Technology Risks

January 2018

Table of contents

I. Foreword

The State of Qatar is committed to enhancing cyber security initiatives in the financial sector. Large projects and investments are pushing the economy to compete with leading nations worldwide. In order to ensure its competitiveness and efficiency, the banking sector needs to keep up with the pace of technological evolution considering the current threat environment. Cyber attacks threaten financial stability by disrupting the vital functions that the financial sector performs for the economy. As with financial risk, cyber risk can be amplified by the interconnectedness of the global financial system.

To this effect the Qatar Central Bank (QCB) has enhanced its modern technology and e-Banking services risks to address cyber security requirements. The bank should put a cyber security strategy in place to meet cyber security needs. Boards need to assure themselves that effective risk management arrangements are in place, having considered the threats, criticality of assets and likely cyber attack scenarios. In the current threat landscape, boards have an enhanced role and a responsibility to provide confidence to investors, adherence to regulations, liaise with providers of cyber insurance and take steps to work towards minimizing potential litigants.

II. Purpose and applicability

The main purpose of the QCB cyber security circular is to provide guidance to bank users, employees, contractors and other authorized users, of their obligatory requirements for protecting the technology and information assets of the bank. The cyber security circular provides measures of how the information assets can be protected by implementing controls on these assets.

Banks in the State of Qatar are required to comply with the requirements of the circular. To this effect, banks should implement a cyber security framework to ensure alignment with the requirements of the circular.

Banks are expected to perform, at a minimum, an annual assessment for compliance to the requirements of this circular.

Note: For the purpose of this circular, information security and cyber security have been used interchangeably in the context of the requirement.

III. Relationship to other standards

The ‘Modern technology and e-Banking services risks circular’ has been enhanced to include requirements from National Information Assurance Policy (NIAP) v2.0, NIST cyber security core framework and ISO 27001:2013.

In addition, guidance has also been included from technology risk rules or regulations issued by other central banks across the globe.

IV. Acronyms and abbreviation

QCB	Qatar Central Bank
3DES/TDES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
AML	Anti-money Laundering
AP	Access Point
ATM	Automated Teller Machine
BCP/BCM	Business Continuity Plan/Management
BIOS	Basic Input Output System
BYOD	Bring Your Own Device
CAM	Card Authentication Method
CDA	Combined data authentication
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CIA	Confidentiality, Integrity and Availability
CTO	Chief Technology Officer
CC/EAL	Common Criteria/Evaluation Assurance Level
CCMP	Cyber Crisis Management Plan
CISO	Chief Information Security Officer
CISA	Certified Information Systems Auditor
CISSP	Certified Information Systems Security Professional
CMS	Card Management System
CNP	Certified Network Professional
COBIT	Control Objectives in Information
CSP	Certificate Service Provider
DBA	Database Administrator
DC	Data Centre
DDA	Dynamic data authentication
DDS	DoS Defense System
DES	Data Encryption Standard
DISA	Defense Information Systems Agency

DoS	Denial of Services
DDoS	Distributed denial of service
DMZ	Demilitarized Zone
DNS	Domain Name System
DRP	Disaster Recovery Plan
DSS	Decision Support System
EEPROM	Electrically Erasable Programmable Read Only Memory
EFTPOS	Electronic Funds Transfer at Point of Sale
EMV	Europay MasterCard Visa
EoL	End of Life
EoS	End of Support
FIPS	Federal Information Processing Standard
FSP	Financial Services Professional
HLD	High Level Diagram
HSM	Host/Hardware Security Module
IAIS	International Association of Insurance
ICMP	Internet Control Message Protocol
ICT	Information Communication Technology
ID/QID	Identity/Qatari Identity
IOSCO	International Organization of Securities
IPR	Intellectual Property Rights
IDS	Intrusion detection system
IPS	Intrusion prevention system
IPSEC	Internet Protocol Security
IRC	Internet Relay Chat
ISO	Information Security Officer
ISACA	Information Systems Audit and Control Association
ISAE	International Standard for Assurance Engagements
ISC2	International Information System Security Certification Consortium
ISO27001	Industry Standard Organization 27001
ISO22301	Industry Standard Organization 22301
ISO31000	Industry Standard Organization 31000

ISO11770	Industry Standard Organization 11770
ISP	Internet Service Provider
ITIL	IT infrastructure library
KYC	Know Your Customer
LDAP	Lightweight Directory Access Protocol
LLD	Low level diagram
MAC	Media Access Control
MDM	Mobile Device Management
MFD	Multi-functional Devices
MoCT	Ministry of Information and Communication Technology
MOI	Ministry of Interior
NAC	Network access control
NDA	Non-disclosure Agreement
NIA	Network Interface Adapter
NIAP	National Information Assurance Partnership
NIST	National Institute of Standard and Technology
NIST CSF	NIST Cybersecurity Framework
NTP	Network Time Protocol
OWASP	Open Web Application Security Project
OEM	Original equipment manufacturer
PCI	Peripheral Component Interconnect
PCIPED	PCI Pin Entry Device
PEAP	Protected Extensible Authentication Protocol
POS	Point of Sale
POTS	Plain Old Telephone Service
PTS	Profile Tuning Suite
PD	Personal device
Q-CERT	Qatar Computer Emergency Response Team
RCE	Remote Code Explanation
RBAC	Role based access control
RTO	Recovery time objective
S-SDLC	Secure software development life cycle

SANS	System Administration Networking and Security
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPF	Sender Policy Framework
SOC	Security Operations Centre
SLA	Service Level Agreement
SOP	Standard Operating Procedure
SSH	Secure Shell
SSL	Secure Sockets Layer
SSID	Service Set Identifier
SYN	A form of Denial of Services Attack
TACACS+	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TDES	Triple Data Encryption Standard
TIA-942	Telecommunications Industry Associations-942
TLS	Transport Layer Security
UAT	User Acceptance Testing

1. Cyber security within the organization

1.1. Overview - Managing cyber security risks

1.1.1. The bank shall ensure that a cyber security function (team, committee, etc.) and framework are established. These shall be approved by the board/board authorized committee.

1.1.2. The board shall request the senior management to periodically review (at least annually) the adequacy of cyber security controls in line with the emerging cyber threats. Senior management shall provide reasonable justification to the board for any identified material gaps.

1.1.3. The board must have oversight of technology and cyber security risks, and ensure that measures are in place to support their business strategies and objectives. The board must approve an overall cyber risk appetite. Risk appetite is the defined level of risk that may be accepted by the bank. The board must have adequate technical representation to guide them on matters pertaining to cyber security. These technical representative members shall have adequate experience in cyber security or must be experts in cyber security.

1.1.4. The board must approve a cyber security policy to manage security risks and safeguard information assets.

1.1.5. The board must approve the overall cyber security strategy and budget. The budget must contain built in contingency considerations.

1.1.6. The board shall put in place, a cyber security/information security function for effective implementation of cyber security controls. It shall have adequate representation from relevant departments such as IT, banking technology, risk, information security, human resources (HR), business continuity, legal and compliance.

1.1.7. Cyber security policies, standards and procedures must be updated and reviewed at least on an annual basis.

1.2. Cyber security policy and the organization

1.2.1. The board and senior management shall have oversight of technology risks and ensure that the organization's IT function (team, committee, etc.) is capable of supporting its business strategies and objectives. The bank must establish IT policies, standards and procedures, which are critical components of the framework, to manage technology risks and safeguard information system assets in the organization. The bank shall form committees that oversee IT Strategy, IT Steering and technology risk management.

1.2.2. The bank shall put in place a cyber/information security organization responsible for designing, establishing, operating and improving cyber security/information security program. These shall consider leading industry practices.

1.2.3. The security program shall include, but not limited to the following:

- **Development and ongoing maintenance of security policies**
- **Assignment of roles, responsibilities and accountability for information security**
- **Development/maintenance of a security and control framework that consists of standards, measures, practices and procedures**
- **Classification and assignment of ownership of information assets**
- **Periodic risk assessments and ensuring adequate, effective and tested controls for people, processes and technology to enhance information security**
- **Ensuring security is integral to all organizational processes**
- **Processes to monitor security incidents**
- **Effective identity and access management processes**
- **Generation of meaningful metrics of security performance**
- **Information security related awareness sessions to users/officials, including senior officials and board members.**

1.2.4. The bank must put in place a policy, that clearly defines the strategy and documents the approach to address cyber threats given the level of complexity of business and acceptable levels of risk; and this must be duly approved by their board. It should highlight the risks from cyber threats and the measures to be taken to address/mitigate these risks.

1.2.5. The bank shall form a separate Information Security function/group (team, committee, etc.) to focus exclusively on information/cyber security. There must be segregation of duties between the Information Security Group and the IT division which actually implements the IT requirements.

1.2.6. The Information Security Group shall be able to address the requirements of the bank considering the size and nature of activities (such as banking and delivery channels).

1.2.7. The bank must appoint a Chief Information Security Officer (CISO), responsible for the Information Security Group. The CISO must report to an independent governing body and shall not have a direct relationship with the IT head/ Chief Information Officer (CIO)/Chief Technology Officer (CTO). CISO must have a working relationship with the CIO/CTO to understand IT infrastructure and operations, to build effective cyber security across the bank, in line with business requirements and objectives.

1.2.8. The bank shall form a security forum comprising of responsible parties from various functions, such as the Chief Executive Officer (CEO); Chief Financial Officer (CFO); business unit executives; the CIO/IT head, heads of HR, Legal, Risk Management, Audit, Operations and Public Relations. The forum meetings shall be facilitated by the CISO.

1.2.9. The Information Security Committee shall be responsible for the following activities, including but not limited to:

— **Reviewing and facilitating the implementation of information security policies, standards and procedures to ensure that all the risks are managed within the bank’s cyber risk appetite.**

— **Approving and monitoring major information security projects and the status of information security plans and budgets, establishing priorities, approving standards and procedures.**

— **Supporting the review and implementation of a bank-wide Information Security Management Program.**

— **Reviewing security incidents, information security assessments and monitoring activities across the bank.**

— **Reviewing the status of the security awareness program.**

— **Assessing new developments or issues relating to information security.**

— **Reporting to the board of directors on information security activities.**

1.2.10. The Information Security Group shall be adequately resourced in terms of number of staff members, level of skills and tools or techniques, such as risk assessment, security architecture, vulnerability assessment and forensic assessment.

1.2.11. It must be ensured that the CISO has the following responsibilities:

- **Ensuring the development, maintenance, updating and implementation of security risk management plans, system security plans and any security procedures used.**
- **Providing technical security advice regarding system development, acquisition, implementation, modification, operation, support and architecture.**
- **Assisting the system manager to develop system security standards/policies.**
- **Performing regular review of system security, system audit trails and logs and the integrity of system configurations.**
- **Presenting and justifying the information security program and related framework(s) to the CEO, and maintaining a dedicated budget.**
- **Developing a security architecture that is in line with the business strategy.**
- **Managing other levels of personnel who implement the security architecture and perform information security duties.**
- **Performing risk assessments that will validate the security architecture and uncover flaws that need attention.**
- **Communicating the security policy, practices and procedures, as well as managing a security awareness program**
- **Identifying potential threats and vulnerabilities, in order to formulate proper information security techniques to counter them.**
- **Ensuring appropriate organizational involvement in the critical infrastructure protection efforts for the countries where the organization does business.**

1.3. Cyber security preparedness indicators

1.3.1. The bank shall have cyber resilience capabilities assessed and measured through the development of indicators to assess the level of preparedness/risks.

1.3.2. These indicators shall be assessed through independent compliance checks/audits carried out by qualified and competent professionals.

1.3.3. The board shall periodically (at least semi-annually) monitor cyber security key indicators. Senior management shall put in place a remedial action plan to address the deviations, if any.

The cyber security indicators are shown below:

Risks:

- coverage
- top risks.

Compliance:

- external
- internal
- readiness.

Incidents:

- statistics
- incident management.

Awareness and culture:

- learning scores
- training coverage
- incidents and other violations associated with awareness.

Threat level:

- external
- internal.

Key cyber security projects in progress:

- impact on risk reduction
- progress.

2. Cyber security in the Human Resources (HR) department

2.1. Personal security

2.1.1. The bank shall define HR policies and processes in line with the organization’s Information Security Policy. HR policies shall document information security responsibilities for employees, third party and contractors.

2.1.2. Information security responsibilities shall be included as part of the employees’ role responsibilities and job descriptions. These responsibilities should be monitored throughout an individual’s employment.

2.1.3. HR policies shall be made available to all staff. It must be ensured that employees are aware of, and comply with, policies and their obligations to information security.

2.1.4. The bank must define a disciplinary process as a part of HR policy. It shall be ensured that the process is enforced and the employees are aware of it.

2.1.5. The bank shall ensure that all employees, contractors and third party staff sign terms and conditions, as well as a confidentiality and non-disclosure agreement when joining, or in the event of a change of job profile.

2.1.6. The bank shall handle personally identifiable information, collected from personnel with due care and diligence, in line with requirements for handling personal information specified by Information Privacy and Protection Law.

2.1.7. The bank must ensure that vendors, contractors, delegates or guests visiting bank’s premises are:

- **Logged with unique identifiable information including date, time and purpose of admittance.**
- **Provided with a visitor badge or identification tag.**
- **Wearing a noticeable sign displaying their status as ‘Visitor’ at all times.**
- **Made aware of their obligations in compliance with the security policies of the bank.**
- **Escorted by the bank’s employees while accessing secure areas.**

2.1.8. The bank must ensure that a change request from the HR department is generated when there is a change of:

- **Duties or termination of contract of an employee, contractor or third party occurs, ensuring that employees, contractors and third parties return bank’s physical and logical assets.**
- **Access are amended/removed as appropriate.**

2.1.9. The bank shall ensure that user rights are restricted to the minimum of information an individual will need to fulfill their job requirements, as per least privilege and need to have principles.

2.1.10. The bank shall implement adequate controls to prevent employees, vendors, contractors and visitors from making unauthorized disclosures, misusing or corrupting information, as per the bank's security policies.

2.1.11. The bank should consider risk exposures from internal users, including altering data; deleting production and back-up data; disrupting/destroying systems; misusing systems for personal gain or to damage the bank; holding data hostage and stealing strategic or customer data for espionage or fraud schemes, as part of its risk assessment process.

2.2. Staff competency and training

2.2.1. The bank shall establish a security awareness program and allocate adequate budget for initiation, execution and maintenance of the program.

2.2.2. Content of security training and awareness shall be reviewed and updated at least annually to reflect new trends, new threats and changes in bank IT systems, and applicable laws and regulations.

2.2.3. The training program material shall include bank's security requirements; legal and regulatory requirements; business specific processes and controls; enforcement and disciplinary process; contact information for reporting security incidents, as well as the acceptable usage of information processing systems, including customer information educating them about cyber security risks and the protection measures at their level.

2.2.4. Security training material, IT Security policies, standards and procedures shall be made available, either electronically or in hard copy, to all bank employees and any relevant long-term onsite vendors/contractors acting in the same capacity as staff.

2.2.5. All employees of the bank, contractors and third party (long term or may be acting as staff) shall be provided with appropriate training regarding the bank's policies and procedures, as relevant for their job function, roles, responsibilities and skills.

