Central Bank of Jordan

Cloud Computing Guideline

March, 2018

Table of Contents

Introduction

The financial and banking sectors have recently witnessed a major development in the information and communication technology field and using it to provide financial and banking services. Whereas all business companies in the world continuously seek to take advantage of this technology to minimize their operational costs and maximize their profits, these companies have tended to benefit from external parties that provide the resources they need to manage and provide their services by accessing all applications and services by technology users, anywhere and anytime, via the internet in a manner which guarantees their durability; this is known as Cloud Computing Technology.

This technology provides many advantages; however, it may increase the risks on the companies, such as strategic, reputational, compliance, and operational risks that arises from the inability of external parties to provide services at the agreed level, or from security breaches. This requires companies to adopt a sound and highly responsive framework to manage these risks and make the most of this technology.

The guideline provides clarification of the concept of Cloud Computing Technology and its essential characteristics as well as the deployment and service models related to it. It also includes guidance on some major issues to be considered carefully by the companies upon the utilization of this technology, including Cloud Computing Governance, Risks Management, Business Continuity, in addition to the controls and mechanisms used to protect the data for a safe and efficient usage.

This guideline also included an appendix for the instructions and circulars issued by the Central Bank of Jordan, which are related to outsourcing, as licensed banks operating in the Kingdom are required to fully comply with these instructions and circulars. This is because Cloud Computing Technology falls within the outsourcing, and such instructions will make easy reference for banks.

Scope and Objectives

Due to the Central Bank of Jordan's endeavor to keep up with the best international practices that positively affect on the financial sector's components, in order to realize financial stability and the strengthening of the soundness of the financial and banking sectors in providing their services safely and efficiently; this guideline comes to regulate the utilization of Cloud Computing technology by banks, financial institutions, money exchange companies, microfinance companies, and credit bureau companies which are subject to the supervision of the Central Bank of Jordan in a manner which realizes their targets with an adequate level of safety, and assists them in understanding the Cloud Computing Technology and its risks for a safe and efficient usage.

Terms

The following words and terms shall have the meanings assigned to each hereunder Wherever they should occur herein. Furthermore, the definitions mentioned in the Central Bank of Jordan Law, the Electronic Transactions Law, Banking Law and any other related instructions issued by the Central Bank of Jordan shall be adopted wherever they appear in this guideline unless the context indicates otherwise:

Company	**:**	The bank, the Islamic bank, the financial institution, money exchange company, credit bureau company, or microfinance company
Senior Executive Management	**:**	Includes the company's general manager/regional manager; deputy general manager/deputy regional manager, assistant general manager/assistant regional manager, as well as the financial manager, operations manager, risks management manager, treasury(investment) manager, compliance manager, and any employee who has an executive authority equivalent to those managers and directly related to the general manager.
Customer	**:**	every natural or legal person obtaining the financial services from the company.
Cloud Consumer	**:**	the party that requests and uses resources and services available on the Cloud.
Cloud Provider	**:**	the party that provides Cloud resources and services, and the activities required to provide these services and guarantee their delivery to Cloud Consumers.
Cloud Computing Technology	**:**	is 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) at the Cloud provider.
Cloud Infrastructure	**:**	a group of hardware and software component such as servers, storage, networks, virtual simulations programs necessary to support Cloud Computing requirements

Cloud Service Level Agreement	**:**	a contractual agreement between the Cloud provider and company, where the company's requirements, service level, and guarantees provided by the Cloud provider regarding the availability, performance and support level of the services are identified
Risk Assessment	**:**	measuring and identifying the probability of risk occurrence and severity and anticipate the expected impact on the company.
Change Management	**:**	managing, controlling and documenting any change on the services that outsourced to the Cloud provider.
Access Control	**:**	rules and mechanisms used to allow use and access of authorized personnel only to information assets in accordance with the nature of their responsibilities.
Information Classification	**:**	Determine the appropriate level of sensitivity to the information that is created, altered, transferred, modified or stored on any media or by any available techniques, depending on the risks emerging from unauthorized access to and illicit use of such information.
Recovery	**:**	a set of actions taken and followed to recommence the company's business to natural conditions, and restore the technology resources relied on for resuming the company's operations as it was before the event.
Vulnerability Scanning	**:**	a mechanism used to determine system characteristics and associated weaknesses.
Penetration Testing	**:**	a test wherein specialized assessors attempt to search for security vulnerabilities, and circumvent the security features of information systems and security controls and utilize them to penetrate these systems, from inside or outside the company, to test the effectiveness of the security controls used by the company to protect its systems
Recovery Time Objective (RTO)		the maximum time allowed to restore the services or operations after disruption.
Recovery Point Objective (RPO)		The ultimate age of data, that might be lost upon the restoration of services after disruption.

First Chapter: Cloud Computing Technology

1.1 Preface

Cloud Computing Technology is deemed a model for enabling ubiquitous, convenient, on-demand network access to a shared physical resources or virtual resources such as networks, servers, storage, applications and services that could be readily available and used with minimal effort. This model consists of five essential characteristics, three service models, and four deployment models.

