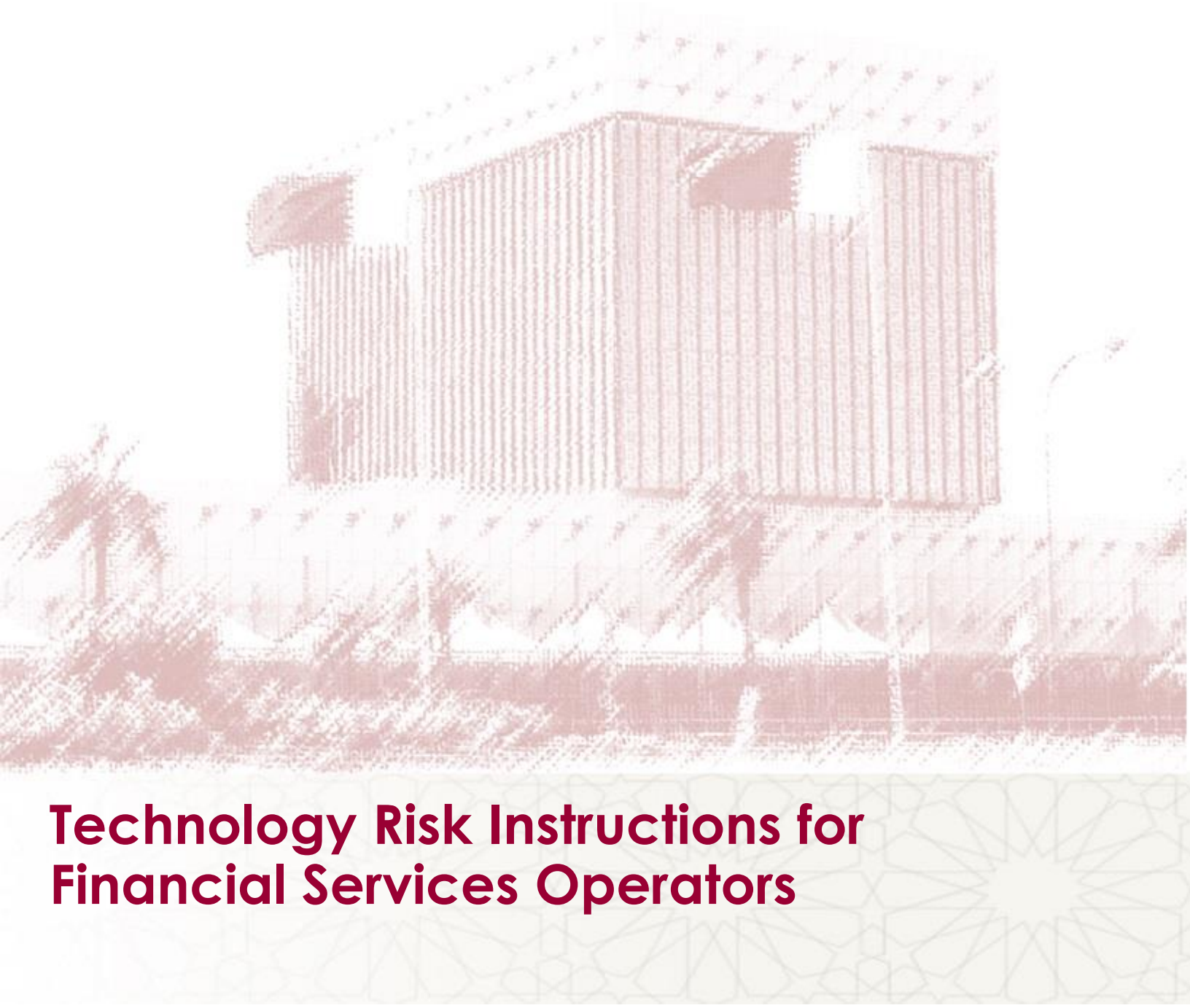
2022



Technology Risk Instructions for Financial Services Operators

Document Overview

Manual Name	Technology Risk Instructions for Financial Service Operators
Reference	QCB-ISR-FSO
Classification	Restricted
Effective Date	
Issue Date	

Revision History

Revision	Date	Summary of Changes
V0.5	29/11/2021	Review draft
V1.1	10/04/2022	Final draft
V1.2	9/6/2022	Revised

CONTENTS

Introduction

The increase in digital transformations in the financial sector has led to a deeper integration of modern information technology tools within business operations. This regulation provides the security requirements and mechanisms to secure Financial Service Operators (FSOs) from cyberattacks and security risks. Financial Service Operators (FSO) refers to exchange houses, investment companies, finance houses and their relevant brokers.