2.2.6. The bank must provide the Information Security awareness training to the new employees as part of the wider induction program. Refresher training must be conducted on an annual basis at least. Employees shall be trained to recognize social engineering attempts and to not disclose any information that could violate the bank's policy.

2.2.7. The bank shall perform an assessment following the training to ascertain the effectiveness of the training program. The attendance records of the security awareness training programs along with the employee's acknowledgement of having received and understood the training, should be maintained. The bank shall ensure the commitment of the entire organization in managing cyber risks, and ensure awareness among staff at all levels. Senior management and board members shall be made aware of the nuances of cyber threats through appropriate training sessions.

2.2.8. The bank shall actively promote, among their customers, vendors, service providers and other relevant stakeholders, an understanding of bank's cyber resilience objectives, and require and ensure appropriate action to support their synchronized implementation and testing. Measures shall be taken to ensure that all the relevant stakeholders are aware of the potential impact of a cyber-attack and that they play a role in supporting the security preparedness of the bank.

2.2.9. The bank shall consider implementing a training awareness program to ensure security awareness:

- **Focuses only on the methods used by hacker for intrusions which can be blocked through individual action.**
- **Is updated on annual basis to represent the latest attack techniques.**
- **Is mandated for completion by all employees on an annual basis at minimum.**
- **Is monitored for employee completion.**
- **The bank shall opt to deliver the training through a computer based online training or class room based session.**

3. Cyber security in the Legal and Compliance department

3.1.1. The bank shall ensure that an information security and governance program is in place to address legal and compliance requirements pertaining to cyber security.

3.1.2. The bank shall comply with relevant current provisions of laws and regulations, and those which may be amended and added at a later date in time.

3.1.3. The bank shall ensure that an audit of its information systems (infrastructure, people and processes) is carried out at least once every year, or whenever it undergoes a change that may impact the security of the bank. The scope of the audit process shall include all information assets, people and processes. It shall be ensured that all non-conformance highlighted in audit/assessment are fixed within defined timelines.

3.1.4. The bank shall carry out a reassessment where any change or new finding invalidates or questions the current assessment. Full reassessment shall be carried out for major changes affecting the basic security design of a system.

3.1.5. The bank shall ensure that all infrastructure, people and processes are part of the audit. If an exemption is needed, a case shall be presented to the QCB/authority designated by QCB, defining scope of exemption, reason for exemption, risk analysis of exception and approval from the relevant head of department and the Risk department.

3.1.6. The bank shall put in place a well-defined organizational structure for addressing legal and compliance enforcement across the bank.

— **The Risk Management Forum at board-level needs to put processes in place to ensure that legal risks arising from cyber laws are identified and addressed. The forum must ensure that the concerned functions are adequately staffed and that the HR members are trained to carry out all relevant tasks.**

— **The bank must establish a legal function to advise the business groups on the legal issues arising out of use of IT with respect to the legal risk identified and referred to it by the Operational Risk Group.**

— **The Operational Risk Group must be established to address legal risks as part of an operational risk framework, and take steps to mitigate the risks involved in consultation with the bank’s legal functions.**

3.1.7. Legal risks shall be periodically communicated to the senior management and board/Risk Management Forum of the board. This shall be enforced by incorporating at a minimum the legal instruments listed below:

— **Identification of applicable legislation - all relevant statutory, regulatory and contractual requirements, and the bank's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system.**

— **Intellectual Property Rights (IPR) - appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect to IPR and on the use of proprietary software products.**

— **Protection of organizational records - important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual and business requirements.**

— **Data protection and privacy of personal information - data protection and privacy shall be ensured as required in relevant legislation, regulations and, if applicable, contractual clauses.**

— **Regulation of cryptographic controls - cryptographic controls shall be used in compliance with all relevant agreements, laws and regulations.**

3.1.8. The bank shall comply with Payment Card Industry Data Security Standard (PCI-DSS) and Payment Application Data Security Standard (PCA-DSS) standard.

3.1.9. The bank shall prepare an audit charter or policy to guide the internal audit function. The charter shall contain a clear description of its mandate, purpose, responsibility, accountability and authority of members in respect of an Information Security (IS) audit, namely the IS auditor, management and Audit Committee. Additionally, it must include relevant references to service-level agreements for aspects such as availability for unplanned work; delivery of reports; costs; grievance redressal; quality of service; review of performance; communication with the auditee; needs assessment; control risk self-assessment; agreement of Terms of Reference (ToR) for audit, reporting process and agreement of findings.

3.1.10. It shall be ensured that a well-planned, structured audit program is established to evaluate risk management practices, internal controls systems and compliance with policies concerning IT related risks. To achieve this, the bank must consider risk based internal audit and shall include understanding of IT risk assessment, IS audit planning, defining audit universe and scope of audit, execution, evidence of audit and documentation of audit.

3.1.11. The bank shall establish an organizational structure and reporting lines for IT and security audit in a way that preserves the independence and objectivity of the audit function.

— **The audit charter or policy, or engagement letter (in case of external professional service provider), must address independence and accountability of the Audit function.**

— **In case independence is impaired (in fact or appearance), details of the impairment shall be disclosed to the Audit Committee or board.**

— **Independence must be regularly assessed by the Audit Committee. In case of rotation of audit staff members from IT department to the IS Audit, care must be taken to ensure that the previous role of such individuals does not impact their independence and objectivity as an IS auditor.**

— **A follow-up process to track and monitor IT audit issues, as well as an escalation process to notify the relevant IT and business management of key IT audit issues, must be established.**

3.1.12. The bank must establish an audit cycle that determines the frequency of IT audits. The audit frequency should be commensurate with the criticality and risk of the IT system or process.

The maximum length for audit cycles, based on the risk assessment process for 'very high' to 'high risk' applications, can be at a frequency ranging from 6 to 12 months, medium risk applications can be 18 months (or below) and up to 36 months for low-risk areas. Audit cycles should not be open-ended.

3.1.13. The bank shall perform an impact assessment due to legal risks arising from cyber security incidents at least annually. This must consider impact in the event there is a data breach, litigation from shareholders, customers and suppliers. The legal risks must be discussed and remedial actions must be approved by the board.

3.1.14. The bank shall include application control audit in a risk based manner as part of regular internal audit with a focus on data integrity.

3.1.15. The bank shall define, adopt and follow a suitable risk assessment methodology which is in line with the focus on risks to be addressed as a part of the overall internal audit strategy. The methodology must detail upon audit scoping, execution, sample collection, analysis, resource management, documentation requirements, use of computer assisted audit techniques, reporting, escalation measures, communication guidelines, quality review and assurance.

4. Cyber security in the Procurement department

4.1.1. The bank shall define procurement policy for procurement of hardware, software assets and consulting services from a third party. The policy shall include guidelines and criteria to select vendors or service providers, contractual and cyber security requirements.

4.1.2. The bank, at the time of initiation of the procurement process, shall assess the vendor and evaluate whether controls are in place, such as ensuring the reliability of the third party company and that the technology chosen will not pose a risk to the business. The vendors shall be selected based on evaluation criteria with ethical conduct and due diligence.

4.1.3. The bank shall ensure that the contract with vendors includes clauses related to confidentiality, cyber security and right to audit. The agreements shall also clearly mention responsibilities, obligations and liabilities, bank policies, reference to standards to which vendors need to comply such as PCI DSS compliance for payment systems.

4.1.4. Security controls and provisions that apply to a bank must apply to vendors the bank engages as contractors, so that policies and regulations are inherited and shall be highlighted in any third party agreement.

4.1.5. The bank shall conduct independent audits of the vendors especially if a vendor has access to bank premises and systems on an annual basis at least, or a self-security assessment report shall be obtained from the vendors and evaluated.

4.1.6. Vendor devices and equipment must be hardened as per the hardening guidelines and internal checklists to ensure that default and insecure configurations are removed from the devices.

5. Cyber security in the Risk department

5.1. Risk management framework

5.1.1. The bank shall define and establish a risk management framework to manage technology risk. The framework should encompass the following:

- — **roles and responsibilities in managing technology risks**
- — **identification and classification of assets**
- — **identification and assessment of impact and likelihood threat, risk and vulnerabilities on bank systems and operations**
- — **development of a plan that contain policies, procedures and best practices that address risks**
- — **implement and regular testing of the plan**
- — **monitoring of risks and regular update of the plan to take into account the evolution of technologies, legal requirements and other mandatory requirements.**

5.1.2. The bank shall ensure that procedures are in place to test the effectiveness of risk management practices and internal controls on periodic basis. The implemented controls shall be monitored to ensure that the desired level of risk mitigation is achieved.

5.1.3. The bank shall establish an Information Asset Protection Policy, to ensure that the criticality of information system assets are identified and ascertained in order to develop appropriate controls to protect them.

5.1.4. The bank shall prepare a detailed inventory of information assets and classify the assets based on the information classification/sensitivity criteria. The assets inventory shall be kept up-to-date and include business information, customer information, business applications, supporting IT infrastructure and facilities hardware/software/network devices, key personnel, services etc. indicating their business criticality.

5.1.5. The inventory record of the assets shall include the following:

- — **clear identification of asset**
- — **location**
- — **security/risk classification**
- — **asset group and its owner**
- — **designated custodian.**

5.2. Risk assessment

5.2.1. The bank shall define a risk assessment process to identify threats and vulnerabilities to bank's environment and information assets, which comprises of internal and external networks, hardware, software, applications, system interfaces, operations and human elements. The bank shall define a risk assessment methodology/risk assessment process aligned to leading practices.

5.2.2. Following the risk identification, as per the risk assessment process, the bank shall perform an analysis and quantification of the potential impact and consequences of these risks on business and operations.

5.2.3. The bank shall develop a threat and vulnerability matrix, which includes cyber security threats, to assess the impact of threat to its environment. The matrix will help the bank in prioritizing the risks.

5.2.4. Security threats such as denial of service attacks, internal sabotage, malware infestation and other cyber security threats shall be a part of a threat register. The bank shall monitor such risks, as it is a crucial step in the risk containment exercise.

5.2.5. The risk assessment process shall define the risk appetite. Risk appetite is the defined level of risk that may be accepted by the bank.

5.2.6. Based on the risk assessment, the bank shall define a risk treatment plan to address the threats and vulnerabilities. The risk treatment plan and residual risk selected for information assets, with an aggregate level of high, shall be vetted by the senior management in the bank. Following risk mitigation and control strategies should be considered:

Avoid risk: It may be prudent to avoid risks altogether due to its inherent nature. For example, modify or terminate the process that induces risk.

Transfer risk: In some cases, it may be advisable to transfer the risk to another entity. For example transfer risk by insurance.

Mitigate risk: It is not possible, most of the time, to avoid or transfer the risk. In such cases, it is necessary to reduce the risk to an acceptable level by implementing controls.

Accept risk: Even after applying controls, the risk may still not be reduced to an acceptable level; in such cases, a bank may decide if they are prepared to accept the risk.

5.2.7. Risk assessment shall be integrated within business processes and revised whenever there are changes in the business environment or legal/regulatory requirements. Whenever there is a change in business environment, risk assessment must be performed to ensure that changes are aligned to the risk appetite.

5.3. Risk monitoring and reporting

5.3.1. The bank shall ensure that an effective procedure is in place to assess the effectiveness of the implemented controls. The process shall ensure that implemented controls remain effective in the changed scenarios and are able to meet the new challenges.

5.3.2. The bank shall maintain a risk register which facilitates monitoring and reporting risks. Risks with the highest priority should be monitored closely, with regular reporting on actions taken to mitigate them. The risk register shall be reviewed and updated periodically.

5.3.3. To facilitate risk reporting, the bank shall develop a risk matrix to highlight systems, processes or infrastructure with the highest risk exposure. The bank shall consider risk events, regulatory requirements and audit observations when determining risk matrices.

5.3.4. The bank must consider various threat intelligence feeds, both from internal and external sources, to ensure that risk mitigation measures for the new and evolving risks are put in place.

6. Business continuity management

6.1. BCP/DR considerations

6.1.1. The bank must ensure compliance to the QCB *BCM Circular Part (VII) - Instructions of Supervision and Control Section Eleventh: Business Continuity*. Additionally, the BCM policy, procedures and plans shall be formulated in line with a global standard such as ISO 22301, and it must be updated with the latest standards.

6.1.2. The bank must formulate an emergency response plan that details evacuation procedures, command center operations, media and communications strategy.

6.1.3. At a minimum, the banks must identify threat scenarios, natural and man-made (including cyber) and put in place incident management procedures.

6.1.4. A senior management official must be appointed and designated by the bank as head of the BCM function (team, committee, etc.), who must be responsible for the following:

- **Creation of a BCM plan that includes necessary planning to include the recovery maintenance of all aspects of the business functions.**
- **Regularly updating BCP plans based on changes in business models, audit recommendations and key learnings from BCM drills.**
- **Ensure that Business Impact Analysis (BIA), risk assessment, monitoring and testing are performed on at least on an annual basis. The types of testing are defined in Section 6.1.9.**
- **Evaluate all factors and advise senior management on declaration of a ‘crisis’. A crisis management plan shall be defined and roles and responsibilities communicated to stakeholders.**

6.1.5. A committee consisting of senior officials from departments such as IT, HR, Legal, Business and Information Security must be formed to exercise, maintain and invoke BCM plans during drills and crisis situations. Additionally, it must be ensured that they are responsible for the following:

- **BCM communication, training and awareness across organization**
- **review of the BCM plan to ensure its completeness**
- **review and liaise over BCM budgets**
- **coordination of recovery, continuity and response teams, and handling key decision-making**
- **determine BCP activation.**

6.1.6. The bank must ensure the formation of teams for various aspects of BCP, such as incident response, IT, damage assessment, logistics and administrative support at central office, standalone offices and at a branch level, as required.

