Central Bank of Jordan

(Cloud Computing Guideline)

March, 2018

Table of Contents

Introduction

Recently, the financial and banking sector has witnessed a great development in the area of information and telecommunications technology and their use for providing financial and banking services. Since companies and financial institutions worldwide always seek to benefit from this technology in reducing their business cost and increasing their profits, they have approached external parties that provide many sources nessecary for companies to manage and provide their services by enabling consumers of this technology to access all applications and services from anywhere and at any time via the internet in a manner that ensures its sustainability. This is what is known as "Cloud Computing Technology".

This technology provides many benefits; however, it increases companies' risks including strategic risk, reputation risk, compliance risk, and operational risk resulting from the failure of external parties to provide the service at the agreed level. It may also lead to security penetration; thus, requiring companies to adopt a sound and responsive framework to manage these risks and benefit from this technology as much as possible.

This guideline provides a clarification for the concept of cloud computing techology, its essential characteristics, related deployment and service models, and guidelines on some important issues that should be considered carefully by institutions when using this technology. Such issues include cloud computing governance, risk management, business continuity, and controls and mechanisms for protecting related data, so it can be used safely and efficiently.

Moreover, this guideline contains an appendix of instructions and circulars issued by the Central Bank of Jordan (CBJ) regarding the outsourcing operations in light of the nessecity to fully abide by these instructions and circulars by licensed banks operating in the Kingdom. The cloud computing technology is basically part of the outsourcing operations, so as it can be easily refered to by banks.

Scope and Objectives

In light of CBJ's keenness to keep abreast with the best international practices which positively affect the components of the Jordanain financial system to achieve financial stability and reinforce the soundness of the financial and banking sector in providing its business and offering its services safely and efficiently; this guideline comes to organize the use of cloud computing technology by banks and fianacial institutions, exchange companies, microfinance institutions, and credit bureaus subject to the oversight and supervision of CBJ in order to achieve their objectives at an appropriate level of security and protection, in addition to helping such institutions understand the cloud computing technology, along with its risks, so as to be used safely and efficiently.

Terms

The following words and phrases wherever mentioned in this guideline shall have the meanings ascribed thereto hereunder and the definitions indicated in the Central Bank's Law, Electronic Transactions Law, Banks Law, and any other related instructins issued by the Central Bank wherever mentioned in this guideline shall be adopted unless the context indicates otherwise:

Company	The bank, Islamic bank, financial institution, exchange company, credit bureau, and micro-finance institution.
Senior Excutive Management	It includes the company's general manager or regional manager, vice general manager or vice regional manager, assistant general manager or assistant regional manager, financial manager, operations manager, manager of risk management, treasury manager (investment), and compliance manager, in addition to any other employee in the company having an excutive authority parallel to any of the powers of the mentioned above and is functionally linked to the general manager.
Customer	Any natural or legal person receiving financial services from the company.
Cloud Consumer	The party that requires and uses the sources and services available on the cloud.
Cloud Provider	The party that provides cloud- related sources and services, along with the activities needed

	for offering such services and ensuring that they are delivered to the cloud consumer.
Cloud Computing Technology	It is a model that enables appropriate network access from anywhere, and on demand to a joint group of configurable computing sources (such as networks, servers, storage media, applications, and services) with the cloud provider.
Cloud Infrastructure	A set of hardwares and softwares including servers, storage media, networks, and virtual simulation programmes nessecary to support cloud computing requirements.
Cloud Service Level Agreement	A contractual agreement between the cloud provider and the company. It identifies the company's requirements, level of service, and guaranties submitted by the cloud provider regarding the availability of services, their performance, and level of support thereto.
Risk Assesement	Measuring and identifying the likelihood and severity of risk, in addition to predicting its degree of impact on the company.
Change Management	Managing, controlling, and documenting any change on any of the services assigned to the cloud provider.