Scope

Technology risk instructions shall apply to all Financial Service Operators including exchange houses, investment companies, finance houses and their relevant brokers which are operating in Qatar, and are regulated by Qatar Central Bank.

Acronyms and Abbreviations

AES	Advanced Encryption Standard
CEO	Chief Executive Officer
CIO	Chief Information Officer
DoS	Denial of Services
DDoS	Distributed denial of service
DMZ	Demilitarized Zone
DSS	Data Security Standard
FSO	Financial Service Operator
IAIS	International Association of Insurance
ICMP	Internet Control Message Protocol
ICT	Information Communication Technology
IDS	Intrusion detection system
IPS	Intrusion prevention system
IS	Information Security
ISO	Information Security Officer
ISAE	International Standard for Assurance Engagements
ISO27001	Industry Standard Organization 27001
ISO22301	Industry Standard Organization 22301
ISO11770	Industry Standard Organization 11770
MOI	Ministry of Interior
NAC	Network access control
NDA	Non-disclosure Agreement
NIST	National Institute of Standard and Technology
OWASP	Open Web Application Security Project

PCI-DSS	Payment Card Industry Data Security Standard
PEAP	Protected Extensible Authentication Protocol
QCB	Qatar Central Bank
RBAC	Role based access control
RTO	Recovery time objective
S-SDLC	Secure software development life cycle
SANS	System Administration Networking and Security
SNMP	Simple Network Management Protocol
SLA	Service Level Agreement
SSID	Service Set Identifier
TLS	Transport Layer Security

1 Organizational Security

Given the importance of safeguarding organizations against cyber threats, and in reference to the relevant Information Security (IS) standards including ISO 27001, ISO 27005, NIST SP800-53, and also PCI-DSS in the payment card industry, QCB highly recommends utilizing these standards when establishing the information security practice within each respective organization.

The information security practice starts with a governance model which includes the following responsibilities:

1.1 General Requirements

1.1.1 Financial Service Operators shall identify the resources required to establish and assign the Information Security (IS) function.

1.1.2 The board and executive management of the FSO shall ensure that an Information Security program is in place and as such the IS function is well supported by allocating sufficient resources.

1.1.3 The executive management shall oversee and be accountable for all the risks including those related to the use of technology.

1.1.4 The FSO shall establish an information and cyber security framework that defines the relevant functions, roles and responsibilities

1.1.5 Where appropriate, the executive management will establish an Enterprise Information Security Steering committee, with representation from relevant functions such as IT, Risk Management, Information Security, Human Resources (HR), Business Continuity, Legal, Compliance and relevant Business Units.

1.1.6 Financial Service Operators shall appoint an Information Security officer and create the related mandate. The Information Security officer should be an independent party, reporting directly to the organization's CEO.

1.1.7 The Information Security officer shall be in charge of:

- Developing and maintaining the Information Security program, strategy, IS policies and procedures, and communicating them to the FSO employees.
- Monitoring information security risks.
- Reporting risk and security program status to the management.
- Collaborating with IT in order to implement security controls in line with the policies and the security strategy of the FSO.
- Creating awareness within the organization and customers when needed.

- Protecting the FSOs information and technology assets.

1.1.8 The IT Department shall ensure that the security controls are implemented and maintained.

1.1.9 The IT security operations function will exchange information regarding security threats and risks to the main strategic security function.

