-known/well publicised/reported attacks exploiting the vulnerability patched, the banks must have a mechanism to apply them expeditiously following an emergency patch management process.

2.4 Have a clearly defined framework including requirements justifying the exception(s), duration of exception(s), process of granting exceptions, and authority for approving, authority for review of exceptions granted on a periodic basis by officer(s) preferably at senior levels who are well equipped to understand the business and technical context of the exception(s).

3) Environmental Controls

3.1 Put in place appropriate environmental controls for securing location of critical assets providing protection from natural and man-made threats.

3.2 Put in place mechanisms for monitoring of breaches / compromises of environmental controls relating to temperature, water, smoke, access alarms, service availability alerts (power supply, telecommunication, servers), access logs, etc. Appropriate physical security measures shall be taken to protect the critical assets of the bank.

4) Network Management and Security

4.1 Prepare and maintain an up-to-date network architecture diagram at the organisation level including wired/wireless networks;

4.2 Maintain an up-to-date/centralised inventory of authorised devices connected to bank’s network (within/outside bank’s premises) and authorised devices enabling the bank’s network. The bank may consider implementing solutions to automate network discovery and management.

4.3 Ensure that all the network devices are configured appropriately and periodically assess whether the configurations are appropriate to the desired level of network security;

4.4 Put in appropriate controls to secure wireless local area networks, wireless access points, wireless client access systems.

4.5 Have mechanisms to identify authorised hardware / mobile devices like Laptops, mobile phones, tablets, etc. and ensure that they are provided connectivity only when they meet the security requirements prescribed by the bank.

4.6 Have mechanism to automatically identify unauthorised device connections to the bank's network and block such connections.

4.7 Put in place mechanism to detect and remedy any unusual activities in systems, servers, network devices and endpoints.

4.8 Establish Standard Operating Procedures (SOP) for all major IT activities including for connecting devices to the network.

4.9 Security Operation Centre to monitor the logs of various network activities and should have the capability to escalate any abnormal / undesirable activities.

4.10 Boundary defences should be multi-layered with properly configured firewalls, proxies, DMZ perimeter networks, and network---based IPS and IDS. Mechanism to filter both inbound and outbound traffic to be put in place.

5) Secure Configuration

5.1 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,

5.2 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 Centres, in third party hosted sites, shared-infrastructure locations.

6) Application Security Life Cycle (ASLC)

6.1 Incorporate/Ensure information security across all stages of application life cycle.

6.2 In respect of critical business applications, banks may consider conducting source code audits by professionally competent personnel/service providers or have assurance from application providers/OEMs that the application is free from embedded malicious / fraudulent code.

6.3 Secure coding practices may also be implemented for internally /collaboratively developed applications.

6.4 Besides business functionalities, security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, session management, security event tracking and exception handling are required to be clearly specified at the initial and ongoing stages of system development/acquisition/implementation.

6.5 The development, test and production environments need to be properly segregated.

6.6 Software/Application development approach should be based on threat modelling, incorporate secure coding principles and security testing based on global standards and secure rollout.

6.7 Ensure that software/application development practices addresses the vulnerabilities based on best practices baselines such as Open Web Application Security Project (OWASP) proactively and adopt principle of defence-in-depth to provide layered security mechanism.

6.8 Consider implementing measures such as installing a “containerized” apps on mobile/smart phones for exclusive business use that is encrypted and separated from other smartphone data/applications; measures to initiate a remote wipe on the containerized app, rendering the data unreadable, in case of requirement may also be considered.

6.9 Ensure that adoption of new technologies shall be adequately evaluated for existing/evolving security threats and IT/security team of the bank reach reasonable level of comfort and maturity with such technologies before introducing for critical systems of the bank.

7) Patch/Vulnerability & Change Management

7.1 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.

7.2 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.

7.3 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

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

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

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

7.7 Periodically evaluate the access device configurations and patch levels to ensure that all access points, nodes between (i) different VLANs in the Data Centre (ii) LAN/WAN interfaces (iii) bank's network to external network and interconnections with partner, vendor and service provider networks are to be securely configured.

8) User Access Control / Management

8.1 Provide secure access to the bank's assets/services from within/outside bank's network by protecting data/information at rest (e.g. using encryption, if supported by the device) and in-transit (e.g. using technologies such as VPN or other secure web protocols, etc.)

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

8.3 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.