1.2 Essential Characteristics

- **On-Demand Self-Service:** a characteristic that enables the Cloud consumer to request storing and processing services automatically as requested, in order to minimize the need to face-to-face interaction with the Cloud provider.
- **Broad Network Access:** includes network access from anywhere to the Cloud provider's resources via the company's platforms such as mobile phones, tablets, laptops, and workstations.
- **Resource Pooling:** various computing resources are aggregated by the Cloud provider to serve the Cloud consumers via a multi-tenant model, along with assigning different physical and virtual resources dynamically and then reallocating it according to the request of Cloud consumer without the Cloud consumer control or knowledge of the location of the resources available to them by the Cloud provider, while retaining their right to determine the location at a certain level (for example, country or data center).
- **Rapid Elasticity: the** Capabilities of processing in the Cloud could be offered in a flexible and automatic form, with the ability to control the size of used resources in line with the size of work required by the Cloud consumer; whereas the available capabilities are unlimited and readily allocated at any time through the contracts concluded between the Cloud provider and Cloud consumer.
- **Measured Service:** the use of the Cloud resources could be automatically controlled, improved, monitored, audited and reported, thus offering transparency for both the

Cloud provider and Cloud consumer; provided that the Cloud consumer incurs the cost according to the required resources.

1.3 Service Models

- **Software as a Service (SaaS):** a model to distribute and offer programs to the Cloud consumer via internet, whereas the applications are hosted by the Cloud provider without the need to install or run applications on the consumer's devices where they may use the applications on the provider's infrastructure. Access to these applications by the consumer could be made via different devices through an interface such as the web explorer or program, while limited settings could be configured on the applications without managing or controlling the Cloud infrastructure by the Cloud consumer.
- **Platform as a Service (PaaS):** the platform provides a comprehensive Computing environment which includes the operating system, the programming languages execution environment, databases, and web servers to enable the Cloud consumer from developing and running their own applications, deploying their applications on the Cloud infrastructure, and controlling their settings without managing or controlling the Cloud infrastructure by the Cloud consumer.
- **Infrastructure as a Service (IaaS):** Cloud provider offers computers, virtual or physical, and other resources such as networks and storage to support operations related to the Cloud consumer, whereas the consumer is able to deploy and run some programs such as the operating systems and applications. The consumer does not manage or control the Cloud infrastructure, but may control the operating systems and storage as well as the deployed applications; a limited control could be granted on some of the network's components (such as firewalls).

1.4 Deployment Models

- **Public Cloud:** The Cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. The Cloud infrastructure exists on the premises of the Cloud provider. The Cloud consumer's data may be stored

in unknown locations, and may not be easily retrieved; the Cloud consumer's data may be stored on the same Cloud with another Cloud consumer.

- **Community Cloud:** The Cloud infrastructure is provisioned for exclusive use by a specific community of Cloud consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, the community Cloud is more expensive than the public Cloud where the cost is distributed among the number of Cloud consumers with a higher level of commitment, privacy and security and it exists on premise or off premises of the company, and the data of each of the companies may be stored along with their competitors on the same community Cloud.

- **Private Cloud:** The Cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. The private Cloud is considered the least risky deployment models but the services it offers may not be as flexible as the public Cloud.

- **Hybrid Cloud:** The Cloud infrastructure is a composition of two or more deployment models (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability. This may lead to risks due to the merger of more than one deployment model, at which point, the Cloud consumer is responsible for the classification of information to be stored on the deployment model. Table (1) below shows a comparison between different deployment models.

Table 1: Comparison between Different Deployment Models

Deployment Models	Manager of Cloud 's infrastructure	Owner of Cloud 's infrastructure	Location of Cloud 's infrastructure	Can be accessed and used by
Public	Cloud provider	Cloud provider	Off-premises of Cloud consumer	Any Cloud consumer

Private/Community	Cloud provider or consumer	Cloud provider or consumer	Off or on premises of Cloud consumer	Trusted entities
Hybrid	Cloud provider and consumer	Cloud provider and consumer	Off and/ or on premises of Cloud consumer	Trusted and untrusted entities

1.5 Cloud Actors

The parties effectively sharing operations and/ or tasks related to Cloud Computing, whether companies or individuals in the Cloud, are as follows:

1. **Cloud Consumer**
2. **Cloud Provider**
3. **Cloud Broker:** is an intermediary between the Cloud provider and consumer, and assists the Cloud consumer in managing and choosing various Cloud Computing services which are offered by the Cloud provider, in addition to offering further services to the Cloud consumer. The services provided by the Cloud broker are as follows:
    - **Intermediation**: the broker promotes a specific service through improving and offering services with added value to the consumers, and the improvement may be represented in managing access to the Cloud Computing services, identification management, and security promotion...etc.
    - **Aggregation**: the broker collects and merges various services in one or more new services and provides such for the Cloud consumer, also offers data and services integration in addition to guaranteeing safe transition of data between the Cloud provider and consumer.
    - **Arbitrage**: is similar to the aggregation service, except that the aggregated services are not fixed, as the broker holds flexibility in choosing the services from more than one Cloud provider.
4. **Cloud Auditor**: the Cloud auditor monitors the performance of the Cloud services and security controls that are implemented on the Cloud to verify the compliance to the security policies of the Cloud Computing.
5. **Cloud Carrier:** the Cloud carrier transfers the Cloud services and data between the Cloud provider and consumer, provided that the Cloud provider is responsible for

preparing the Cloud service level agreement with the Cloud carrier to ensure the delivery of data and services to the Cloud consumer within the agreed level.

