مصرف قطر المركزي
Qatar Central Bank
State of Qatar • دولـــة قطـــر

Cloud Computing Regulation

Regulating the use of Cloud Computing

by QCB-Licensed Entities

Table of Contents

PART A (GENERAL PROVISIONS)

1. Short Title and Commencement

The instructions set forth herein are titled the "Cloud Computing Regulation" and will enter into force as of 15 /04 /2024.

2. Definitions

For the purpose of this regulation, the following terms are defined as follows, unless the context otherwise suggests.

S. No.	Term	Explanation
1	Cloud Computing	A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
2	Cloud Computing Arrangement	Any arrangement with a CSP to outsource Cloud Computing (inclusive of Primary Sub-Contractors) or an arrangement with a third party that utilizes a CSP in the services it provides to an Entity.
3	Cloud Computing Outsourcing	An outsourcing arrangement where an Entity outsources some or all of its computing.
4	Cloud Service Provider (CSP)	An organization that provides Cloud Computing services to an Entity.
5	Entity	An organization regulated by the Qatar Central Bank.
6	International Standard on Assurance Engagements (ISAE) 3402 Standard	A report for a service organization providing a written assertion attesting to the fair presentation and design of controls (in a Type 1 report) or the fair presentation, design, and operating effectiveness of controls (in a Type 2 report).
7	Key Management System (KMS)	The system responsible for the secure generation, storage, distribution, and lifecycle management of cryptographic keys, ensuring the protection and control of private keys, regardless of where data is stored or processed.

8	Legal Entity Identifier (LEI)	LEI is a 20-character, alpha-numeric code based on the ISO 17442 standard. It connects to key reference information that enables clear and unique identification of a legal Entity participating in financial transactions. Each LEI contains information about an Entity's ownership structure and thus answers the questions of 'who is who' and 'who owns whom'.
9	Materiality	An expression of the relative significance or importance of a particular matter in a given context.
10	Material Arrangements	Cloud Computing Arrangements which: (a) In the event of a service failure or security breach, has the potential to impact an institution's; (i) business operations, reputation or profitability; or (ii) ability to manage risk and comply with applicable laws and regulations, or (b) Involves customer information and, in the event of any unauthorized access or disclosure, loss or theft of customer information, may have a negative impact on an institution's customers.
11	Personal Identifiable Information (PII)	Any information relating to an identified or identifiable natural Person. This information can directly or indirectly identify an individual, such as name, identification number, location data, etc.
12	Primary Sub-Contractor	Sub-contractors processing an Entity's data on behalf of the CSP.
13	Qatar	The State of Qatar.
14	QCB	The Qatar Central Bank, which has been established as per the QCB Law.
15	QCB Law	Law of the Qatar Central Bank and the Regulation of Financial Institutions No. (13) of 2012.
16	Register	Inventory of an Entity's Cloud Computing Arrangements, for which a regulated Entity is required to maintain an updated Register recording them.
17	Sector-Specific Security Regulation	QCB Information Security regulations that are applicable to Entities from a specific subsector within the financial sector in Qatar.

18	Service Level Agreement (SLA)	The part of the contract that defines exactly what services the CSP will provide, and the required level or standard for those services.
19	System and Organization Controls Audit (SOC Reports)	An independent assessment of the risks associated with using service organizations and other third parties. SOC 1 audits relate to organizations' ICFR (internal control over financial reporting). SOC 2 audits assess service organization's security, availability, processing integrity, confidentiality and privacy controls.

3. Introduction

Cloud Computing and related Cloud Computing Outsourcing have become ubiquitous in the business world over the last decade. Cloud Computing may provide operational flexibility, reliability and recovery speeds.

Even though Cloud Computing can be beneficial, it also raises significant new risks that this regulation intends to address, especially in relation to outsourcing. Security concerns are the foremost issue as the placement of data externally raises many concerns.

This regulation requires an Entity to conduct appropriate due diligence, preparation and maintenance of a Cloud Computing Arrangements. This regulation must be considered in conjunction with QCB's Sector-Specific Security Regulation for each Entity.

4. Purpose

This regulation aims to set requirements for a well-structured and secure usage of Cloud Computing Arrangements by an Entity. The Cloud Computing regulation defines the minimum baseline for an Entity to establish and maintain the necessary controls regarding the selection, usage and exit of Cloud Computing services, in conjunction with QCB's Sector-Specific Security Regulation for each Entity.