1.2 Information Security Risk Management

1.2.1 The FSO's IS function shall define and establish a risk management framework to manage technology risks. The framework should encompass the following:

- Roles and responsibilities relevant to managing technology risks.
- Identification and classification of assets.
- Identification of risk and risk owners.
- Identification and assessment of impact and likelihood of threats, risks and vulnerabilities.
- Treatment of risk based on asset classification.
- Implementation and maintenance of a regular testing plan.
- Monitoring and reporting of the overall risks and their impact on the risk posture.

1.2.2 As part of the security program, the IS function shall ensure the organization of the FSO's assets by defining a classification scheme and related security controls requirements which entails:

- Coordinating the identification of information assets and maintenance of an asset registry across the organization's departments.
- Ensuring the labeling of these assets based on criticality.
- The definition of the related security controls including but not limited to data encryption, and isolation.
- The protection of these assets using defined security controls.

1.2.3 Information system assets shall be protected with proper risk-appropriate controls from unauthorized access, misuse or fraudulent modification, insertion, deletion, substitution, suppression or disclosure as per the FSO's IS Policy.

1.2.4 Systems operating the core applications shall be classified as critical assets since their disruption could lead to a direct impact on the business.

1.2.5 Financial Service Operators shall employ measures to actively monitor their exposure to threat actors and ensure that security measures against cyberattacks including but not limited to, Dos/DDoS, sabotage and sophisticated malware are in place.

1.3 Documentation Requirements

1.3.1 Financial Service Operators shall develop, document and maintain the organization's information security policies.

1.3.2 Financial Service Operators shall review and update all documentation regularly and at every change.

1.3.3 Financial Service Operators shall maintain an adequate level of documentation as an essential element of the organization, which includes keeping traces of a particular events or keeping security configurations of systems.

1.3.4 Financial Service Operators shall document the key assets of their infrastructure as well as key security processes including the changes of security configurations and appliances, the network components configurations and infrastructure diagrams, the system security policies, the security logs from key endpoints security and systems, managed by the FSO directly or any third-party.

1.4 Incident Management

1.4.1 Financial Service Operators must develop and maintain an information security incident management policy and plan with various levels of escalation and response.

1.4.2 Financial Service Operators shall ensure periodic exercising and simulation of incident response plans relevant to critical business processes and key risks.

1.4.3 Financial Service Operators shall ensure that their employees have access to the required contact information to report information security incidents.

1.4.4 Financial Service Operators shall document all incidents with levels of severity, track and oversee the remediation actions.

1.4.5 Financial Service Operators shall communicate all incidents internally according to the escalation plan, ensuring QCB and NCSA are notified immediately based on the severity of the incident, in case of a cybercrime, the FSO must notify MOI.

1.5 Security Awareness

1.5.1 Financial Service Operators shall implement a security awareness program that caters to both the FSO employees and its customers.

1.5.2 The security awareness program shall highlight the organization's key risks and inform the users about emerging threats, security best practice, and the potential technical and legal implications

1.5.3 The security awareness program shall include the regular testing of the employees via social engineering techniques, amongst other techniques.

1.6 Disaster Recover and Business Continuity Plan

1.6.1 Financial Service Operators shall develop a business continuity plan as per QCB instructions regarding business continuity for each relevant sector.

1.6.2 Financial Service Operators shall develop a crisis and emergency response plan as part of a business continuity strategy that details evacuation procedures, command center operations and media and communications strategy.

1.6.3 Financial Service Operators must identify all threat scenarios that may impact the operation and put in place all necessary response procedures and recovery mechanisms.

1.6.4 Financial Service Operators shall ensure that it replicates the technical infrastructure that supports its operations, in addition to establishing flexible backup plans to ensure resiliency.

1.6.5 Financial Service Operators shall periodically exercise their business continuity plans.

1.7 Third-Party Security

1.7.1 Financial Service Operators shall define a third-party policy that takes into consideration the organization's risk appetite, defines the different types of third-parties, the degree of engagement and the permitted level of information sharing.

1.7.2 Prior to engaging with third-parties, FSOs shall:

- Conduct risk assessments associated with the intended third-party engagement.
- Conduct background checks and perform due diligence.