1.5.1 The relationship between the Cloud Actors

- The Cloud consumer may request Cloud Computing services from the Cloud provider directly or via a broker. In case of dealing with a broker, the Cloud consumer must consider that the requirements applied to the Cloud broker are the same for the Cloud provider in case a contract is concluded between them.
- The Cloud auditor conducts auditing processes independent from other actors and collects necessary related information.
- There are roles assigned to both the Cloud provider and consumer upon the use of different service models as demonstrated in Table (2).

Table (2): The various roles of both the Cloud Consumer and Provider upon the use of the three service models

Service Model	Cloud consumer Activities	Cloud provider Activities
Software as a Service (SaaS)	Use of applications available at the Cloud to conduct operations related to the scope of their work	Installs, manages, maintains, and supports the available applications pertaining to the Cloud consumer on their Cloud infrastructure
Platform as a Service (PaaS)	Develops, tests, deploys and manages applications hosted on the Cloud platform	Allocating and managing the Cloud infrastructure, and providing tools for development, deployment and management for the Cloud consumers
Infrastructure as a Service (IaaS)	• Create/install, manage, and monitor their Cloud infrastructure services • Control of virtual machines used on the Cloud in terms of operating systems, storage, and application deployed on the level of these devices	Providing and managing the physical processing, storing, networks, hosting environments, and the infrastructure of the Cloud consumers

Second Chapter: Guidelines for utilizing Cloud Computing Technology

2.1 Preface

This chapter provide guidance regarding the Cloud Computing Governance, company's policy in the use of Cloud Computing Technology, contracts and agreements conducted between the company(Cloud consumer) and the Cloud provider, data protection, change and risks management, measuring the performance of the Cloud provider and oversee it. The guidelines also deal with monitoring logs and security events, access management, business continuity and exit plans for Cloud provider outsourcing arrangement. These guidelines aim to protect companies from risks they may be exposed to upon the use of Cloud Computing Technology.

2.2 The Cloud Computing Governance

Effective governance when utilizing the Cloud Computing Technology is critical to guide the management procedures and making decisions to optimally use the Cloud Computing Technology according to the company's needs. The Cloud Computing governance strategy of the company should be clear to the Cloud provider to enable cooperation in terms of operational performance, problem- solving, and sharing decisions regarding managing risks associated with the services outsourced to the Cloud provider, whereas the duties and responsibilities of the Board and the senior executive management must be defined, while considering the following:

- The Board or its delegated committees shall adopt the Cloud Computing policy of the company and follow up on its implementation
- The executive management shall tackle the following tasks and responsibilities according to their position:

    - Developing an effective framework for governance and Cloud Computing risk management in a sound manner.

- Ensuring that there are Cloud Computing policy as well as oversee its implementation and review and update it periodically and whenever the need arises.
- Approving the agreements conducted between the company and the Cloud provider.
- Ensuring that Cloud provider due diligence and evaluation process are conducted before concluding any agreement with them
- Reviewing the risks assessment result of all Cloud Computing agreements based on the risk assessment framework approved by the Board.
- Reviewing the periodic evaluation reports of the Cloud provider performance.
- Ensuring that disaster recovery plans are developed based on realistic and potential disruptive scenarios, breaches, and disruptive actions, and are tested periodically.
- Ensuring the existence of a proper mechanism for constant monitoring of the Cloud provider in accordance with the terms and conditions of the Cloud service level agreement between the company and the Cloud provider.
- Ensuring that the relevant entities in the company review all activities and services outsourced to the Cloud provider, and notifying the Board regularly of risks that may arise as a result.

2.3 The Cloud Computing Policy

The company should set a Cloud Computing policy, review and update it periodically, provided that it includes the following as a minimum:

- The services, operations, and data to be outsourced to the Cloud provider, and classifying it in terms of its importance and degree of sensitivity to be a reference to be relied upon in utilizing the Cloud Computing services, and the company is responsible for classifying them.
- The best deployment model (public Cloud, private, Community, hybrid) and the best service model (IaaS, SaaS, PaaS) of the services and operations to be outsourced depending on the following:
    - Type of service, information classification, and operations to be outsourced to the Cloud provider.

- Risk Assessment.

- The mechanism of maintaining company's data , it's storage locations, the mechanism of data disposal, processing and transferring it with the Cloud provider's systems.
- The security controls to be followed when dealing with any Cloud provider.
- The principles of Cloud provider due diligence and evaluation process before concluding any agreement with Cloud provider
- The requirements and expected results from employing Cloud providers to perform the operations in line with requirements and changes in the work environment.
- The relationship between the internal operations of the company and the operations to be transferred to the Cloud provider's systems.
- the mechanism to ensure the compatibility and interconnection between the various services that outsourced to more than one Cloud provider.
- Controls to protect the customer's data and disclosure to the customer, in case any personal data are outsourced to the Cloud provider in line with relevant laws and regulations.
- The minimum requirements that must be met in the agreements concluded with the Cloud provider.
- The mechanisms of monitoring and auditing the services that outsourced to the Cloud provider.

2.4 Risks Management

The company shall identify and manage any risks that may result from utilizing the Cloud Computing services, taking into consideration the following:

- Include the risks of utilizing the Cloud Computing services within the comprehensive risk assessment framework of the company, documenting and updating it continuously, provided that it includes the following as a minimum:

    - Identifying the role of the Cloud provider in the company's business strategy.
    - Setting comprehensive procedures to cover connectivity requirements with the Cloud provider to identify and mitigate key risks.

