Modern Technology and E-Banking Services Risks

Circular no. (105/2012)

Dated 22/11/2012

Part VII – Chapter 3

Table of Contents

Abbreviations .....

Chapter 3 –Technology Risks .....

3.1. Management of Technology Risks .....

3.1.1. Identification & Assessment .....

3.1.2. Monitoring and mitigation .....

3.2. Technology Risk Organizational Structure .....

3.2.1. Information Security Organization .....

3.2.1.1. The Chief Information Security Officer [CISO] .....

3.2.1.2. Information Security Officer (ISO) .....

3.2.1.3. Security Operators .....

3.2.2. Technology Risks Awareness .....

3.2.3. Data Protection .....

3.2.4. Physical Security .....

3.2.4.1. Data Centers .....

3.2.4.2. Control Rooms .....

3.2.4.3. Specific Data processing rooms .....

3.2.5. Logical Security .....

3.2.5.1. Applications Security .....

3.2.5.2. System Security requirements .....

3.2.5.3. Network controls .....

3.2.6. Core Banking Systems .....

3.2.6.1. Integrity and Resiliency .....

3.2.6.2. Confidentiality .....

3.2.6.3. Documentation .....

3.2.7. Internet and Mobile Banking .....

3.2.8. Payment Systems .....

3.2.9. Electronic Fund Transfer .....

3.3. Handling cheques .....

3.4. Business Continuity
3.5. Incident and Fraud Management
3.5.1. Incident handling
3.5.2. Internal Fraud
3.5.3. External Fraud
3.6 Outsourcing the Information Technology function
3.6.1. Data Centers Organization
3.6.2. Operating abroad
3.6.3. Cloud Computing Security
3.7. Process Risk controls
3.7.1. Access control
3.7.1.1. Principles
3.7.1.2. Identification
3.7.1.3. Authorization
3.7.1.4. Authentication
3.7.1.5. Segregation of duties
3.7.2. Change Control
3.7.3. Key Management
3.7.4. Audit Journals/Event Logging
3.7.5. Data Retention & Archiving
3.7.6. System Life-cycle & Software Development
3.7.7. ICT Disaster Recovery
3.7.8. ICT Procurement
Appendix
Appendix

Abbreviations

QCB	Qatar Central Bank
3DES/TDES	Triple Data Encryption Standard
AML	Anti-money Laundering
ATM	Automated Teller Machine
BCP/BCM	Business Continuity Plan/Management
CAM	Card Authentication Method
CEO	Chief Executive Officer
CC/EAL	Common Criteria/Evaluation Assurance Level
CISO	Chief Information Security Officer
CMS	Card Management System
COBIT	Control Objectives in Information Technology
DBA	Database Administrator
DES	Data Encryption Standard
DRP	Disaster Recovery Plan
EMV	Europay MasterCard Visa
FIPS	Federal Information Processing Standard
FSP	Financial Services Professional
HSM	Host/Hardware Security Module
IAIS	International Association of Insurance Supervisors
ICT	Information Communication Technology
ID/QID	Identity/Qatari Identity
IOSCO	International Organization of Securities Commission
ISO	Information Security Officer
ISO27001	Industry Standard Organization 27001 on information Security

	Management
MOU	Memorandum of Understanding
PA-DSS	Payment Application Data Security Standard
PAN	Primary Account Number
PCI-DSS	Payment Card Industry Data Security Standard
PCI-PED	Payment Card Industry Pin Entry Device
PCI-PTS	Payment Card Industry Pin Transaction Security
PIN	Personal Identification Number
POS	Point of Sale
QTEL	Qatar Telecom Company
RBAC	Role-Based Access Controls
RSA	Rivest Shamir Adelman public key encryption
SHA	Secure Hash Algorithm
TCP/IP	Transport Control Protocol/Internet Protocol
PKI	Public Key Infrastructure
VPN	Virtual Private Network
SSH	Secure Shell
SDLC	Software Development Life-cycle

Chapter 3 –Technology Risks

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 technology evolutions as well as its implications.

Technology risks are defined by the type, nature of threats targeting and impacting a banking environment through the usage of information communication technology infrastructure, generating events that may lead to the disruption or damage of banks information systems or data.

The technology risk process resides in the establishment of procedures and controls to monitor and mitigate the risks that may affect the technologies supporting the business activity, whether the risks are on the business or on the technical side, banks must define a set of appropriate controls to mitigate these risks.

As banks rely heavily on technologies such as the World Wide Web or applications to operate in many areas, the understanding and acknowledgment of technology risks must be acquired. In a highly interconnected and market driven world, it is of utmost importance that banks have a reliable, flexible, complete and integrated set of operating processes as well as sound operational risk management systems in place.

The importance of technologies in electronic services and banking operations has heavily grown in the past years to become a mandatory and critical tool for any financial institution. Technologies involved in the daily operations are critical as they are responsible to keep the business activity performance healthy.

The increase of the usage of internet technologies to deliver banking services, payments, corporate cash management or fund transfer brings benefits to customers, while it introduces a lot of security issues and constraints.

International organizations such as The Basel committee have addressed these risks through different frameworks. these organizations proposed frameworks for internal control systems issued in September 1998, sound practices for the management and supervision of operational risk issued in February 2003, Risk Management for Electronic Banking and Electronic Money Activities issued in March 1998 and Risk Management Principles for Electronic Banking. These frameworks amongst others represent a good baseline to define key principles that will address the technology risks in a banking environment.

Prior to "*know your customer*" principles, it is now critical that banks apply a "*know your organization, processes, infrastructure and risks*" principles.

3.1. Management of Technology Risks

Technology risks are better handled when the financial institutions are well prepared. Therefore a segregation of risk control functions and daily operations is a must and it will benefit the resiliency efforts of financial institutions. A central information security dedicated function is also necessary as long as it is implemented on the side of the daily technology operations.

As described on corporate governance section of QCB instructions, the board of directors and management of a bank are accountable for the risks a bank may face, which includes technology related risks. A sound risk management practice requires a phased approach that should include the following steps:

- Identify and classify the risks on the bank's systems and operations
- Develop a plan that will contain policies, procedures and best practices that address those risks
- Implement and regularly test the plan
- Monitor those risks and update the plan regularly to take into account the evolution of technologies, legal requirement and other mandatory requirements

Risk controls are better managed through dedicated resources and functions. So a role/function must be in place and fully dedicated to the management and controls of the risks related to the use of systems, software applications and automated information processing. The person in charge who is responsible for designing policies and procedures will enable security controls by providing the information technology department with the standards and identified controls. This function will report directly any security incidents, issues, events to the Chief Executive Officer and will keep dotted line reporting with the internal audit to follow-up on any auditing issues.

3.1.1. Identification & Assessment

QCB understands that banks are handling risks by establishing an internal risk assessment practice that covers technology risks. At a central stage, policies must be aligned with the business objectives, focusing on key critical processes and business operations.

A bank should define the set of critical processes where controls need to be applied. Not only a complete inventory of these processes and related assets will be necessary, but also a detailed description of potential threats will help in determining what is highly probable to impact key critical assets of a bank. The assessment phase will highlight the

most vulnerable parts of the environment that draw specific attention. So in order to implement the basics the bank should:

- Assess the risks of potential threats on the banks assets
- Assign a risk rating to each area of vulnerability
- Determine the applicable security controls

Prior to the assignment of the risk ratings, the bank must implement a well defined set of procedures that helps to identify key critical processes and assets.

3.1.2. Monitoring and mitigation

Risks identified should be constantly monitored. After a risk assessment exercise, banks must take necessary measures to address them and keep them under close monitoring.

Banks must ensure that key risks controls are in place on key critical assets. Those assets holding critical sensitive information such as bank account records, customer/corporate client's information and databases should draw specific attention. This exercise is efficient only when collaboration across different units exist. Therefore it is highly recommended that technology risk assessment, monitoring and mitigation is done by establishing key risk indicators raised with key stakeholders. Management should be involved in reviewing and validating the results. These Key Risks Indicators will make sure that a regular monitoring of technology risks exist as well.

Banks must share immediately with QCB Banking Supervision department any information related to loss incidents, cyber attacks and security related events, according to the chapter nine on other banking issues of the instructions to banks book. These events must be properly documented with analysis and incidents reports as soon as they arise. The risk indicators should highlight the number of attempts of cyber attacks, vulnerabilities discovered, breaches …etc.