1.7.3 Financial Service Operators shall ensure that the contractual agreement includes security requirements as well as a non-disclosure agreement (NDA). Security requirements shall be in line with this regulation and international best practices such as ISO27001, PA-DSS, PCI-DSS (when payment acquiring scheme is involved) and NIST SP 800.

1.7.4 Financial Service Operators shall ensure that all key risks it has identified are communicated and reported by the third-party as well.

1.7.5 Financial Service Operators shall establish a joint incident management process, for incidents associated with the third-party engagement, ensuring the process adheres to the requirements of these instructions.

1.7.6 Financial Service Operators shall ensure that third-parties immediately report to the FSO, in case of a security breach.

1.7.7 Financial Service Operators shall be aware of all relevant sub-contracting arrangements, and ensure the third-party is enforcing appropriate security requirements on these arrangements.

1.7.8 Financial Service Operators shall ensure their third-parties monitor any service delivery and the third-party's adherence to security requirements.

1.7.9 Financial Service Operators shall ensure that third-parties regularly report on their security posture.

1.7.10 Financial Service Operators shall include exit clauses that ensure that any data will be wiped out of any of the third-party assets in its contractual agreements.

1.7.11 Financial Service Operators shall follow QCB outsourcing instructions when contracting a third-party, ensuring that they seek approval from QCB before engaging with third-parties.

1.8 Cloud Computing

1.8.1 Financial Service Operators must establish a cloud computing policy that must be approved by the FSO's management. The policy must be reviewed periodically.

1.8.2 Financial Service Operators shall only utilize a cloud service provider that has data centers within the State of Qatar. If an exception is required, the FSO must seek approval from QCB.

1.8.3 The data shall be protected while it is in transit and at rest in the cloud where the FSOs shall ensure that data is secured end-to-end.

1.8.4 Financial Service Operators must obtain International Standard on Assurance Engagements (ISAE) or assurance reports on the security controls incorporated from a services organization perspective.

1.8.5 Financial Service Operators shall consider and mitigate the associated risks when accessing cloud services including but not limited to data leakage, data interception, intrusion/unauthorized access, cloud application interfaces risks, integrity of data and availability of cloud services or legal risks.

1.8.6 Financial Service Operators shall ensure that the cloud service provider addresses the key security domain via documented evidence prior to contracting with the cloud service provider. The key security domains include: access controls, auditing, authentication, awareness and education, business continuity, configuration management, data security, incident management (cyber incident reporting responsibility matrix and SLA), maintenance and support, media protection, personnel security, physical security, planning, procurement, risk management, security assessment, system security and integrity controls.

1.8.7 Financial Service Operators shall control cryptographic keys. This includes the entire Key Management System (KMS), and in particular the generation and issuance of private keys.

1.8.8 Financial Service Operators must ensure that the encryption mechanism is under its full control, including the Key Management System and the generation and storage of the private keys outside of the cloud environment, on-premises in Qatar.

1.8.9 Financial Service Operators must ensure that sensitive data is not stored in a non-controlled cloud environment. A private cloud facility under control of the FSO shall be considered as an alternative.

1.8.10 When using cloud computing, Financial Service Operators must ensure that the agreement with the cloud computing service provider contains key security controls limiting cloud computing risks. This must include informing the FSO in case of any cyber incident that occurs on the cloud computing environment that may impact the FSO. The agreement must include the key security domains detailed in this regulation.

1.8.11 While performing due diligence for the cloud service provider, Financial Service Operators shall consider attributes and risks specific to cloud service.

1.8.12 Financial Service Operators shall have contractual power to conduct a penetration test on the hosting infrastructure and application instances provided to the FSO by the cloud service provider.

1.8.13 Financial Service Operators must have the contractual power and the means to migrate or destroy data stored within the service provider's systems and backup, in addition to an exit strategy that ensures business continuity, in the event of contract termination or expiry.

1.8.14 Financial Service Operators 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.

1.9 Auditing

1.9.1 Financial Service Operators shall conduct regular audit of their Information Technology and Processing environment, including compliance with the current security requirements, at least annually.