5. Scope

5.1. This regulation covers the use of Cloud Computing by all QCB regulated Entities. This regulation is only applicable to an Entity looking to adopt Cloud Computing deployments and Entities that currently have Cloud Computing deployments.

PART B (GOVERNANCE)

Cloud Computing governance requires the creation of a strategic plan, oversight protocols for an Entity board and senior management and a function overseeing a detailed regulation for managing Cloud Computing.

6. Strategy

6.1. An Entity must create a defined Cloud Computing strategy based on the Entity's needs and risk appetite. It must also be consistent with the Entity's relevant strategies and internal policies and processes.

6.2. An Entity must conduct a periodic review of its Cloud Computing strategy consistent with other strategic reviews.

6.3. An Entity must ensure that its strategy addresses information and communication technology, information security, and operational risk management (including business continuity and resiliency framework).

6.4. An Entity's Cloud Computing strategy must define an implementation plan and architectural roadmap that covers the target IT environment, the transition from the current environment to the target environment, and the operating model, including any organizational change or additional skillsets that may be necessary.

6.5. An Entity must allocate sufficient resources to handle all Cloud Computing Arrangements.

6.6. An Entity must establish policies within the Cloud Computing strategy, defining parameters for acceptable engagements within its Cloud Computing Arrangements.

6.7. An Entity may adopt a multi-cloud service provider strategy in order to mitigate risks associated with single point of failure, security risks and maintain operational continuity.

6.8. An Entity's Cloud Computing strategy must be consistent with the Entity's overall outsourcing strategy.

6.9. An Entity entering into outsourcing arrangements remains fully accountable for complying with all regulatory obligations and cannot delegate accountability within its Cloud Computing Arrangements.

7. Corporate Governance

7.1. An Entity's board of directors and senior management must ensure effective internal controls and risk management practices are implemented to achieve security, reliability and resilience of its Information and Communication Technologies (ICT) operating environment.

7.1.1. Both the board of directors and senior management may have members with the knowledge to understand and manage technology risks, which include risks posed by cyber threats.

7.1.2. An Entity's senior management must be responsible for the assessment, understanding and monitoring of the Entity's reliance on Cloud Computing and CSPs for material services.

7.2. An Entity's management must provide information that is clear, consistent, robust, timely, well targeted, and contain an appropriate level of technical detail to facilitate effective oversight and challenge by the board.

7.3. An Entity that enters into Cloud Computing Arrangements remains fully accountable for complying with all their regulatory obligations.

7.4. An Entity must define risk appetite and tolerance levels for Cloud Computing Arrangements.

7.5. An Entity must establish a function overseeing internal and external Cloud Computing Arrangements or delegating its responsibility to an existing function within the Entity.

8. Cloud Governance Policy

8.1. An Entity must establish approved and documented cloud governance policies for effective decision-making and proper management and control of risks arising from Cloud Computing Arrangements. The governance policy must:

8.1.1. Develop a cloud governance policy as per relevant industry leading practices, global standards and regulations.

8.1.2. Define the roles and responsibilities for the operation and management of Cloud Computing, security controls and risk management controls. Where a CSP is involved, the division of roles and responsibility between an Entity and the CSP must be clearly defined.

8.1.3. Define the process to conduct a risk-based analysis to identify and classify the information and technology assets involved in or deployed by the Cloud Computing Arrangements based on Materiality and confidentiality. The process should conform to the Entity's internal risk assessment measures.

8.1.4. Require the maintenance and updating of the asset list of information and technology assets in the cloud environment elements including, but not limited to, ownership, security controls and business criticality.

8.1.5. Establish strong authentication, access controls, data encryption and other security and technical controls to meet all Entity requirements and these should align with the Entity's internal security policies and the relevant Sector-Specific Security Regulation.

8.1.6. Establish appropriate policies, procedures, and controls to govern the use of Cloud Computing, covering risk management, due diligence on the CSPs, access and confidentiality.

8.1.7. Define a process to review and approve Cloud Computing Arrangement contracts with relevant approvals from the function's management as per clause (7.5).

8.2. An Entity must define how they apply their Cloud Computing policy to each Cloud Computing Arrangement.

8.3. An Entity must consider its data classification framework and the sensitivity of data within its cloud computing policy.

8.4. An Entity must develop a policy on the applicable global standards and the compliance to those standards for Cloud Computing Arrangements.