Access Controls	The rules and mechanisms followed to allow only the authorized persons to use and access information sources in accordance with their responsibilities.
Information Classification	Identifying the appropriate level of sensitivity to the information created, changed, transferred, modified, or stored on any media and by any possible techniques, based on the risks resulting from the illegal review and use of such information.
Recovery	A set of measures taken and followed to restore the company's business to their normal status and re- operate the technology resources that are relied on in running the company's operations to the way as they were before the event.
Vulnerability Scanning	A mechanism used to identify the characteristics of systems, along with the related points of weakness.
Penetration Testing	A test through which specialists try to search for security bugs and manipulate the security characteristics of information systems and security controls, and, then, use them in an attempt to penetrate such systems whether from inside or outside the company in order to

	identify the extent to which the security controls used by the company to protect its systems are effective.
Recovery Time Objective (RTO)	The maximum time allowed to restore the service or operation after being disrupted.
Recovery Point Objective (RPO)	The maximum age allowed for the data to be lost when restoring the service after being disrupted.

First Chapter: Cloud Comupting Technology

1.1 Prologue

Cloud Comupting Technology is considered a model for enabling an appropriate network access from anywhere and on demand to a joint group of physical or virtual resources such as networks, servers, storage media, applications, and services that can be quickly provided and used with a minimal effort. This model consists of five essential characteristics, along with three service models and four deployment models.

1.2 Essential Characteristics

- **On-Demand Self- Service:** It is a feature through which the cloud consumer will be able to request storage and processing services as nessecary and automatically in order to minimize the need for direct interaction with the cloud provider.
- **Broad Network Access:** This includes network access from anywhere to the cloud provider sources through the company's platforms such as: mobiles, tablets, labtops, and workstations.
- **Resource Pooling:** Different computing resources are gathered by the cloud provider to serve many cloud consumers using the Multi- tenant model, in addition to dynamically allocating different physical and virtual resources and reallocating them according to the cloud consumer request. Moreover, the cloud consumer does not need to have a control over or knowledge of the deteremined location of available resources provided to him/ her by the cloud provider. As well, the cloud consumer shall preserve his/ her right to determine the location at an appropriate level (for example the country or data centre).
- **Rapid Elasticity:** Cloud processing capabilities and capacities can be provided in a flexible and an automated manner. As well, the volume of resources used can be adjusted in accordance with the work required by the cloud consumer since the available resources

shall be unlimited and can be allocated at anytime through contracts between the cloud consumer and provider.

- **Measured Service:** The use of cloud resources can be automatically controlled, improved, monitored, audited, and reported; thus, providing transperancy for each of the cloud provider and consumer, provided that the latter shall bear the cost based on the resources required.

1.3 Service Models

- **Software as a service:** It is a model for distributing and providing programmes to the cloud consumer via the network, where the applications will be hosted by the cloud provider without the need to be installed or run on the consumer devices as he/ she can use the applications working through the provider infrastructure. The consumer can access such applications through different devices via a certain interface including the web or programme browser, in addition to developing limited settings on these applications without managing or controlling the cloud infrastructure.
- **Platform as a service:** The platform provides an integrated computing environment including the operating system, programming languages implementation environment, databases, and web servers to enable the cloud consumer to develop, operate, deploy, and control the settings of his/ her own applications on the cloud infrastructure, without managing or controlling the cloud infrastructure.
- **Infrastructure as a Service:** Physical or virtual computer devices, together with other resources including netwrorks and storage media are provided by the cloud provider to support the cloud consumer- related operations. The consumer shall be able to deploy and operate some programmes such as operating systems and applications. As well, the consumer shall not manage or control the cloud insfrastructure; however, he/ she can control the operating and storage systems, as well as the deployed applications, with a probable limited control over some network components (such as firewalls).

1.4 Deployment Models

- **Public Cloud: The** cloud infrastructure is provided for open pubic use, and it may be owned, managed, or operated by a commercial, academic, or government institution, or a group of these institutions thereof. The cloud infrastructure exists in a location affiliated to the cloud provider. In addition, cloud consumer- related data can be stored in unknown

locations and cannot be also easily recovered. As well, cloud consumer data may be stored with the data of another consumer on the same cloud.

