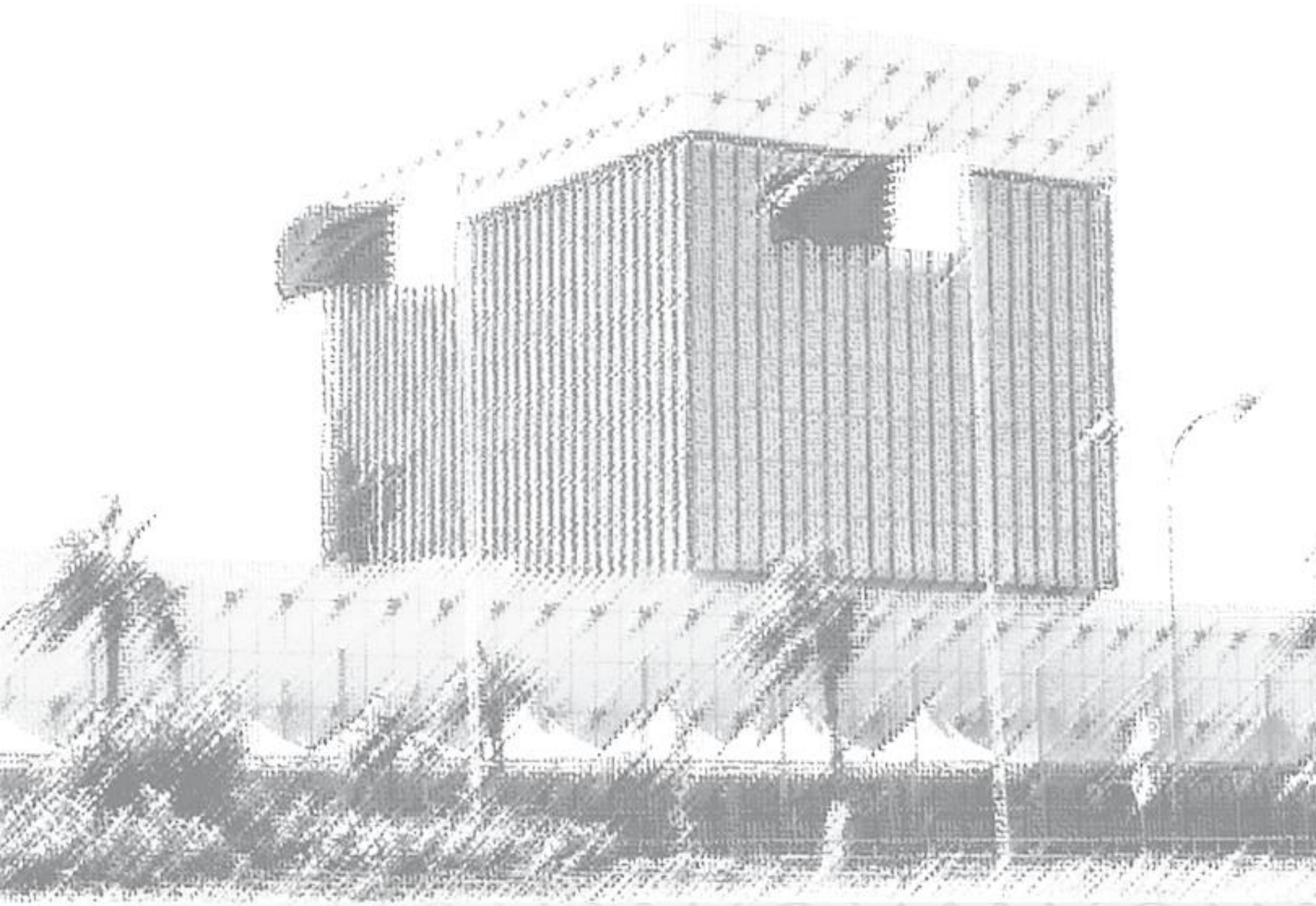
2022



Information and Cyber Security Regulation for Payment Service Providers

Document Overview

Manual Name	Information and Cyber Security Regulation for Payment Service Providers
Reference	[QIS-ISR-PSP]
Classification	Restricted

Revision History

Revision	Date	Summary of Changes
V 1.0	December 2021	First Draft
V 1.1	March 2022	Review
V 1.2	April 2022	For Release

Definitions:

QCB	Qatar Central Bank
QCB Law	Law of the Qatar Central Bank and the Regulation of Financial Institutions No. (13) of 2012.
Payment Service Providers	Individuals or entities engaged in providing any of the payment services specified in Clauses (5) and (6) of the Payment Services Regulations (for licensing and regulating the services of payment service providers).
Cyber Security	Set of defensive controls that aim to protect the computers, servers, portable device, electronic systems, network, associated data and information, from electronic and cyberattacks.
AML/CFT	Anti-money Laundering and Combating Financing of Terrorism
QFIU	Qatar Financial Information Unit

Contents

Introduction

The growth of emerging technologies within the financial sector creates opportunities for more efficient financial solutions that cater to the modern age of banking. Given the importance of the development and evolvement of payment services, this regulation provides the security requirements and mechanisms to secure the Payment Service Providers (PSPs) from cyberattacks and security risks.

It is the responsibility of QCB to ensure that all Payment Service Providers are legitimate entities that comply with the laws of the State of Qatar, QCB regulations and relevant circulars in order to protect the stability and integrity of the State of Qatar's financial sector.

Purpose

The aim of this regulation is to regulate the use of technology within the financial sector. Therefore, any applicant intending to provide payment services within the financial sector in the State of Qatar shall abide by it.

Scope

This regulation applies to all Payment Service Providers as defined in the QCB Payment Services Regulation (Payment Services Regulation for Licensing and Regulating Payment Service Providers) while the Payment Service Provider is in the sandbox, and will be used as an information and cyber security regulatory baseline for the subsequent phases after the sandboxing process.

A. Infrastructure and Operations Information and Cyber Security Requirements

1. Organization of the Information Security Governance

As a minimum, the Payment Service Providers must:

- Establish and implement a documented security policy that defines the risks and controls associated with sensitive information.
- Document the set of security controls that apply to the technology used in the proposed solution.
- Have resources dedicated to verify and remediate the risks identified.

2. Governance Controls

2.1. The Payment Service Providers shall establish an information and cyber security framework that defines the relevant functions, roles and responsibilities.

2.2. The board must oversee technology, information and cyber security risks and ensure that measures are in place to support their business strategies and objectives. The board must approve an overall cyber risk appetite.

2.3. The board must have representation with technical expertise to guide them on matters pertaining to information and cyber security. These representatives shall have adequate expertise in information and cyber security.

2.4. The board shall ensure that dedicated and adequate resources are put towards the information and cyber security function in order to verify and control all security risks, and effectively implement the security controls.

2.5. Information and cyber security policies, standards and procedures must be updated and reviewed at least on an annual basis.

2.6. An information and cyber security program shall be implemented to support the requirements listed in this regulation.

2.7. A committee shall be formed to oversee the information and cyber security activities with adequate representation from relevant departments such as IT, Risk Management, Information Security, Human Resources (HR), Business Continuity, Legal, Compliance and AML/CFT.

2.8. The Payment Service Provider shall have their cyber resilience capabilities assessed and measured with key indicators defining the level of preparedness/risks.

2.9. The information and cyber security indicators shall be able to cover the following domains:

- Risks: coverage, top risks.
- Compliance: external, internal.
- Incidents: statistics, management.
- Awareness and Information and Cyber Culture: training and knowledge from incidents.
- Threat levels: external, internal.
- Information and Cyber Security projects: progress, impact level on risk posture.

3. Information and Cyber Risk Management

3.1. The Payment Service Provider 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 and assessment of impact and likelihood of threats, risks and vulnerabilities on the PSP’s systems and operations.
- Development of a plan that contains policies, procedures and best practices that address the risks.
- Implement and maintain a regular testing plan.
- Monitor the overall risks and the updates that impact the risk posture.

3.2. The Payment Service Provider shall define a risk assessment process aligned with the best practices to identify threats and vulnerabilities to the PSPs environment and related assets, which includes internal and external networks, hardware, software, applications, systems, operations, data and human elements.

3.3. Following the proper identification of the risks and assets, the Payment Service Provider shall maintain a risk register and the associated threats.

3.4. The Payment Service Provider shall monitor these risks on a daily basis and develop reporting mechanisms and oversee the action plans to mitigate them.

4. Resiliency and Response Requirement

4.1. The Payment Service Provider must formulate an emergency response plan as part of a business continuity strategy that details evacuation procedures, command center operations, media and communications strategy.