3.1.3. The Information Security Program

Prior to the implementation of security controls and risk mitigation measures, banks must develop a whole set of documentation related to such program. International standards such as ISO27001:2005 and its set of controls ISO27002 provide good basis to initiate such program me. However QCB expects that each bank will develop its own set of policies tailored to each of the bank's strategy, size and management approach.

In order to develop such polices banks should follow key steps such as:

1-Develop an information security policy covering key areas of controls that need to be addressed.

2-guidance and security practice documents help in enforcing the policy should exist.

3-Develop procedures that needs to be followed consist ant with rules and best

Practices.

3.1.3.1. The information Security policy

The policy document is a central document that will highlight key areas of concerns that a bank need to supervise internally and establish related controls. Practice shows that in order to implement policies in a most efficient manner, a policy document should be more precise than its related practice documents.

The policy should be an abstract, with clear scope and objectives and must follow key principles such as:

- The policy document must be approved by the board of directors, who is the main stakeholder.
- The document must be developed in accordance with best practices and regulatory requirements, as the document must adhere to local and international regulations the bank is subject to.
- The policy should be available to all users, signed by all users in acknowledgement of having had a copy of the policy document. Various methods like internal communication, human resources department processes and a dedicated awareness plan must be in place as per paragraph 3.2.2 of these instructions.
- Maintenance and updates is the responsibility of the information security lead person.

3.1.3.2. Practice and guidance

A security practice document defines the controls to be implemented as specified by the policy. The security practice should cover each area defined in the bank's information security policy. Such a document must be a practical guide, adaptable to the evolution and needs of the bank.

Practice and guidance documents should be developed depending on the size of the bank, defining the scope and users of the security practice documents. Owners must be clearly defined, with business units or technical departments as well.

3.1.3.3. Security procedures

Operational security procedures documents as derived from security policy and practice documents, must also comply with the requirements of the corporate policy. The scope of the security procedures should be clear, precise and focused to technological issues and bank's systems.

The security procedures documents are initiated by the Information Technology related function. Procedures must take into account all requirements from regulations, standards and practice documents.

3.2. Technology Risk Organizational Structure

Risk Management in banks should take into consideration the evolving aspects of technology risks by implementing roles and functions for mitigating those risks. Information security is a function that deals with technology security risks and threats.

This section describes roles and responsibilities that will enable banks to handle such risks, and QCB will ensure that these principles are planned and appropriately implemented by banks. The objectives of this structure are to have an independent reporting function to key managing authority within the bank. Such structure might vary depending on the size of the organization or on the structure defined earlier.

3.2.1. Information Security Organization

The development of an information security program is a must in any financial institution taking steps in mitigating technology risks. In order to do so, the Management of a bank must ensure that a dedicated functional organization is setup. Thus the management of all information security components is part of the overall organization strategic plans. Depending on the roles and security objectives, the information security functions will be independent from the Information Technology operations, while IT Security operations will remain within the information technology departments. The Appendix A describes the best practice for establishing a technology risk and security function within an organization. As per this organizational structure it is important to keep the audit department updated with any issues highlighted in the management letter, during the audit process, as such a dotted-line reporting exist where the auditor could be a member of the security committee.

The profiles listed below abide to this structure, ensuring a clear segregation of duties and are provided as guidelines, which also depend on the size of organizations and structure.

3.2.1.1. The Chief Information Security Officer [CISO]

The Chief Information Security Officer is mainly responsible for the design, implementation and management of the information security management system program (ISMS). Under the direction of the CISO, personnel at the other levels perform duties that are required under the policy and practices of the information security framework implementation.

The CISO could have dedicated staff and exercise administrative controls over the information security personnel. In smaller banks or financial institutions, the CISO may have limited operational control of personnel who perform information security duties in addition to their other duties related to banking. Regardless of the size or management style of the organization, the CISO is the person who is ultimately responsible to the directors and executive officers for the execution of the information security program. To discharge the responsibilities, the CISO should be assisted by security committees adhering to the requirements of the framework, policies and controls.

The CISO manages the information security program according to the conditions that have been identified by the organization as relevant to the success of the business activity. The CISO is responsible for:

- Presenting and justifying the information security program and related framework(s) to the chief executive officer, 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.
- The identification of 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.

3.2.1.2. Information Security Officer (ISO)

An Information Security Officer or a specifically designated Security Architect [SA] is any person(s) in the financial institution who is responsible for developing, implementing and maintaining the information security program under the direction of the CISO. Some ISOs may possess specialized expertise in information security techniques such as risk assessment, threat awareness, etc. and act as a resource for the entire organization.

Other ISOs will provide guidance and advice to a particular business unit on information security concerns. The ISOs will be most effective if they understand the business objectives as well as the internal processes of the organization. The ISOs should:

- understand the security architecture, practices and procedures;
- develop local practices, communicate them and update as appropriate;
- conduct risk assessments;
- monitor and audit security practices;
- assist in recovery from attacks on the IT systems;
- make recommendations for improved practices and procedures;
- keep up-to-date on information security threats, technologies and techniques;
- Promote information security awareness.

3.2.1.3. Security Operators

Security operators perform the most detailed day-to-day actions in order to accomplish the objectives of the information security program. Security Operators are usually part of the Information Technology department but fall under some obligations of reporting to the information security department. They must be knowledgeable of the hardware, system, software and security procedures necessary for their business units. Because of the variety of technology that might be utilized in security architectures, security operators will need to perform a set of procedures. Some representative duties that might be required are: install and

maintain security settings on network equipments; install security updates on operating systems; maintain and update accurate access control files; collect information on security issues, audit information and monitor system or network activity to discover security problems.

The wide variety of tasks shows the importance of security operators in the successful implementation of the information security program. The security operator shall be responsible for:

- understanding how the security operator role supports the security architecture and program;
- implementing and maintaining security practices and procedures;
- monitoring security procedures and reporting their status as appropriate;
- acting to correct security failures and to counter attacks

3.2.2. Technology Risks Awareness

Risks are best handled when related information and threats are shared with stakeholders. Those risks might exist either internally or externally, therefore a dedicated information security awareness program should be part of the overall security strategy program established by the bank for internal users as well as for customers.

- ***Awareness to users***

As part of its internal organization, banks must establish procedures in order to educate and communicate on the risks and security issues that may exist to the internal users. It should be addressed on a regular basis and should help protecting the banks most valuable assets.

New employees should be educated as early as possible about the risks, even briefed before starting using bank systems. Ideally such awareness exercise is done in collaboration with a bank human resources department as part of the HR induction process. The information security function should work closely at developing materials required to communicate and educate.

- ***Awareness to customers***

A bank has also an obligation to disclose to its customers any information about potential issues related to the customer's personal information data. Preventive measures such as developing campaigns to inform about the technology risks should

be developed by the banks in order to make customers aware about potential threats and security issues.

Domains such as the usage of the payment cards, online banking or any other electronic banking technology risks must be covered under such campaign amongst others.

3.2.3. Data Protection

Banks hold sensitive information such as customer records, account information as well as personal information such as names, birth dates, addresses, Qatar Identity number and many others. Banks must take all necessary measures to ensure proper protection of these records such as:

- Using encryption methods on data as per paragraph 3.2.6.2.
- Having systems and networks well protected against misuse, internal and external threats following the requirements listed in paragraphs 3.2.5.2 and 3.2.5.3.
- Having sufficient organization around the processing of information: segregating roles is an example
- Monitoring the access to sensitive information

Customer records must not be sent across non secure environments, via the internet or non secure electronic means such as electronic mails without securing the communication channels. Customer records must be secured also when offline, whether stored or archived and sufficient measures must be in place to prevent data loss and leakage of their customer records.

Online banking systems should be provided via secure authentication mechanisms, encrypted pages and security validation processes, thus ensuring a trustable place to do banking operations. Retention of data shall be following requirements listed on paragraph 3.7.5.

Data protection practice must be in line with Qatar laws and regulations.

3.2.4. Physical Security

Secure areas should be clearly defined and implemented around sensitive data processing environments. Data Centers require specific controls while areas such as the card processing environments must be protected in a more secure way following the principles of:

- Strict segregation of functions: the Card creation and data input/processing room must be separated, allowing single entrance through logged access only
- Pin processing room must be secure against potential unauthorized access, fire hazards or other risks impacting the production process or allowing data leakage.