- Evaluating the Cloud provider's ability to employ high standards of the service performance to ensure high efficient service delivery.
- Analyzing the impact of utilizing the Cloud Computing technology on the comprehensive risks profile of the company.
- Evaluating the considerations related to the applicable laws and law enforcement provisions in addition to the political and security stability of the country of the Cloud provider, including data protection laws.
- Identifying financial, operational and legal risks on the company and its reputation in case the Cloud provider fails to perform operations as required.
- assessing the overall security risks associated with the service outsourced to the Cloud provider, and identifying the role and responsibility of the company and Cloud provider in managing it, and determining the steps to be taken to mitigate the risks and documenting this assessment.

- Setting key performance standards to monitor the level of risks related to utilizing the Cloud Computing services (Key Risks Indicators) to ensure that the risk appetite and the degree of risk tolerance are not exceeded.
- Identifying the best practices in utilizing the Cloud Computing technology, including the requirements of information security management, cybersecurity risks, and related regulations.
- Monitoring risks and identifying the measures to be taken in case the Cloud provider fails to provide services within the agreed level.
- determining the impact on the company's customers in case the Cloud provider fails to perform the service or if the confidentiality of their data is violated.
- Managing security risks associated with storing data and running company's applications on the Cloud provider's systems.
- Monitoring concentration risks arising from reliance on a single Cloud provider for all services intended to be outsourced to the Cloud provider and consider actions that will be taken in the case the Cloud provider fails to perform operations as required.

2.5 Contracts and Agreements between the Company and the Cloud Provider

The company should ensure that the contract (s) concluded with the Cloud provider is consistent with the Cloud computing policy approved by the company, taking into account that the contracts include, at the minimum, the following:

- The name of the Cloud provider and the name of its parent company, if any, address, and full contact information.
- The activities and services to be outsourced to the Cloud provider.
- Duration of the contract.
- The Cloud provider's commitment with the privacy, confidentiality and security of the company's data.
- The Cloud provider's commitment with the business continuity plan of the company.
- The auditing and supervisory procedures on the Cloud provider.
- The performance standard, internal control and risks management.
- The Cloud service level agreement and the Cloud provider's performance requirements.
- Roles and responsibilities of both parties.
- Disputes resolution processes.
- Reporting mechanism to the company.
- The applicable law governing the contract.
- The regulatory and legal arrangement to be followed by the Cloud provider.
- The requirements and responsibilities for technical support and maintenance.
- The penalty clauses in case the Cloud provider fails to provide Cloud Computing services.
- That the contract allows for renewal and negotiation to enable the company to maintain an appropriate level of supervision on the Cloud provider outsourcing arrangement.
- Maintaining confidentiality and security of the information and ownership of the company's data, and taking proper measures to prevent the access of any other person or party to the data without prior approval.
- The commitment of the Cloud provider to inform the company of any proposed significant changes on the contracts or contracted services that may affect the provider's ability to fulfill its responsibilities and obtain the company's approval. The reporting period for these changes must be agreed in advance to allow the company to conduct a risk assessment to

consider the effects of the proposed changes before making the actual change and testing these changes.

- Determining the geographic location of the data, and obtaining prior approval of the company when the Cloud provider changes work locations or data centers, and the operations related to the outsourced services.
- Agreeing on the security and operational requirements to guarantee the adequacy and efficiency of the security policies and practices, including the existing circumstances in which each party has the right to change those requirements.
- Obliging the Cloud provider to cooperate with any third party that the company contracts with, if the scope of work of that party intersects with the scope of services outsourced to the provider.
- If the Cloud provider has contracted with a third party regarding the service outsourced to the provider, the company must be notified immediately and its approval must be requested and the Cloud provider remains responsible for providing the service, and the effectiveness of the controls agreed upon in the contract concluded between them, including the security and operational requirements.
- determining reporting mechanisms and escalation process and ensuring that the Cloud provider has immediate notification of any violation or events arising from any defect in the Cloud computing services and the actions taken and / or proposed by the provider to remedy the defect.
- Clauses that allow the Central Bank to perform their supervisory tasks, and obligate the Cloud provider with any requirements, circulars, and instructions issued by the Central Bank in relation to the services outsourced to the provider.
- The contract must clearly state the cases in which both parties have the right to terminate the contract, and among the cases in which the company has the right to terminate the contract, for example, but not limited to:
    - Breach of security or confidentiality.
    - Failure of the Cloud provider to notify the company of security events that may affect the company's business.
    - The inability of the Cloud provider to perform the contracted service within the agreed level.
    - Change of the Cloud provider’s ownership.

- Cloud provider insolvency and liquidation.
- Foreclosure on the Cloud provider whether in the country or elsewhere

There should be no restrictions or impediments in the contract that might may impede the immediate termination of the contract if the company so desires.

2.5.1 The Cloud Service Level Agreement

The Cloud service level agreements between the company and the Cloud provider are an important element of managing Cloud Computing service, as the complex and changing nature of the Cloud technology requires advanced means to manage the service level agreement to ensure the service quality agreed upon between the company and the provider. The company needs a service level agreement to identify the Cloud services performance requirements. These agreements contain as minimum the following:

- Quality of service, performance level and required security controls.
- The level of availability, integrity and confidentiality of the service outsourced to the provider, and access controls applied to it.
- The mechanism for separation of the provider's data from the company's, and the data related to the outsourced service.
- The mechanism for maintaining and processing data of the company and its customers.
- The back-up mechanism and records keeping.
- The mechanism for disaster recovery and contingency plans.
- The details of infrastructure and security standards to be maintained by the provider and review of their compliance.
- The periodic examination of the Cloud provider to ensure their compliance to the service performance level and the agreed- upon security standards.