4.2. At a minimum, the Payment Service Provider must identify all threat scenarios that may impact the operation and put in place all necessary response procedures.

4.3. The Payment Service Provider shall ensure that it replicates the technical infrastructure that supports its operations, in addition to establishing flexible backup plans to ensure resiliency.

5. IT Security Operations

5.1. The Payment Service Provider must define and implement a proper change management policy, process and procedures.

5.2. The Payment Service Provider shall document changes to applications, systems and infrastructure in a change management register.

5.3. The Payment Service Provider shall define and document an incident management process with various levels of escalation and responses.

5.4. The Payment Service Provider shall document all incidents with levels of severity, track and oversee the remediation actions.

5.5. The Payment Service Provider shall have a defined security monitoring policy that includes the security events being monitored.

5.6. The Payment Service Provider shall enable the logs on all systems in order to monitor security events that include but is not limited to user access activity, privilege management and anomalies on systems or applications.

5.7. The Payment Service Provider shall review security events in real time basis and retain logs for a minimum of 6 months.

5.8. The Payment Service Provider shall store data properly with regular backups as per a defined backup policy and apply strong encryption methods to the data.

5.9. The Payment Service Provider shall ensure that all systems have a proper maintenance plan with scheduled updates.

5.10. The Payment Service Provider shall enable logging 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, and the integrity of the logs shall be monitored continuously.

5.11. The Payment Service Provider shall keep logs for at least 6 months before storing the logs in the archives and the logs shall be protected against tampering.

5.12. The Payment Service Provider 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).

5.13. The Payment Service Provider shall review user access to systems and applications on a regular basis and apply measures including the principle of least privilege.

5.14. The Payment Service Provider shall monitor the performance of systems constantly.

5.15. The Payment Service Provider 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.

6. Cloud Computing

6.1. The Payment Service Provider must establish a cloud computing policy that must be approved by the PSP’s management. The policy must be reviewed periodically.

6.2. The Payment Service Provider shall only utilize a cloud service provider that has data centers within the State of Qatar. If an exception is required, the PSP must seek approval from QCB.

6.3. With reference to 6.2, the Payment Service Provider shall ensure that the processing and storage of transactional data that holds client information, sensitive data and other transaction information is secured locally within the State of Qatar. The data shall be protected while it is in transit and at rest in the cloud where the PSPs shall ensure that data is secured end-to-end as per the requirements defined in 6.7 and 6.8.

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

6.5. Use of cloud computing services shall not be used to delegate the risk controls that surround the data/system that is deployed in the cloud. Therefore, the Payment Service Provider 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.

6.6. The Payment Service Provider 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, maintenance and support, media protection, personnel security, physical security, planning, procurement, risk management, security assessment, system security and integrity controls.

6.7. The Payment Service Provider shall control cryptographic keys. This includes the entire Key Management System (KMS), and in particular the generation and issuance of private keys.

6.8. The Payment Service Provider 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.

6.9. The Payment Service Provider must ensure that sensitive data is not stored in a non-controlled cloud environment. A private cloud facility under control of the PSP shall be considered as an alternative.

6.10. When using cloud computing, the Payment Service Provider must ensure that the agreement with the cloud computing service provider contains key security controls limiting cloud computing risks including those detailed in this regulation.

6.11. While performing due diligence for the cloud service provider, the Payment Service Provider shall consider attributes and risks specific to cloud service.

6.12. The Payment Service Provider shall have contractual power to conduct a penetration test on the hosting infrastructure and application instances provided to the PSP by the cloud service provider.

6.13. The Payment Service Provider must have the contractual power and the means to migrate or destroy data stored within the service provider’s systems and backup, in the event of contract termination or expiry.

6.14. The Payment Service Provider 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.

7. Access controls

7.1. The Payment Service Provider shall define an access control policy and relevant procedures which shall include identification, authentication and authorization of users, based on the Role Based Access Control (RBAC) principles.

7.2. The Payment Service Provider shall enable auditing capabilities on access and monitor all access logs.

7.3. The Payment Service Provider must ensure the placement of controls to identify all users, contractors, third party and temporary staff with a unique identifier to ensure that actions are accountable and traceable.

7.4. The Payment Service Provider shall define a password policy and enforce it to safeguard user accounts from unauthorized access.

7.5. The Payment Service Provider shall authenticate administrative access or access to sensitive information via two-factor authentication mechanism.