- **Community Cloud: The** cloud infrastructure is provided for exclusive use by a particular community of cloud consumers from the companies sharing the same interests such as their duties, security requirements, policies, and compliance considerations. It may be also onwed, managed, or operated by one or more of the companies in that community, or by a third party or a mix of these companies thereof. Moreover, this cloud is more expensive than the public cloud where the cost is distributed on a number of cloud consumers against a higher level of commitment, privacy, and security. It may also exist inside or outside the locations of such companies. Furthermore, data of each company may be stored with the data of its competitors on the same community cloud.
- **Private Cloud:** The cloud infrastructure is provided for exclusive use by a group of cloud consumers and it may be owned, managed, or operated by this group, a third party, or both. The cloud infrastructure may be on- premises or off- premises. As well, the private cloud is considered one of the least risky deployment models; however, its services may not be as flexible as those provided in the public cloud.
- **Hybrid Cloud:** The cloud infrastructure is composed of two or more of the deployment models, whether it is a private, community, or public cloud. It is also considered an independent entity; however, it is linked together by a unified technique enabling data and applications to move. This may lead to risks due to the integration of more than one deployment model. In such a case, the cloud consumer shall be responsible to classify the information to be stored on the related deployment model. Table no. (1) below shows a comparison between different deployment models.

Table no. (1): A comparison between different deployment models

Deployment model	**Cloud infrastructure Manager**	**Cloud infrastructure owner**	**Cloud infrastructure location**	**Accessible and used by**

Public	Cloud provider	Cloud provider	Outside the cloud consumer location	Any cloud consumer
Private/ Community	Cloud consumer or provider	Cloud consumer or provider	Outside or inside the cloud consumer location	Trusted parties
Hybrid	Cloud consumer and provider	Cloud consumer and provider	Outside and/ or inside the cloud consumer location	Trusted and untrusted parties

1.5 Cloud Actors

The cloud actors who share related cloud computing operations and/ or tasks, whether they are companies or persons, are represented in the cloud as follows:-

1- **Cloud Consumer.**
2- **Cloud Provider.**
3- **Cloud Broker** who works as a broker between the cloud consumer and provider, and helps cloud consumers select and manage different cloud computing services presented by the provider. Moreover, the cloud broker provides additional services for the consumer. The services provided by the cloud broker include the following:-
    - **Intermediation:** The broker promotes a particular service by improving and providing value- added services for the consumers. Such an improvement may be done through access management to the cloud computing services, in addition to identification management, security enhancement, …etc.
    - **Aggregation:** The broker aggregates and integrates several services into one or more of the new services in order to provide them for the consumers. As well, the

broker provides data and service integartaion, in addition to ensuring secure data traffic between the cloud consumer and providers.

- **Arbitrage:** It is similar to the aggregation service except that the aggregated services are not fixed since the broker has the flexibility to choose services from more than one cloud provider.

4- **Cloud Auditor**: The cloud auditor monitors the performance of cloud services and security controls over the cloud in order to ensure compliance with the security policies related to cloud computing.

5- **Cloud Carrier**: The cloud carrier transfers cloud services and data between cloud consumers and providers, provided that the latter shall bear the responsibility of conducting cloud service level agreement with the cloud carrier to ensure delivery of data and services to cloud consumers upon the agreed level.

1.5.1 Relationship between Cloud Actors in Cloud Computing

- The cloud consumer may request cloud computing services from the cloud provider either directly or through a cloud broker. If the dealing is done with the cloud broker, the cloud consumer shall take into consideration that what applies to the cloud provider shall apply to the cloud broker if being contracted.
- The cloud auditor shall conduct audits independent of the other actors, in addition to collectting necessary information thereto.
- There are certain roles for each of the cloud consumer and provider when using different service models as indicated in table no. (2).

Table no. (2): Different Roles for Each of the Cloud Consumer and Provider when Using the Three Service Models

Service Model	Cloud Consumer Activities	Cloud Provider Activities
SaaS	Using applications available on the cloud to conduct related operations.	He/ She installs, manages, maintains, and supports availables applications related to the cloud consumer on his/ her cloud infrastructure.