2.6 Supervising the Cloud Provider

Outsourcing some of Company's services to the Cloud provider does not mean that the company will transfer its responsibility to the provider, as the company bears full responsibility for services outsourced to the provider according to legislations and instructions issued by the Central Bank. Therefore, the Company must undertake the following:

- Notify the Central Bank upon contracting any Cloud provider.
- Identify the tasks of constant supervision by the company on the service, and ensuring that the company's employees have sufficient training, skills and resources to supervise and test these services.
- Possess the right to conduct a visit to the provider's premises, as this right should not be restricted, according to the prior agreement between the two parties.
- Setting measures that allow the Central Bank to perform its supervisory duties, including the below:
    - ensure that all the company's data and Cloud Computing services are available for review or inspection by the Central Bank at any time.
    - Obtain any records, documents, data or information that the Central Bank deems necessary and related to the company's works outsourced to the Cloud provider.
    - Access to any reports or audit results conducted by external or internal auditors assigned by the company or Cloud provider with relation to the outsourced service.

2.7 Data Security

Maintaining data security is one of the most important issues that the company must ensure when utilizing the Cloud provider due to the distributed nature of the Cloud Computing environment. Therefore, it is necessary to consider the measures and controls to be followed to protect data when transferring, processing, storing, and destroying it. Therefore, the company must undertake the below:

- Ensure that the Cloud provider data centers meet the physical protection requirements.
- Adopt a specific classification of data according to its sensitivity, as the company is obliged to bear the responsibility of data classification with the need for a periodic review of this classification.
- determine the data to be transferred to the Cloud based on the approved data classification of the company, while taking into consideration the risks emerging from placing sensitive data on the public or hybrid Cloud.
- Ensure that the company is provided with proof of separating the company's data from another Cloud consumer's data or the provider's data.
- determine the responsible for taking back-up copies of data and determine the mechanisms and location of its storage.
- Take appropriate measures to mitigate the security risks associated with transferring data to the Cloud.
- Identify the nature and scope of risks resulting from loss of the company's data and mitigate such risks through the following:
    - Distributing the data and applications in several locations.
    - Adherence to the best practices in business continuity and disaster recovery.
- That the data (stored or transferred) and back-up copies, particularly sensitive ones, are subject to appropriate encryption control which include the following:
    - Setting detailed policies and measures to organize encryption keys in terms of creating, storing, using, blocking, expiring, renewing, archiving and reviewing them on regular basis.
    - Reviewing the details related to the encryption algorithms and the encryption keys' length, in addition to the adequate data flow by experts to identify possible weaknesses.
    - ensure that the secret keys used in encryption are securely created and managed, for example HSM device (Hardware Security Model).

- Ensuring that appropriate controls are in place to manage the encryption keys and digital certificates.
- Placing adequate security equipment, such as the hardware security Unit and other tools used in encryption on separate secure networks to control access to it carefully, so that it can't be accessed from subnets that may be used by other companies that deal with the Cloud provider or used by the provider's employees.
- That the encryption keys used to encrypt the company's data are unique and specific to the company's data only, and should not be used for the data of other companies that dealing with the provider

- In case of using tokenization which aims at minimizing the amount of data, particularly sensitive ones, and which the company shares with the Cloud provider and ensure that only authorized parties are able to access the company's data when utilizing the Cloud provider; the following should be considered:
  - Conducting an accurate risks assessment, especially those related to the solutions used in the tokenization, and identifying the unique characteristics used to access the data.
  - Ensuring that the Cloud provider is unable to retrieve tokenized data through accessing the tokenization system.
- Addressing violations and other event that have negative impact on the Cloud Computing services.
- Conducting periodic penetration tests on the systems related to the services outsourced to the Cloud provider, most particularly, the operating systems on the virtual environment of the Cloud. This should be in cooperation with the provider due to the exposure to many risks resulting from sharing of the Cloud consumers of physical components.
- Conducting vulnerability scanning periodically on the systems and software related to the services outsourced to the Cloud provider to detect vulnerabilities and deal with deficiencies, in coordination with the provider, proactively to avoid the possibility of these system being exposed to risks.

2.8 Access Management

2.8.1 Consumer's Access Management and Segregation of Duties

When the Cloud provider possesses the ability to access and manage the systems or software of outsourced service, the company must take into consideration the following:

- Ensure that the provider implements its policy for access management.
- Separate between the duties of software and systems' users, especially for the sensitive and critical roles.
- Log user's access to systems or software in the access logs of the Cloud provider, and reviewing them at least annually.
- Control access to the service, general accounts, and the accounts of the company's systems managers, which exist which are located at the Cloud provider via access management controls for users, especially for those with high privileges, and record the activities on these systems to review them.
- The Cloud provider developers shouldn't have any access to the company's production environment located on the Cloud.