9. Register

9.1. An Entity must develop a Register with a complete inventory of Cloud Computing Arrangements.

9.2. An Entity must disclose to QCB the criteria it is using to determine if a contract is material or not.

9.3. An Entity must maintain an updated inventory internally.

9.4. An Entity must disclose the full Register to QCB on an annual basis and upon request by QCB.

9.5. An Entity must maintain an updated Register of information on all its Cloud Computing Arrangements, distinguishing between Material Arrangements and other arrangements.

9.6. The Register must include:

9.6.1. Background check performed on CSP (Yes or No).

9.6.2. Risk assessment conducted on CSP (Yes or No).

9.6.3. The start date, as applicable.

9.6.4. The next contract renewal date.

9.6.5. The end date and/or notice periods for both the CSP and for the Entity.

9.6.6. A description of the activities and data to be outsourced.

9.6.7. Classification of data processed or stored.

9.6.8. PII or transactional data (Yes or No).

9.6.9. A category assigned by an Entity that reflects the nature of the outsourced function (for example information technology function, control function), which must facilitate the identification of the different types of cloud outsourcing arrangements. Whether the outsourced function supports business operations that are time critical.

9.6.10. The name and the brand name (if any) of the CSP.

9.6.11. Where an Entity uses a service provider as an intermediary to access a CSP this must be recorded in the Register.

9.6.12. Where the country of registration, local corporate registration number and LEI (where available).

9.6.13. Registered address and relevant contact details.

9.6.14. When applicable, name of its parent company.

9.6.15. Governing law of the cloud outsourcing arrangement and, if any, the choice of jurisdiction.

9.7. An Entity must include within the Register its vendors' CSP arrangements, when the Entity's data is processed by the vendor's CSP, and all the items mentioned in clause (9.6) must be included.

9.8. For any Primary Sub-Contractor of the CSP, the Entity must ensure all the items mentioned in clause (9.6) are included.

PART C (CLOUD COMPUTING LIFECYCLE)

10. Entity Outsourcing Implementation Planning

10.1. An Entity must plan and manage its transition to a Cloud Service Provider (CSP). This should include an evaluation of the CSP's technical support capabilities and any guidance or tools they can provide to facilitate a smooth transition of functions.

10.2. An Entity must review its governance and data requirements, and check for any constraints before planning a transition to the cloud, this includes but is not limited to:

10.2.1. An Entity must conduct a legal due diligence to ensure that it is not restricted by legal obligations, QCB issued regulations, or agreements, or data use agreements that might restrict the transfer of data to third parties, even if these third parties are service providers.

10.2.2. An Entity must check that the required consent has been received as per the Law No. (13) of 2016 on Personal Data Privacy Protection, if the company plans to subcontract the processing of the Customer's data to a third party.

10.2.3. An Entity must review the legal and regulatory requirements, contractual obligations and other corporate policies. Corporate policies and standards must be reviewed to see if they need to be updated to allow a third party to handle data.

10.2.4. An Entity must ensure data governance policies and practices extend to data processed on the cloud.

10.2.5. An Entity must review whether the existing data or technical architectures are optimal for a cloud environment prior to migrating to the cloud.

11. Cloud Computing Arrangement Due Diligence

11.1. An Entity must undertake due diligence on the CSP whether it is directly contracted with the CSP or has contracted with a CSP via a broker or other intermediary.

11.2. An Entity must undertake due diligence on prospective CSP and appropriateness of the prospective CSP and services selected, considering the intended usage of the Cloud Computing service.

11.3. An Entity must have a clear and documented business case or rationale in support of the decision to utilize the cloud.

11.4. An Entity must consider the CSP's data confidentiality, security maturity, financial, operational, and reputational factors and the CSP's ability to comply with its obligation under the outsourcing arrangement, in its due diligence of a service provider.

11.5. An Entity must consider its data classification framework and the sensitivity of data in scope prior to any Cloud Computing Arrangement.

11.6. An Entity must ensure that the depth of the due diligence must commensurate with the criticality and Materiality of the Cloud Computing Arrangement.

11.7. An Entity must establish risk mitigating controls that align with the criticality and Materiality of the Cloud Computing Arrangement and deploy cloud model-specific (SaaS, PaaS, IaaS) controls.