Qatar Central Bank emphasizes the necessity of keeping sensitive documents such as the banknotes, cheques and other monetary instruments inside safe rooms and in fireproof safe under proper custody. It also emphasizes the necessity to attach these safe rooms with an alarm device system connected to the police department; installing camera inside and outside the safe room connected to the control room or at the branch manager's office and where control rooms must be accessed only by authorized staff. Additionally banks must have dedicated procedures to recover operations in case of disasters, through the banks disaster recovery plan as per the principles listed on paragraph 3.7.7 of these instructions.

3.2.4.1. Data Centers

Data Centers host mission critical systems supporting business operations. As the main repository of business data through IT and Telecom infrastructure, the data centre requires a high level of protection.

Banks should therefore take all measures to ensure resiliency, continuity and integrity of the systems. Therefore it is important to make sure that the following requirements exist:

- The overall layout of the room will allow enough space for the staff to work efficiently, adequate airflow, while leaving adequate space for future potential growth.
- Access control mechanisms: allowing only individuals with proper credentials related to their function to access the Data Center, following RBAC (Role-based Access Controls) principles. Another layer of controls will be required on computer racks, depending on the organization of the data center, especially when it is using shared premises.
- Sufficient monitoring of activities taking place inside the data centre as well as in surrounding areas.
- Fire protection systems should be in place with smoke detection mechanisms as well as manual and automated fire extinguishing systems:

- Inside the data centre: automated fire extinguishing systems using for example distilled water, foam or CO2/Halon gas must be implemented.
- Outside the data centre: manual fire extinguishers must be available.

- Sufficient power should be provided to ensure that systems will continue functioning properly with redundant power supplies as well as uninterruptible power systems, batteries or generators.
- Proper cooling system must be in place to avoid system disruption due to overheating.
- Cabling should be organized in a way to avoid wrong manipulations, wire tapping or wire cutting hazards. Standards such as EN 50173-5 or ISO11801/18019 can be used as best practice.
- False floor and roofs allow cabling guides and airflow circulation, as well as resistance to natural hazards might be considered.
- The infrastructure must be fault tolerant and redundant.

Best practices such as TIA-942 might be taken into consideration while organizing a data center.

3.2.4.2. Control Rooms

The requirements defined on paragraph 3.2.4.1 apply also to banks specific areas such as Control Rooms. These rooms in banks are important as they are dedicated to the monitoring of all activities (logical and physical). Therefore additional security controls must be in place such as:

- proper video monitoring equipments
- Screens focusing at various camera angles.
- Recording period in line with retention requirements.
- Set of centralized monitoring systems for critical applications and systems (for logical controls)

People involved in such functions should be trained properly and remain available in the room during their time of duty.

Banks must have back-up control rooms to respond to potential disasters or in case of crisis, as per the banks business continuity principles and disaster recovery procedures.

3.2.4.3. Specific Data processing rooms

Rooms where highly sensitive equipments such as cryptographic materials and cryptographic keys are maintained must be subject to additional scrutiny and controls. Cryptographic keys must be kept in a safe located in a secure area. Access to those keys must be limited to authorized personnel depending on roles and responsibilities.

Handling equipments that store or process cryptographic material are subject to paragraph 3.7.3 of the instructions on key management process. The following controls must be considered when dealing with cryptographic rooms:

- Close monitoring of activities: CCTV network and recording must be in place.
- Also additional access control and physical protection levels might be needed depending on the risk assessment results.

Cryptographic devices are used for validating secure payment operations of the bank payment devices; therefore controls listed above are considered as a minimum baseline to avoid risks of manipulation and rogue accesses. Automated Teller Machines or payment terminals for example are using such facilities to authorize payment cards to operate. ATMs are also subject to specific controls as described on paragraph 3.2.8.5 of the instructions.

3.2.5. Logical Security

Banking operations are heavily relying on software, systems and networks to support their business applications. The IT Infrastructure has become the backbone of the entire business structure, as such security controls must be considered on logical layers as well to mitigate the risks that may arise from potential cyber attacks.

The requirements defined in standards such as ISO27001:2005 and its associated controls, COBIT or other best practices can be identified as baselines, while additional requirements might be added by experience and practice.

Electronic transactions are subject to the provisions of e-transaction and e-commerce law, decree law No 16 of 2010. Therefore, when conducting transactions by means of electronic communications, the requirements that fall under the purview of

this law relating to the protection of data messages transmitted or received should be complied.

3.2.5.1. Applications Security

Applications are keys in the daily activity of a bank. Following a risk assessment exercise, banks must determine the level of criticality of applications, which should be based on the importance and impact to the business as per the risk management approach.

A sound security approach to applications starts with defining the right process by ensuring that responsibilities and ownership of critical applications exist at business level. This process empowers the business function to assign the necessary roles and privileges in their defined applications. Although the IT function remains the provider of the applications, the head of a business unit function has controls over the dedicated application, thus making the head of the business unit the main application owner. The application owner is involved in any change related to the application he is responsible for and as such is part of the change management process of the bank as per paragraph 3.7.2.

Banks should make sure they acquire applications that include security considerations by adopting information security standards and best practices such as ISO27001 as well as OWASP for web applications.

Applications should be tested, certified and validated prior to the implementation in production environment as per the change management process defined by the bank in its software delivery life cycle. The security review of application codes is a must and should be an integral part of each phase of the software delivery life-cycle.

Policies and procedures should prohibit the use of production data in testing phases while exceptions could be allowed under specific circumstances, only by a proper approval process involving a hierarchy of officials that should be defined by the bank policies and procedures. This process will follow the change control process as described in paragraph 3.7.2 for traceability purposes.

A well defined application delivery life-cycle process includes the following processes:

- Change Controls to the application.

- Testing, certifying and validating application development or changes prior to put-in production phase.
- Protect applications against potential vulnerabilities via regular updates.
- Applications must be subject to an IT audit process.

Sensitive data processed within the bank should be protected against unauthorized access or data leakage using encryption or equivalent compensating control methods, such as proper network infrastructure segmentation, host security applications, separation of duties or others.

The same set of requirements listed above applies to the core banking application database including a well documented change control process. As such a database administrator must ensure that all events on those sensitive databases are monitored. Those logs will be generated by the database and kept as per the data retention requirements. A security policy will determine the security configuration of the database that will allow those events to be recorded.

Web applications are provided for the convenience of the customers to do banking operations from any place. Risks are high when operating transactions from the internet as it is a non-trusted network. Therefore web applications must be scrutinized against vulnerabilities, threat factors and tested against those risks prior to put in production. OWASP or SANS top 10 are recommended as a baseline to assess these applications. External controls will help mitigating those risks, as defined in 3.2.5.2 and 3.2.5.3.

3.2.5.2. System Security requirements

Bank systems should conform to bank's internal security policies and best practices. Therefore mechanisms to prevent unauthorized access, modification and control of these systems must be in place. Key security processes highlighted on paragraph 3.7.6 need to be thoroughly implemented.

The standard ISO27001:2005 provides detailed set of guidelines and best practices to ensure systems are secure and well managed. Complying with such standard will help achieve good security level; while such practice needs to be constantly reviewed as the threat landscape evolves continuously.

Capacity management and planning must be in place to ensure that appropriate management organization is applied on banks defined systems, including a well

defined maintenance plan that includes controls of equipments prior to implementation. The change control process is defined in paragraph 3.7.2.

Critical systems of the banks are those systems supporting critical information related to the core banking applications and databases. These critical systems will be subject to specific attention and must meet the required controls described in this document, especially those controls outlined on paragraph 3.2.6 and 3.6 of the instructions.

Any disruption must be mitigated by ensuring adequate redundancy and disaster recovery planning in line with the business continuity plan strategy.

Controls should limit media access to systems; input/output ports should be controlled to minimize the risks of malicious software spread.

3.2.5.3. Network controls

Networking equipments must be secured as per their function in the bank. Three main areas of networks would exist in any banking environment today that will provide several layers of segregation.

- **Internal network:** organizing the internal network infrastructure by layers will help isolating the core banking systems and database from uncontrolled access weather from inside or outside world. A top-down network hierarchy approach based on the functions of the network layers should be used to separate existing LANs (or VLANs).

- **External network:** usually depending on the local telecommunication service provider, external networks are those layers that are connected to other entities or public networks. An external network is never connected directly to the core banking applications.

- **De-Militarized Zone (DMZ):** is defined as an isolated network that needs to be accessed from external networks such as the Internet. The applications residing in such network are often used for providing web banking services, online payment services or any other internet based service. DMZs are protected with multi-layer security controls such as network packet filtering, intrusion detection and prevention systems, application level firewalls and other security mechanisms that would help mitigate the risks of intrusions or spread malware.