2.8.2 Active Access to Data

It is necessary for the company to be able to effectively access its data related to the services outsourced to the Cloud provider and which exist on the Cloud infrastructure, and therefore the company should undertake the following:

- Ensure that data can be accessed as agreed upon with the Cloud provider.
- Ensure that there are no restrictions on the number of company's requests to access or obtain data.
- Ensure that the data are not stored in countries and locations which might hinder the company from effectively access its data.

2.9 Monitoring Security Events and Records

In order to monitor the security incidents that may be exposed to the services outsourced to the Cloud provider, the company should verify the existence of adequate detection mechanisms in the network, systems, and applications of the provider to analyze the activities that may affect the security and stability of the outsourced service. The company normally maintains records documenting the event that occur on its data and applications, and as the records related to the service are at the provider, the company should ensure that it has unrestricted access authorities to these records, and therefore the company should undertake the following:

- Providing what is necessary to monitor and analyze the records of the outsourced services automatically.
- Reviewing the event logs continuously according to the classification of the importance of the event, and documenting the review.
- Reviewing, auditing and maintaining the login records to ensure that only authorized users have access to the data.
- Ensuring the obtainment of security event logs for all services outsourced to the Cloud provider.

2.10 Business Continuity Management

The company should take proper measures to ensure the continuity of its works related to the services outsourced to the Cloud provider in case of the occurrence of a disaster, failure or abrupt disruption on these services, provided that the measures include the following in the least:

- developing a business continuity and disaster recovery plan, testing it in cooperation with the provider, and contractually agree with the provider on the requirements and obligations related to planning of business continuity, provided that it includes both the Recovery Time Objective(RTO) and Recovery Point Objective(RPO).

- Ensure that the company's crisis management team is fully aware of the provider's disaster recovery plan.
- Considering the possibility and impact of abrupt disruption of the outsourced services on the company's business continuity.
- Ensuring that back- up copies of data and software are maintained in an alternative site, and testing the restoration of back-up copies of data.
- developing a contingency plan where the company documents a alternative provider and the measures to be taken in case the contract conducted with the current provider is abruptly terminated, or in case the provider is unable to meet their obligations for any reason whatsoever.

2.11 Change Management

Some risks may occur when conducting changes to Cloud Computing environment, and to avoid such risks, the company should consider the following:

- Agreeing on and arranging of the reporting method used to notify the company of the changes which might occur on the Cloud Computing environment with the Cloud provider, in addition to the company's ability to review these changes to facilitate the company's supervision of these changes.
- Ensuring supervision of the major changes which might impact the stability and security of the operation environment in the Cloud, and reveal erroneous or unauthorized changes.
- Agreeing on the change management procedures with the Cloud provider. These procedures include requesting change, approval and reporting, as well as the contingency measures, standard changes, roles and responsibilities of change management.
- Identify the mechanism of testing approved changes.

2.12 Data Sovereignty

- Before the company sets its data in the country of the Cloud provider, it should consider the following:
    - Regulatory requirements of the provider's country.
    - Political, economic, and social conditions of the provider's country.
    - The diplomatic relations, government policies and legal requirements of the provider's country.
    - event and disasters that may limit the provider's ability to provide its services.
        - The company should not deal with Cloud providers in countries where laws allow for immediate and forced access to their data and information.
        - The company should set contractual obligations requesting the Cloud provider to report any legal obligations by the country of the data centers to disclose the company's data to a third party, so as to take proper measures to ensure its data protection.

2.13 Exit Plan

The company must have a specific and documented plan to ensure its ability to terminate agreements of utilizing Cloud Computing services, without disrupting its services or affecting its compliance to instructions and legislations issued by the Central Bank. Therefore, the company must undertake the following:

- developing exit plans and arrangements that are fully understood, documented and periodically tested in cooperation between the company and Cloud provider.
- determine the mechanism for moving to an alternative Cloud provider, or returning to the company's system and maintaining business continuity.

- A specific mechanism to retrieve and delete the company's data and all records and documents from the Cloud provider's systems upon the termination of the contract with the Cloud provider, wherever it has been stored, including the locations of back-up copies and online data storage media.
- Monitor risks and consider measures, which might be taken in case the Cloud provider stops working.
- establishing special arrangement to ensure obtaining the company's data or transferring it to an alternative provider if the provider fail to meet their obligations, the contract is terminated, or for any reason, and obliges the current provider to cooperate with alternative provider or the company to finalize the transfer process.

Third Chapter: The Standards Related to Cloud Computing

Considering the challenges faced by the companies, which might impede their adoption of Cloud Computing Technology, and seeking to enable companies to use this technology in a safe manner that mitigates their exposure to related risks; companies shall take all necessary measures to protect themselves from these risks via use of the common security standards around the world that support the Cloud Computing Technology and through which the confidentiality and security of data could be maintained when utilizing the Cloud provider. These standards offer many advantages, which include the following:

- Promoting compatibility of the company's systems with other systems, making the transition between Cloud providers simpler.
- Ensuring companies and Cloud providers' adherence to the best related practices.
- The standards are considered an effective mean that enables companies to compare between Cloud providers to choose the most suitable.
- The use of standards offers an easier path to regulatory compliance.