11.8. An Entity must consider the track record of the CSP in achieving acceptable outcomes in areas such as information security policies and awareness, due diligence and risk assessment of practices related to sub-contracting, system vulnerability assessments, penetration testing and technology refresh management.

11.9. An Entity must verify the CSP's ability to recover the outsourced systems and/ or IT services within the stipulated Recovery Time Objective ("RTO") & Recovery Point Objective ("RPO").

11.10. An Entity must cover all zones that support the Entity's processing and data storage requirements in its due diligence of a CSP. It must not be assumed that controls are consistent across all locations. An Entity must set the scope of the due diligence assessment appropriately to cover an adequate set of controls and individual assessments of all locations expected to be relevant in the arrangement.

11.11. An Entity must ensure that CSP implement strong authentication, access controls, data encryption and other security and technical controls to meet the Entity's requirements.

11.12. An Entity must verify that the CSP's controls adhere to the QCB Sector-Specific Security Regulation.

11.13. Prior to implementing Cloud Computing services and undertaking an outsourcing arrangement, an Entity must conduct an initial security and risk assessment of the service to identify any information security, cybersecurity other IT control weaknesses. This must be done as per the Entity's internal processes and the Sector-Specific Security Regulation.

11.14. An Entity must ensure that the security and risk assessment identifies security threats including information security threats and operational weaknesses and develop safeguards to mitigate those threats and weaknesses. The factors considered during the risk assessment must include, but are not limited to the following:

11.14.1. Nature of the service (including specific underlying arrangements).

11.14.2. Provider and the location of the service.

11.14.3. Criticality and confidentiality of the assets involved.

11.14.4. Transition process including handover from an Entity and/ or other service providers to the potential outsourcing service provider.

11.14.5. Adherence to recognized technical security standards.

11.14.6. Compliance with international and domestic standards.

11.14.7. An Entity may also take any external assurance that has already been provided by independent auditors when conducting their own due diligence.

11.15. An Entity must conduct a Threat & Vulnerability Risk Assessment (TVRA) or an equivalent independent assessment on the CSP's data centers where these data centers support the Entity's operations.

11.16. An Entity must ensure the CSP has a disaster recovery and business continuity plan.

11.17. An Entity must conduct a detailed review of any financial information publicly available, provided by the CSP or other sources, in its due diligence.

11.18. An Entity must assess its Cloud Computing Arrangements compliance to the global standards as per the clause (8.4) and this regulation. For such purposes, an Entity may rely on an independent reputable auditor's assurance demonstrating the CSP's compliance.

12. Sub-Contractors Due Diligence

12.1. If the Entity, by the contract with the CSP, permits sub-contracting of material or important functions (or material parts thereof), the Cloud Computing Arrangement must:

12.1.1. Specify any part or aspect of the outsourced function that are excluded from potential sub-contracting.

12.1.2. Indicate the conditions to be complied with in case of sub-contracting.

12.1.3. Specify that the CSP remains accountable and is obliged to oversee those services that it has sub-outsourced to ensure that all contractual obligations between the CSP and an Entity are continuously met.

12.1.4. Include an obligation for the CSP to notify an Entity of any intended sub-contracting, or material changes thereof, in particular where that might affect the ability of the CSP to meet its obligations under the cloud outsourcing arrangement with the Entity. The notification period set in the written agreement must allow an Entity sufficient time at least to carry out a risk assessment of the proposed sub-contracting or material changes thereof and to object to or explicitly approve them.

12.1.5. Ensure that an Entity has the right to object to the intended sub-contracting, or material changes thereof, or that explicit approval is required before the proposed sub-contracting or material changes come into effect.

12.1.6. Where an Entity does not have the contractual right to reject any proposed subcontractor, it is recommended that an Entity must retain a right to terminate the agreement.

12.2. An Entity must review the sub-contracting arrangements relevant to the provision of a regulated activity to determine if these sub-contacting arrangements ensure its compliance with regulatory requirements.

12.3. The Entity must ensure that any subcontractor processing an Entity's data must adhere to the same QCB requirements adhered to by the CSP.

13. Contractual Considerations

13.1. An Entity must ensure that the respective rights and obligations of an Entity and its CSP are clearly set out in a written agreement, either directly or through an intermediary (who may also be providing elements of the Cloud Computing).

13.2. An Entity must ensure that written agreement expressly allows the possibility for an Entity to terminate it, where necessary.