Since the network administrators or operators function is dedicated to maintaining the network infrastructure, through network management processes, they should not be allowed to access data packages content. Such access shall be provided under specific conditions that would require a formal approval process that can be traced during an audit process.

Changes to any configurations shall be in line with paragraph 3.7.2 of the instructions. Data such as non-encrypted banking operations might be circulating over the banks local network making it an easy prey to capture by rogue network tools.

Banking systems will be subject to specific scrutiny as described on paragraph 3.2.6 of the instructions.

Direct network connectivity with production systems from outside the banking network environment perimeter is prohibited, excluding specific business connectivity requirements such as settlement process requirements or payment processes (Swift, SIBNET, NAPS, Payment Cards licenses networks, etc…).

Cross border connectivity might be allowed for a limited access to some non secretive information. In case the bank is outsourcing its IT functions, the requirements to use such facility should be in line with paragraph 3.6 of the instructions on outsourcing controls.

Payment systems networks are subject to specific security requirements that will include those mentioned in paragraph 3.2.8, as well as additional guidance for encryption, key management and network security principles required by Qatar Central Bank.

Any existing wireless network infrastructure must be a stand-alone infrastructure without any connection with the banking business network. The wireless network will be an isolated separate network.

3.2.6. Core Banking Systems

One of the most critical assets, where the entire business activity of the bank relies on, is the Core Banking System. The criticality of such system is defined by the business activity and a risk assessment process. The risk assessment will enable a classification of systems, data and applications for the purpose of implementing necessary controls to maintain its confidentiality, integrity and availability. A core banking system usually relies on:

- A set of reliable and resilient hardware equipments to handle, process and store data
- A database supporting all the information
- A set of applications linked to the main database that will enable the business processes (examples: inter-banking transactions, rates injection, reconciliation, etc…)

Key security requirements should be applied as measures to counter potential threats, whether it is occurring internally or externally. The controls provided in the following paragraphs are the minimum baseline that any bank should seek to apply to ensure a safer environment.

3.2.6.1. Integrity and Resiliency

Maintaining critical information available permanently and ensuring data has not been compromised or changed without authorization are main challenges that banks have to face.

In order to mitigate disasters, banks must be prepared to provide continuous services to their customers. At the same time, financial information will remain secure and protected against threats. Therefore, banks should ensure that:

- The core banking system is resilient through specific business continuity mechanisms at business and technical levels, as described in the ICT Disaster recovery paragraph 3.7.7. And the Business Continuity paragraph 3.4.
- A policy to ensure compliance, security requirements and security events exists. Archiving of such events will be necessary for subsequent analysis and complying with the legal requirements for data retention in Qatar, as well as paragraph 3.7.5 of 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.

3.2.6.2. Confidentiality

An increasing trend in the threat activity and sophisticated attacks is witnessed worldwide. Ensuring the security of data processed in a core banking system is important to protect against various fraud attempts such as account takeover, sensitive information disclosure and many other risks.

Therefore it is a must that the core information is hidden from unauthorized access through a secure mode such as encryption methods and/or layered

infrastructure. The core banking application database sensitive information records might be protected by using methods such as hashing (SHA-256 or other…) or encryption (3DES, AES, RSA, etc…) processes. The data that needs to be encrypted will depend on the risk assessment results.

Banks must use authentication mechanisms that will ensure that only authorized and clearly identified personnel has access to sensitive information, using RBAC principles internally as per paragraph 3.7.1.

3.2.6.3. Documentation

Documenting any banking environment is required especially in case of incidents where a need to recover operations or follow-up on changes is rising. Every change, modification, update or development on the core banking systems must be documented as per the change control process described on paragraph 3.7.2 of the instructions.

3.2.7. Internet and Mobile Banking

The Internet poses several risks to any bank willing to propose online services for customers or corporate organizations. The attraction by fraudsters to internet related technologies is due to the un-trusted nature of the Internet zone.

Banks are providing services online on the Internet allowing customers to access those banking services on computers or mobile devices. Websites are identified in three types as described below:

A- Information Site: It is the simplest online banking services by which customer can contact the bank to inquire about services and products without online interaction with the banking environment.
B- Interaction Site: allows a customer to interact with the bank and enable the view of banking information such as a bank account(s) details.
C- Transactional Site: Customers can make transactions like payment of invoices/bills or making internal and external funds transfers.

A prior approval from QCB should be obtained if a bank wishes to implement an online banking service of type (C) (transactions site). Type (a) and (b) do not require QCB approval.

To mitigate the risks of threats impacting financial information circulating over the internet, banks must implement controls and security measures that will guarantee the confidentiality and integrity of data provided to their customers, based on the result of

a dedicated risk assessment process. The following set of measures must be considered in order to increase the level of confidence within the financial institution.

- **Online Authentication:** simple password access is no more sufficient. Strong authentication mechanisms using at least two factor authentications are required.
- **Trust:** most of the banks would have already implemented the usage of digital certificates to ensure authenticity of their websites, PKI technologies might be used to develop a strong authentication process for online banking or payments.
- **Data Security:** Any transaction occurring during an online banking session on the internet must be processed in a secure channel, using encryption as one way to secure data online.

Enrolment for customer authentication tools shall take in place in a trusted environment, whether it is happening online or in the bank premises, procedures shall take into consideration the risks related to the process.

Banks could face large scale cyber attacks such as phishing attacks or botnets resulting in theft of data. Therefore Banks must report any potential threat event to QCB and coordinate with the nation's cyber security unit, Q-CERT to respond to such attacks.

QCB recommends that at least two full penetration testing sessions per year and four regular vulnerability assessments exercises per year are conducted to assess properly the level of security of any internet/mobile banking applications.

Banks should develop a comprehensive security awareness program for the customers using mobile and internet banking applications as highlighted in paragraph 3.2.2.

3.2.8. Payment Systems

Banks are providing payment card services via a whole dedicated chain of processes which brings with it various risks to the financial information residing in the card, whether it is processed or stored.

The EMV standard, known also as "chip and pin" has now been accepted widely. In Qatar all payment cards and related terminals must be EMV compliant with no fallback to the magstripes data, as payment operations should accept only chip and pin authentication. Switching to magstripes will be allowed only for international non-EMV cards.

The payment process is based on the usage of the credit or debit card for payments, whether at a Point of Sale terminal (POS), online via the internet or at an Automated Teller Machine (ATM).

Whenever a bank deploys a payment device such as a POS or an ATM, minimum safety and security measures should be implemented.

Issuing Banks are responsible for their issued cards and should take necessary measures to protect the financial information contained in those smartcards.

QCB would seek evidence of compliance with international security standards 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 (PCI-PTS) and PCI-PIN Entry Device Security. Assuming that most of the banks are dealing with payment card processes, QCB understands that such security validation standards are already in place in Qatar, to ensure the security and safety of the financial market place.

3.2.8.1. Payment Card data

A payment card carries with it a set of banking account related information, including personal information and card account details. As per the implementation of EMV standards, the cardholder data is located mainly on the chip, while other data remains available also on the magstripe.

When this data is processed, there are risks that such information could be stolen via various methods. The payment card industry council has issued the PCI-DSS standard which highlights two main types of data that need to be protected:

- Cardholder data: the PAN, Expiration date, service code, cardholder name
- Authentication data: magstripe data such as ISO2 track, CVV2/CVC, PIN, PIN blocks

According to the PCI-DSS standard, cardholder data can remain stored in an encrypted manner, while authentication data must not be kept stored in any way after the payment authorization process. Authentication data serves only once at a time, therefore it must not be used for data retrieval, transaction replay or any stored process operation. Cardholder data is considered as a sensitive data the banks need to protect efficiently.

3.2.8.2. Payment Card Creation process

Several requirements are outlined in the Data Center security paragraph related to the physical security for a bank sensitive area. Additional levels of security are required for the payment card creation process rooms.

When making a Card several steps are mandatory such as embedding data on the chip and magnetic stripe, designing the plastic card and embossing the characters seen on the face of the card. All these processes must be secured and limited access to the area as per physical security requirements, one person should be allowed at a time to the card creation room while another staff will be allowed at a time in the pin processing room

The personalization process requires several steps which includes the embossing/writing of cardholder data on the card, data on the chip and magstripes. All cards issued must be EMV compliant, following deployment of EMV applications on ATMs and POS terminals.