7.6. The Payment Service Provider 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.

7.7. The Payment Service Provider shall monitor the administrators' accounts and log all activities.

7.8. The Payment Service Provider shall avoid generic accounts and they ensure that they are able to trace users' activities on systems.

7.9. The Payment Service Provider shall encrypt passwords using strong encryption methods and hashing algorithms that adhere to security best practices.

7.10.The Payment Service Provider shall only provide remote access on a need-to-have basis, with authorization from the relevant management function.

8. Network Architecture

8.1. The Payment Service Provider shall document and maintain the network infrastructure supporting its business activities.

8.2. The Payment Service Provider shall define network segregation zones with the various levels of segmentations based on the information asset classification.

8.3. The Payment Service Provider shall log network activity and monitor the infrastructure for any suspicious behavior, traffic activity, breach or disruption attempts.

8.4. The Payment Service Provider shall define proper security zones to receive network traffic from untrusted domains such as the Internet.

8.5. The Payment Service Provider shall ensure that all user accounts used for administering and maintaining the network infrastructure must follow the principles of user access controls defined in section A.7 (Access Controls).

8.6. The Payment Service Provider shall harden the network infrastructure prior to deployment for production.

8.7. The Payment Service Provider shall encrypt data at rest and in transit in the network. They shall use strong encryption algorithms that must adhere to security best practices, such as the use of digital certificates for authentication.

8.8. The Payment Service Provider shall secure all network equipment with the principles defined in this regulation and additional physical protection methods on cabling, devices, communication links and data centers.

8.9. The Payment Service Provider shall use VLANs to segment the network.

8.10. The Payment Service Provider shall use string encryption mechanisms on wireless networks when deployed, and use authentication for user access.

8.11. The Payment Service Provider shall implement a process to detect rogue wireless network access points.

8.12. The Payment Service Provider shall harden wireless access points and gateways as per the PSP's defined hardening guidelines. The parameters include SSID, encryption keys, SNMP strings and any insecure configuration that require to be changed at the time of installation.

8.13. The Payment Service Provider 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.

8.14. The Payment Service Provider shall implement DNS controls to ensure that zones are digitally signed, limiting the risks of malware spreading, name resolution interception and redirection.

8.15. The Payment Service Provider must harden DNS servers.

8.16. The Payment Service Provider shall put the following controls in place:

a. Several layers within the DMZs to separate the web front-ends, the web-based backend systems, databases and application servers using firewalls covering at least layer-3, IPS and IDS.

b. The internal DMZ layer shall be separated with additional firewalls that will cater to layer 5 to 7 protection.

8.17. The Payment Service Provider shall place the internal network behind the second or third layer DMZs.

8.18. The Payment Service Provider shall implement deep packet inspection to ensure that internet traffic is screened properly.

8.19. The Payment Service Provider shall monitor internet traffic.

8.20. The Payment Service Provider shall secure email communications with proper implementation of SPF (Sender Policy Framework) to detect email spoofing.

8.21. The Payment Service Provider shall harden email servers prior to deployment.

8.22. The Payment Service Provider shall protect NTP servers against threats including automatic unauthenticated NTP requests.

8.23. The Payment Service Provider shall synchronize all devices to the NTP server which shall be synchronized with the ISP or universal atomic clock time servers.

8.24. The Payment Service Provider must enable two-factor authentication for VPN connections prior to establishing the VPN tunnel. A hardware or software token shall act as primary authentication followed by an integrated Radius, LDAP, AD or TACACS+ authentication.

8.25. The Payment Service Provider shall secure VPN tunnels, for example through the use of IPSEC with Internet Key Exchange (IKE Certificates) or TLS 1.2. (GMC or CTR) for web application access.

9. Virtualization

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

9.1. The Payment Service Provider must ensure that limits are set on the use of resources such as processors, memory, disk space, virtual network interfaces on each VM.

9.2. The Payment Service Provider must enforce role-based access controls and the principle of least privilege individually on each VM.

9.3. The Payment Service Provider shall configure VMs to disallow peripheral physical devices by default unless explicitly configured with a business need.

9.4. The Payment Service Provider shall disallow file sharing between the host machine and VMs unless adequate risk assessment has been performed to prevent attacks.

9.5. Wherever possible, the Payment Service Provider shall ensure that separate credentials are used for managing VM and host OS.

9.6. The Payment Service Provider shall protect VMs by the placement of a local firewall and a firewall configured on the host OS.