1.9.2 QCB has the right to audit the FSOs at any time, and as such the FSO shall make the necessary arrangements to enable such an audit to take place on demand.

2 Technical Security

Qatar Central Bank requires every financial services organization to protect their assets with the necessary technical security controls. As in every information processing environment, Financial Service Operators will define the appropriate security measures for each of the application, system and network layers of the organization, by following the requirements laid out in this chapter.

2.1 General Requirements

2.1.1 Financial Service Operators are consumers and processors of sensitive financial and customer information; hence they shall implement the proper technical environment inclusive of security by design.

2.1.2 Financial Service Operators shall implement security controls on the overall information-processing environment and architecture as defined in the subsequent paragraphs.

2.1.3 Financial Service Operators shall ensure that security best practices are put in place for the technologies used including but not limited to encryption algorithms, hashing algorithms and testing methods.

2.1.4 Financial Service Operators shall regularly perform vulnerability assessments, code reviews and penetration testing for their network, systems and applications. They shall ensure that these exercises are performed by an external, reputable penetration testing provider that has the required certificates, with regional offices.

2.2 Infrastructure Security

2.2.1 Financial Service Operators shall ensure that the network infrastructure that supports the environment is layered by isolating the production environment from the internet/external services, in order to avoid interactions between untrusted networks and the production network.

2.2.2 The network infrastructure shall be segmented using VLANs internally and DMZs for external networks. Financial Service Operators shall use security appliances such as firewalls, NIDS, HIDS, IPS, Reverse Proxies or security gateways in order to ensure that such segmentation is in place, secured and monitored.

2.2.3 Restrict the access to the Internet from the production network. If internet access is required to fulfill business requirements, limit such access by whitelisting through web proxy and security appliances.

2.2.4 When deploying web services, ensure that the web frontend is separated from the backend servers with multiple DMZs.

2.2.5 Remote access shall only be provided on a need-to-have basis, with authorization from the relevant management function.

2.2.6 When deploying remote access services, ensure that VPNs are employed allowing secure tunnels between the user and the organization.

2.2.7 Use DMZs to ensure that endpoint connections for VPN/remote access are monitored, restricted and separated from the rest of the network.

2.2.8 Network access must be granted based on the principle of least privilege and Role Based Access Control principles (RBAC).

2.2.9 The network and security appliances administrators shall limit the use of the high privilege accounts and not use generic accounts.

2.2.10 Ensure that network VLAN configurations and network routes are reviewed regularly and retained.

2.2.11 Network security logs shall be enabled, monitored, reviewed and retained for a period of at least 6 months before storing them in archives.

2.2.12 On firewalls, the security administrators shall ensure that the default rule in the security policy is to deny all traffic unless authorized by defined rules, and remove unused rules, and maintain backups of the configurations.

2.2.13 The web services' underlying network infrastructure shall enable the data to flow securely between the customer devices (mobile or computer) and the core backend systems of the FSO. Therefore, network connections shall be secured by using network encryption that is compliant with the industry best practice.

2.2.14 Data received from unknown senders shall be verified on an isolated host located in a separate network in a DMZ from the rest of the web server frontends and production servers, away from the production network.

2.3 Wireless Security

2.3.1 When deploying wireless network access points, Financial Service Operators must secure such access by hiding the SSID. Additionally, they shall create strong passwords using either auto-generated or manually-created complex passwords with 10-12 long mixed characters passkeys, and never keep default passwords and change the administrator password.

2.3.2 Financial Service Operators shall implement a process to detect rogue wireless network access points.

2.3.3 Financial Service Operators shall use AES or TLS at minimum to encrypt and secure wireless network authentication, and this must be updated in accordance with security best practices.

2.3.4 Ensure that any guest networks are set up in a separate network from the FSO's company production network. The guest or public network should still be traceable and leverage strong encryption as means of authentication.

2.4 System Security

2.4.1 Security logs must be enabled on the application, database and backend servers. User authentication and access connections shall be logged, monitored and periodically reviewed as per security best practice.