3.2.8.3. Card Activation

Banks must make sure that cards are activated only after the customer has received it. Banks must have a dedicated process to identify and authenticate the cardholder prior to hand the card to the customer.

Payment cards must always be assigned to the bank account holder where it is issued from, and clearly identifies the cardholder. Anonymized payment cards are prohibited for a long term use, but can be considered for short term replacement while waiting for receiving the final payment card.

3.2.8.4. Card Management systems

Information security should be more rigorous in a Card Management System (CMS) of a bank. Such environment can be subject to fraudulent activity if not well organized.

By the CMS, Qatar Central Bank means the complete set of management software and systems that allow banks to monitor, modify, update or block the cards issued by the bank remotely whether it is used on ATMs, POS terminals or online.

The access to the CMS shall be limited to the users who are assigned with such tasks of handling the payment cards operations. The systems shall be separated

from other banking applications and strict access controls must be in place: access logs must be generated by the system, limitations of privileges shall be in place and split of high privileges accounts (administrator roles and above) that control changes shall be implemented.

QCB insists on the importance of having a specific change management process related to such environment as per paragraph 3.7.2.

3.2.8.5. PIN Security

The generation of PIN must take place in a secure area segregated from the Card data creation and processing room, where only selected personnel can access and room is under permanent video surveillance. Standards such as ISO 9564-1 to -4 specify the minimum requirements for handling PINs, preventing from unauthorized interception by fraudulent persons. The following list highlights some of the key requirements that a bank need to be compliant with:

- PIN generation must take place only in Tamper-resistant Security modules.
- ATM and POS Terminals using encrypting keypads only, are allowed in Qatar as PIN and sensitive data must always be encrypted during the processing time.
- Cryptographic keys used to generate PIN code must not be used in testing environments.
- Host Security Modules (HSM) used for PIN generation and processing must be at least FIPS 140-2 level 3 or CC/EAL4 compliant.

Additional awareness programs shall include PIN protection information for the customers as per the obligations listed in paragraph 3.2.2.

3.2.8.6. Payment devices security

Payment devices are those tools that will enable the usage of a payment card from various networks either on trade/merchant establishments or at a bank automated teller accepting payment cards. Payment devices have improved in terms of usability and level of security whether it is on a Point of Sale Terminal or on an Automated Teller Machine and have become more open to standard network protocols such as TCP/IP or common operating systems found on desktop computers.

When processing over TCP/IP networks, banks must ensure that data passing through network cables from a terminal is fully secured via encryption. Methods such as tunneling over VPN, SSH or other secure tunnels are available for safe implementation to the acquiring processor or the payment authorization center.

When getting a device from the vendor, the bank must ensure that a proper hardening process has been applied to each device prior to deployment at the merchant site.

- ***Point Of Sales Terminals***

Point of Sales terminals allow payments at merchant sites which are more often target of fraudsters. Cardholder data can be stolen by either technological or non technological methods.

The merchant payment receipt ticket shall not contain cardholder data in clear, data shall be masked on both the merchant and customer receipt.

Banks should 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 may lead to theft of data.

POS terminals should comply with best practices and standards such as PCI-PED/PTS and PIN Security requirements. Terminals must:

- Protect customers against shoulder surfing. Terminals should 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.

Banks must have approved the deployment of these terminals before putting them into production environment through a dedicated and approved system life-cycle procedure.

Additional measures such as the request to present the cardholder id should become a standard practice; the bank may consider this practice as a must for certain payment transactions thresholds. Cardholder must be the owner of the payment card, so physical Card authentication Method (CAM) should be used to validate the authenticity of cards.

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.

- ***Automated Teller Machines***

ATMs are generally outside a banks security perimeter. Therefore Automated Teller Machines have been constantly targeted by people trying to get access to easy money. ATMs have faced several steps in theft of money, from direct robbery at the ATM to insider fraud attempts.

Banks should take appropriate measures to secure ATMs. The following security requirements must be at minimum in place on ATMs:

- Camera must be installed to cover the ATMs surrounding space with angle not less than 70 degree.
- Pinhole camera installed should 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 should 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 should cover retention period mentioned in the latest instructions issued by QCB.
- Real-time monitoring of ATM logical and physical events must be implemented.
- Screen displays must be inclined and side view protection should exist in addition to installing keypad typing cover protection in order to avoid shoulder surfing that could lead to personal information stealing.
- Keypad security: keypads must be placed in a way that will avoid key loggers to be implemented. Also when typing the PIN information, data must be encrypted, so keypad must be an encrypting PIN pad, supporting at least TDES (Triple DES) or AES.
- ATM screen position: position of screen must avoid easy reading from shoulder
- Anti-skimming protection must be implemented.
- ATMs should have systems to detect when a key logger or any other additional device is placed over the ATM.

- ATM alarms must be configured to detect unusual events.
- Access to inner portion of the ATM by third parties must be covered by agreements, including a third party ICT access agreement.
- Access to inner portion of the ATM for maintenance must be done in conjunction with banks authorized personnel. Access to remote ATMs for maintenance can be organized with a security dedicated company and the vendor.
- Access to ATM data center part by third party vendor must be strictly authorized only if accompanied with banks authorized personnel. Vendors must never be left alone in banks premises, especially when working on banks systems. This type of access must be logged and monitored as per the requirements given in this chapter.

Simple awareness messages for customers will help in preventing theft of cardholder's information from ATMs. The following checks could be communicated on regular basis to the customers in order to improve their awareness towards those risks, 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.

Banks must make sure that a call center/hot line phone number is accessible at any ATMs area to allow an immediate reporting of unusual events and the call center staff is properly trained to handle these issues.

The following additional security requirements should be complied with when installing ATM equipment facilities:

- Access to ATM enclosures when applicable must be allowed only for a single person at the time.
- Overall physical security of ATMs must be compliant with QCB instructions.

Instructions to obtain license to install and operate ATM machines mentioned in QCB instructions must be complied with.

3.2.8.7. On-line Payment

A payment card issuer in Qatar must deploy means for ensuring the payment card authentication when a customer wishes to operate online payments.

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

3.2.9. Electronic Fund Transfer

Electronic Fund Transfer operations may be subject to fraud, security risks and errors. In order to prevent loss occurring during such transactions several controls need to be implemented:

- **Source must be authenticated:** security procedure must be in place in order to authenticate the originator through mandate and registration with the bank providing such services. Technologies such as digital signature or authentication mechanisms should be used in the authentication and verification process.

- **Full message text must be authenticated:** to ensure integrity of messages and prevent unauthorized changes of payment date, value date, amount, currency, beneficiary name, account numbers, authentication using cryptographic mechanisms is required. Encryption keys shall follow a secure key management process as described in paragraph 3.7.3.

- **Uniqueness of messages must be identified:** this must be part of any message authentication process.

- **Retention of messages must be in place** in accordance with legal requirements for data retention as per paragraph 3.7.5 of this document: in order to preserve evidence when needed to replay transactions, as a proof of payment or transfer of funds. Cryptographic methods and authentication should be used to keep the records safe from integrity, confidentiality and availability issues.

- **Agreements and mandate from the customer must be in place** when establishing EFT operations prior to usage, covering legal and identity risks aspects.

- **Only authorized personnel** will be able to access and use EFT related applications.

3.3. Handling cheques

Security issues could appear during a manual or an automated process of handling cheques, if controls are not properly implemented. As an example, cheques that are being digitized through computer scanning devices can leave traces of complete data that contains sensitive information which may be accessed on that computer.

Information such as personal account numbers, account holder's name and signature must be kept in a secure area. If digitally scanned, data must be secured by cryptographic techniques. Encryption methods as described in paragraph 3.2.6.2 shall be considered.

Measures for identifying customers must be in line with best practices such as "know your customer" and banks must maintain the same level of controls when identifying and registering new customers. Banks must observe controls in order to avoid that:

- Documents provided for identification are not altered or forged.
- Photograph on ID is inconsistent with appearance of customer.
- Information on ID is inconsistent with information provided by a person opening an account.
- Information on ID, such as signature, is inconsistent with information on the file at the financial institution.
- Application appearing forged or altered or destroyed and reassembled.
- Information on ID not matching the customer QID, address or passport ID.
- Personal identifying information is associated with any known fraud activity.
- unprotected Personal identifying information.

Each cheque payment transaction has to be protected through various methods or requirements described in this chapter to ensure the compliance with the instructions above.