There are many standards related to the security of Cloud Computing Technology, which were recently published, including ISO/IEC 27018 and ISO/IEC 27017, which provide more detailed guidelines for both companies and Cloud providers. In addition, there are many general standards for information technology, which could be applied while using the Cloud Computing technology as these standards are not specific to Cloud Computing but are general and could be applied to the Cloud Computing environment. Therefore, companies and Cloud providers should pay attention to these standards as they offer guidelines and recommendations in detail for both the company and provider, particularly the following standards which are classified per topics as shown in Table (3) below:

Table 3: The Most Important Standards Used in Cloud Computing Technology

Standards	Topic
• COBIT • ISO/IEC 20000 • SSAE 16 or ITIL depending on type of workload • ISO/IEC 27001 and ISO/IEC 27002 • ISO/IEC 27017 & ISO/IEC 27018 • ISO/IEC 38500 – IT Governance • Cloud Security Alliance (CSA) Cloud Controls Matrix • National Institute of Standards and Technology (NIST) • Cybersecurity Framework (CSF)	Governance, risks management and compliance
• SSAE 16 • ISO/IEC 27000	Operational and commercial operations
• LDAP, SAML 2.0, OAuth 2.0, WS-Federation, OpenID Connect, SCIM • XACML • PKCS, X.509, OpenPG	Roles management
• HTTPS, SFTP, VPN using IPSec or SSL • OASIS KMIP • US FIPS 140-2	Data and information protection
• ISO/IEC 27018	Privacy policies
• ISO/IEC 27033 or FIPS199/200 standards	Network protection and security
• ISO/IEC 27002 • ISO/IEC 27017 & ISO/IEC 27018	Security controls on infrastructure
• ISO/IEC 19086 • ISO/IEC 27004:2009, TM Forum TR 178, NIST Special Publication 800-55, CIS Consensus Security Metrics V1.1.0, and ENISA Procure Secure	Security conditions in the service level agreement

• **CWE list** • **CSA STAR registry** • **PCI DSS** • **FedRAMP program**	
• **ISO/IEC 19086**	**Termination/Exit operations**

Central Bank Instructions and Circulars

The instructions and circulars issued by the Central Bank regarding outsourcing for licensed banks operating in the Kingdom have been compiled below in order to regulate the utilization of Cloud Computing Technology in the Kingdom.

1. **The instructions on Governance and management of information and related technology no (65/2016) date (25/10/2016)**

- Article (3/C): upon the signing of outsourcing agreements with others to provide the human resources, services, programs, and information technology infrastructure to facilitate bank's operations, banks must ensure that others adherence to the implementation of the provision of these instructions, fully or partially, to the extent appropriate to the importance and nature of the bank's operations, services, programs, and infrastructure before and after the contractual period. This does not relieve the Board and the senior executive management from the ultimate responsibility to attain the requirements of the instructions, including the auditing requirements mentioned in article (9). The instructions' enforcement period or contractual period shall be considered the period during which the contractors must reconcile their conditions, whichever comes first.
- Appendix no (6) of the instructions on (Policies systems) regarding (outsourcing)
  Adopting a general policy to employ resources generally and information technology resources specifically, those resources whether owned by the bank (in-sourcing) or owned by third parties (outsourcing) should consider the instructions, bylaw, and laws and simulate the best related accepted international practices. They should also take into account the production location (on-site, off-site, near-site and off-shore), the service level requirements, activating audit right by trusted and neutral third parties, and realization of business continuity requirements and required security controls necessary to meet the integrity and confidentiality requirement as well as requirements of efficiency and effectiveness in exploiting resources.
- Appendix (8): the services, programs and infrastructure of information technology, hosting and physical and environmental security controls of main server rooms, communication and power supply rooms, as well as providing physical and environmental security controls at minimum, per the following:

- Rooms' location and building infrastructure design should be remote and protected from threats of possible floods, water leaks, and sewerage, whether below or at the end of the building near roofs or any other exposed location. Furthermore, the size of rooms must be adequate, meets the current needs of the bank and takes into consideration the possible future expansion.
- The location of the room and the building in general must have unlimited access (whether due to the nature of the geographic location or per exclusive contractual agreements) by all telecommunication companies and different providers.
- The main server rooms, communication rooms such as (Routers, Switches, etc.) and power supply rooms must attain environmental and physical protection, whereby they are surrounded by reinforced windowless walls and protected from electromagnetic effects, which negatively impact computers. The rooms must be served with a robust spare entrance for use by individuals upon emergencies. Moreover, the rooms should be, as designed, served with entrances for power and firefighting devices (such as FM 200) per related domestic and international standards. They should also have raised floor and contain highly sensitive detectors for smoke, water temperature, and humidity as well as recorded television monitoring. Furthermore, conditioning must be available and distributed fairly over the size of the room to protect the devices from high temperature and humidity in addition to dust extractors. The entrance must be controlled and guarded to prevent unauthorized access, while taking into consideration that no signals are placed indicating the location of these sensitive rooms in the bank without authorized escorts.
- The servers and communications rooms must be provided with a multi-source power outlet and the transfer between them is automatic; i.e. providing UPS batteries in addition to power generators able to operate the banks' devices and operations (at least those that are sensitive) in case of the main power disruption.
- The requirements of the Civil Defense Directorate and Jordan Standards and Metrology Organization should be taken into consideration (wherever necessary).
- The mentioned above also applies to the disaster recovery sites of server, communications, and power rooms.