6.1.7. The bank must formulate a formal strategy for communication with key stakeholders such as regulators, investors, customers, counterparties, business partners, service providers and the media. Activities outlined in the strategy must include:

- **A well trained media relations spokesperson shall be designated by the bank to provide information to stakeholders via communication channels**
- **The bank must prepare draft press releases and communication templates as a part of their BCP.**
- **Communication drills must be regularly exercised as a part of BCM drills.**

6.1.8. As an essential component of effective BCM, bank shall test their business continuity plans to evaluate their ability to recover operations in the event of a major disruption. Accordingly, the bank should comply with the following:

- **Testing business continuity plans and strategies, BCM updating should be conducted on at least an annual basis.**
- **Tests relating to the nature, scope and frequency shall be determined by the criticality of the applications and business functions, the bank's, role in broader market operations and the material changes in the bank's business. Testing shall identify the need to modify the bank's responsibilities, systems, software, hardware, personnel and the external environment.**
- **The test program shall incorporate conducting tests from alternate sites with the relevant systems, devices, and personnel. In addition, testing is also essential for promoting awareness, familiarity and understanding among key personnel of their roles and responsibilities in the event of a major operational disruption**
- **Internal audit shall assess the effectiveness of the bank's testing program, review test results and report their findings to the Audit Committee**
- **External auditing shall be undertaken annually by an independent experienced auditor and should include assessment of the bank's testing programs effectiveness in the view of the recent international practices and standards,**

- **The bank must, at minimum, conduct four unplanned BCM drills (at least one hot test and three cold tests) on an annual basis, with only a restricted set of identified personnel being made aware of the drill. The bank shall incorporate test results and key learnings from these drills to tailor their BCP plan. The hot test shall be a full simulation test, where all activities are relocated from the original site to the alternative site (announced or unannounced); all necessary employees, suppliers, the moderator, observers and auditors will participate. The cold test shall be conducted so that certain components of the BCP are tested based on the criticality of the business requirements.**

6.1.9. Annual BCP testing shall include the following:

- **Table-top testing – discussing business recovery arrangements using example interruptions.**
- **Simulation testing – to train personnel in post incident and crisis management roles.**
- **Technical recovery testing – to ensure all information systems can be restored effectively. This may also include component testing which is an in-depth testing of individual components, such as ATM switch testing.**
- **DR testing – business operations to be run in parallel from DR site.**
- **Tests of supplier facilities and services – to ensure contractor and vendor Service Level Agreements (SLAs) are met, as per contract.**
- **Complete rehearsals – to test if the organization, personnel, equipment, facilities and processes can cope with a crisis situation.**

6.1.10. The bank shall provide an approved copy of the BCP to the QCB on annual basis which must include summary of BCP results describing the status of bank IT systems, key BCM learnings and the bank’s strategy to implement them.

6.1.11. The bank must have procedures in place to ensure the recovery of key critical systems, applications and its related infrastructure. DR plans and processes should include a full description of bank IT assets, data, information system and information flow, including recovery mechanisms. Key resources and documentations should be rendered available in times of crisis, according to the overall BCP strategy of the bank and QCB instructions.

6.1.12. The bank’s BCP/DR capabilities must support the bank’s cyber resilience objectives and must enable the bank to recover rapidly from cyber-attacks to safely resume critical operations aligned with defined and measured recovery time objectives (RTO) while ensuring security of processes and data. Additionally, collaborative and coordinated resilience testing must be performed with vendors and partners to ensure the readiness of such capabilities in all interconnected systems and networks.

6.1.13. As cyber risk is different from many other risks, the traditional BCP/DR arrangements may not be adequate. A Cyber Crisis Management Plan (CCMP) must be immediately formulated by the bank. The CCMP must include the four aspects, i.e. detection, response, recovery and containment of cyber attacks.

6.1.14. The bank shall deploy measures to prevent threats and cyber-attacks and to promptly detect any cyber intrusions so as to respond/recover/contain the fall out. The bank shall be prepared to face emerging cyber threats such as 'zero day' attacks, remote access threats and targeted attacks. Additionally, the bank shall take necessary preventive and corrective measures in addressing various types of cyber threats, such as DDoS, ransomware/crypto ware, malware, spam, spear phishing, vishing frauds, drive by downloads, browser gateway fraud and password related frauds. In addition to this, communication strategies must be documented to respond to such attacks.

- **The CCMP must include documented incident response procedures, including the roles, responsibilities and response strategies to meet various incident scenarios based on situational awareness and potential/post impact, consistent communication and coordination with stakeholders during response. Additionally, the bank must also provide specialized training to personnel handling incidents, post incident review and periodically test incident response plans. The bank shall implement an effective Incident Response Program approved by the board/senior management.**
- **The CCMP must define incident severity, type of incidents, indicators of compromise (IOC), method of detection, incident reporting channels, periodicity of monitoring, collection/sharing of threat information, expected response in each scenario/incident type. Additionally, the bank must establish and implement systems to collect and share threat information from local/national/international sources.**
- **Cyber Crisis Management Plan (CCMP) must define controls to quarantine the affected devices and systems.**

6.1.15. The bank must take effective measures to prevent cyber-attacks and to promptly detect any cyber-intrusions so as to respond/recover/contain the fall out.

6.1.16. ’Work from home’ arrangements should not be considered for employees performing critical functions .However, if required, high privileged users shall only be allowed to connect with prior approval and on an as-needed basis.

7. Compliance with QCB circular

7.1. Reporting compliance to QCB circular

7.1.1. The bank shall prepare a reporting framework based on this circular. A compliance report based on this framework shall be submitted to QCB on an annual basis at a minimum.

7.1.2. The material gaps in controls shall be identified, and remedial actions taken under the guidance of the board/board authorized committee shall be initiated immediately. Should the advisory and recommended requirements not be met, an action plan to address these shall be documented and shared with QCB. The action plan shall be adequately supported by placing mitigation measures. The report needs to be duly signed by the board/board authorized committee.

7.1.3. QCB reserves the right to audit the bank to ensure compliance to this circular at any point in time.

7.2. Exception handling

7.2.1. In case the bank seeks an exception to any mandatory requirement in this circular, the bank shall provide a suitable business justification for these requirements. These justifications shall be approved by the board/board authorized committee.

8. IT operations

8.1. Change management

8.1.1. The bank shall define a Change Management Policy and supporting procedures. The policy shall include planned major changes, maintenance and minor changes and emergency or unplanned changes across hardware, software and infrastructure. All changes shall be documented along with 'rollback' procedures and its impact on business shall be assessed before implementing them in bank's environment.

8.1.2. The Change Management Policy shall also include classification of changes to ensure proper use of resources required to execute a change.

8.1.3. A cross functional Change Management Committee shall be formed which include representatives from various business divisions/functional units, process owners, and must include representation from the Information Security and Risk Management functions.

8.1.4. The Change Management Committee shall assess if the system requires reassessment in the event that the change has an impact on the security posture of the bank. Risk analysis shall be conducted as part of a change process to keep residual risk at an acceptable level.

8.1.5. The bank must adequately test the impending changes and ensure that it is accepted by the stakeholders and users by performing User Acceptance Testing (UAT) prior to migration to production systems. The bank shall develop and document appropriate test plans for impending changes. Explicit sign-off must be obtained from the users on test results prior to implementation of change in the production.

8.1.6. It must be ensured that the person requesting the change is not the same individual who is implementing the changes, and the changes must be implemented by skilled and competent individuals.

8.1.7. Separate physical and logical environments for systems development, testing, staging and production must be established and maintained.

8.1.8. Post successful implementation of the change in production environment, the change shall also be replicated in the disaster recovery system/environment for consistency and resilience.

8.1.9. The Change Management Committee must ensure that post implementation of the change, all related processes and system related information is documented and updated.

8.1.10. Following implementation of the change, verification of the changes shall be carried out to confirm that the change has met its objective, and there have been no unexpected side effects.

8.1.11. The bank should ensure that a logging facility is enabled to record activities that are performed during the change process. It is recommended that the bank reviews the change management process and change classification structure for effective change management at least once every six months.

8.2. Incident management

8.2.1. The bank shall establish an incident management framework and define an Incident Management Policy and procedures to protect, detect, evaluate and respond to cyber incidents. At minimum the procedures shall include following:

- **Procedure for the detecting, monitoring and reporting of cyber incidents shall be defined. Tools for network monitoring, intrusion detection/prevention systems shall be configured to automatically alert and report suspicious events, both IT and non-IT incidents.**
- **Evaluation of a cyber incident shall be performed to assess if an incident is a false trigger or hoax, type and extent of the problem.**
- **Prioritization of the cyber incident, as per severity, and an action plan shall be prepared accordingly.**
- **Identification of the source of the problem, vulnerability that caused the incident or breach and containment of the breach, shall be documented.**
- **Evaluation of damage done if the breach has already occurred and estimation of rough schedule of recovery or control measures.**
- **Restoration of the services following resolution of the incident, and monitoring of the system for any further problems.**

8.2.2. The bank shall identify dedicated resources to handle incidents and roles/responsibilities of staff involved in the incident management process shall be defined and documented, which include recording, analyzing, remediating and monitoring incidents.

8.2.3. The bank shall appoint a person who owns and manages the incident management program, including point of contact for information security communications. The person shall be completely responsible for the functioning of the incident management program, including managing budget, defining the program and executing program.

8.2.4. The incident management program shall adequately address all incidents within corresponding resolution timeframes and monitor all incidents as per the incident management framework.

8.2.5. Incidents shall be classified and prioritized according to criticality to ensure uniformity and optimum resource utilization. The bank shall establish corresponding escalation and resolution procedures where the resolution timeframe is commensurate with the severity level of the incident. The bank shall delegate the function of determining and assigning incident severity levels to a centralized incident response team.

8.2.6. The bank shall perform root cause and impact analysis and shall take measures to address major incidents which resulted in severe disruptions. Root cause analysis shall include timelines of incidents, revenue loss, costs, number of customers affected, implications and consequence to reputation and confidence, corrective and preventive measures.

8.2.7. Evidence related to incidents shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s) where follow up action against a person or organization involves legal action.

8.2.8. A communication plan and procedure to report information security incidents internally and externally (QCB and other agencies, such as the Ministry of Interior) shall be defined. The bank shall also include all relevant functions such as Public Relations or Communications in their incident response procedure and communication plan.

8.2.9. The incident management process shall be integrated with security awareness training. All users must be trained to report any incidents to the incident management team, and trained to respond to certain incidents (e.g. fire, natural disasters).

8.2.10. All critical incidents must be reported to QCB and the relevant governmental authorities within 1 hour of identification.

8.2.11. The predetermined escalation and response plan for security incidents shall be tested on an annual basis to simulate how the organization responds to cyber-attacks, such as ransomware, extortion, DDoS and Level 1 severity incidents. These tests shall be carried to check the efficiency of the processes and the incident response plan.

8.2.12. All information regarding incidents shall be compiled and documented. Lessons learned during an incident shall be identified and evaluated to be used to improve incident handling process.

8.2.13. The bank shall raise customers security awareness through notifications, press releases etc.

8.2.14. The bank shall keep the QCB and MOI informed of any incident, such as large scale cyber incidents; where proactive measures can be initiated and the security risk to the financial sector can be minimized.

8.2.15. The bank shall consider an IT Infrastructure Library (ITIL) framework to enhance the incident management process.

8.3. Patch management

8.3.1. The bank shall define a patch management process which includes roles and responsibilities, methods of obtaining and validating patches, assessing impact of patches and the process to deal with failed deployment of patches. At a minimum, the patch management process and procedure shall include:

— **Methods of obtaining and validating patches to ensure that they are obtained from an authorized source.**

— **Identifying the vulnerabilities that are applicable to application and systems used by bank.**

— **Assessment of the business impact of implementation and non-implementation of the patches.**

— **Testing of the patches and methods of deployment of patches.**

— **Procedures and methods to deal with failed deployment of patches (for e.g. rollback, redeployment)**

8.3.2. The bank shall ensure that all products, such as operating systems, network and infrastructure devices, security software, and remote access computers are updated and patched regularly, in accordance with patch management policy/process. The upgrades and updates shall be performed after a due risk assessment and shall be in line with bank’s Change Management Policy.

8.3.3. The bank shall continuously monitor the release of the patches by vendors and OEMs. If the patches are released for protection against any well known, publicly reported vulnerability or attack, the bank shall have the mechanism in place to apply them expeditiously following an emergency patch management process.

8.3.4. The bank must ensure that the critical patches are tested in a test environment before implementing in production systems. If such patches break critical business applications on test machines, the organization must devise other mitigating controls that block exploitation of the system.

8.3.5. It must be ensured that appropriate methods are established to protect information systems if no patch is available for an identified vulnerability, for example disabling services, adding additional access controls.

8.3.6. The bank shall measure delay in patching new vulnerabilities and ensure that the delay in patching is not beyond the baseline set by the organization.

8.4. Logging and security monitoring

8.4.1. The bank shall define a policy for logging and security monitoring, which includes (a) identification (b) continuous monitoring and (c) logging of access, changes and modification to information systems. The process shall define the IT assets and processes that shall be monitored and logged.

8.4.2. The bank must employ suitable processes/technology for enabling continuous monitoring of information system assets, such as applications, network and infrastructure devices and servers. The process shall include a clear allocation of responsibilities for regular monitoring of the assets.

8.4.3. The bank shall ensure that monitoring practices are established based on the criticality of the information, processes and infrastructure, and 4 eye principle shall be in place to monitor processes.

8.4.4. Logging must be enabled on all infrastructure and data processing equipment, and applications that are associated with access, transmission, processing, security and storage of critical information. Access to the logs shall be restricted to prevent modification or deletion. Integrity of the logs shall be monitored continuously.

8.4.5. The bank shall establish and implement a Security Operations Centre (SOC) functioning 24x7 onsite or in Qatar, for the centralized and coordinated monitoring of cyber risks and management of security related incidents.

8.4.6. Audit trails of daily activities of users, such as system administrators and users with elevated privileges, shall be reviewed in case of an alert/ incident.

8.4.7. The logs must be retained for a minimum of six months (180 days) and the maximum depending on criticality of the system/application and as per local laws and regulations. The logs shall include basic elements such as date, time, command executed, IP address and authentication information to ensure that adequate information is available to assist reconstruction of an incident, if required. The bank shall ensure that all logs must be monitored via automated systems and through SOC and logs with significant interest shall be reviewed manually.

8.4.8. User access reviews shall be performed on a semi-annual basis to disable or remove accounts that are no longer required or assigned to any user.

8.4.9. The bank shall implement a Security Information Event Management (SIEM) system to collect, aggregate, correlate and perform analysis of disparate data from various sources and an alert in case suspicious events are detected.

8.4.10. The bank shall implement enterprise log repository solutions for managing, aggregating and retention of logs efficiently.

8.4.11. If the bank has outsourced monitoring and event management services to a Managed Security Service Provider (MSSP), the bank shall obtain as much information as possible on the incident from the MSSP and implement the security measures suggested by the provider.

8.4.12. Logs containing personal information shall have the appropriate privacy protection measures in place and shall be in line with the proposed information privacy and protection law.

8.4.13. It must be ensured that all monitoring and logging activities are in line with the various regulatory and legal frameworks.

8.4.14. The bank must ensure that security logs of the systems and applications are classified according to their criticality. Access controls should be defined to ensure that security logs are protected from unauthorized access and tampering.

8.4.15. System monitoring processes must be integrated with incident handling, exceptions observed should be recorded and acted upon as per the incident management process.

8.4.16. The bank shall implement network surveillance and security monitoring with use of network security devices, such as intrusion detection and prevention systems to protect the bank against network intrusion attacks.

8.5. Capacity management

8.5.1. The bank shall define capacity management policy to set out guidelines for system utilization threshold, system performance and corresponding precautionary measures. The following key activities shall be included as part of capacity management, at a minimum:

- **Capacity plan which depicts current level of resource utilization and service performance and for casting of future requirements.**
- **Guidelines for translating business needs into requirement for IT service and supporting infrastructure.**
- **Guidelines for management, control and prediction of end to end performance and capacity of live and operational IT service usage.**
- **Guidelines to identify and understand the performance, capacity and utilization of individual component within a technology used to support IT services.**

8.5.2. The bank shall define and implement a process to ensure that system performance is continuously monitored to determine if the system meets or exceeds the agreed performance targets.

8.5.3. The capacity planning shall take into account the possibility of a sudden upsurge in transactions during particular timings or situations, and diagnosis of performance and capacity related incidents and problems.