8.4 Implement centralised authentication and authorisation system or accessing and administering applications, operating systems, databases, network and security devices/systems, point of connectivity (local/remote, etc.) including enforcement of strong password policy, two-factor/multi-factor authentication depending on risk assessment and following the principle of least privileges and separation of duties.

8.5 Implement appropriate (e.g. centralised) systems and controls to allow, manage, log and monitor privileged/superuser/administrative access to critical systems (Servers/OS/DB, applications, network devices etc.).

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

8.7 Monitor any abnormal change in pattern of logon.

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

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

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

9) Authentication Framework for Customers

9.1 Implement authentication framework/mechanism to provide positive identify verification of bank to customers.

9.2 Customer identity information should be kept secure.

9.3 Banks should act as the identity provider for identification and authentication of customers for access to partner systems using secure authentication technologies.

10) Secure mail and messaging systems

10.1 Implement secure mail and messaging systems, including those used by bank's partners & vendors, that include measures to prevent email spoofing, identical mail domains, protection of attachments, malicious links etc.

10.2 Document and implement email server specific controls

11) Vendor Risk Management

11.1 Banks shall be accountable for ensuring appropriate management and assurance on security risks in outsourced and partner arrangements.

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

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

11.4 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.

11.5 Banks shall ensure and demonstrate that the service provider (including another bank) 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.

11.6 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.

11.7 Further, banks have to adhere to the relevant legal and regulatory requirements relating to geographical location of infrastructure and movement of data out of borders.

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

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

12) Removable Media

12.1 Define and implement policy for restriction and secure use of removable media/BYOD on various types/categories of devices including but not limited to workstations/PCs/Laptops/Mobile devices/servers, etc. and secure erasure of data on such media after use.

12.2 Limit media types and information that could be transferred/copied to/from such devices.

12.3 Get the removable media scanned for malware/anti-virus prior to providing read/write access.

12.4 Consider implementing centralised policies through Active Directory or End-point management systems to whitelist/blacklist/restrict removable media use.

12.5 As default rule, use of removable devices and media should not be permitted in the banking environment unless specifically authorised for defined use and duration of use.

13) Advanced Real-time Threat Defence and Management

13.1 Build a robust defence against the installation, spread, and execution of malicious code at multiple points in the enterprise.

13.2 Implement Anti-malware, Antivirus protection including behavioural detection systems for all categories of devices – (Endpoints such as PCs/laptops/ mobile devices etc.), servers (operating systems, databases, applications, etc.), Web/Internet gateways, email-gateways, Wireless networks, SMS servers etc. including tools and processes for centralised management and monitoring.

13.3 Consider implementing whitelisting of internet websites/systems.

13.4 Consider implementing secure web gateways with capability to deep scan network packets including secure (HTTPS, etc.) traffic passing through the web/internet gateway

14) Anti-Phishing

14.1 Subscribe to Anti-phishing/anti-rouge app services from external service providers for identifying and taking down phishing websites/rouge applications.

15) Data Leak prevention strategy

15.1 Develop a comprehensive data loss/leakage prevention strategy to safeguard sensitive (including confidential) business and customer data/information.

15.2 This shall include protecting data processed in end point devices, data in transmission, as well as data stored in servers and other digital stores, whether online or offline.

15.3 Similar arrangements need to be ensured at the vendor managed facilities as well.

16) Maintenance, Monitoring, and Analysis of Audit Logs

16.1 Consult all the stakeholders before finalising the scope, frequency and storage of log collection.

16.2 Manage and analyse audit logs in a systematic manner so as to detect, understand or recover from an attack.

16.3 Enough care is to be taken to capture audit logs pertaining to user actions in a system. Such arrangements should facilitate forensic auditing, if need be.

17) Audit Log settings

17.1 Implement and periodically validate settings for capturing of appropriate logs/audit trails of each device, system software and application software , ensuring that logs include minimum information to uniquely identify the log for example by including a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or event and/or transaction.

18) Vulnerability assessment and Penetration Test and Red Team Exercises

18.1 Periodically conduct vulnerability assessment and penetration testing exercises for all the critical systems, particularly those facing the internet.

18.2 The vulnerabilities detected are to be remedied promptly in terms of the bank's risk management/treatment framework so as to avoid exploitation of such vulnerabilities.

18.3 Penetration testing of public facing systems as well as other critical applications are to be carried out by professionally qualified teams.

18.4 Findings of VA/PT and the follow up actions necessitated are to be monitored closely by the Information Security/Information Technology Audit team as well as Senior/Top Management.