10. Database security

10.1.The Payment Service Provider shall harden databases and its subsystems as per the Payment Service Provider defined hardening guidelines. Parameters such as default password, connection strings, SNMP communities or any insecure configuration shall be changed at the time of installation.

10.2.The Payment Service Provider shall govern access to information in a database according to the principle of least privilege and role-based access controls. Information stored in the database shall be classified as per the PSP’s information classification policy.

10.3.The Payment Service Provider shall ensure that the core production database is not directly accessible from outside the Payment Service Provider’s environment.

11. Data Security

11.1. The Payment Service Provider must properly identify and classify data assets as per the PSP’s information classification policy.

11.2. The Payment Service Provider must secure data with proper encryption algorithms whether the data is at rest or in transit using strong cryptographic methods and standards such as AES, RSA, SHA with high key sizes.

11.3. The Payment Service Provider shall consider sensitive data assets as confidential by default and protect them with adequate measures as mentioned in 11.2.

11.4. The Payment Service Provider shall control data leakage risks effectively with proper end user and system controls such as limitations on using I/O ports, sending sensitive information to unauthorized recipients or network.

11.5. The Payment Service Provider shall ensure that data integrity controls are place during the processing and storage of data.

11.6. The Payment Service Provider shall ensure that data protection controls are not downgraded in case of migration or archival of data.

11.7. The Payment Service Provider shall establish a data retention policy in line with local regulations for the regulated data.

11.8. The Payment Service Provider shall limit the use of mobile storage devices, they shall not leave the Payment Service Provider premises with sensitive data except if authorized explicitly by the management of the Payment Service Provider and in accordance to business requirements justifications.

12. Web Application Security

12.1. The Payment Service Provider shall follow confidentiality requirements and related security measures in line with Qatar Personal Data Privacy (Law No.13 of 2016).

12.2. The Payment Service Provider shall ensure that customer registration data is transmitted securely over encrypted channels to the PSP as stipulated in the current set of controls of this document.

12.3. The Payment Service Provider shall ensure that captured registration data is stored temporarily in an encrypted manner in the end-user's device and shall be wiped out once transmitted to the PSP for verification using strong encryption algorithms that adhere to security best practices.

12.4. The Payment Service Provider shall test its applications against OWASP Top 10 and SANS Web application security.

12.5. The Payment Service Provider shall test its applications against error handling, access control risks, sensitive data protection, weak authentication, input and output handling and session interference risks.

12.6. The Payment Service Provider shall secure APIs using strong encryption methods that adhere to security best practices

12.7. The Payment Service Provider shall use strong hashing methods such as SHA-256/384 when using key derivation functions (Pbkdf2), this must be updated as per security best practices.

12.8. The Payment Service Provider shall use multi-factor authentication with OTP for user authentication.

12.9. The Payment Service Provider shall employ code tampering techniques to detect any attempt to modify the application code and stop any detected tampering attempts.

13. Cryptographic Security

13.1. The Payment Service Provider must define its cryptographic policy by referring to industry standards.

13.2. The Payment Service Provider shall ensure that the Key Management System (KMS) limits the key handling cycle within the Payment Service Provider where private keys are stored securely.

13.3. When deploying Public Key infrastructure, the Payment Service Provider shall ensure that they follow PKCS#7 and X509 for digital certificates.

13.4. The Payment Service Provider shall distribute private keys for PKI use in a secure manner through a security device or by secure transmission to the end user.

13.5. When using Cloud services, the Payment Service Provider private keys shall be used as part of its own KMS as defined in 13.2.

13.6. The Payment Service Provider shall secure confidential data at rest, in transit or in use, such as securing web traffic, file transfers, remote access, emails, secure data hashing, HDD/data at rest encryption, symmetric key encryption, asymmetric key encryption and hardware security modules (HSM's) whenever sensitive data is processed.

13.7. The Payment Service Provider shall align its use of cryptography with its information classification policy.

14. Threat and Vulnerability Risk Assessment

The Payment Service Provider shall not only demonstrate that it is capable of defining security controls, but also identifying the risks properly in order to design, maintain and update the adequate information security controls.

14.1. The Payment Service Provider shall perform an annual gap analysis and risk assessment to determine if the current controls are adequate, and that their response and recovery plans are effective. Additionally, the Payment Service Provider shall put a roadmap in place to promptly address any gaps that are found.