8.5.4. Impact of the changes on the systems shall be assessed and determined on the basis of its effects on capacity planning and performance of IT services.

8.5.5. The bank shall implement tools/scripts on technology systems to continuously monitor and capture the CPU, network and memory utilization. This will also be useful when casting for upgrades or technology refresh.

8.5.6. Capacity planning shall be extended to include backup systems and disaster recovery environment and facilities.

8.6. Problem management

8.6.1. The bank shall implement a problem management framework to minimize the adverse impact of incidents on IT Infrastructure and business by identifying root cause; logging known errors and providing and communicating work around them;

finding permanent solutions and preventing recurrence. The problem management process shall include following:

- **Process to perform root cause analysis of an incident and determine resolution.**
- **Implementation of solution through change management and release management.**
- **Turnaround and resolution for incidents that cannot be resolved due to business case or technical short fall.**
- **Periodic trend analysis of the problem with respect to customer or system facing channels.**

8.6.2. The bank shall establish roles and responsibilities of staff involved in the problem management process. The bank must identify, classify, prioritize and address all problems in a timely manner and within predefined service levels.

8.6.3. A helpdesk shall be set up to provide front line support to users on all technology related problems and to relay the problem to the relevant IT functions for investigation and resolution.

8.6.4. Problem management shall include activities required to identify root cause, finding permanent solutions and preventing the recurrence of incidents.

8.6.5. The bank shall consider an ITIL framework to enhance the problem management process.

8.7. Data backup management

8.7.1. The bank shall define a process for data backup and archiving critical business information and shall include frequency of data backup and archiving, details of backup media, access privileges to backup and classification. The backup and archiving policy shall be in line with local regulations.

8.7.2. The bank shall implement a backup process and archiving technologies to enable backup and retrieval of critical business information. The bank shall implement the following strategies for protection of data:

- **Backup the data on tapes and sent offshore.**

- **Backup made on disks to be copied to offsite disks or made directly to offsite disks**
- **Replication of data to an offsite location.**
- **High availability systems that keep both data and system replicated offsite at real time.**

8.7.3. The bank shall encrypt backup tapes and disks containing sensitive information before they are transported to offsite storage.

8.7.4. The bank shall carry out semi annual testing and validation of recovery capability of backup media, and assess if backup media is adequate and effective to support the bank’s recovery process.

8.8. Technology refresh management

8.8.1. The bank must establish an IT refresh policy and shall be approved by management. The policy must consider standardization; a refresh plan; cycles and timelines; hardware and software acquisition; decommission and disposal.

8.8.2. The bank must maintain an up to date inventory list of software and hardware components used in production and the disaster recovery environment, which includes all relevant associate warranty and other support contract-related information.

8.8.3. The bank shall establish a technology refresh plan and actively monitor its IT systems and software, so that outdated and unsupported systems which increase exposure to security risks are replaced and/or upgraded on timely basis.

8.8.4. The bank must track and monitor a product’s end of life (EOL) and end of support (EOS) dates, and phase out or upgrade the outdated devices. The bank shall also perform risk assessment of these systems to assess the risk of continued usage of the systems and establish mitigating controls where necessary.

8.8.5. The bank must maintain the inventory list of software and hardware components in UAT, test, staging, store and stock.

8.9. Cloud computing

8.9.1. The bank must establish a cloud computing policy and should be approved by management. The policy must be further reviewed periodically. The policy should cover details on applications and data that will be hosted in cloud environments with their potential risks and risk of the cloud service providers infrastructure, process and operations.

8.9.2. The agreement with the cloud service provider shall cover at a minimum: (a) contract cancellation and modification fees, (b) additional overhead costs, (c) run-away costs from poor planning, (d) data leakage from malicious sources (,external or insider), (e) unauthorized data access by service provider, (f) data leakage due to shared infrastructure, (g) lack of encryption controls, (h) monitor for operations and security compliance, (i) cloud migration plan, (j) cloud transition to a second provider, (k) service roll back plan, (l) notification/alert mechanisms in place in the event of requests to access data by any other third parties or governments.

8.9.3. The policy must take into consideration, risk factors of which geography and jurisdiction the data hosted/backed up at the cloud service provider will physically reside.

8.9.4. The bank must obtain periodic security compliance reports on the VM instance/cloud service and overall security of the cloud service provider.

8.9.5. The bank must obtain International Standard on Assurance Engagements (ISAE) or assurance reports on the security controls incorporated from a services organization perspective.

8.9.6. Use of cloud computing services shall not be used as justification to delegate the risk controls that surround the data/system that is deployed in the cloud. Several risks exist and shall be considered when accessing cloud services including: data leakage, data interception, intrusion/unauthorized access, cloud application interfaces risks, integrity of data and availability of cloud services or legal risk.

8.9.7. The bank must seek the existence of the following key security domains, via documentation evidence, prior to contracting with a cloud service vendor: access controls, auditing, authentication, awareness and education, business continuity, configuration management, data security, incident management, maintenance and support, media protection, personnel security, physical security, planning, procurement, risk management, security assessment, system security and integrity controls.

8.9.8. The bank must make sure critical data is not stored in a non-controlled cloud environment. Private cloud facility under control of the bank shall be considered as an alternative.

8.9.9. When using cloud computing, the bank must make sure that the agreement with the cloud computing service provider contains key security controls limiting the aforementioned risks.

8.9.10. While performing due diligence for the cloud computing service provider, the bank shall consider attributes and risks specific to cloud service, such as sovereignty, platform multi-tenancy, recoverability, regulatory compliance, auditing and data offshoring.

8.9.11. The bank shall have contractual power to conduct a penetration test on the Virtual Machine (VM) image/infrastructure and application instance provided to the bank by the cloud provider, if feasible.

8.9.12. The bank must have the contractual power and the means to destroy data stored within the service provider's systems and backup, in event of contract termination or expiry.

8.9.13. The bank shall have contractual power to conduct a penetration test and audit of the cloud provider's Layer 3 (L3) switch connected to the VM image/infrastructure and applications provided to the bank.

8.9.14. The bank shall verify the service provider's ability to recover the outsourced systems and IT services within the stipulated Recovery Time objective (RTO) prior to contracting with the service provider.

8.10. Access controls

8.10.1. General principles

8.10.1.1. The bank shall define the access controls policy and relevant procedures which shall include identification, authentication and authorization of users.

8.10.1.2. The policies shall be based on the concepts of Role Based Access Controls (RBAC) and least privilege, and governed by the principles of 'need-to-know' and 'need-to-have' basis for logical access.

8.10.1.3. The segregation of duties principle shall be used to minimize the conflict of interest. In the same manner, systems must allow application of the 4 eye principle. Segregating the roles through user account privileges based on roles is a key process in minimizing unauthorized access or change on bank systems or applications.

8.10.1.4. The bank shall implement job rotation and cross training to minimize risk of dependency and coercion to commit fraud.

8.10.1.5. The bank shall document processes for dealing with lost, stolen or compromised passwords and users are made aware of the process. The policy shall require users to change the password after theft or compromise, notification to the information security team and identification of the user before replacement of the password.

8.10.1.6. Any accounts processing critical information must be audited periodically to ensure that they are current and up to date. The audit shall confirm that, in cases where an employee's status, roles and responsibilities have changed due to promotion, demotion, transfer, termination etc., these changes are reflected in the system.

8.10.1.7. Access rights of users to create, update, delete or transmit information shall be based on access control matrix defined by business rules. The access control matrix shall be defined by the owner of the information or the system.

8.10.1.8. The bank must implement a division of responsibilities over sensitive security processes and tasks, using principles of least privilege and 4 eye principle to ensure the avoidance of a single individual having full control over critical processes or tasks.

8.10.1.9. Logical access to bank's networks must be controlled. Additional controls such as Network Access Control (NAC) should be deployed to ensure that access is restricted to authorized devices/services.

8.10.1.10. The bank must implement banners that: a) Proclaim that access is only permitted to authorized users; the user has to abide by the relevant security policies and the system is monitored, b) Defines acceptable usage of the system. c) Spells out legal ramifications against misuse of the system.

8.10.1.11. Effective controls shall be in place to mitigate bypass/compromise of the access control system to gain access to information. If bypassing the access control mechanism is required, proper approval should be sought from the appropriate authorities. Any unauthorized attempts to circumvent access controls shall be perceived as security incidents and shall be dealt with under incident response procedures, as well as HR policy and procedures.

8.10.1.12. The bank shall ensure that no-one has concurrent access to both production and backup systems. It must be ensured that any person who needs access to backup files or system recovery resources is duly authorized for a specific reason and timeframe.

8.10.2. Identification and authentication

8.10.2.1. The bank must ensure that all users, contractors, third party and temporary staff are identified by a unique identifier to ensure the actions are accountable and traceable. These identified users must be held responsible and accountable for actions performed using their IDs.

8.10.2.2. Anonymous guests and shared accounts carry a potential risk of non-repudiation and therefore their use should be discouraged. In cases that such accounts are necessary due to system limitations, operational procedures or emergency access they should be tightly controlled by technical or procedural mechanisms.

8.10.2.3. Default accounts, such as admin, root, operator, etc., where technically feasible, must be renamed and the default password must be changed. All the changes must be documented.

8.10.2.4. All user accounts, including privileged accounts, should be monitored and logged for historical purposes.

8.10.2.5. In case there are technical, or any other limitation to assign unique IDs, the bank must ensure that the shared IDs are tied to authorized users based on factors such as time of use, location etc.

8.10.2.6. Any individuals who are not an employee, contractor or third party must not be granted user account access or given any privilege within the bank's system. Any exceptions to this must be approved by the proper authority.

8.10.2.7. Access to the system shall be managed and controlled through an appropriate authentication mechanism, such as password, access card etc. Based on sensitivity, the system owner shall implement multifactor authentication.

8.10.2.8. User access rights to create, read, update, delete or transmit the bank's information assets shall be based on an access control matrix defined by the business rules established by owners of the information.

8.10.2.9. It must be ensured that system authentication data, while in use, is protected and it is not susceptible to attacks such as replay, man in the middle and session hijacking.

8.10.2.10. The bank shall define password policy and related procedures, such as password reset. The password policy shall employ best practices, and enforce strong and complex password creation and take two factor authentication into consideration.

8.10.2.11. Password must be changed at least every 60 days and minimum age of 1 day. It must be ensured that users are forced to change the password at logon after expiry or after reset. In addition to this, controls should be implemented to ensure that the system complies with password policy.

8.10.2.12. Systems or devices must be configured to lock the screen as per the bank's policies.

8.10.2.13. Access to the system must be suspended after no more than three failed authentication attempts, to prevent the guessing of passwords by brute forcing. The login must be delayed for at least 30 minutes after the suspension of the account.

8.10.2.14. There must be a policy in place for users of locked accounts to contact the helpdesk for resetting passwords post confirmation and verification of users.

8.10.2.15. Accounts that are not active for more than 60 days must be suspended. In case account is no longer needed, necessary actions shall be taken to initiate deletion of the account from the system.

8.10.2.16. It must be ensured that an audit trail is enabled for accounts processing highly classified information; Audit trails such as all successful and failed logins shall logged for and shall be reviewed in case of an alert/ incident.

8.10.3. System access

8.10.3.1. The bank shall define standard operating procedures for system access with details on which data type can be accessed by whom (users or groups), within which timeframe (schedules) and method of access (internal, external, VPN). The bank shall also define the type of access local/remote, access to employees, contractors, third parties and vendors.

8.10.3.2. The bank shall also define the approval process for system access and related access controls.

8.10.3.3. The bank must ensure that system users are vetted in line with the requirements specified in personnel security requirements.

8.10.3.4. The bank shall put in place controls to educate the users on their responsibilities, security awareness and acceptable usage prior to providing them with access to the system.

8.10.4. Privileged access

8.10.4.1. System management logs shall be configured to record activities performed by privileged accounts. The activities shall include sanitization activity; system start up and shut down; system failure; maintenance activities; backup and archiving activity; system recovery activity and out of office hour activity.

8.10.4.2. System administrators shall be assigned a different user account for performing normal day to day activities. Users with privileged access must be closely supervised and all their system activities logged and reviewed periodically

8.10.4.3. Updates, additions, deletions of privilege user accounts and/or passwords must be notified to the director and Information Security Officer (ISO), approval for changes must be provided by the director and ISO.

8.10.4.4. Post approval and changes reflected, the ISO must update the master list of privileged users and their access boundaries.

8.10.4.5. Privileged account users must not have access to the system logs in which their activities are being logged. Privileged accounts must not be shared between multiple users.

8.10.5. Remote access

8.10.5.1. The bank shall not provide remote access to its users unless it is warranted by business requirements and authorized by the relevant department head and the security team/department. Risks associated with this shall be considered before providing remote access to users.

8.10.5.2. Two factor authentication must be used when accessing critical systems via remote access.

8.10.5.3. Remote access sessions must be encrypted from end to end to secure information in transit. Encryption must begin with the initiation of session and must include all user identification and authentication, and not end until the session is terminated.

8.10.5.4. It must be ensured that users cannot remotely access the organization’s system without sufficient controls such as personal firewall and anti-malware software to protect user sessions.

8.10.5.5. Security software on the remote access systems must be patched and kept up to date.

8.10.5.6. Reconfiguration of a remote access system for the purpose of split-tunneling or dual homing shall not be permitted.

8.11. System usage security (acceptable usage)

8.11.1.1. System users shall be responsible for information assets provided to them to perform their daily job responsibilities. They shall handle and operate the information assets in line with the bank's acceptable usage policy.

8.11.1.2. Users shall be made aware that resources provided by the bank, including access to the internet, are for business purpose. Personal usage of the assets shall be prohibited and governed by policies of the bank.

8.11.1.3. The bank shall define an acceptable usage policy for its information assets, including the internet and email.

8.11.1.4. The bank must make sure that security controls are put in place to protect information systems assets against all types of cyber-attacks.

8.11.1.5. The bank shall define policy and procedures for the usage of social media, forums etc.

8.11.1.6. The bank must make sure that users, third party, contractors are educated on the acceptable usage of information assets and usage of the internet and email provided to them. The bank shall ensure that security awareness courses conducted by them highlight effective usage of the internet and email.

8.11.1.7. Public web based email services shall not be used to send emails from the bank's systems.

8.11.1.8. The bank shall ensure that external recipients or originators understand and agree on the usage of classified data. Non-disclosure and confidentiality agreements shall be signed with external parties and necessary risk assessments shall be conducted before exchanging data with them.

8.11.1.9. The bank shall implement controls to prevent access to unauthorized web sites and downloading and installation of unauthorized software on the user's workstations.

8.11.1.10. The web access shall be provided through secure proxies and filtering gateways.

8.11.1.11. Email shall be protected against potential threats, such as viruses, phishing and spam. The bank shall implement email gateways to filter and manage the email and its contents.

8.11.1.12. The bank shall educate users in basic security hygiene to further enhance its security posture and shall follow the guidelines below, at a minimum:

a. Users shall log off the online session after completion of tasks.

b. Users shall not install software or run programs of unknown origin.

c. Users shall delete spam or chain emails and report them to bank’s security team.

d. Users shall not open email attachments from strangers and shall report them to bank’s security team.

e. Users shall be sensitized to social engineering practices and shall be educated to not to divulge their personal and financial information to untrusted sources.