13.3. An Entity must ensure that its written agreement for a Material Arrangement addresses the following issues including, but not limited to:

13.3.1. A clear description of the outsourced function.

13.3.2. SLAs: Enforceable and measurable SLAs must include a definition of the governance to be put in place to manage the contract on an ongoing basis. This must define any management information and other deliverables that will form the basis for that governance.

13.3.3. The start date and end date, where applicable, of the agreement and the notice periods for the CSP and for the Entity.

13.3.4. The roles, relationships, obligations and responsibilities of all contracting parties.

13.3.5. Ownership and control over IT Assets, if the CSP is expected to be given some level of control over IT Assets, this level of control must be defined in the relevant outsourcing agreement.

13.3.6. Provisions regarding information security and protection of personal data and proof these satisfy the requirements of the Law No. (13) of 2016 on Personal Data Privacy Protection in addition to the Sector-Specific Security Regulation issued by QCB.

13.3.7. The requirement for the CSP to grant the Entity, its competent authorities, and any other person appointed by an Entity or the competent authorities the right to access data and business premises and audit the same.

13.3.8. An Entity must have the right to monitor, review and audit Cloud Computing Arrangements. This can be by the Entity's internal control functions, and regulators, or persons employed by them, including for the purposes of supervisory reviews by QCB.

13.3.9. An Entity must ensure that it receives reports relevant to its security function and key functions from the CSP, such as reports prepared by the internal audit function of the CSP.

13.3.10. An Entity must receive detailed data on cyber security arrangements from the CSP such as but not limited to: Malware protection, cryptographic controls, security testing, technical compliance, KPI (Key Performance Indicators) & KRI (Key Risk Indicators).

13.3.11. The agreement must specify whether sub-contracting is permitted by the CSP directly or via other parties, and if so, what types of sub-contracting under which conditions.

13.3.12. The agreement must contain provisions regarding the management of incidents by the CSP, including the obligation for the CSP to report to the Entity without undue delay incidents that have affected the operation of the Entity's contracted service.

13.3.13. The agreement must contain provisions regarding digital forensic evidence generation, including whether the original copies of forensic evidence will be utilized or a copy with a chain of custody. The chain of custody pre-requisites should be communicated and stated in the contract.

13.3.14. The agreement must address e-discovery costs and forensics requirements including cost and response times.

13.4. An Entity must receive official QCB approval prior to signing any Material Arrangement(s), or to any material modification of an existing one.

13.5. An Entity's contract with the CSP must include clauses that ensures data confidentiality, availability and integrity at all times, depending on the nature of service being provided by the CSP.

14. Post Outsourcing Implementation Review

14.1. Prior to signing the contract, an Entity must plan and schedule an initial post outsourcing implementation review, set at a time after the implementation of the Material Arrangement.

14.2. The post outsourcing implementation review must address the following:

14.2.1. An Entity must review the effectiveness and adequacy of the Entity's controls in monitoring the performance of the service provider and checks to ensure that the risks associated with the outsourcing activity are managed appropriately as planned.

14.2.2. An Entity must develop a process for CSP assessments, in collaboration with the CSP. For the initial review this must at a minimum include:

14.2.2.1. Contract review.

14.2.2.2. CSP self-reported compliance review.

14.2.2.3. Documentation and policies review.

14.2.2.4. Available audits and assessments.

14.2.2.5. SLA performance.

14.2.2.6. Vulnerability assessments.

14.2.2.7. Penetration testing.

14.2.3. An Entity is required to actively seek improvements in the assessment parameter's capability to supply the necessary information for effective contract monitoring. The CSP is obligated to collaborate in this endeavor.

15. Compliance Assessments

15.1. An Entity is required to conduct a full annual assessment of each Cloud Computing Arrangement.

15.1.1. The annual assessment must include an update and review of all the contracts in the Register, material or otherwise.

15.1.2. The annual assessment must report on all contracts where there has been a failure to meet contractual requirements.

15.1.3. The annual assessment must include information from the CSP about breaches of data, security or confidentiality in relation to the contract. A report of any such breaches at the CSP level as a whole.

15.1.4. The annual assessment must report any changes of location by the CSP and any (approved) changes of location for the contract itself.

15.1.5. The annual assessment must report the CSP's financial situation.

15.1.6. For Material Arrangements the assessment must cover:

15.1.6.1. A report of performance versus the SLA.

15.1.6.2. A report recording all monitoring and review of Cloud Computing Arrangements by the Entity's internal control functions, regulators, or persons employed by them, including for the purposes of supervision by QCB.