14.2. The Payment Service Provider shall document and monitor key risks with defined indicators.

14.3. The Payment Service Provider shall perform vulnerability assessments, code reviews and penetration testing at least twice a year, or more frequently as needed, for the entire application infrastructure. They shall ensure that these exercises are performed by an external, reputable penetration testing provider that has the required certificates, with regional offices.

14.4. The Payment Service Provider shall deploy a combination of automated tools and manual techniques to perform a comprehensive Vulnerability Assessment (VA) exercise in a continuous basis. Industry practices and standards shall be followed while performing these tests, such as OWASP, OSSTMM and SANS. At a minimum, the Payment Service Provider must compare the results from previous vulnerability scans to verify that these vulnerabilities were addressed and mitigated.

14.5. The Payment Service Provider shall prepare an action plan to address identified vulnerabilities and raise them to the senior management.

15. Malware Protection and Cyber Attacks

15.1. The Payment Service Provider shall implement solutions and related controls to detect and mitigate malware at server, network and endpoint level.

15.2. The Payment Service Provider shall properly maintain anti-malware solutions with up to date malware signature databases and engines.

15.3. The Payment Service Provider 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.

15.4. The Payment Service Provider shall protect emails with SPF as specified by A 8.20 as well as DKIM and digital signatures to limit the risks of phishing emails.

15.5. The Payment Service Provider shall identify and mitigate any single-point of failure of the critical functions on the network, systems and applications to avoid disruption. Additionally, the Payment Service Provider shall subscribe to DDoS services to limit the risks of disruption.

15.6. The Payment Service Provider shall periodically conduct cyberattack simulation testing on their systems. The coverage and scope of testing shall be based on the cyber security risk profile and threat intelligence available. The PSPs shall take appropriate actions to mitigate the issues, threats and vulnerabilities identified in the cyber-attack simulation testing exercise in a timely manner, based on the impact and risk exposure analysis.

15.7. The Payment Service Provider shall have an incident management response plan in case of cyberattacks.

15.8. The Payment Service Provider shall document cyberattacks with impact, preservation of evidence and resolution plans.

16. Physical Security

16.1. The Payment Service Provider shall ensure that the Information Technology processing environment is adequately protected against unauthorized access, tampering or destruction with physical security controls guided by a security policy.

16.2. The Payment Service Provider shall use security gates to limit the entry of non-authorized persons.

16.3. The Payment Service Provider shall ensure that data centers are accessible only to authorized technical staff. All access shall be documented, monitored and regularly reviewed.

16.4. The Payment Service Provider 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).

16.5. The Payment Service Provider shall place an evacuation plan across the premises in case of emergency situations.

16.6. The Payment Service Provider shall monitor sensitive areas such as data centers using methods that include video monitoring and recording.

17. Software Development and Acquisition

17.1. The Payment Service Provider shall practice secure code reviews and implement security by design as part of a well-defined software development life-cycle (SDLC).

17.2. The Payment Service Provider shall review its application thoroughly against malicious code injections as part of their secure coding practice.

17.3. The Payment Service Provider shall have clearly segmented development, testing and production environments where each environment is separate from the other.

17.4. The Payment Service Provider shall ensure that the security specifications are designed from the initial step of a software's development cycle.

17.5. In case of third-party development, the Payment Service Provider shall ensure that the third-party is aligned with these principles and the Payment Service Provider's security policies.

17.6. The Payment Service Provider shall check any acquired application for potential backdoors, vulnerabilities and any security risks.

17.7. The Payment Service Provider shall practice DevSecOps principles to automate application vulnerability scanning during the SDLC and data security at various levels (application to databases).

18. Media Security

18.1. The Payment Service Provider shall carefully use media and ensure that it follows the level of sensitivity of the information it may carry, and therefore encryption shall be used when carrying such information on media.

18.2. The Payment Service Provider shall ensure that only authorized personnel carry out repairs and maintenance work on classified media.

18.3. The Payment Service Provider shall ensure that media is sanitized, destroyed by degaussing non-volatile media and physically destroyed through smashing and drilling.

19. Data Center

19.1. The Payment Service Provider shall ensure that their data center(s) are resilient and protected against physical intrusion.

19.2. The Payment Service Provider shall apply power redundancy and fault tolerance principles across the data center(s).

19.3. The Payment Service Provider shall use uninterruptible power supplies and generators on critical systems to avoid loss of data or systems due to sudden power failure disruption.