8.11.1.13. Use of email on the public forums and non-work related web sites must be restricted. The user shall ensure the emails are suitably classified, as per the bank’s classification policy.

9. Enterprise security

9.1. Network and infrastructure security

9.1.1. Network and infrastructure device management

9.1.1.1. A High Level Diagram (HLD) covering the overview of network and security architecture of the bank and a Low Level Diagram (LLD) showing detailed connections of this architecture, shall be maintained by the bank. Additionally, it must be reviewed on every significant network change, or on quarterly basis.

9.1.1.2. The bank shall maintain a detailed inventory of network devices, servers and workstations, as per asset management guidelines.

9.1.1.3. Establishing a network protection strategy and layered security based on the principle of ‘defense in depth’ is an absolute necessity for a bank. The bank must ensure that networks are designed as per ‘secure by design’ paradigm in order to limit the compromise of confidential information. This shall be achieved by following leading practices, industry wide benchmarks and vendor recommendations, and include the following:

a. Network must be segregated physically using routers, switches and firewalls and logically using (VLANs. Switches must be deployed instead of hubs in order to prevent network sniffing on the same subnet.

b. At minimum, port security, MAC filtering or sticky MAC address must be configured on routers, switches and wireless controllers to prevent unauthorized access and enhance security posture. Additionally, unused network ports must be disabled.

c. Single point of failure must be identified and eliminated in the production network.

d. Network control and management traffic such as SSH, SNMP must be transmitted through a separate management VLAN or a physically separate segment.

e. Infrastructure changes must be performed and executed, as per the guidelines specified in the change management section.

f. The bank must ensure that configuration of network devices is documented and updated post every change. Controls must be enforced to ensure that the configuration is reviewed on a quarterly basis to identify any unauthorized changes. Additionally, the running configuration of network devices must be compared against the documented configuration to ensure its integrity.

g. Network edge authentication, such as 802.1X, NAC must be implemented to prevent unauthorized access to the bank network.

h. The bank must implement Intrusion Prevention and Intrusion Detection systems (IPS/IDS) in their critical internal and external network segments to prevent/detect network attacks.

i. The bank must establish a 24/7 network and security operations center (SOC) for the monitoring of network and infrastructure devices.

j. Management access to the network and infrastructure devices must be provisioned through secure channels, such as SSH, IPSEC through multifactor authentication, wherever applicable.

k. An Authentication, Authorization, and Accounting (AAA) server must be deployed for managing access, enforcing policies and auditing usage of network, security and infrastructure devices.

9.1.1.4. Audit trails of daily activities for critical devices must be maintained and reviewed in case of an alert/ incident.

9.1.1.5. Vulnerability assessment and penetration testing of infrastructure and network devices must be performed on a semi-annual basis as specified in the vulnerability assessment and penetration testing guidelines.

9.1.1.6. The bank must disable or remove default accounts (if applicable), such as root and administrator, and must change the default passwords. The passwords must be set, as per the password management policy defined by the bank.

9.1.1.7. Risk analysis must be performed and documented for each application requiring network access. Unnecessary and unidentified connections to critical networks must be terminated.

9.1.1.8. A minimum security baseline for the hardening of infrastructure devices, such as servers, virtual machines, printers, firewalls, routers and switches, must be defined by the bank. These guidelines shall be formulated based on industry leading practices, existing standards and vendor recommendations. These baseline and hardening documents must be reviewed and updated on a biannual basis.

9.1.1.9. Access to the bank's network and infrastructure by administrators must be monitored and reviewed as per the logging and security monitoring guidelines

9.1.1.10. Access to the logs shall be restricted to prevent modification or deletion. Logs must be reviewed and backed up, as per the log management and backup guidelines.

9.1.1.11. The bank must have an assessment process in place to ensure security for additions or changes to network devices and infrastructure. This ensures that the change does not impose a point of vulnerability to other parts of network.

9.1.1.12. The bank shall implement strong application level encryption mechanism (such as AES or TLS) for transport and strong network level encryption to protect the data used, and processed by the application.

9.1.2. Communication security

9.1.2.1. The bank must ensure separate cabling, routing and distribution for information systems dealing with highly confidential, critical and sensitive information. This will ensure physical segregation of infrastructure and protection against attacks if systems of lower classifications are compromised.

9.1.2.2. A cable register must be maintained for data that at least documents the following attributes: cable identification number, classification, source, destination and floor plan diagram. The cables must be inspected, in accordance with the cable register, for inconsistencies at least on an annual basis.

9.1.2.3. Remote initiation of conferencing equipment shall be disabled to mitigate the risk of conversation snooping by remote means.

9.1.2.4. Facsimile (fax) devices or fax enabled Multi-functional Devices (MFDs) must be secured by implementing end to end encryption, if applicable, by the means of hardware appliance or software application to avoid sniffing of data.

9.1.2.5. Cables must be protected from tampering, sabotage or accidental damage by encasing them into appropriate conduit.

9.1.2.6. Redundant communication pathways shall be provisioned to ensure continued connectivity through auxiliary routes. This will ensure availability of the communication network in case of sabotage or accidental damage.

9.1.2.7. Conduits installed in public or visitor areas must not labelled in a manner that discloses their purpose or attracts undue attention.

9.1.3. Virtual Local Area Networks (VLANs)

9.1.3.1. The bank must ensure that administrative access and network control traffic is permitted from a separate management VLAN to ensure isolation and security. Additionally, it must be ensured that VLAN 1 is disabled or not used for management traffic.

9.1.3.2. Network control or administrative traffic must be categorized with prioritized QoS values. Additionally, administrative VLAN and network control traffic VLAN must be run in a separate Spanning Tree Protocol (STP) instance to ensure path resilience.

9.1.3.3. It must be ensured that VLAN’s are pruned on the trunk interface to avoid piggy backing of data.

9.1.3.4. VOIP traffic must be segregated (either logically or physically) to prevent attacks on voice networks. Appropriate Quality of Service (QoS) must be dedicatedly defined for VOIP traffic for ensuring uninterrupted and optimized network flows.

9.1.4. Multifunctional devices

9.1.4.1. A minimum security baseline for hardening of the MFDs must be defined by the bank. Additionally, users must be educated on the proper usage of MFDs governing the use of the equipment.

9.1.4.2. The bank shall ensure that appropriate authentication, encryption and auditing functions are enabled on MFDs, if applicable.

9.1.4.3. MFD’s shall be subjected to appropriate physical security controls against thefts in line with the physical security guidelines.

9.1.4.4. The bank are recommended to conduct a review on the version of the firmware of the MFD devices.

9.1.5. Domain Name Service (DNS)

9.1.5.1. The bank must ensure that zone files are digitally signed and the integrity of zone transfers is maintained. Additionally, it must be ensured that cryptographic origin and mutual authentication is maintained.

9.1.5.2. Traditional firewalls and IPS do not generally intercept and map DNS communications to malicious locations. A dedicated DNS firewall must be implemented to protect against malware that uses DNS to communicate with command-and-control (C&C) sites and botnets.

9.1.5.3. Redundant internal and external DNS must be implemented for segregation of name server information. Public facing DNS must be hardened as per established baselines and should be placed in a Demilitarized Zone (DMZ). Furthermore, a dedicated DNS firewall or Next Generation Firewall (NGFW) must be implemented to protect against malware that uses DNS to communicate with command-and-controls sites and botnets.

9.1.6. Internet security

9.1.6.1. Dedicated firewalls and content filtering gateways must be implemented to ensure that software and files downloaded from the internet or public networks are scanned and verified. In addition to this, mechanisms to perform Deep Packet Inspection (DPI) shall be enabled.

9.1.6.2. Internet gateways must have an explicit deny rule configured to block traffic unless specifically allowed on an exceptional basis. Additionally, it must be ensured that internet gateways (router, firewalls or L3 switch) must be hardened, as per bank hardening guidelines.

9.1.6.3. The bank must have the capability to monitor internal and external traffic to identify and understand traffic patterns.

9.1.7. Email security

9.1.7.1. Sender Policy Framework (SPF) is designed to detect email spoofing by checking that incoming mail comes from a trusted source authorized by that domain's administrators. It must be ensured that the email sever is configured to send undeliverable or bounce emails to senders that can be verified via SPF.

9.1.7.2. The bank must ensure that the use of email distribution lists is restricted, as much as possible, for internal usage. Additionally, auto responses, such as out-of-office reply emails, should be limited to approved and specific roles in order to curb the spread of malicious or spam emails. Legally binding disclaimers shall be incorporated into outgoing emails.

9.1.7.3. It shall be ensured that redundant email servers are implemented in the infrastructure to ensure high availability.

9.1.7.4. Email servers must be hardened as per the bank’s hardening guidelines.

9.1.7.5. The bank shall integrate an anti-spam gateway with the email server to prevent spam emails. Additionally, scanning and content filtering solutions shall be implemented to ensure emails comply with the bank’s security policy. Email encryption such as TLS must be enabled on the email server in accordance with the cryptographic policy.

9.1.8. Wireless security

9.1.8.1. The bank must ensure Wireless Local Area Networks (WLANs) are deployed with authentication and transmission security measures. Wireless Access Points (WAP) connected to the bank’s network must be registered and approved by the bank’s Information Security team/department. A risk assessment must be performed prior to implementation of a WLAN. Wireless LAN (WLAN) network used at banks shall be a logically and physically isolated network with no connectivity to the bank infrastructure.

9.1.8.2. The bank must ensure that the wireless network is configured with the latest encryption in place. Wired Equivalent Privacy protocol shall not be implemented within the network. Additionally, wireless clients shall use EAP/Transport Layer Security (TLS) or Protected Extensible Authentication Protocol (PEAP) to mitigate the risk of unauthorized access from compromised credentials.

9.1.8.3. Dynamic key exchange with encrypted VPN shall be deployed if confidential data is required to be communicated over wireless networks.

9.1.8.4. Inventory of wireless interface cards including APs, repeaters, laptops and workstations must be maintained in accordance to bank’s asset management policy. In case, a device is reported stolen or missing, the bank must change the encryption keys and SSID parameters for all the users. Personal devices shall not be connected on bank’s network without the approval of the Information Security function.

9.1.8.5. The bank shall periodically scan for rogue and improperly configured wireless infrastructure devices. Identified devices shall be removed from the network, or have their configurations altered to comply with the information security requirements of the bank. Additionally, wireless infrastructure shall be subjected to quarterly penetration tests and audits, as per the vulnerability assessment and penetration testing guidelines.

9.1.8.6. Wireless access points and gateways shall be hardened, as per the bank’s hardening guidelines. Parameters such as SSID, encryption keys, SNMP strings or any insecure configuration shall be changed at the time of installation. Additionally, it shall be ensured that SSID shall remain hidden and must not divulge any information such as the bank's name, system name or product name.

9.1.8.7. Wireless LAN networks must be secured by implementing a firewall between the access point and the internal network. In addition, firewalls must be configured to explicitly deny incoming connections on unknown ports. Wherever applicable MAC address filtering shall be considered.

9.1.9. Clock synchronization

9.1.9.1. Network Time Protocol (NTP) servers must be hardened as per the bank's hardening guidelines.

9.1.9.2. NTP authentication using MD5 must be configured for devices synchronizing with an NTP server. Additionally, the NTP server must not respond to unauthenticated NTP requests.

9.1.9.3. The network and infrastructure devices must synchronize to the NTP server and the NTP server shall itself sync to an agreed real time standard. These standards can be national atomic clocks, international atomic clocks or a government NTP server. Additionally, controls shall be in place to test for variations between the NTP server and standard reference time source.

9.1.10. VPN

9.1.10.1. The bank shall establish policies restricting VPN access and enforce controls to monitor remote-access devices. VPN access shall be restricted by enforcing controls unless a compelling business need exists and must require management approval. User access reconciliation shall be performed and reviewed on a monthly basis, to revoke accesses that no longer have a compelling business justification.

9.1.10.2. Two factor authentication must be enabled for VPN connections prior to establishing the VPN tunnel. A hardware or software token shall act as primary authentication followed by an integrated Radius, LDAP, AD or TACACS+ authentication.

9.1.10.3. Split tunneling shall not be permitted for VPN connections unless suitable controls such as host based content filtering agents, end point proxy systems and data leakage solutions are implemented at the bank.

9.1.10.4. Bank’s must establish, document and enforce cryptographic standards for VPN encryption and parameters. These must be uniform across organization.

9.1.10.5. Posture assessment must be configured for remote computers connecting to bank’s networks via VPN. This would ensure that the systems are equipped with updated security software, latest security patches, anti-virus, anti-malware software and repair configurations.

9.1.10.6. VPN inactivity timeouts must be configured for VPN connections, following expiration of these connections the user shall be required to re-login to the system. It will curb the risk of exploitation of an unattended VPN session by a malicious user. Additionally, this will ensure better utilization of network and system resources. This control must further be extended to site-to-site VPN tunnels as per the network design.

9.1.10.7. The bank must enable logging, monitoring and recording of VPN access in line with logging and monitoring guidelines.

9.1.10.8. Modems must be unplugged or disabled by default. If required, VPN access through modems must be provided for authorized requests. Once the request is completed, modems shall be disabled.

9.1.10.9. VPN concentrators shall be deployed in a DMZ, protected by a firewall and an IPS solution. Gateway firewalls and IPS will help in controlling, monitoring and analyzing traffic from VPN endpoints to trusted sources.

9.1.11. Information exchange

9.1.11.1. Prior to establishing trusted network connectivity, the bank must perform a thorough risk assessment which shall consider the risks of any identified cascaded connections particularly with an untrusted network. Additionally, the bank must evaluate, understand and accept the threats and risks of other domains. The subjected risk assessment shall be documented for compliance requirements.

9.1.11.2. The bank shall ensure that a reliable and trusted courier service is used for transporting physical assets. Controls shall be ensured to maintain adequate levels of protection for physical media in transit and at rest against any hazard that may render the contents unreadable or unrecoverable.

9.1.11.3. Controls shall be formulated by the bank to protect information exchanged via electronic channels from unauthorized access or interruption of service.

9.1.11.4. A well-trained media relations spokesperson shall be appointed by the bank to provide approved information to stakeholders and general masses via media outlets.

9.1.11.5. Prior to exchanging any information, it must be ensured that the required agreements between the entities exchanging information have been signed. The subjected agreements must detail responsibilities, information exchange notification procedures and technical standards for transmission, identification of couriers, liabilities, ownership and controls. Additionally, for vendors and third parties, a formal Non-Disclosure Agreement (NDA) shall be signed.

9.1.12. Gateway security

9.1.12.1. The bank shall ensure that the administrative access to gateways transmitting confidential information is provided on dual control and on the 4 eye principle. The bank shall ensure that network gateways are maintained by trained, experienced and authorized staff.