15.1.6.3. Any cases where the CSP was not fully co-operative with the Entity's request or those of QCB.

15.1.6.4. A report relevant for the Entity's security function and key functions, such as reports prepared by the CSP's internal audit function.

15.1.6.5. A report from the CSP to provide information on security measures such as: Malware protection, cryptographic controls, security testing, technical compliance, KPI (Key Performance Indicators) & KRI (Key Risk Indicators).

15.2. An Entity must regularly assess a CSP's compliance with the defined policy as per clause (8.4).

15.3. An Entity must regularly assess a CSP's compliance with the relevant requirements of this regulation.

15.4. An Entity must use the compliance to the policy as per clause (8.4) and requirements in this regulation as a criterion to renew a Cloud Computing Arrangement.

16. Access, Audit and Information Rights

16.1. An Entity must aim to have enforceable contractual rights that allow an Entity to have the same access rights as if it was directly managing its Cloud Computing environment.

16.2. An Entity must ensure that QCB has the same rights to audit as if the function were not outsourced in its Cloud Computing Arrangement contracts as per clause (13.3.8).

16.3. An Entity must contractually have reasonable access to necessary information to assist in any investigation arising due to an incident in the cloud or audit inspection, to the extent that it is does not contravene any other legal obligations.

16.4. An Entity must ensure that there are no restrictions on the number of requests the Entity or its auditor can make to access or receive data.

16.5. An Entity must have access to information on controls applied on the business premises in scope of the Cloud Computing Arrangement.

16.6. An Entity must be able to conduct an onsite visit to the relevant premises, as permitted by the CSP.

16.7. An Entity must ensure that QCB has the right to access the CSP's business premises and to communicate with the CSP's subject matter experts, as permitted by the CSP.

17. Business Continuity

17.1. An Entity must integrate its Cloud Computing Arrangements within its Business Continuity Plans (BCP).

17.2. An Entity must detail how to switch over to the Cloud Computing disaster recovery environment and then switch back to normal cloud production within its IT disaster recovery plan.

17.3. An Entity must assess its ability to find alternate vendors. For each CSP:

17.4. Assess the CSP's substitutability as easy, difficult or impossible.

17.5. Identify an alternate service provider, where possible.

17.6. An Entity must evaluate if the CSP's BCP against required standards to determine that the CSP has satisfactory BCP in place.

17.7. An Entity must evaluate and satisfy itself that the interdependency risk arising from Cloud Computing Outsourcing can be adequately mitigated.

17.8. An Entity must evaluate the likelihood and impact of an unexpected disruption to the continuity of its operations.

17.9. An Entity must proactively seek assurance on the state of the CSP's BCP preparedness.

17.10. An Entity must integrate the CSP within its BCP test.

17.11. An Entity must regularly update its BCP and test arrangement with the CSP to ensure their effectiveness.

17.12. An Entity must have a defined incident response plan and develop effective crisis communication measures integrated with the CSP.

18. Termination

18.1. In the event of contract termination with the CSP, either on expiry or prematurely, an Entity must have the contractual right to promptly render data inaccessible at the CSP's systems, including backups.

18.2. Upon termination, the CSP must transfer all data from its environment to the Entity and remove it from its environment.

18.3. An Entity must ensure that the contract clearly stipulates the situations in which the Entity must have the right to terminate the outsourcing agreement in the event of default, or under circumstances, including but not limited to:

18.3.1. The CSP undergoes a change in ownership.

18.3.2. The CSP becomes insolvent or goes into liquidation.

18.3.3. The CSP goes into receivership or judicial management whether in Qatar or elsewhere.

18.3.4. There has been a material breach of data, security or confidentiality.

18.3.5. There is a demonstrable deterioration in the ability of the service provider to perform the contracted service.

18.3.6. The CSP proposes to move data to a new location which is unacceptable to the Entity.

18.4. An Entity must specify a minimum period to execute a termination provision in its agreement.

18.5. An Entity must have a legal agreement that commits the CSP to assist in the exit process so as not to unreasonably impede the exit. These must include the format and manner in which data is to be returned to the Entity, as well as support from the CSP to ensure the accessibility of the data to ensure there is a smooth transition.

18.6. An Entity must agree on the CSP's data removal process, and the tools used for deletion of data in a manner that data is rendered irrecoverable.