19.4. The Payment Service Provider shall document a procedure that involves a strict review of authorized staff accessing the data center(s), as per A 16.3.

19.5. The Payment Service Provider shall ensure that there is proper notification and approval process for non-Payment Service Provider personnel, such as vendors or system administrators who require temporary access to the data center(s) to perform maintenance or repair work.

20. Managing Outsourcing Risk

20.1. The Payment Service Provider shall only outsource or enter into agreements after they perform the required due diligence which includes a thorough third-party risk assessment exercise and background check. The PSP shall ensure that its third parties are legitimate and reputable.

20.2. The Payment Service Provider shall ensure that all key risks it has identified are communicated and reported by the third party as well.

20.3. The Payment Service Provider shall ensure that the contractual agreement with a third party shall include security requirements 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.

20.4. The Payment Service Provider shall consider the following in their third-party risk assessments: location of data when it is processed, stored and transmitted and any relevant vendor contracted by the third party.

20.5. The Payment Service Provider shall include exit clauses that ensure that any data will be wiped out of any of the third-party assets in its contractual agreements.

20.6. The Payment Service Provider must seek approval from QCB before signing any contractual agreement with regards to outsourcing functions related to the operation of its core services.

B. Business Applications

21. Digital Fraud Risk Management

21.1. The Payment Service Provider shall ensure that fraud is monitored across financial transactions in its platforms.

21.2. The Payment Service Provider shall define a policy to ensure that the accountability and responsibility surrounding the fraud monitoring activity are assigned with dedicated resources.

21.3. The Payment Service Provider shall assess and check any system or application used to deliver payment services, in addition to assessing the risk of fraudulent activities stemming from the system or application.

21.4. The Payment Service Provider shall only grant access to fraud risk monitoring and related transactions on a need to know basis.

21.5. The Payment Service Provider shall keep data from financial transactions secure with data encryption practices as defined in this regulation and as per security best practices.

21.6. The Payment Service Provider shall follow QCB eKYC Security Controls Principles Regulation.

21.7. The Payment Service Provider's internet-based financial application(s) must adhere entirely to the set of measures defined in this regulation with appropriate access mechanisms that limit the risk of interception and fraudulent transaction operations.

21.8. The Payment Service Provider shall train its employees and raise awareness with regards to fraud risks and the associated technical and legal implications.

21.9. The Payment Service Provider shall ensure that their customers are aware of the information and cyber risks that may lead to fraudulent activities and they shall provide them with methods to directly report such fraudulent activities via an appropriate means.

21.10. The Payment Service Provider shall have the required procedures in place to identify, detect, prevent and respond to fraudulent activities.

21.11. The Payment Service Provider must immediately report any digital fraud and cybercrime in general to the NCSA, MoI, QFIU and QCB.

22. Online System Security

22.1. The Payment Service Provider shall ensure that no sensitive data is stored in clear text on the end user's device. This applies to web applications and mobile applications. Such data if necessary may reside encrypted in memory for the time of utilization by a process but shall not be kept stored on the end user device. If encrypted, encryption keys shall not be stored in the same location as the encrypted data.

22.2. The Payment Service Provider shall undertake a vulnerability assessment and penetration testing of its online application(s) as indicated in A 14.3 to minimize exposure to other forms of cyberattacks such as man-in-the-middle attack (MITM) or man-in-the-browser attack.

22.3. The Payment Service Provider shall ensure a high resiliency and availability of its application(s) and ensure protection against Distributed Denial of Service attacks.

22.4. In case of connecting to the Payment Service Provider back office systems, the PSP shall prohibit direct connections and they shall place relays in the DMZ only as per network security requirements of the section A 8 (Network Architecture).

22.5. The Payment Service Provider shall design clear segmentation of networks and support the creation of multiple DMZs for web connectivity of the applications as per section A 8 (Network Architecture).

23. Payment Systems Security

23.1. When using payment operations, the Payment Service Provider shall adequately secure the whole payment value chain with proper encryption methods, this shall be implemented for customers when processing payment operations through payment cards and authentication data.

23.2. The Payment Service Provider must ensure that its applications that accept payments from payment card industry council member cards must abide to PCI-DSS requirements as an acquiring processor.

23.3. For online PIN authentication usage from payment card, the Payment Service Provider must abide to the PCI-PIN Transaction Security (PCI-PTS) requirements as well as PCI PA-DSS for Payment Applications security.