2.4.2 All IT systems operated by the FSO shall be adequately protected to ensure confidentiality, integrity and availability in order to minimize the risk of unauthorized access, use, disclosure, disruption, modification or destruction. Systems operating sensitive financial transactions shall be secured according to a defined security life cycle.

2.4.3 Financial Service Operators shall deploy endpoint security software and/or EDR across systems in order to protect against malicious and sophisticated programs, viruses, trojans and rootkits.

2.4.4 Financial Service Operators shall ensure that their systems are up to date, receiving regular patches according to a patch deployment plan in order to cover potential vulnerabilities.

2.5 Database Security

2.5.1 Financial Service Operators shall utilize encryption algorithms for databases, ensuring that they adhere to the evolving industry best practice, to protect the data at rest.

2.5.2 Financial Service Operators shall harden databases and its subsystems as per the FSO's defined hardening guidelines. Parameters such as default password, connection strings, SNMP communities or any insecure configuration shall be changed at the time of installation.

2.5.3 Segregation of duties shall be enforced to ensure that no single person can access, modify or use information without authorization and detection. Access shall be granted on the basis of the principle of least privilege and implementing role-based access controls (RBAC).

2.5.4 Financial Service Operators shall ensure that the core production database is not directly accessible, when needed for maintenance purposes, the direct access to databases shall be performed only by assigned and responsible personnel.

2.6 Email Security

2.6.1 Financial Service Operators shall utilize domain registered corporate emails. FSOs shall put in place security measures including access controls, DKIM and domain security, anti-malware solutions and endpoint detection response (EDR) to secure against email-based attacks.

2.6.2 Financial Service Operators shall raise awareness for employees on the risks associated with emails-based attacks such as phishing and social engineering.

2.6.3 Financial Service Operators shall restrict their employees from sending sensitive information via email, as per the FSO's information classification policy and related security controls.

2.7 Malware Protection and Cyberattacks

2.7.1 The FSO shall implement solutions and related controls to detect and mitigate malware at server, network and endpoint level.

2.7.2 The FSO shall properly maintain anti-malware solutions with up to date malware signature databases and engines.

2.7.3 The FSO shall have anti-malware solutions at endpoints and the network perimeters with the use of multi-layered firewalls, IDS/IPS, filtering gateways with proper monitoring of the security events.

2.8 Application Security

When developing customer facing applications, Financial Service Operators shall take certain measures that will ensure that sensitive data is protected while on the customer device or on the backend systems.

2.8.1 **Security Design**

2.8.1.1 Financial Service Operators shall practice secure code reviews and implement security by design as part of a well-defined software development life-cycle (SDLC).

2.8.1.2 Use of APIs shall be restricted to the defined service and application.

2.8.1.3 Applications must be tested against security risks, such as OWASP Top 10 and SANS Web application security.

2.8.1.4 Financial Service Operators shall secure APIs using strong encryption methods that adhere to security best practices.

2.8.1.5 Strong hashing methods shall be used when using key derivation functions, in line with the evolving industry best practices.

2.8.1.6 Financial Service Operators shall use multi-factor authentication with OTP for user authentication.

2.8.1.7 Financial Service Operators shall employ code tampering techniques to detect any attempt to modify the application code and stop any detected tampering attempts.

2.8.2 **Application Monitoring**

2.8.2.1 Applications must be able to detect any fault during the user registration process, and prompt the FSO to handle or deal with the fault.

2.8.2.2 Financial Service Operators shall employ security features to block online user registration if multiple unsuccessful registration attempts are detected, in order to ensure the authenticity of the user identity.

2.8.2.3 Financial Service Operators must be able to detect any abnormal security events in the application and its supporting infrastructure layers.

2.9 Identity and Access Management

2.9.1 **Authentication and Access**

2.9.1.1 Financial Service Operators shall define an access control policy and relevant procedures, employing role-based access control (RBAC) principles, and the principle of least privilege.

2.9.1.2 Segregation of duties shall be enforced to ensure that no single person can access, modify or use information without authorization and detection.

2.9.1.3 The system owner within the FSO shall ensure access is granted to, reviewed and removed from users as per the access control policy.