2. **Circular on Instructions of Business Continuity Plan no (10/1/9943) date 17/8/2014**

- Article (11): taking into consideration that agreements signed with external providers, regarding technical support for services in general and sensitive services in particular, should include their responsibilities in providing the required support within an appendix of conditions in the agreement (Service Level Agreement) which guarantee availability at the highest levels and details in all circumstances as compatible with the banks' requirements per their related business continuity plan.
- Item (12): The outsourcing policies of banks must consider the availability of business continuity plans with others that are reliable and independently reviewed by a neutral side on at least an annual basis. These plans must ensure availability and confidentiality of the data and operations of banks upon emergencies that might disrupt offering these services. Complying with this rule as a standard is paramount in choosing providers to utilize their services; the contracts and agreements signed with providers must include items to reflect these requirements, and correspond with current providers to reconcile their conditions to meet the requirements.

3. **Instructions of Internal Control Systems No (35/2007) date 10/6/2007**

- Article (10/e) 'The quality of the services presented by external parties and the mechanism of presentation from the aspect of maintaining the confidentiality, accuracy, availability, and integrity conditions where such conditions are controlled through duly documented agreements'

4. **Circular on principles of electronic banking risks management no (10/1/3344) date 21/3/2005:**

- article (First/3): the Board and Senior Management must work to establish a system and mechanism to manage the contracted external parties' services (outsourcing regulations) in order to support the operation of offering the electronic banking services and continuing to develop them.

5. **Instructions for Conducting Banks' Activities via Electronic Means No. (8/2001) date 26/7/2001**

- Article (7): "Regulating the agreements between the bank and any of the serving, providing and supporting companies, without any contradiction to the banking confidentiality provisions. These regulations should be carried out in a way, which ensures the security of the systems and information."

References

1. **ABS Cloud Computing Implementation Guide 1.1 For The Financial Industry in Singapore**, The Association of Banks in Singapore, 2 Aug 2018.
2. **Banking on Cloud (A discussion paper by the BBA and Pinsent Masons),** BBA Cloud Working Group, 5 December 2016.
3. **NIST Cloud Computing Standards Roadmap**, NIST Cloud Computing Standards Roadmap Working Group, NIST Cloud Computing Program, July 2013.
4. **NIST Guidelines on Security and Privacy in Public Cloud Computing**, National Institute of Standards & Technology Gaithersburg, MD, United States , 2011
5. **Australian Government Cloud Computing Policy Smarter ICT Investment**, Australian Government, Department of Finance, Version 3.0, October 2014
6. **International Standard ISO/IEC 17788 First edition 2014-10-15**, ISO/IEC 17789, 2014
7. **Cloud Security Policy for Government Agencies,** Qatar National Information Assurance, 2014
8. **Practical Guide to Cloud Computing Version 2.0,** Cloud Standard Customer Council, April, 2015
9. **Cloud Security Standards "What to Expect & What to Negotiate Version 2.0",** Cloud Standard Customer Council, 2016.
10. **Security for Cloud Computing Ten Steps to Ensure Success Version 2.0 March**, Cloud Standards Customer Council, 2017
11. **Security Guidance for Critical Areas of Focus in Cloud Computing V3.0,** Cloud Security Alliance
12. **PCI DSS Cloud Computing Guidelines,** Cloud Special Interest Group PCI Security Standards Council, February 2013
13. **Best Practices for Security in Cloud Adoption by Indian Banks**, Members of The Open Group Security Forum, March 2015
14. **How Cloud is Being Used in the Financial Sector: Survey Report**, CSA, March 2015
15. **Towards a Generic Value Network for Cloud Computing**, Markus Böhm*, Galina Koleva, Stefanie Leimeister, Christoph Riedl, and Helmut Krcmar, 2010
16. **Secure Use of Cloud Computing in the Finance Sector / Good practices and recommendations,** European Union Agency for Network and Information Security, December 2015.
17. **A Reference Guide to Cloud Computing Dimensions: Infrastructure as a Service Classification Framework,** Jonas Repschlaeger, Stefan Wind, Ruediger Zarnekow, Klaus Turowski, 2012

18. **Security Guidance for Critical Areas of Focus in Cloud Computing V2.1,** CSA, December 2009
19. **Cloud Computing-Software as Service,** Gurudatt Kulkarni, Jayant Gambhir, Rajnikant Palwe, March, 2012
20. **FG 16/5 - Guidance for firms outsourcing to the 'Cloud ' and other third- party IT services,** FCA, July 2016.
21. **Framework for Risk Management in Outsourcing Arrangements by Financial Institutions,** State Bank of Pakistan, 2017
22. **Circulaire Cloud Computing,** De Nederlandsche Bank, 2012
23. **Cloud Computing: Business Benefits with Security,** Governance and Assurance Perspectives/ISACA, 2009
24. **Outsourcing in Financial Services,** Basel Committee on Banking Supervision, February 2005
25. **Guidelines on Outsourcing,** Monetary Authority of Singapore, 27 JUL 2016
26. **Guidelines on Business Continuity Planning,** Monetary Authority of Singapore, June 2003
27. **Public Consultation on Guidance on Outsourcing,** Response to Feedback Received, July 2016
28. **سبل الإفادة من تطبيقات الحوسبة السحابية في تقديم خدمات المعلومات بدولة الإمارات العربية المتحدة،** كلية الدراسات الإسلامية والعربية بدبي، 2014/3

(Means of utilizing Cloud Computing applications in providing information services in the UAE, faculty of Islamic and Arabic studies- Dubai 3/2014).