9.1.12.2. Network gateways shall be hardened prior to deployment in the production environment, as per the hardening guidelines. It shall be ensured that gateways are hardened following the below mentioned parameters at a minimum:

a. Latest vendor approved and tested firmware for protection against malicious code and firmware vulnerabilities.

b. Configured as per leading secure practices.

c. Account compromise and privilege escalation.

d. Rogue network monitoring.

e. Denial of service (DoS) attacks.

f. Information leakage.

g. Deny connections by default unless authorized.

9.1.12.3. Gateways must be integrated with logging and real time monitoring solutions to detect security breaches and network intrusions.

9.1.12.4. It is recommended that gateways be integrated with big data analytics, IP reputation services and advanced threat management solutions for enhancing the security posture of the bank.

9.1.13. Virtualization security

9.1.13.1. The bank must evaluate and identify the risks associated with virtualization technologies with respect to legal regulations and legislations. Additionally, risk assessments must be performed to understand the impact of virtualization on the existing infrastructure and current risk posture.

9.1.13.2. VM, Operating System (OS) hypervisor, administration systems and other systems connected to VM environment shall be hardened, as per the hardening guidelines. The following practices shall be observed for securing the VMs at a minimum:

a. It must be ensured that limits are set on the use of resources such as processors, memory, disk space, virtual network interfaces on each VM.

b. Role-based access controls based on the principal of least privileges must be individually enforced on each VM.

c. VMs shall be configured by default to disallow peripheral physical devices unless explicitly configured with a business need.

d. File sharing shall be disallowed between the host machine and VMs unless adequate risk assessment has been performed to prevent attacks such as VM hyper jacking and VM escape.

e. Unnecessary programs and services must be disabled on VMs.

f. Wherever possible, separate credentials must be used for managing VM and host OS.

g. VMs must be protected by a local firewall and a firewall configured on the host OS. The firewalls need to be configured as per the bank’s Information Security practices.

9.1.13.3. Physical and logical security controls shall be enforced to prevent unauthorized access to the virtual environment.

9.1.13.4. The change management policy shall be adhered to prior to any changes in the virtual environment. Additionally, VMs shall be patched and updated as per the patch management policy.

9.1.13.5. Logging for the VM’s shall be enabled, monitored and stored as per the logging and system monitoring guidelines.

9.1.14. Database security

9.1.14.1. Databases and its subsystems shall be hardened as per the bank’s hardening guidelines. Parameters such as default password, connection strings, SNMP communities or any insecure configuration shall be changed at the time of installation.

9.1.14.2. Access to information in a database shall be governed by the principle of least privilege and role based access controls. Information stored in the database shall be classified as per the information classification policy.

9.1.14.3. It must be ensured that the normal access controls of database are not bypassed to protect it from unauthorized access. This can be achieved by restricting access to database file using techniques, such as implementing database views and system kernel functions.

9.1.14.4. It is recommended that operating system accounts used by DBA staff to login to data server machines for administrative duties shall be individual accounts and not a shared group account. A group account shall be permitted for running automated DBA maintenance and monitoring jobs, such as backups.

9.1.14.5. Access to databases must be logged and reviewed by the DBAs and information security team on a periodic basis. The logs must be archived on an enterprise log server based on the log retention policy of the bank.

9.1.14.6. Database storing critical and confidential information shall be encrypted and procedures for secure key management shall be documented as per cryptographic policy.

9.1.14.7. Database shall be patched, as per the patch management policy. Provisions must be made to maintain security patch levels in a timely fashion.

9.2. Data security

9.2.1. Data classification and labelling

9.2.1.1. The bank shall define an information classification policy based on leading industry standards, such as ISO 27001, NIST. The scheme shall classify the data based on the sensitivity and impact. The classification of data determines the appropriate safeguards for security on data. At minimum, the data shall be classified as for example ‘restricted’, ‘private’ and ‘public’.

9.2.1.2. Information assets which are not classified or labelled due to reasons such as the document is in draft stage, is incomplete or the existing label has been tampered with or damaged, it shall be ensured that these assets are labelled as ‘confidential by default’.

9.2.1.3. All information should be marked as ‘private’ unless it is specifically created for public release or consumption.

9.2.1.4. The business process owners within the bank shall be responsible for identifying and classifying all tangible and intangible data assets that the business process collects or maintains and their removal.

9.2.1.5. All classified information shall be suitably marked for identification in line with the C-I-A ratings.

9.2.1.6. Users and audiences of information which includes staff, employees and partners shall be made aware of data labelling, need to know and its implication on information security.

9.2.1.7. The bank must ensure that details of internal networks, system configurations, personally identifiable data, employee details, media, directory services and other sensitive information are stored safely and encrypted.

9.2.1.8. Information must be made available on specific requirements and on a need to know basis. Access to information shall be provided based on request and after getting approvals.

9.2.2. Data leakage prevention

9.2.2.1. To contain and minimize the possible impact of incidents involving stealing, loss or leakage of customer data (privacy incidents), the bank must define and enforce comprehensive incident handling and reporting procedures in line with bank’s security incident management guidelines. The bank may refer to best national and international standard practices.

9.2.2.2. The bank must encipher sensitive data which is transmitted to external parties by using cryptographically strong industry standards, such as RSA, SHA to ensure protection of data at rest, in transit or in use as per the cryptographic policy.

9.2.2.3. The bank must put in place controls for detection of suspicious activities regarding access, modification or transfer of data.

9.2.2.4. The bank must enforce measures to address the risk of unauthorized downloading of customer data to portable storage media and loss of such media containing sensitive information by implementing endpoint DLP solutions.

9.2.2.5. The bank shall disable the portable storage media ports of computers and use isolated environment to access portable storage media

9.2.2.6. For outsourcing arrangements that involve storage of and/or access to bank' customer data, the bank shall require their outsourcing operators and other service providers which store, transport or have access to customer data to comply with the bank' data security, data leakage policies and procedures, including the controls set out in this document and signing non-disclosure agreement. The bank shall ensure that effective controls are enforced to monitor and validate the service provider's compliance with the said controls. Such requirements shall be specified clearly in the agreements and the bank shall conduct a regular assessment to ensure that the service providers comply with all relevant requirements and audit.

9.2.3. Migration control

9.2.3.1. The bank shall define and document a migration policy specifying migration plan and methodology for data migration to verify completeness, consistency and integrity of data and processes during migration of the data

9.2.3.2. The policy shall also list down pre- and post-migration activities along with responsibilities and timelines for activities.

9.2.3.3. Explicit sign off must be obtained from users/application owners after each stage of migration and after completion of the migration process.

9.2.3.4. Audit trail/logs must be available to document the conversion, including data mappings and transformations.

9.2.4. Data retention and archival

9.2.4.1. The data retention and archival policy must define appropriate access rights to prevent any unauthorized access to archived privileged information in order to avoid any compromise of confidentiality, integrity and accessibility of the said information.

9.2.4.2. The bank must ensure that integrity of information hosted on respective environments/media is preserved by implementing file/data integrity tools. Processes for backup, archival and recovery of data must have corresponding procedures which ensure that the integrity and confidentiality of the data is retained.

9.2.4.3. The policy must document and determine the archival frequency and retention periods of information assets including but not limited to the critical information that they hold governed by compliance to regulatory and legislative requirements. The bank must ensure that the financial information transactions or track records are retained for at least 15 years. Additionally, it must be ensured that data archival and retention periods must be in line with the requirements for handling personal information as specified in the Data Privacy Protection Law.

9.3. Portable devices security

9.3.1. The bank shall implement a mobile device management (MDM) solution that will bring in the aspect of containerization to ensure that only components of corporate data is encrypted and not the entire personal device.

9.3.2. A Bring Your Own Device (BYOD) policy shall be defined by the bank on the usage of Personal Devices (PDs) in the bank's environment.

9.3.3. The bank shall formulate these guidelines in accordance with their data classification and risk assessment policies. These shall cover areas such as data security, data storage, system recovery and training. At minimum, the bank shall ensure the below mentioned guidelines are followed regarding the security of personal devices (PDs):

a. PDs must be encrypted and password protected to secure the information they store. Additionally, they must be kept under supervision when not in use. PDs shall not be allowed into environments such as high risk areas without prior approval from the Information Security team/department.

b. PDs which do not comply with the BYOD policy shall not be allowed to connect to the bank's network. Additionally, PDs shall be managed and accounted in the same manner as bank owned devices.

c. Measures such as deployment of firewalls, IPS and monitoring systems shall be undertaken for protection of PD's.

d. If there is a guest, they should be connected to a segregated network.

e. In case of loss or theft of the PDs, incident management procedures shall be followed, as per bank's policies. Additionally, it must be ensured that remote wipe/or emergency lock features are enabled for PDs.

9.4. Cyber threat and vulnerability management

9.4.1. Threat and vulnerability risk assessment

9.4.1.1. The bank shall formulate and enforce risk assessment and management controls, for each asset, to identify the threat/vulnerability combinations that have the likelihood of impacting the confidentiality, availability or integrity of that asset - from a business, compliance or contractual perspective.

9.4.1.2. An annual gap analysis and risk assessment shall be performed to determine if the current controls are adequate, and their response and recovery plans are effective. Additionally, the bank shall put a roadmap in place to promptly address any gaps that are found.

9.4.1.3. The bank shall ensure that the risk assessment program must contain, at a minimum:

a. Asset identification and estimation of their value: Identifying, selecting and implementing controls for providing proportional response including considerations like productivity, cost effectiveness and the value of the asset.

b. Evaluating the effectiveness of the control measures.

c. Ensuring the controls provide the required cost-effective protection.

d. A threat assessment that shall include aspects such as acts of nature, acts of war, accidents, malicious acts originating from inside or outside the organization.

e. A vulnerability assessment for each vulnerability and calculating the probability that it will be exploited. Additionally, policies, procedures, standards, trainings, physical security, quality control and technical security shall also be evaluated.

f. Following risk identification, the bank shall calculate the business, operational and financial impact analysis that each threat would have on each asset through qualitative or quantitative analysis. The extent of risk impact depends on the likelihood of the various threat and vulnerability pairings or linkages capable of causing harm to the organization when an adverse event occurs.

g. The bank shall develop a threat and vulnerability matrix to assess the impact of the threat to its IT environment and will also assist in prioritizing IT risks.

9.4.1.4. Senior management must establish clearly a function for implementing and managing the risk management process. Accordingly, the risk management function (team, committee, etc.) shall formulate a formal technology risk acknowledgement and acceptance process for reviewing, evaluating and approving any major incidents of non-compliance with IT control policies. The process shall include at a minimum:

a. Risk assessment and description being considered for acknowledgement by the risk owner.

b. Identification of mitigating controls.

c. Formulation of a remedial plan to reduce the risk

d. Approval of the risk acknowledgement from the risk owner and senior management.

9.4.1.5. As a part of risk identification and assessment, the bank must identify events or activities that could disrupt operations, or negatively affect the reputation or earnings, and assess compliance to regulatory requirements. Risks identified can be broadly categorized into the following categories:

a. Strategic failures: This may include improper implementation, failure of supplier, inappropriate definition of requirements, incompatibility with existing application infrastructure etc. It will also include regulatory compliance.

b. Design failures: This may include inadequate project management, cost and time overruns, programming errors and data migration failures among others.

c. Transition failures: This may include inadequate capacity planning, inappropriately defined availability requirements, SLA/OLA/Underpinning contracts not appropriately defined and information security breaches, among others.

Biannual gap analysis and risk assessments shall be performed to determine if the current controls are adequate, and their response and recovery plans are effective. Additionally, the bank shall put in place a roadmap to promptly address any gaps that are found.

9.4.2. Web application security

9.4.2.1. Web Application Firewall (WAF) shall be deployed for securing applications in the infrastructure.

9.4.2.2. The bank shall conduct application security testing of web/mobile applications throughout their lifecycle (pre-implementation, post implementation and post any major changes). The reports shall be shared with stakeholders and tracked to closure.

9.4.2.3. The bank shall also perform vulnerability assessments, code reviews and penetration testing at a minimum of two, or more frequently as needed, on an annual basis for the entire application infrastructure.

9.4.2.4. The bank shall formulate secure application development guidelines in accordance with industry standards such as Open Web Application Security Project (OWASP), CERT secure code standards and MITRE CWE standards.

9.4.2.5. Information while at rest, in motion and in use in web applications shall be secured as per the guidelines outlined in the cryptographic security section.

.

9.4.3. Vulnerability assessment and penetration testing

9.4.3.1. The bank shall deploy a combination of automated tools and manual techniques to perform a comprehensive Vulnerability Assessment (VA) exercise at a minimum of two, or more frequently as needed, on an annual basis. Industry practices and standards shall be followed for performing these tests, such as OWASP, OSSTMM, SANS. At a minimum, the bank must compare the results from previous vulnerability scans to verify that these vulnerabilities were addressed and mitigated.

9.4.3.2. An action plan to address identified vulnerabilities shall be prepared and shared with the senior management.

9.4.3.3. The bank shall conduct two penetration testing exercises, or more frequently as needed, on an annual basis.

9.4.3.4. Acceptance of business risks for existing vulnerabilities shall be reviewed semi-annually to determine if more recent controls or patches can address vulnerabilities that were previously accepted, or if conditions have changed increasing the risk.

9.4.4. Anti-phishing

9.4.4.1. The domains shall be protected to provide recourse against an agent who register similar domain names for malicious purposes. Additionally, the bank must procure domain monitoring services that monitor recent domain registrations and highlight them if a deceptive domain is being registered similar to their domain.

9.4.4.2. Email servers and DNS must be hardened, as per best practices such as Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) and digital signing will be followed to prevent phishing.

9.4.4.3. The bank should educate their customers through customer notification and awareness with regards to phishing emails and suspicious emails. The bank must provide an email address, such as spoofmail@bank.com, to which the customers can submit a suspicious email to determine its authenticity. The bank must inform QCB about the discovery of all phishing incidents.

9.4.4.4. The bank shall preserve the evidence of phishing attacks for subsequent prosecution of the phishers if such a recourse is taken.

9.4.5. Security measures against malware

9.4.5.1. The bank shall formulate and enforce controls to detect and mitigate malware at host, network and user level.

9.4.5.2. The bank must keep their anti-malware software and signature up to date.

9.4.5.3. Auto run functionality shall be disabled on laptops, workstations and servers. Additionally, an automated anti-malware scan of removable media must be performed when inserted into the system.

9.4.5.4. The bank must filter attachments at the email gateway.

9.4.5.5. Logs from firewalls, IPS/IDS, DNS servers and proxy server logs must be monitored on a daily basis for indicators of compromise.

9.4.6. Protection against DOS and DDOS

9.4.6.1. The bank shall identify potential bottlenecks and single points of failure which can be vulnerable to DOS/DDoS attacks. This could be identified by performing network design analysis and configuration testing.

9.4.6.2. The bank must consider DOS/DDoS attacks in their ISP on application and volumetric layer selection process.

9.4.6.3. The bank shall formulate an incident response framework which shall be periodically validated to facilitate a fast response to a DOS/DDoS attack.

9.4.7. Early detection of cyber intrusions

9.4.7.1. IPS capabilities shall be present at both internal and external level.

9.4.7.2. The bank must monitor suspicious activities on servers, network and endpoint devices. Mechanisms shall be deployed to detect, alert and block anomalies on the affected devices.