2.9.1.4 The IS function shall monitor all provisioning and de-provisioning of access rights to users.

2.9.1.5 All employees shall have non-administrative privileges on their machines by default.

2.9.1.6 The FSO shall define a strong password policy, with at least a 12-character requirement that consists of a random sequence of letters, numbers, special characters, and upper and lower casing, while changing the password every 3 months. Ensuring that the policy is updated per industry best practices.

2.9.1.7 The FSO's password policy shall adhere to security best practice, and use strong encryption and hashing algorithms.

2.9.1.8 Financial Service Operators shall ensure that access to the system is suspended after detecting multiple failed authentication attempts. The suspension must be placed based on the access privileges of the user account.

2.9.1.9 Financial Service Operators shall ensure that any third-party access to the environment abides by the FSO's policies and is covered in the contractual agreement. Terms shall include security and confidentiality clauses as well as non-disclosure terms.

2.9.1.10 All access, including third-party access, shall be monitored through the FSO's security monitoring tools.

2.9.1.11 Financial Service Operators shall enable application logging including access and changes to systems. These logs should be kept for a minimum of 6 months, before placing them in archive.

2.9.1.12 Financial Service Operators shall ensure that logs containing personal information have the appropriate privacy protection measures in place and shall be in line with the Qatar Personal Data Privacy Law (law No. 13 of 2016).

2.9.1.13 User access to application and web services shall employ multi-factor user authentication as per security best practices.

2.9.2 Biometric Authentication

2.9.2.1 Financial Service Operators can leverage the use of biometric authentication techniques for customers authentication, including but not limited to the use of fingerprint or facial recognition.

2.9.2.2 The FSO shall ensure that biometrics data is kept only in secure enclaves protected by strong symmetric encryption algorithms, adhering to evolving industry best practice.

2.9.2.3 Controls for formal registration and de-registration of customers will only be activated after the successful completion of the customer acceptance and identification procedure, where no abnormality is detected.

2.9.3 Credentials Protection

2.9.3.1 Credentials shall never be hardcoded within the application code.

2.9.3.2 An account lockout policy shall be implemented in order to limit the risks of brute force attacks on user credentials.

2.9.3.3 Passwords and authentication tokens results must be hashed as per industry best practice to ensure that credentials cannot be intercepted during transmission.

2.9.3.4 The choice of algorithm used in the user credential protection when stored shall align with the industry best practice for password encryption.

2.9.3.5 Financial Service Operators shall develop a password policy that adheres to security best practice, and ensure all users utilize password that adhere to the policy.

2.9.3.6 Financial Service Operators must ensure that the credentials of the users are never shared with any other party, this must be clearly specified in the terms of use of the application provided to the customer.

2.10 Security Monitoring and Detection

2.10.1 Financial Service Operators 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, including security events.

2.10.2 Financial Service Operators 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.

2.10.3 Financial Service Operators 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.

2.10.4 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.

2.10.5 Financial Service Operators shall establish and implement systems for the centralized and coordinated monitoring of cyber risks and management of security related incidents.

2.10.6 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.

2.10.7 Financial Service Operators shall ensure that all logs must be monitored via automated systems and logs with significant interest shall be reviewed manually.

2.10.8 User access reviews shall be performed on regular basis, based on the user access policy and system criticality, to disable or remove accounts that are no longer required or assigned to any user.

2.10.9 Financial Service Operators shall implement a security system to collect, aggregate, correlate and perform analysis of disparate data from various sources and give alerts when suspicious events are detected.

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

2.10.11 Financial Service Operators shall implement network surveillance and security monitoring with use of network security devices, such as intrusion detection and prevention systems to protect the FSO against network intrusion attacks.

2.11 Data Protection

2.11.1 Financial Service Operators shall properly identify and classify data assets as per the FSO 's information classification policy.

2.11.2 Financial Service Operators must secure data with encryption algorithms, whether the data is at rest or in transit, using strong cryptographic methods

2.11.3 **Sensitive Data Transmission**

2.11.3.1 Financial Service Operators shall consider sensitive data assets as confidential by default.

2.11.3.2 All sensitive data must be encrypted using strong encryption mechanism while at rest, as per industry best practice.