3.4. Business Continuity

QCB instructions regarding business continuity are considered an integral part of these instructions and should be strictly adhered to.

3.5. Incident and Fraud Management

Banks must have established processes to deal with incidents management and fraud cases in two ways: preventive and detective. A set of measures have to be implemented to

avoid misuse or abuse of internal systems and preventing information being leaked to external fraudsters.

Money laundering is one of the frauds that can occur if controls are not in place. Banks must have procedures and controls to prevent, monitor and report any suspicious activity as per the AML laws and regulations.

3.5.1. Incident handling

An incident management plan should be well established and known to all people involved in dealing with incidents. Several issues must be considered like: out of office hours incidents, escalation processes, communications requirements, contingency and backup plans.

Banks must have dedicated resources to handle the incidents that may arise from cyber attacks, system failures, sabotage or theft of information. Therefore it is important that all banks have appropriate resources to deal with such cases. Centralized coordination, reporting and response mechanisms must be clearly defined to protect confidential information during an event.

3.5.2. Internal Fraud

Banks should have procedures and controls in place to prevent insiders from committing fraud. Segregation of duties is one of the key principles adopted by the industry to minimize the fraud activity.

With the heavy use of electronic operations, banks should apply security controls defined in these Instructions. Applications or systems used in daily operations must be subject to specific scrutiny to avoid potential abuse where financial transactions can be subject to manipulation to obtain illegal financial gains.

Fraud monitoring systems must be in place for monitoring suspicious transactions on payment systems and organized as per the requirements listed in paragraph 3.7.

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 should be stored in an area limited to only authorized personnel. Production and issuing processes for cards should be kept physically separated from the PIN generation and issuing environments.

3.5.3. External Fraud

External fraud attempt might happen through physical or electronic means. As networks are more and more interconnected, applications are available online which enables fraudsters from operating through remote access.

The tools used by the banks will always attract fraudsters to enable substantial financial gains. The tools such as the payment devices or the online interface are potential doors to access any financial information.

Monitoring of transactions processed online, on ATM or POS terminals is one of the key action to take to deter any potential fraudulent activity happening at a merchant place or for money laundering detection. Qatar Central Bank requires that the bank have a real-time fraud monitoring systems running to detect suspicious activities on financial transactions.

Payment Cards are mainly targeted by criminals or fraudsters. Measures to counter frauds must be in place in banks to be able to take actions on any fraudulent transactions after alarms are raised by systems. Principles such as velocity checks must be at minimum enabled with reference to current transactions and previous transactions.

Any fraud attempt on ATM's or point of sales must be reported to the Ministry of Interior hotline as stated in QCB instructions, and QCB should be notified. In addition, as stated in the instructions embezzlement crimes have to be reported, including attempted embezzlement through electronic means. QCB should be notified, in case of any hacking, penetration, fake web-sites, or forged credit cards. However, banks will be responsible for compliance of law and notifying security authorities in this regard.

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

3.6 Outsourcing the Information Technology function

Outsourcing means delegating a particular function to a trusted third party. By trusted it would mean that necessary controls and measures are in place between the outsourced financial institution and the outsourcing service provider to guarantee the integrity, confidentiality and availability of the outsourced function. Outsourced IT services contribute

to operational risks. Institutions should have controls, to ensure quality and strict protection of confidential information entrusted to them by their customers. This exercise must be done in accordance with the risk assessment practice of the bank.

Risk management controls are best achieved when the Information Technology function of the bank is supported by its own department, organized and supervised by Board approved policies and procedures and a set of internal controls established by the Management. Generally, the bank will have in its premises in Qatar its own IT Systems, applications and other computer software suitable to pursue its business activity, duly documented and managed by its own competent staff. Furthermore, the bank must be able to function normally in case of failure of its systems and prepare a continuity plan and backup solution for this purpose as per QCB instructions regarding business continuity plan.

Banks are permitted to have their own systems, but use the services of third parties in consulting, advising, programming, maintaining or managing their systems would be organized as per QCB regulations on outsourcing. This third party may include any IT company specialized in the domain that may belong to the bank or not, or an IT specialized company which is jointly setup by or with other institutions (regulated banks or finance sector professionals) that cooperate in information technology. However, the responsibility to maintain the secrecy of financial information would rest with the board of directors of the bank.

While using the services of third parties, banks face a higher risk of theft of data or unauthorized disclosure of sensitive data than in case of the systems being managed by bank's own staff. Given the potential for such risk, banks should comply with the following:

a. Any area of work with a third party service provider must be formalized by a contract of services.
b. The use of an IT third party service provider shall not end up with a transfer of the core banking business functions within the third party entity.
c. A clear and detailed scope of the service subject to outsourcing must be submitted to QCB for approval prior to contracting the third party.
d. In order for the bank to assess the reliability and integrity of data generated by IT systems as well as the compliance with the accounting and internal controls requirements, it shall:
    i. Provide that any intervention by a third party, including any changes to software, programs or application source codes are subject to approval, prior to these changes as part of a change management practice.

ii. Have among its staff the necessary knowledge in information technology to understand the impact and effect of such changes on the core banking system.
iii. Have sufficient documentation of systems, applications, software and programs used.

e. The bank must ensure that there is no legal obstacle to access the applications or computer programs source codes developed by third parties through escrow arrangements in an event of failure of the developer. Therefore, the agreement should specify the necessity to transfer the applications or source codes to the bank and be legally owned. For privacy and confidentiality reasons such Third parties cannot gain access to documents that contain confidential data.
f. The prohibition of access to confidential data is also for those individuals who are responsible for managing the systems. Except in case, as part of a major disruption or failure of the systems and considered necessary for assistance from third parties to allow access to these data, the bank must ensure that the third party in charge of troubleshooting is accompanied throughout its mission by a person of the bank in charge of the systems or system owners.
g. Each bank will appoint one or more of its employees who will be responsible for managing the access to confidential data.
h. Whatever the nature of the intervention on applications or programs is (consulting, management, maintenance or change), the third party can only work in a test environment and require the express consent of the institution for each intervention. Exceptions may arise in case of system failure, crash or heavy software bugs that require the intervention of the vendor. A change management policy and a set of dedicated procedures shall be in place to ensure controls on such intervention.
i. In case of provision of services by remote access using telecommunication networks, the bank must ensure that adequate safeguards are in place to prevent unauthorized persons from gaining access to its system. The bank shall ensure that telecommunications are encrypted or protected from end-to-end by other equivalent secure and reliable technology available.

   Banks must ensure that QCB examiners have the right to examine the third party outsourcing related activities.

   The bank must also ensure that measures are in place at the outsourced site to enable it to continue to function normally when there is a communication line failure, breakdown or extended time periods of disruption.

3.6.1. Data Centers Organization

When the specified conditions and restrictions set out below are met, it would be considered that all obligations for organizing the IT function are also met by the bank that is processing data through a data center that may not belong to it or that it is a co-owner for the centre and linked through networking telecommunications.

When the data processing center is outside the State of Qatar, it must be with the parent (or, in case of branches can be related to the company's headquarter) or a subsidiary thereof, or with a company that is specialized in IT processing, controlled by the group to which the institution belongs to. An entity housing the IT function must fall within the scope of the prudential and supervisory controls reviewed by the foreign supervisory authority which shall confirm that the security and safety standards and controls on communication network are appropriate and safe.

When the data center is in Qatar, it must be housed by the bank or a company owned or controlled by the bank that deals exclusively with operations on behalf of the bank. Furthermore, it is acceptable that the data center is housed in a company which is owned and controlled jointly by several institutions (banks or a professional of the finance sector) that cooperate in information technology. In this case, the common shared data center can process only transactions of these banks.

Banks that intend to make use of an external data center will not escape their responsibilities in ensuring the confidentiality of any information entrusted to them during their professional obligations. In such cases, banks face a high risk of disclosure even more importantly than when using one of the solutions listed previously. Banks seeking to use the services of any of these organizations as stated above should seek prior approval of QCB before entering into any agreements for such services.