23.4. In the case of bank to bank payment transactions, the Payment Service Provider shall ensure that the same principles of identification, authentication and authorization apply with a complete end-to-end encryption of the transactions.

23.5. When deploying mobile payment applications, the Payment Service Provider shall ensure that the virtual pin-pad used in the case of using payment card PIN data is encrypting all keystrokes as per PCI PED security and is separate from the non-secure virtual keyboard of the mobile operating system.

23.6. When authenticating, the Payment Service Provider shall use payment OTP as one of the factors for authenticating the customer. It is recommended to also combine OTP with another factor of authentication such as PIN code, password or secure biometrics.

23.7. The Payment Service Provider shall monitor all transactions and they shall receive alerts on suspicious transactions.

C. Emerging Technologies

Emerging technologies are used as a subset of an information processing environment; hence their usage shall not contradict or supersede the security requirements set forth in other sections of this regulation. Therefore, the implementation of the following technologies referred to hereafter must comply with the previous requirements of this regulation.

24. Artificial Intelligence

The Payment Service Provider shall:

24.1. Implement a solid data governance framework (roles and responsibilities for data ownership, data dictionaries, etc.).

24.2. Perform due diligence reviews on the data provider, perform risk and impact assessments and implement safety controls when required.

24.3. Ensure that the source code is tamper proof to limit the possibility of interception and manipulation.

24.4. Ensure that all AI tasks are under control, depending on the criticality of the task being automated, the Payment Service Provider shall implement and demonstrate a human oversight/dual control over the AI use.

24.5. Continuously monitor the AI model performance and update the model (re-training) when new (disruptive) events occur.

24.6. Implement code specific non-discriminatory rules to minimize risks of discrimination and generate alerts when needed.

24.7. Ensure that adequate audit log retention is placed in line with legal requirements and based on data sensitivity as per data retention defined in this regulation.

24.8. Follow development and testing processes as per best practices with a documented and strict SDLC, and develop change management process that include version tracking and security by design implementation as per section A 17 (Software Development and Acquisition).

25. Blockchain

Payment Service Providers must follow the best practices and requirements of the current regulation to ensure that the blockchain operations are protected along its value chain, and therefore they shall:

25.1. Link the validation and integrity of transactions over blockchain to smart contract based policies that shall include requirements for endorsement of parties involved using for example multiple signatures for specific organizations depending on their role.

25.2. Include the defined rights of individuals and third-party participants into the blockchain as a part of identity and access control.

25.3. Perform authentication with strong tokenized and encrypted mechanisms. OAUTH, OIDC and SAML2 should be used then for authentication, verification and authorization for all members of the blockchain.

25.4. Enable audit logs with alerts in case any malicious activity is identified, if the policy is breached.

25.5. When using an HSM to securely store the blockchain identity keys, ensure that the HSM partition process shall grant each separate partition its own admin rights and roles to perform partition operations on each different partition.

25.6. Secure smart contracts with granular access controls.

25.7. Encrypt and secure all communications as per section A 8 (Network Architecture) requirements.

26. APIs (Application Programming Interfaces)/Middleware

The risks of interception, manipulation or disruption can be high when using APIs depending on how well the security has been taken into consideration in its design phase. When using APIs for financial operations the Payment Service Provider shall:

26.1. Use stateful REST APIs and limit SOAP to transport only encrypted messages.

26.2. Use tokens to ensure trust in identities and control their accesses.

26.3. Configure REST API to avoid the security risks as defined in section A 12 (Web Application Security) of this regulation.

26.4. Encrypt data crossing over these APIs following methods defined in the section A 8 (Network Architecture) as minimum.

26.5. Identify vulnerabilities by using sniffers to detect data leaks and weak spots.

26.6. Define quotas on how often APIs can be called and throttling rules to protect APIs from Denial-of-Service attacks.

26.7. Use an API gateway as the central point to enforce API traffic authentication and security controls.

26.8. Encrypt API keys with strong cryptographic algorithms as defined in this regulation and as per security best practices.

26.9. Test APIs against OWASP Top 10 API security principles.

D. Compliance with QCB regulation

Failure to comply with the requirements may lead to financial penalties as per article (216) of QCB Law No. (13) of 2012 and article (44) of Anti-money laundering and financing of terrorism act (20) of 2019.