2.11.3.3 All communication channels supporting the transmission of such data shall be protected with strong encryption mechanisms, as per industry best practice.

2.11.3.4 Sensitive data must be encrypted during transmission and storage in the customer device for mobile applications and at the server and web application level for web-based applications.

2.11.3.5 Processing personal information requires the FSO to follow the requirements of the Qatar Information Privacy Protection law of 2016.

2.11.3.6 Financial Service Operators shall establish a data retention policy in line with local laws and regulations for the regulated data.

2.11.3.7 Cryptographic controls to protect confidentiality, authenticity and integrity of information, and the level of protection required should be based on risk treatment subsequent to risk assessment exercises, and identify the chain of activities and events for using encryption for protecting the information transported by mobile phones and across communications lines.

2.12 Physical Security

2.12.1 The FSO shall ensure that the Technology processing environment is adequately protected against unauthorized access, tampering or destruction with physical security controls guided by a security policy.

2.12.2 The FSO shall use security gates to limit the entry of non-authorized persons.

2.12.3 The FSO shall ensure that data centers are accessible only to authorized technical staff. All access shall be documented, monitored and regularly reviewed.

2.12.4 The FSO will ensure that their computing environment including the data center is protected against hazards such as fire, therefore monitoring mechanisms for the detection of compromises of environmental controls such as temperature, water, smoke, access alarms and service availability alerts (power supply, telecommunication, servers).

2.12.5 The FSO shall monitor sensitive areas such as data centers using methods that include video monitoring and recording.

2.13 Data Backup

2.13.1 Financial Service Operators shall make backups of the information with a proper frequency (daily/weekly/monthly/yearly) as per regulatory and legal requirements.

2.13.2 Financial Service Operators shall keep financial data records as per applicable laws and QCB instructions. They shall develop a data retention and backup policy as well as procedures to ensure the safeguard of all sensitive information: personal data, financial records, company strategic documents, etc. FSOs shall specify the data retention period as per the law.

2.13.3 External media such as tape, optical drive, memory key and external drive shall be used with proper security measures to protect its access, disposal and use.

2.13.4 Financial Service Operators shall build a data backup schedule that employees can follow and the business can track. They shall automate the backup process, especially if network shared drives are used (backup of the file server providing these user shared drives).

2.13.5 Financial Service Operators shall store additional back up copy, preferably on a tape in a waterproof and fireproof safe, locked in different location.

2.13.6 Financial Service Operators shall have a data retrieval procedure in order to check if the backed-up information is retrievable twice a month.

2.13.7 Financial Service Operators must encrypt the backup information, and ensure that the encryption keys are protected and saved in a separate yet retrievable media location.

2.13.8 Financial Service Operators shall consider the implementation of a fault tolerant solution for sensitive servers. They shall ensure to have more than one server to avoid loss of information in case of hardware failures (hard disk, storage, servers, motherboard, etc.) and that configurations of devices (networks, servers and appliances) are in a backup too.

3 Compliance

3.1 Instructions

3.1.1 Financial Service Operators are required to comply with the requirements defined in this instructions document. The guidelines outlined here are minimum requirements and FSOs are therefore expected to put in place more robust security measure as per evolving security risks.

3.1.2 Financial Service Operators shall report their compliance to the requirements of this document, at least on annual basis and upon QCB's request.

3.1.3 Financial Service Operators shall ensure that their report on compliance includes the identification of gaps in their controls and remedial action taken to mitigate any risks that may arise from such gaps.

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

3.2 Laws and Regulations

Financial Service Operators shall understand, integrate in their operations and comply with the provisions of the following Qatar laws:

- QCB Law No. 13 of 2012
- Qatar Cybercrime Law No. 14 of 2014
- Qatar Information Privacy Protection Law No. 13 of 2016
- Qatar Law on Combating Money Laundering and Financing of Terrorism Law No. 20 of 2019 and the relevant QCB Regulation