Banks that want to seek the services of external data centers must meet at least the following conditions in addition to those listed above:

a) The network infrastructures should allow the bank in Qatar to access information stored in the outsourced IT function unit in a fast and reliable manner. Data input and printing will take place entirely in Qatar in its premises. Exceptionally, data can be entered or printed outside the premises of the bank by a customer or an agent initiating transactions through a dedicated and secured link. The bank will get the balance of all accounts and all accounting movements on daily basis.
b) The system must allow keeping proper accounts in accordance with the standards in force in Qatar.

c) Communications between the facility and data center must be encrypted or protected by other means technologically available and capable of ensuring the security of communications. No client information will be entered or recorded on systems to which third parties have accesses to.

d) 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.

e) The external auditor, the internal audit department of the bank and QCB examiners should be able to perform audit on the data centers in order to ensure the adequacy of the systems and the communication channels with security controls.

f) The communications between systems should be detailed and formalized in the service contract. Specifications shall take into account the conditions listed above, in this chapter.

Banks that are currently processing data through such service provider and not complying with the previously mentioned instructions are requested to submit a detailed action plan in order to meet the requirements of this regulation to QCB.

3.6.2. Operating abroad

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

3.6.3. Cloud Computing Security

The cloud computing services have been promoted as a way to bring more flexibility and dynamism. The use of Cloud computing services shall not end up as a justification to delegate risk controls that may surround a portion of data 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, availability of cloud services or legal risk.

As data in the cloud is available on systems that may be shared physically but compartmentalized logically, risks of interferences may appear on the cloud application layers, disrupting such separation at the cloud level.

Banks must make sure that core sensitive information is not placed on a non controlled cloud computing environment, while private cloud facility may be considered as an alternative and would remain under local control of the bank.

When using cloud computing, banks must make sure that the agreement between the cloud computing service provider contains key security controls limiting the risks mentioned before. Therefore a bank must seek the existence of the following key security domains 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

3.7. Process Risk controls

Banks should implement a set of controls and procedures to ensure that proper security measures are surrounding potential risks on existing business processes. The security controls proposed in this chapter are considered as highly important and crucial for the safety of the banking environment.

3.7.1. Access control

Access control is one of the identified processes that lead to limiting the privileges of access to logical information, data, systems or even physical areas.

3.7.1.1. Principles

- A core banking system should be accessible to only those individuals who have been identified as qualified and matching a specific role/function in the bank. The following are the set of categories with their roles and privileges:

- The end-user: will be related to a business unit user and will gain access to applications to process banking operations. These users will never be able to administer, manage, and change applications, systems settings or part of the core banking functionalities.
- The system administrator: is a technical function which ensures that systems are maintained, supported, updated properly and according to the banks policies.
- The database administrator (DBA): is responsible to maintain the structure, the functions and the availability of the database. A DBA will also be restricted access to the content of the database. Clear role description and areas of functionality on the database should be defining where he will operate. Databases access privileges will be defined by the application owner and assigned by the DBA to a specific user, following a request that would have been duly validated by the application owner.
- The system or application owner: will enable and validate changes to the functionality he is responsible for and as part of the bank' change management policy. The owner usually is the head of a business unit using such functionality/application dedicated to his department role in the bank.

Banks should define a role-based access control approach in order to help them minimize the internal risks. A well defined and structured organization will improve the identification and detection of potential threats, helping at protecting the bank against internal and external issues.

3.7.1.2. Identification

The verification of user identity is obviously a must when it comes to initiating the generation of user accounts. As a best practice, Qatar Central Bank insists that identification of roles and privileges is established in conjunction with the human resources department as well as the business unit owner or system owner.

Policies on verification of identity should be enforced in order to increase the level of confidence. Each user will be made unique and allow traceability to the user and the initiator.

Controls and privileges assigned by roles help to define proper user accounts. Banks must have a well defined set of procedures for identity management.

3.7.1.3. Authorization

Specific privileges are required for users to work on systems. These privileges will enable a defined set of actions that can be taken on a particular system, application

or even device. Banks must make sure that each user of an organization is assigned with the proper rights to access these systems.

Procedures must enforce that no user will be allowed to access any information or application unless specifically authorized. Principles such as Role Based Access Controls (RBAC) are providing basics for developing such approach.

3.7.1.4. Authentication

User authentication is the process where users 'identity is verified to the system. Failure to do so might result in potential loss or accountability issue related to the actions of an individual.

Several methods of authentication mechanisms exist based on:

- Something the user knows: e.g. passwords, passphrases, PIN codes
- Something the user possesses: e.g. token, smartcards
- Physical characteristics: e.g. biometrics as fingerprints, facial recognition, iris scan or others.

Mature technologies can offer high level of security especially when those methods listed above are combined:

- Passwords: can be easy or complex, the difference might reside in the risks related to the exposure of information to potential threats. Passwords can be generated one time only using One-Time Password generated via an algorithm and provided by a token.
- Digital certificates: based on X509 standards can be used for authentication but also for signing or encrypting as well.
- Biometrics: identifying a person with his physical characteristics such as fingerprints, retinal pattern of the eyes or even the palm of the hand.

3.7.1.5. Segregation of duties

The segregation of duties aims at minimizing the risks of conflict of interests, by separating roles in operations: as an example input and validation are two processes that cannot be done by a same person. In the same manner, systems should allow applying a four-eye principle. In case this is not possible, banks could request a change to the targeted application or should act with due diligence by incorporating such principles manually and on specific access to critical systems.

When identifying key critical systems, banks must implement sufficient control to minimize risks of misuse or compromise on those systems identified as highly important or critical, depending on the banks internal classification. Segregating the

roles through user account privileges based on roles is a key process in minimizing the unauthorized access or change on banks systems or applications.

3.7.2. Change Control

To protect the integrity of banks' information-processing facilities, change control policy and procedures shall be implemented. Without change control mechanisms, financial and productivity losses may occur due to improper processing or loss of services.

Change control procedures shall exist for hardware changes, software changes for both applications and operating systems, covering automated as well as manual changes. These change control procedures must also address management of emergency changes.

Business managers must ensure proper change control processes for the systems under their control. The information security team should be prepared to help manage security-related changes and to manage changes on security systems that the information security team is directly responsible for.

3.7.3. Key Management

The incorporation of cryptographic techniques like encryption and authentication into computer systems and networks can achieve many security objectives. However, these techniques are of no value without the secure management of the cryptographic keys.

Key management is the part of cryptography that provides the methods for the secure generation, exchange, use, storage and discontinuation of the cryptographic keys used by a cryptographic mechanism. This operation requires careful planning, education and precise implementation; standards that address key management principles include ISO 11568.

The major functions of key management are to provide the cryptographic keys required by the cryptographic techniques and to protect these keys from any form of tampering. The specific procedures and security requirements for key management depend on the type of cryptosystem upon which the cryptographic techniques are based, the nature of the cryptographic techniques themselves and the characteristics and security requirements of the computer system or network being protected.

The most important element to consider is that key management must be flexible enough for efficient use within the computer system or network. Key management services must be available when and where they are needed, including at back-up sites.

Key management must be part of an organization disaster recovery plan. The following minimum principles must be applied:

- Facilities providing cryptographic material must be subject to high level security and controls.
- Ideally the cryptographic processing room is separated from data center conventional operation rooms.
- Key Management secrets must be operated under split knowledge.
- Key ceremony procedures must be in place with strict controls.
- In case of high risks environment, the key change process can be recorded by medias.

3.7.4. Audit Journals/Event Logging

Most of the systems running daily operations usually have a capability to generate reports on key events occurring within an application, system or network device. These records help a bank in identifying issues, origin of these issues, date/time stamps as it happens and description of the event related to those issues.

A business process might be supported by a whole chain of systems that includes network devices, applications and computer systems. It is highly important that banks take into consideration the whole business process chain.

In order to trace or replay a critical event, it might be necessary to correlate data from each system involved in a business process. Banks should keep records of all the key systems which have been identified as critical for the legal duration defined by the law and described in chapter 3.7.5.

Integrity of event logs/journals shall be ensured by secure protection mechanisms and automated processes in generation.

3.7.5. Data Retention & Archiving

Banks must have established a procedure for archiving and saving key business information or data. Such a procedure must be in line with the banks corporate policy and local regulations. A backup process and archiving technologies must be in place to enable the retrieval of financial information transactions or track records.

Fifteen years of information or data retention is required legally. So technology lifecycle supporting a bank's business activity must be applied in line with the legal retention requirements. As most of the information resides on backup systems, data must be carefully archived to ensure that legal retention period is complied with.

Therefore, the data archived must be kept stored using means that can be re-used in 15 years from the date of archival. Banks should include data archiving technology in their technology lifecycle plans.

3.7.6. System Life-cycle & Software Development

The lifecycle of systems and applications requires specific attention. Indeed in a SDLC, security needs to be integrated to ensure products are reliable and secure before entering production mode.