18.5 Red Teams may be used to identify the vulnerabilities and the business risk, assess the efficacy of the defences and check the mitigating controls already in place by simulating the objectives and actions of an attacker.

18.6 Periodically and actively participate in cyber drills conducted under the aegis of Cert-IN, IDRBT etc.

19) Incident Response & Management

Responding to Cyber-Incidents:

19.1 Put in place a fully effective Incident Response programme with due approval of the Board / Top Management.

19.2 Have written incident response procedures including the roles of staff / outsourced staff handling such incidents; Response strategies shall consider readiness to meet various incident scenarios based on situational awareness and potential/post impact, consistent communication & co-ordination with stakeholders during response;

19.3 Have a mechanism to dynamically incorporate lessons learnt to continually improve the response strategies.

Recovery from Cyber - Incidents:

19.4 Bank’s BCP/DR capabilities shall adequately and effectively support the Bank’s cyber resilience objectives and should be so designed to enable the bank to recover rapidly from cyber-attacks/other incidents and safely resume critical operations aligned with recovery time objectives while ensuring security of processes and data is protected.

19.5 Banks shall ensure such capabilities in all interconnected systems and networks including those of vendors and partners and readiness demonstrated through collaborative & co-ordinated resilience testing that meet the bank’s recovery time objectives.

19.6 Such testing shall also include testing of crisis communication to customers and other internal and external stakeholders, reputation management. Adequate capacity shall be planned and maintained, in consideration thereof. The following may be considered:

(a) Define incidents, method of detection, methods of reporting incidents by employees, vendors and customers and periodicity of monitoring, collection/sharing of threat information, expected response in each scenario/incident type, allocate and communicate clear roles and responsibilities of personnel manning/handling such incidents, provide specialised training to such personnel, post incident review, periodically test incident response plans.
(b) Establish and implement a Security Operations Centre for centralised and coordinated monitoring and management of security related incidents.
(c) Establish and implement systems to collect and share threat information from local/national/international sources following legally accepted/defined means/process
(d) Document and communicate strategies to respond to advanced attacks containing ransom ware/cyber extortion, data destruction, DDOS, etc.
(e) Contain the level of cyber-attack by implementing shielding controls/quarantining the affected devices/systems.
(f) Implement a policy & framework for aligning Security Operation Centre, Incident Response and Digital forensics to reduce the business downtime/ to bounce back to normalcy.

20) Risk based transaction monitoring

20.1 Risk based transaction monitoring or surveillance process shall be implemented as part of fraud risk management system across all -delivery channels.

20.2 The bank should notify the customer, through alternate communication channels, of all payment or fund transfer transactions above a specified value determined by the customer.

21) Metrics

21.1 Develop a comprehensive set of metrics that provide for prospective and retrospective measures, like key performance indicators and key risk indicators.

21.2 Some illustrative metrics include coverage of anti-malware software and their updation percentage, patch latency, extent of user awareness training, vulnerability related metrics, etc.

22) Forensics

22.1 Have support/ arrangement for network forensics/forensic investigation/DDOS mitigation services on stand-by.

22.2 Periodically and actively participate in cyber drills conducted under the aegis of Cert-IN, IDRBT etc.

23) User / Employee/ Management Awareness

23.1 Define and communicate to users/employees, vendors & partners security policy/ies covering secure and acceptable use of bank's network/assets including customer information/data, educating them about cybersecurity risks and protection measures at their level.

23.2 Encourage them to report suspicious behaviour incidents to the incident management team.

23.3 Conduct targeted awareness/training for key personnel (at executive, operations, security related administration/operation and management roles, etc.)

23.4 Evaluate the awareness level periodically.

23.5 Establish a mechanism for adaptive capacity building for effective Cybersecurity Management. Making cyber security awareness programs mandatory for new recruits and web-based quiz & training for lower, middle & upper management every year. (Recent and past cyber-attacks show, cyber adversaries are also targeting bank employees).

23.6 Board members may be sensitised on various technological developments and cyber security related developments periodically.

23.7 Board members may be provided with training programmes on IT Risk / Cyber-security Risk and evolving best practices in this regard so as to cover all the Board members atleast once a year.

24) Customer Education and Awareness

24.1 Improve and maintain customer awareness and education with regard to cybersecurity risks.

24.2 Encourage customers to report phishing mails/ Phishing sites and on such reporting take effective remedial action.

24.3 Educate the customers on the downside risk of sharing their login credentials / passwords etc. to any third party vendor and the consequences thereof.