18.7. An Entity and the CSP must agree on the data to be returned upon termination of the Cloud Computing Arrangement and review whenever there are material changes to the arrangement.

19. Exit Plan

19.1. An Entity must develop and maintain a documented exit plan, informed by the Cloud Computing Arrangement's Materiality, which must cover and differentiate between situations where an Entity exits an outsourcing agreement.

19.2. An Entity must ensure that its exit plan covers both stressed exit and managed exit.

19.3. An Entity must have plans how it would transition to an alternative service provider (or back to the Entity) and maintain business continuity.

19.4. An Entity may consider the available tools that could facilitate a stressed exit from a Cloud Computing Arrangement.

PART D (OPERATIONAL SECURITY CONTROLS)

20. Key Management Governance

20.1. An Entity must remain accountable for the key management and ensure that the CSP is executing the applicable Sector-Specific Security Regulations and the Entity's requirements, regardless of if the keys are hosted within the CSP data center or in the Entity's premises as long as the key cryptography controls are meeting the applicable standards.

20.2. An Entity must ensure that the CSP retains a record, documents and regularly monitors the implementation of the required and applicable security controls including any changes to such controls.

20.3. An Entity must ensure that a procedure for key management access is documented and implemented.

20.4. CSPs must limit KMS access to specific individuals for a limited time to conduct a task, based on the agreed procedure with the Entity.

20.5. An Entity must ensure that the principle of least privilege is adopted when granting access to the CSP.

20.6. An Entity must retain the right to access all the logs generated by the procured services. This also includes having a full record of any access requests by the CSP to the KMS.

21. Data Protection

21.1. An Entity must only grant service providers access to their information on a need-to-know and need-to-have basis for the purposes of the Cloud Computing Arrangement.

21.2. An Entity must ensure its data and information is segregated where the Cloud Computing Arrangement is using a multi-tenancy environment.

21.3. An Entity must implement technical and process-based controls to protect the integrity, confidentially of the data while the data is at rest or in motion or resident in the memory, as defined in the Sector-Specific Security

Regulations.

21.4. An Entity must ensure that PII and financial information is processed within Qatar only.

21.5. An Entity must receive approval from QCB prior to entering into a Cloud Arrangement.

21.6. When using cloud services for processing personal data, an Entity must ensure compliance with all applicable laws or regulations relating to the protection and processing of personal data and must require CSPs to comply with all requirements relating to the protection and processing of personal data, as applicable to such Entities.

22. Cloud Security Testing

22.1. An Entity may hire a reputable third party to assess and conduct the tests mentioned in clause (22.3) and in accordance with the Sector-Specific Security Regulation.

22.2. When an Entity is not permitted to conduct a certain security assessment on the cloud environment, the CSP must provide the Entity with an assessment report conducted by a reputable third party.

22.3. An Entity should regularly perform the relevant test depending on the cloud service model used in a Cloud Computing Arrangement:

Cloud Service Model Test	IaaS	PaaS	SaaS
Architecture and infrastructure review	✓	×	×
Security configuration review	✓	✓	✓
Compliance review	✓	✓	✓
Application and source code testing	✓	✓	×
Vulnerability assessment	✓	×	×
Penetration testing	✓	✓	✓

23. Exemptions

23.1. An Entity seeking an exemption from any requirement within this regulation must request it from QCB. All exemptions are subject to QCB approval.

23.2. An Entity must link its exemption request to a specific requirement in this regulation from which it is seeking a waiver.

23.3. An Entity must support its exemption request with a clear and documented business case or rationale.

23.4. An Entity must ensure that the appropriate individuals or levels of authority within the Entity consistently approve the exemption.

23.5. An Entity must duly record in the Entity's exemptions Register any approved exemptions and assign an expiration date – the date by which the exemption will be mitigated or resolved by the Entity seeking the exemption.

23.6. An Entity must remain accountable for any risks stemming from approved exemptions.

PART E (SECONDARY REGULATIONS)

24. Compliance with Secondary Regulations

24.1. Along with the QCB Law and this regulation, the Entity must also comply with the below mentioned secondary regulations, and their subsequent amendments, while operating in Qatar:

24.1.1. Sector-Specific Security Regulation.

24.1.2. Regulations or Guidelines that may be issued by QCB, including those related to emerging technology.

24.1.3. Law No. (13) of 2016 on Personal Data Privacy Protection.