Banks are required to have well established process cycle that will cover the procurement, testing, and implementation and decommissioning for any system or application used in a banking environment.

Banks are required to document and monitor the implementation of security requirements throughout the life of their systems. The hardening process must be implemented to prevent default configuration to be implemented without proper security controls in place on vendor equipments.

3.7.7. ICT Disaster Recovery

Banks must have procedures in place to ensure the recovery of key critical systems, applications and its related infrastructure. Disaster recovery plan 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 time of crisis according to the overall BCP strategy of the bank and QCB instructions.

3.7.8. ICT Procurement

Banks may need to hire external third party vendors for acquiring products or services in many domains, but special care is needed when it comes to Information Technology.

When a bank initiates a procurement process of IT equipments several controls must be in place, such as ensuring the reliability of the company and that the technology chosen will not pose risks to the business.

Several key processes need to be implemented to avoid potential weaknesses prior to and after the acquiring process, such as:

- Ensuring ethical conduct, due diligence and proper evaluation criteria have been followed when selecting a vendor from a list of at least minimum three vendors wherever possible.

- Ensuring that the maintenance aspects of the contracts cover the confidentiality aspects and security controls, especially when vendors need to access banks premises and systems. Agreements should clearly mention responsibilities, liabilities, banks policies, reference to standards (ex. PCI DSS obligations in payment systems).
- Hardening systems procedures (network devices, computers or appliances) must be part of the bank internal IT procedures, ensuring that for example no default vendor passwords remain on network devices, default non necessary network ports are remaining opened or non necessary services/processes are kept running on a system.
- Security controls and provisions that apply to a bank must apply to vendors a bank is contracting with, so policies and regulations are inherited and should be highlighted in any third party agreement

3.7.9. Other QCB security controls

Policies and measurements to prevent the use of modern technology and e-banking in money laundering and terrorism financing should be developed and adopted. Compliance with, Anti money laundering and combating terrorism financing and instructions to Banks regarding the use of modern methods and implementation of due diligence procedures should be ensured in add ion to other instructions related to Verification of the real beneficiary, identification and address, create programs to detect unusual transactions, documents registration within a maximum of three working days, and terminate the business relation and report the same to (FIU)if customer does not respond to requirements. Cable transfer, document and records retention, electronic record retention should be according to the retention period mentioned in QCB instructions.

Appendix

A. Information Security Organization Structure best practice

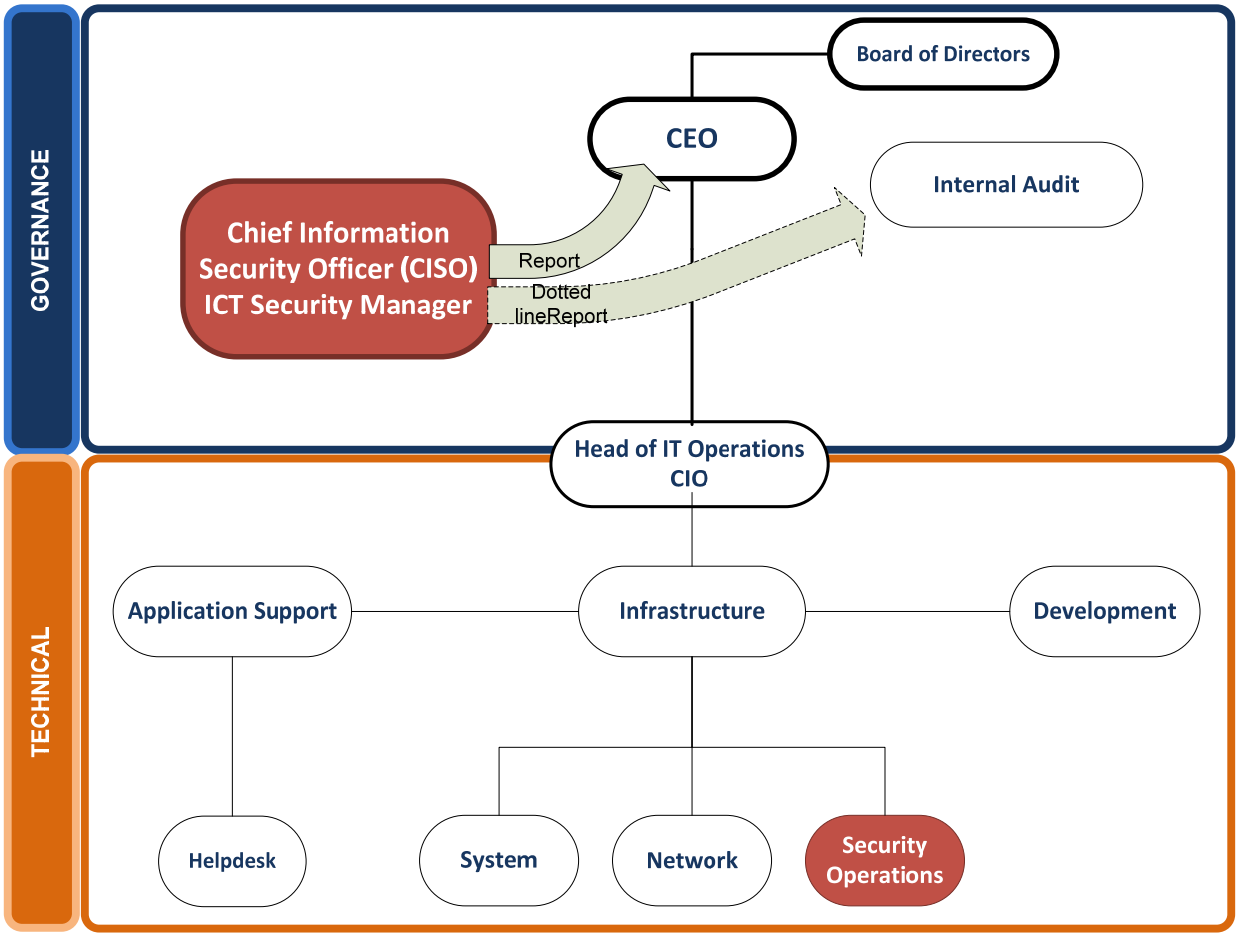

Figure 1 - Technology Risk organization

Figure 1 describes the best practice in organizing information security and IT Security operations. A typical organization will highlight a split between conceptual aspects of security (guidelines, policies, etc…) and operational aspects (administration of security equipments such as firewalls, intrusion detection systems, etc…) as described in figure 2.

The dotted-line reporting with the internal audit is proposed as a collaboration effort to follow-up on yearly audit technical issues highlighted in the management letter or other as per requirement 3.2.1. This is not an operational regular reporting as the audit department by definition is not involved in daily operational tasks.

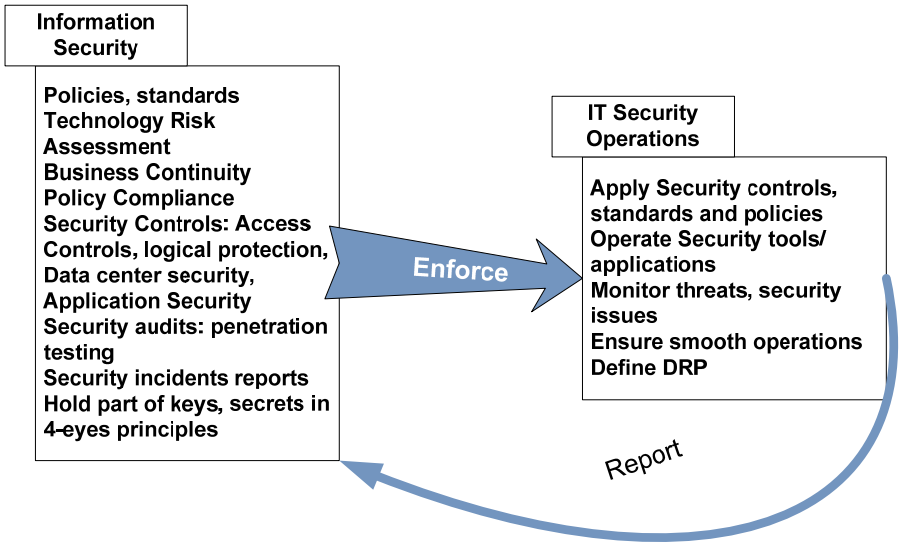

Figure 2 - Information Security vs. IT Security operations