9.4.7.3. A network traffic baseline must be defined by the bank by analyzing network traffic, and any deviations or anomalies must be taken up as a priority.

9.4.7.4. The incident response framework must include a cyber-breach response plan that measures details on countering cyber intrusions.

9.4.7.5. In the event of a cyber-intrusion, the bank must perform a thorough investigation to determine the extent of infiltration and the impact sustained, as well as the vulnerabilities being exploited by the attacker.

9.5. Physical and environmental security

9.5.1. Physical spaces shall be zoned depending upon their security requirements. The requirements for each physically separated zone must be determined through a risk assessment. This must be done during the design phase of a new construction or, for existing workplaces, as part of an on-going risk management process.

9.5.2. Physical and environmental controls must be implemented to monitor environmental conditions which could affect the operation of information processing facilities (e.g. fire, explosives, smoke, temperature, water and dust).

9.5.3. Equipment and facilities shall be protected from power failures and electrical supply interference by, for example, installing Uninterruptible Power Supply (UPS) and a backup generator.

9.5.4. Computer facilities and equipment shall be protected from damage and unauthorized access through physical security controls, including:

a. Security barriers and entry controls must be deployed to protect information processing facilities such as data centers, card and pin generation facilities.

b. Access to these areas must be restricted to authorized personnel and the access rights must be reviewed and updated periodically.

c. Buildings must give a minimum indication of their purpose, with no obvious signs identifying the presence of information processing facilities.

9.5.5. Access control policies and approval processes must be in line with instructions specified in the access control section. It must be ensured that vendors, contractors, delegates or guests visiting bank premises adhere to the bank’s physical and access control policy.

9.5.6. The bank shall formulate a site security plan and Standard Operating Procedures (SOPs) for secure areas. The site security plan shall cover the following, at a minimum:

a. Summary of the security risk assessment.

b. Organization chart detailing upon roles and responsibilities of the facility officer and staff.

c. The administration, operation and maintenance of the electronic access control system and security alarm system

d. Key management, the enrolment and removal of system users and issuing of personal identification.

e. Staff member clearances, security awareness training and periodic briefings.

f. Inspection of the generated audit trails and logs.

g. End of day checks and lockup.

h. Reporting of ICT security incidents and breaches.

9.5.7. The bank must deploy monitoring mechanisms for the detection of compromises of environmental controls such as temperature, water, smoke, access alarms, service availability alerts (power supply, telecommunication, servers) and access log reviews.

9.6. Cryptographic security

9.6.1.1. The bank must define their cryptographic policy by referring to industry standards. The bank shall select encryption algorithms which are well established international standards, and which have been subjected to rigorous scrutiny by the international cryptographer community or approved by an authoritative professional body, reputable security vendor or government agency.

9.6.1.2. The bank must define and adhere to key management standards, such as ISO11770 – 1, to control and manage the lifecycle of cryptographic keys. At minimum, the key management standard must cover the following requirements:

a. key custodians roles and responsibilities

b. key generation

c. dual control and split knowledge

d. secure key storage

e. key usage

f. secure key distribution and in transit

g. key backup and recovery

h. periodic key status checking

i. key compromise

j. key revocation and destruction

k. audit trails and documentation

Additionally, it must be ensured that the lifetime of the key management standards shall be determined by the application and the information infrastructure it is utilized within.

9.6.1.3. Integrity of confidential information shall be ensured by encryption and by ensuring protection against unauthorized disclosure in transit, at rest and in use. Risk assessment must be performed to determine information asset criticality and formulation of cryptographic controls.

9.6.1.4. Practices shall be followed for securing confidential data at rest, in transit or in use, such as securing web traffic, file transfers, remote access, emails, secure data hashing, HDD/data at rest encryption, symmetric key encryption, asymmetric key encryption and hardware security modules (HSM's) etc.

9.6.1.5. Passwords shall be secured and protected against unauthorized disclosure at rest or in transit. Additionally, privileged passwords must be encrypted and stored off-site with backup files each time the password is changed to ensure complete recovery.

9.6.1.6. To ensure cryptographic functions are appropriately randomized and secured, a Hardware Security Module (HSM) must be implemented for key management and cryptographic processing.

9.6.1.7. State licensed and approved digital certificates shall be used in the bank production system. The bank shall ensure that the digital certificates are compliant to standards in use by the CSP-PMA, MICT. Online revocation mechanisms shall be used to curb the risk of fraudulent use of digital certificates.

9.7. Software development and acquisition

9.7.1. Software security

9.7.1.1. The bank shall formulate secure application development guidelines (S-SDLC) in accordance with industry standards such as Open Web Application Security Project (OWASP), CERT secure code standards and MITRE CWE standards to create secure web applications and web services.

9.7.1.2. It must be ensured that test and development environments are isolated from production systems. Access to these systems shall be granted to authorized users with a clear business requirement.

9.7.1.3. Internally developed or externally procured applications must be classified as per the National Information Classification Policy.

9.7.1.4. The bank must perform a source code review to find vulnerabilities arising due to coding issues, poor coding practices or malicious attempts.

9.7.1.5. The source code of custom developed critical applications should be acquired by the bank. If this is not possible, the bank look into options of arranging an escrow for the source code.

9.7.1.6. Security requirements (functional, technical and assurance requirements) shall be developed and implemented as a part of system requirements specifications.

9.7.2. Software application

9.7.2.1. Applications must be reviewed to determine whether they attempt to establish any external connections.

9.7.2.2. Integrity checks must be performed on the backup information to identify if a compromise, or a legitimate but incorrectly completed system modification, has occurred. Additionally, these checks shall be performed on a replica environment. Integrity information must be securely stored on a different server and must be updated after every legitimate change of system or application.

9.7.2.3. High risk servers, e.g. web, email, file and Internet Protocol telephony servers having connectivity to public networks, must be hosted in a DMZ.

9.7.2.4. Any undocumented changes must be resolved in accordance with the bank’s internal security incident management procedures.

9.7.3. End user development

9.7.3.1. The bank must perform an assessment to ascertain the importance of office utility software, and some business applications provide the functionality to create macros and simple applications to automate operations.

9.7.3.2. The bank shall formulate a policy/procedure to review and test user-developed macros and scripts before they are used to ensure the integrity and reliability of the applications.

9.8. Media security

9.8.1. Media classification and labelling

9.8.1.1. The hardware or media shall be classified according to the information contained in the media. The bank shall ensure that security controls are deployed to protect the media.

9.8.1.2. Classification of all media must be visually identifiable, and the labelling scheme be documented and uniformly applied across the organization, and such media should be protected against tampering.

9.8.2. Media sanitization, repairing, maintenance, destruction and disposal

9.8.2.1. The bank shall define the process and procedures for sanitization of media and identify and adopt tools to meet the requirements. Testing shall be conducted at regular intervals to ensure effectiveness of the tool.

9.8.2.2. The bank shall ensure that only authorized personnel carry out repairs and maintenance work on classified media.

9.8.2.3. The bank shall document procedures for the destruction and disposal of media.

9.8.2.4. Media shall be destroyed by degaussing non-volatile media and physically destroying media through smashing and drilling.

9.8.2.5. Staff members shall supervise the destruction of media and that due diligence is carried out during the destruction of the media.

9.8.2.6. It will be ensured that the disposal of the media and media waste does not attract undue attention, which may possibly lead to attempts by malicious users to dumpster diving.

9.8.2.7. It must be ensured that media, including faulty media, containing classified information is completely sanitized as much as possible prior to disposal.

9.8.2.8. Contracts with third party disposal firms must address acceptable disposal procedures.

9.9. Data center protection and controls

9.9.1. Data center resiliency

9.9.1.1. The bank must ensure that the data center(s) is resilient and physically secured from internal and external threats.

9.9.1.2. The bank shall include in the scope of threat vulnerability risk assessment a review of each data centers perimeter and surrounding environment, as well as building and facilities.

9.9.1.3. The bank shall assess the redundancy and fault tolerance in areas such as electrical power, air conditioning, fire suppression and data communications.

9.9.1.4. The bank must implement appropriate fire protection and suppression systems.

9.9.1.5. It must be ensured that an uninterruptible backup power and power supplies, battery arrays and/or diesel generators are installed at each data center.

9.9.2. Data center physical security

9.9.2.1. The bank shall restrict access to the data center to authorized staff only.

9.9.2.2. Physical access of staff to the data center shall be revoked immediately if it is no longer required.

9.9.2.3. For non-bank personnel, such as vendors or system administrators who require temporary access to the data center to perform maintenance or repair work, the bank shall ensure that there is proper notification of and approval for such visits. The bank shall ensure that visitors are accompanied at all times by an authorized employee while in the data center.

9.9.2.4. The bank shall ensure that the perimeter of the data center, the data center building, facility and equipment room is physically secured and monitored.

9.9.2.5. The bank shall employ physical, human and procedural controls

9.9.2.6. The bank shall deploy security systems and surveillance tools, where appropriate, to monitor and record activities that takes place within the data center.

9.9.2.7. The bank shall establish physical security measures to prevent unauthorized access to systems, multi-functional devices, equipment, racks and tapes.

9.10. Managing outsourcing risk

9.10.1. Outsourcing IT

9.10.1.1. The board of directors and bank senior management shall be responsible for the governance, compliance and risk management of outsourced processes, and they must set the proper framework to ensure quality of services provided as if the bank were to provide these services by itself.

9.10.1.2. A bank seeking to use the services of any of the outsourcing service providers must seek prior approval of QCB before entering into any agreements for such services, and the scope of service to be outsourced shall be submitted to QCB for approval.

9.10.1.3. A thorough risk assessment and due diligence exercise must be performed to formulate appropriate mitigating controls of service providers. Additionally, the bank must clarify jurisdiction for their data and applicable regulations at the outset of an outsourcing arrangement.

9.10.1.4. The bank shall formalize any work area to be outsourced to a third party by a contract of service.

9.10.1.5. The outsourcing arrangement must include an approval requirement for significant subcontracting of services and provisions by the original technology service provider.

9.10.1.6. The bank shall ensure that outsourcing agreements include the provisions outlining the right to audit service providers by internal or external auditor and QCB examiners.

9.10.1.7. The bank must ensure International Standards on Assurance Engagements (ISAE) standard reports on assurance of controls are required from the outsourcing vendor or remote service provider.

9.10.1.8. The reports provided by third party service provider shall be continuously monitored and reviewed, and audits conducted to ensure adherence to SLA's.

9.10.1.9. In case third party services are provided by using remote access, the bank shall ensure that communication channels are encrypted or protected end to end through the latest secure mechanisms.

9.10.1.10. The bank must ensure that third party vendors and technology outsourcing companies are subjected to the bank's change management for any changes to software, program or application source code. In addition to this, it must be ensured that third party developers work only in a test environment.

9.10.1.11. The bank must ensure it develops the technology skillset among relevant team members etc. that is being outsourced to technology outsourcing companies as a contingency measure.

9.10.1.12. The bank must ensure that there are no legal obstacles to access and obtain the application source code developed by the third party and such clauses shall be specified in any outsourcing agreement.

9.10.1.13. The third party shall be contractually required to regularly report on the outsourced service security posture and incidents.

9.10.1.14. The bank shall ensure measures are in place at the service provider's site to enable normal operation in case of exceptional events, such as the disruption of communications with the data center or malfunction for extended periods of time.

9.10.1.15. When the bank operates abroad through professional intermediary services (which are part of the group to which the establishment belongs), or when there are representative offices, intermediaries or representatives of these offices, these individuals will not have access to its IT systems in Qatar.

9.10.1.16. The bank shall ensure that the service provider implements security policies, procedures and controls that are at least as stringent as it would expect for its own operations.

9.10.1.17. Security controls and baseline policy specified in the NIAP Manual are included in the third party service delivery agreement or contract. This shall also apply to subcontractors used by the third party.

9.10.2. Data center organization

9.10.2.1. Prior to onboarding of a data center or technology provider, due diligence exercises shall be carried out to determine its viability, capability, reliability, track record and financial position.

9.10.2.2. The bank shall ensure that all hosting of applications and data within data center or application service providers should be physically located within the State of Qatar.

9.10.2.3. The bank must ensure that third party vendors and technology outsourcing companies are subject to the bank's change management and monitoring controls. Additionally, it must be further ensured that the quality and availability of banking services to end users and customers is not negatively affected due to the outsourcing arrangements.

9.10.2.4. A thorough risk assessment must be performed to formulate mitigating controls for service providers across multiple geographies. Since banks are exposed to the jurisdiction of multiple geographies as a part of their outsourcing arrangements, the bank shall proactively evaluate such risks as part of its due diligence process and develop mitigating controls and, as required, an effective exit strategy. Additionally, the bank must clarify the jurisdiction for their data and applicable regulations at the outset of an outsourcing arrangement. This information shall be reviewed periodically and, in case of significant changes, performed by the service provider.

9.10.2.5. Data center and technology outsourcing contracts shall be formulated and agreed in a manner that does not obstruct or hinder the ability of the bank or regulatory authorities to perform periodic audits/inspections and assessments. The bank must notify QCB as a matter of priority in the event that the rights of access for the bank and/or the regulator are likely to be impeded.

9.10.2.6. The outsourcing arrangement must include an approval requirement for significant subcontracting of services and provisions by the original technology service provider.

9.10.2.7. The requirements and conditions covered in the data center and technology outsourcing agreements shall include performance targets, service levels, availability, reliability, scalability, compliance, audit, security, contingency planning, disaster recovery capability and backup processing facilities.

9.10.2.8. The bank shall require the service provider to develop and establish a disaster recovery contingency framework which defines its roles and responsibilities for documenting, maintaining and testing its contingency plans and recovery procedures. In addition to this, the bank must be able to continue to operate normally in case of exceptional events, such as the disruption of communications with the data center, or malfunction for extended periods of time.

9.10.2.9. The disaster recovery plan shall be reviewed, updated and tested periodically in accordance with changing technology conditions and operational requirements. The plan shall be based on credible worst case scenarios for service disruptions and must incorporate identification of viable alternatives for resuming its IT operations elsewhere; an exit management plan and identification of additional or alternate technology service providers for such support and services.

9.10.2.10. The bank must ensure that the service provider implements security policies, procedures and controls that are at least as stringent as it would expect for its own operations. Additionally, the bank shall monitor and review the security policies and controls of the service provider on a periodic basis, including obtaining periodic expert reports on security adequacy and compliance in respect of the operations and services provided by the service provider.

9.10.2.11. The bank, seeking to use the services of any service providers as stated above, must seek prior approval of the QCB before entering into any agreements for such services.

10. Business applications

10.1. Internal fraud

10.1.1. The bank shall have policies, procedures and controls in place to prevent employees from committing fraud.

10.1.2. The bank must have an internal control framework to prevent fraud. The fraud risk management team, along with the business/operations/support groups, periodic reviews of various systems and controls, shall address gaps, if any, to strengthen the internal control framework.

10.1.3. A fraud review group comprising of senior leaders of the bank shall be set up at the bank. The group shall meet at least once a quarter to review fraud trends and preventive steps taken by the business group, and report the same to the board of directors.