PaaS	Developing, testing, deploying, and managing applications hosted on the cloud platform	Allocating, managing the cloud infrastructure, and providing development, deployment, and management tools for the cloud consumers.
IaaS	• Creating/ installing, managing, and monitoring related cloud infrastructure services. • Controlling virtual machines used on the cloud in terms of operating and storage systems, and applications deployed at the level of such machines.	Providing and managing physical processing, storage, networks, hosting environment, and cloud infrastructure to cloud consumers.

Second Chapter: Guidelines on the Use of Cloud Computing Technology

2.1 Prologue

In this chapter, guidelines are developed on the cloud computing governance as well as the company's policy (cloud consumer) regarding the use of cloud computing technology, the contarcts and agreements conducted between the company and the cloud provider, protection of data security, risk management, change management, and measurement and supervision of cloud provider performance. These guidelines also include monitoring of log files and security events, access management, business continuity, and termination plans relating to the arrangements of

utilizing a cloud provider in order to protect companies from the risks they may face when using cloud computing technology.

2.2 Cloud Computing Governance

Effective governance when using cloud computing technology is considered essential to guide management and decision- making processes to benefit from cloud computing services according to the company's needs and in the optimal way. Moreover, the company's cloud computing governance strategy shall be clear enough for the cloud provider in order to enable cooperation between them in terms of operatinal performance, problem solving, and decision sharing in regards to managing the risks associated with the services assigned to the cloud provider. Duties and responsibilities of the board and the senior executive management shall be identified taking into consideration the following:-

- The borad or whom it delegates of its committees shall approve the company's cloud computing policy and follow up its implementation.
- Depending on the post of each, senior executive management shall assume the following responsibilities and duties:-
    - Developing an effective structure for the governance and the operatins of properly managing the risks of utilizing cloud computing services,
    - Ensuring the development of cloud computing policy, supervising its implementation, reviewing, and updating it periodically and when nessecary,
    - Approving the agreements conducted between the company and cloud provider,
    - Ensuring due diligence assessment to cloud provider before entering into any agreement with them,
    - Reviewing risk assessment results for all agreements assocaiated with utilizing cloud computing services based on a risk assessment framework approved by the board of directors,
    - Reviewing periodic assessment reports of the cloud provider performance,
    - Ensuring the development of disaster recovery plans based on scenarios of malfunction, penetration, and actual and potential destructive actions, in addition to testing such plans periodically,

- Ensuring the existence of an appropriate mechanism to continuously monitor 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 all activities and services assigned to the cloud provider are reviewed by relevant parties in the company, as well as regularly notifying the board of directors of the risks which may be incurred.

2.3 Cloud Computing Policy

The company shall develop, review, and update periodically a cloud computing policy which shall include at least the following:-

- The services, operations, and data to be assigned to the cloud provider, in addition to the classification of such according to their importance and degree of sensitivity, so they become a reference when utilizing cloud computing services. It should be noted that the company shall bear the classification responsibility thereof,
- The best deployment model (public, private, community, and hybrid cloud), as well as the best service model (PaaS, SaaS, IaaS) for the services and operations to be assigned depending on:
  - Type of service and the classification of information and operations to be assigned to the cloud provider,
  - Assesment of related risks levels,
- The company's mechanism for archiving, disposing, processing, and transferring data with the cloud provider systems, and it shall also include the storage places of such data.
- Security controls that shall be followed when dealing with any cloud provider.
- Standards of assessment and due diligence of the cloud provider performance before entering into any agreement with them,
- Expected requirements and results from utilizing the cloud provider to perform operations in accordance with the work environment requirements and changes,
- Relationship between the company's internal operations and the operations to be transferred to the cloud provider systems,

- A mechanism to ensure compatibility and interconnection amongst different services assigned to more than one cloud provider,
- Protection controls of customers data, in addition to notifying the customer in case any of his/ her personal data are assigned to the cloud provider in accordance with the related laws and instrcutions thereto,
- Minimum requiremnets to be met in the agreements conducted with the cloud provider,
- Monitoring and auditing mechanisms pertaining to the services assigned to the cloud provider.