10.1.4. Fraud monitoring systems must be in place for monitoring suspicious transactions.

10.1.5. To prevent fraudulent transactions being made through credit/debit card information, the media containing valid account information, account numbers, PIN numbers, credit limits and account balances shall be stored in an area limited to only authorized personnel. Production and issuing processes for cards must be kept physically separated from the PIN generation and issuing environments.

10.2. External fraud

10.2.1. Monitoring of transactions processed online, on ATM or POS terminals shall be undertaken to deter any potential fraudulent activity happening at a merchant place, or for money laundering detection. The QCB requires that the bank must have a real-time fraud monitoring system running to detect suspicious activities on financial transactions.

10.2.2. Measures to counter fraud must be in place for the bank to be able to take actions on any fraudulent transactions after alarms are raised by the systems. Principles, such as velocity checks, must be enabled with reference to current transactions and previous transactions, at a minimum.

10.2.3. Any fraud attempt on ATM's or point of sales must be reported to the Ministry of Interior (MOI) hotline as stated in the QCB instructions, and the QCB must be notified. Embezzlement crimes must also be reported, including attempted embezzlement through electronic means. The QCB must be notified, in case of any hacking, penetration, fake websites or forged credit cards. However, the bank shall be responsible for compliance of law and notifying related authorities in this regard.

10.2.4. Fraud monitoring systems shall include an online authorization decision process, possibilities to initiate queries and a rule-based set of controls that can be tailored to the need of the bank, as well as to cope with future fraud activities trends. This fraud monitoring system must be coupled with the existing payment acquiring system and be a part of the fraud management system which the bank is running.

10.3. Fraud risk management

10.3.1. Fraud vulnerability assessments shall be undertaken across the bank by the Fraud Risk Management team. These assessments shall cover all channels of the bank, such as branches, internet, ATM and phone banking, as well as international branches, if applicable. Appropriate verification procedures shall also be incorporated at all channels, such as phone banking, ATMs, branches and internet, to ensure that only genuine transactions are processed.

10.3.2. New products or processes shall be analyzed for fraud vulnerabilities before being introduced in the bank, and fraud loss limits shall be mandated wherever vulnerabilities are noticed.

10.3.3. All residual/open risks in products and processes must to be covered by setting ‘fraud loss' limits. 'Fraud loss' limits must be monitored regularly by the fraud risk management team and a review needs to be undertaken with the respective business group when fraud loss amount reaches 90 percent of the limit set.

10.3.4. Security measures shall be incorporated during delivery of instruments such as cards/cheque books/internet passwords to customers through couriers.

10.3.5. Internet banking systems must have security features, such as separate transaction passwords, two-factor authentication, multi-channel process for registering payees, upper limit on transaction value and SMS alerts to customers.

10.3.6. Appropriate access controls and procedures shall be in place to ensure that only employees who are required to know particular information have access to this and can validate the transactions.

10.3.7. Know Your Customer (KYC) and know your employee/vendor procedures: The bank must ensure a KYC process is put in for fraud prevention. The bank shall implement strong procedures to carry out due diligence of potential customers, employees and vendors before they are enrolled.

10.3.8. Physical security: All banks must have a dedicated team to take care of the security of the physical infrastructure.

10.3.9. Creation of fraud awareness amongst staff and customers: The bank must create awareness amongst staff and customers on fraud management and its policies on a regular basis.

10.3.10. Fraud prevention practices: A strong internal control framework shall be put in place by the bank. The fraud risk management team along with the business/operations/support groups, should continuously review the various systems and controls, to remove gaps, if any, and to strengthen the internal control framework.

10.4. Fraud detection

10.4.1. The bank must have proper channels for the reporting of fraud. System triggers that throw up exceptional transactions and channels that take note of customer/employee alerts/disputes, seeding/mystery shopping exercises and encouraging employees/customers/well-wishers to report suspicious transactions/behavior, are some of the techniques that must be used for detection of fraud. The exceptional/suspicious transactions/activities reported through these mechanisms must be investigated in detail.

10.4.2. Appropriate mechanisms must be established at the bank, to report disputes/exceptions or suspicions highlighted by various stakeholders, including transaction monitoring teams in the bank and to investigate them thoroughly. The bank must have a well-publicized whistle blowing mechanism.

10.4.3. Dedicated email ID and phone number for reporting suspected frauds: The bank must have a dedicated email ID and phone number for customers to report any fraudulent activities. A dedicated team must be created to reply to customer queries and concerns through the above email IDs. Phone banking officers and branch staff must also be trained on responses to customers' queries and concerns on fraud.

10.5. Fraud investigation

10.5.1. The fraud risk management team must undergo continuous training to enhance its skills and competencies.

10.5.2. The investigating team must share the report with the relevant authority within the bank or track it down to closure.

10.5.3. The bank must adopt various advanced techniques and skills towards computer forensics, forensic accounting and tools to analyze large volumes of data, based on their current risk appetite.

10.6. Reporting of fraud

10.6.1. Any frauds in merchant acquiring business shall be reported to the QCB.

10.6.2. Frauds in ATM acquiring business: In a shared ATM network, the acquirer must report the fraud and not the issuer of the ATM cards. The acquiring bank shall solicit the help of the issuing bank in the recovery of the money.

10.6.3. The bank must share data and documents requested by the police, even in cases where the bank in question is not the victim of the fraud, but has been in receipt of fraudulent money into its accounts.

10.7. Customer awareness of frauds

10.7.1. The bank must aim to continuously provide fraud risk awareness to its customers for their own protection.

10.8. Employee awareness of fraud

10.8.1. The bank must conduct training on fraud prevention practices at various forums and this must be undertaken by the fraud management team.

10.9. Customer education and awareness

10.9.1. The board of directors/senior management must commit towards consumer education initiatives by providing adequate resources, improving customer education measures on an ongoing process.

10.9.2. The bank shall improve and maintain customer awareness and education with regard to cyber security risks. The bank shall encourage customers to report phishing emails/phishing sites and take effective remedial action over such reports.

10.9.3. The bank must undertake awareness activities that shall be conducted on an ongoing basis, using a variety of delivery methods in addition to:

- **Improving and maintaining customer awareness and education with regard to cyber security risks.**
- **Encouraging customers to report phishing mails/phishing sites, and take effective remedial action on these reports.**
- **Educating the customers on the risks of sharing their login credentials/passwords etc.**

10.10. Online system security

10.10.1. The bank must have a security strategy to ensure confidentiality, integrity and availability of its data and systems.

10.10.2. The bank must evaluate the security requirements associated with its internet systems and adopt encryption algorithms, which are of well-established international standards and subjected to rigorous scrutiny by an international community of cryptographers or approved by an authoritative professional bodies, or government agencies.

10.10.3. The bank must implement two-factor authentication for transaction-signing for authorizing internet/ online banking transactions.

10.10.4. Controls shall be implemented to authorize transactions with institutional investors, accredited investors or corporate entities. The bank must perform a risk assessment on such systems and use token-based mechanisms to authorize transactions.

10.10.5. The bank shall provide customers and users of its internet services an assurance that online login access and transactions performed over the internet on the bank website are protected and authenticated.

10.10.6. The bank shall implement physical and logical access controls to allow only authorized staff to access its systems. The bank shall also implement appropriate processing and transmission controls to protect the integrity of systems and data.

10.10.7. The bank shall implement a monitoring system to alert to any abnormal system activities, transmission errors or unusual online transactions. The bank shall develop an action plan to verify and close these issues or errors.

10.10.8. The bank shall undertake a vulnerability assessment and penetration testing of its online banking system to minimize exposure to other forms of cyber attacks such as man-in-the-middle attack (MITMA), man-in-the browser attack or man-in-the application attack.

10.10.9. The bank shall maintain high resiliency and availability of online systems and supporting systems (such as interface systems, backend host systems and network equipment). The bank must put in place measures to plan and track capacity utilization as well as guard against online attacks. These online attacks include DoS attack and DDoS attack.

10.11. Mobile online services and payment security

10.11.1. The bank must implement security measures for mobile online services and payments.

10.11.2. The bank must conduct a risk assessment to identify possible fraud scenarios and put in place appropriate measures to counteract payment card fraud via mobile devices.

10.11.3. The bank must ensure that there is adequate protection of sensitive or confidential information used for mobile online services and payments.

10.11.4. The bank must educate its customers on security measures to protect their own mobile devices from viruses and other errant software which may cause malicious damage and have harmful consequences.

10.11.5. At a minimum, 3D Secure, provided by the major payment card brands, shall be implemented by all card issuers for cardholder authentication. Customers shall be informed about the authentication procedure and enrolled through a dedicated process with the bank.

10.12. Payment card security

10.12.1. The bank must ensure that they are compliant with international security standards / methodologies and best practices such as the Payment Card Industry Data Security Standard (PCI-DSS), PCI Payment Application Data Security (PA-DSS), OWASP, PCI PIN Transaction Security (PCIPTS and PCI-PIN Entry Device Security.

10.12.2. The bank must report the compliance of these standards to the QCB annually.

10.12.3. The bank must deploy secure chips (EMV compliant) to store sensitive payment card data. The payment terminal used must be EMV complaint. The bank must also implement strong card authentication methods such as dynamic data authentication (DDA) or combined data authentication (“CDA”) methods for online and offline card transactions.

10.12.4. The bank must ensure that magnetic stripes are protected.

10.12.5. For transactions that customers perform with their ATM cards, the bank must only allow online transaction authorization. The authentication of customers' sensitive static information, such as PINs, must be performed by the card issuer, and not a third party payment processing service provider. The bank must perform regular security reviews of the infrastructure and processes being used by its service providers.

10.12.6. The bank must ensure that security controls are implemented at payment card systems and networks.

10.12.7. The bank must only activate new payment cards sent to a customer via post upon obtaining the customer’s instruction.

10.12.8. The bank must implement two factor authentication such as one-time-password (OTP) for CNP transactions via internet to reduce fraud risk associated with CNP.

10.12.9. To enhance card payment security, the bank must promptly notify cardholders via transaction alerts when withdrawals/charges exceeding customer-defined thresholds are made on the customers’ payment cards. The bank must include in the transaction alert, information such as the source and amount of the transaction.

10.12.10. The bank shall implement robust fraud detection systems with behavioral scoring or equivalent; and correlation capabilities to identify and curb fraudulent activities.

10.12.11. The bank shall follow up on transactions exhibiting behavior which deviates significantly from a cardholder's usual card usage patterns, and shall investigate these transactions and obtain the cardholder's authorization prior to completing the transaction.

10.13. ATMs and payment kiosk security

10.13.1. The bank must consider putting the following measures in place to counteract fraudsters' attacks on ATMs and payment kiosks:

- **Install anti-skimming solutions on these machines and kiosks to detect the presence of foreign devices placed over or near a card entry slot.**
- **Install detection mechanisms and send alerts to appropriate staff at the bank for follow-up response and action.**
- **Implement tamper-resistant keypads to ensure that customer' PINs are encrypted during transmission; also when typing the PIN information, the data must be encrypted, so the keypad must be an encrypting PIN pad, supporting at least TDES (Triple DES) or AES.**
- **Implement appropriate measures to prevent shoulder surfing of customer PINs.**
- **Conduct video surveillance of activities at ATM machines and payment kiosks, and maintain the quality of CCTV footage.**
- **A camera must be installed to cover the ATMs surrounding space with angle not less than 70 degrees.**
- **ATM screen position: The position of screen must avoid easy reading to protect it against shoulder surfing**
- **Pinhole camera installed be a wide angle camera.**
- **Camera has to be connected to motion detection device and must not cover the keypad entry by customers.**
- **External lighting of the covered space not be less than LUX50.**
- **Camera sensitivity must be not less than 0.5 LUX and resolution shall be at least 3 mega pixels.**

- **Video recording capacity cover retention period mentioned in the latest instructions issued by the QCB.**
- **Screen displays must be inclined and side view protection exist in addition to installing keypad typing cover protection in order to avoid shoulder surfing that could lead to personal information stealing.**
- **ATM alarms must be configured to detect unusual events.**
- **Access to the inner section of the ATM by third parties must be covered by agreements, including a third party ICT access agreement.**
- **Access to inner section of the ATM for maintenance must be done in conjunction with bank's authorized personnel. Access to remote ATMs for maintenance can be organized with a security dedicated third party company and the vendor.**
- **Access to the ATM data center by third party vendor must be strictly authorized only if accompanied with bank's authorized personnel.**
- **Vendors must never be left alone in bank's premises, especially when working on bank's systems. This type of access must be logged and monitored as per the requirements given in this chapter.**

10.13.2. The bank must also ensure awareness messages are communicated to customers on a regular basis towards risk such as:

- **Checking if something abnormal has been fixed on the ATM.**
- **Checking the card slot before inserting a payment card.**
- **Checking the sides of the ATM to verify if any fixture has been added, such as a fake advertisement box that could be used as a container for cameras or other data-capturing devices.**

10.13.3. For point of sale terminals the bank must state clearly in the contract that merchants are not allowed to swipe the card data and to keep it stored in clear text as it can lead to theft of data.

10.13.4. POS terminals must comply with best practices and standards such as: PCIPED/PTS and PIN security requirements. Terminals must:

- **Protect customers against shoulder surfing. Terminals have means to hide the keypad while keying the PIN code.**
- **Encrypt the data all along the way to the terminal and then to the acquirer, for PIN entry, PIN processing and validation, payment validation and printing.**

— **Be tamper proof, evident and responsive.**

— **Must support at least TDES, AES or better encryption.**

10.13.5. Sales or payment receipts must not disclose the credit card details and encoding the data must be a common practice on merchant and customer receipts.

10.14. Handling cheque

10.14.1. Sensitive information on cheque, such as personal account numbers, account holder’s name and signature, must be kept in a secure area.

10.14.2. If the cheque are digitally signed, the data must be secured by cryptographic techniques, as defined in the cryptographic section.

10.14.3. Measures for identifying customers must be in line with best practices, such as KYC, and the bank must maintain the same level of controls when identifying and registering new customers.

10.15. Core banking systems

10.15.1. Core banking servers and infrastructure shall be reliable and resilient. Implementation and management of core banking services to be done in line with network management guidelines.

10.15.2. Core banking applications and databases shall be secured, as per software security and data security guidelines.

10.15.3. VA and PT of set of applications linked to the core banking applications and database shall be performed as per vulnerability assessment and penetration testing guidelines.

10.15.4. Core banking systems must adhere to the cryptographic and key management guidelines.

10.15.5. The bank must ensure that:

— **The core banking system is resilient through specific/business continuity mechanisms at business and technical levels.**

— **A policy to ensure compliance, security requirements and security events exists. Archiving of such events is a must for subsequent analysis and complying with the legal requirements for data retention in Qatar, as well as the requirements mentioned in this document.**

— **Integrity control processes are implemented on the main data residing in the core database, as well as versioning system for the application changes.**

— **It is a must that the core information is hidden from unauthorized access through a secure mode such as encryption methods and layered infrastructure. The core banking application database sensitive information records must be protected by using latest encryption standards.**

— **The bank must use authentication mechanisms that will ensure that authorized and clearly identified personnel have access to sensitive information, using RBAC principles internally.**