2.4 Risk Management

The Company shall identify and manage any risks stemming from utilizing the Cloud Computing services, while taking into consideration the following:

- Integration of the risks of utilizing Cloud Computing into the comprehensive framework of the company's risk assessment, as well as documenting and constantly updating it, provided that it includes at minimum the following:

    - Identifying the role of the Cloud supplier in the business strategy of the Company,
    - Placing comprehensive procedures to cover the connection requirements with the Cloud supplier to identify and mitigate key risks,
    - Evaluating the ability of the Cloud supplier in employing high standards to perform the service in a way that ensures providing the service with high efficiency,
    - Analyzing the impact of utilizing the Cloud Computing services on the comprehensive risks' file of the Company,
    - Evaluating the considerations related to valid laws and law enforcement provisions, in addition to the security and political stability of the Cloud supplier's country, as well as laws related to the protection of data,
    - Identifying the financial, operational, and legal risks on the Company and its reputation in the event of the failure of the Cloud supplier in performing operations adequately,

- Evaluating the comprehensive security risks related to the service assigned to the Cloud supplier, and identifying the role and responsibility of the Company and the Cloud supplier in their management, as well as identifying the steps to be followed to mitigate them, and documenting such evaluation.

- Placing key risk indicators to monitor the level of risks related to utilizing Cloud Computing services to ensure that they do not exceed the risk appetite and the degree of risk tolerance.
- Identifying the best current practices in utilizing Cloud Computing technology, including the requirements for information security management, cyber risks, and related regulatory rules.
- Monitoring risks and identifying the procedures to be taken in case the Cloud supplier fails to provide services at the level agreed upon.
- Identifying the impact on the Company's customers in case the Cloud supplier fails to perform the service or violates the confidentiality of their data.
- Managing security risks related to storing data and operating the company's applications on the systems of the Cloud supplier.
- Monitoring the concentration risks emerging from relying on an individual Cloud supplier to all services intended to be assigned to the Cloud supplier, and bearing in mind the procedures to be taken in case the supplier fails to perform operations adequately.

2.5 Contracts and Agreements between the Company and the Cloud Supplier

The company shall ensure that the contract/s signed with the Cloud supplier are in line with the company's approved policy of Cloud Computing, while taking into consideration that the contracts include in the minimum the following:

- The name of the Cloud supplier and its mother company- if any- and its business address as well as its full contact information,
- The activities and services intended to be assigned to the supplier,
- The duration of the contract,
- The abidance of the Cloud supplier to the confidentiality, privacy, and security of the Company's data,
- The abidance of the Cloud supplier with the business continuity plans of the Company,

- The auditing and supervisory measures on the Cloud supplier,
- The performance, operation, internal control, and risks management standards,
- The Cloud service level agreement and the requirements of the performance of the Cloud supplier,
- The roles and responsibilities of both parties,
- Conflict resolution and settlement measures,
- The mechanism of reporting to the Company,
- The applied law governing the contract,
- The legal and regulatory arrangements to be followed by the Cloud supplier,
- The requirements and responsibilities of the technical and maintenance support,
- The penalty clauses in case the Cloud supplier fails to provide the Cloud Computing services,
- That the contract allows for renewal and negotiation to enable the Company from keeping an adequate level of supervision on the arrangements of utilizing the Cloud supplier,
- Maintaining the confidentiality and security of information and the ownership of the Company's data, and taking necessary measures to prevent viewing or accessing such data by any other person or party without obtaining a prior consent to such,
- The abidance of the Cloud supplier to informing the Company of any suggested vital changes on the contracts or the contracted services, that might impact the supplier's ability to fulfill his responsibilities, while receiving the Company's approval on them. An agreement should be made beforehand on the notification period of these changes to allow the company to conduct an evaluation of the risks in order to consider the effects of the suggested changes before the actual change is made and to test these changes,
- Identifying the geographical location of the storage sites of the Company's data, and receiving the approval of the Company when the Cloud supplier alters the workplaces, data centers, or operations related to the services assigned to the Cloud,
- Agreeing on the security and operational requirements to ensure the efficiency and effectiveness of security policies and practices, including outstanding circumstances where each party is allowed to alter these requirements,

- Obliging the Cloud supplier to cooperate with any third party which the Company contracts with, if the working scope of this party intersects with the scope of services assigned to the supplier,
- In case the supplier contracts with a third party in relation to the service assigned to him, the Company must be informed immediately and asked for its permission; in addition to holding the supplier responsible for providing the service and for the efficiency of the controls agreed upon in the contract signed between them alongside security and operational requirements,
- Identification of the mechanisms of notification, correspondence, and the approved escalations' procedures as well as the assurance of having immediate notifications by the Cloud supplier to the Company about any violations or other events emerging from any dysfunction in the Cloud Computing services, and about the procedures taken and/ or suggested by the supplier to treat the dysfunction,
- Items that allow the Central Bank to perform its supervisory duties, and obligate the Cloud supplier of any requirements, circulars, and instructions issued by the Central Bank in relation to services assigned to the supplier,
- The text of the contract must state clearly the conditions where the two parties have the right to terminate the contract. The following conditions where the Company is allowed to terminate the contract include but are not limited to:
    - A breach of security or confidentiality,
    - The inability of the Cloud supplier to notify the Company of security events that might affect the Company's business,
    - The inability of the Cloud Supplier to perform the service contracted upon at the agreed level,
    - Changing the ownership of the Cloud supplier,
    - Bankruptcy and clearance of the Cloud supplier,
    - Submission of the Cloud supplier to custody whether in the country or any other place.
- Any restrictions or impediments that may hamper the immediate termination of the contract in case the Company wishes to must not be set.

2.5.1 Cloud Service Level Agreement

The Cloud service level agreement between the Company and the Cloud supplier is one of the most vital elements of managing the Cloud Computing service, where the complicated and changing nature of the Cloud Computing technology requires advanced methods for the management of the service level agreement to ensure the quality of service agreed upon between the Company and supplier. The Company needs a Cloud service level agreement to identify the performance requirements of Cloud services. These agreements include at minimum the following:

- The quality and performance level of the service as well as the required security controls,
- The level of availability of the service assigned to the supplier, its integration, confidentiality, and the access controls applied to it,
- The mechanism for separating the supplier's data from the company's data and the data related to the service assigned to the supplier,
- The mechanism of storing and processing data related to the Company and its customers,
- The mechanism of back- up copying and maintaining records,
- The disaster recovery plan and contingency plans,
- The details of the infrastructure and security standards that the supplier should maintain and revise compliance thereto,
- Periodical testing of the Cloud supplier to ensure its compliance to the level of performing the service and to the agreed upon security standards.

2.6 Supervision of the Cloud Supplier

The Company's assignment of some of its services to the Cloud supplier does not mean the transfer of its responsibilities to the supplier. The company is held completely responsible for the service assigned to the supplier in virtue of valid legislations and instructions issued by the Central Bank. Subsequently, the Company should see to the following:

- Notifying the Central Bank upon contracting with any Cloud supplier,

- Identifying the Company's constant supervisory and monitoring duties on the service, and ensuring the attainment of its employees of adequate training, skills and resources to supervise and test these services,
- The right to conduct an on- site visit to the headquarter of the supplier's business. Such right shall not be restricted in accordance with the prior agreement between the two parties,
- Placing procedures that allow the Central Bank to fulfil its supervisory duties, including the following:

    - Ensuring that all Company's data and Cloud Computing services are available for revision or inspection by the Central Bank at any time,
    - Obtaining any records, documents, data, or information which the Central Bank deems necessary and are related to the Company's operations assigned to the Cloud supplier,
    - Accessing any report or auditing results performed by external or internal auditors appointed by the Company or the Cloud supplier in relation to the assigned service.

2.7 Data Security

Maintaining the data security is one of the most important issues that the Company must guarantee when utilizing the Cloud supplier, considering the distributed nature of the Cloud Computing environment. Therefore, the procedures and controls that should be followed to protect the data upon their transfer, processing, storing, and destruction must be taken into consideration. Subsequently, the Company must see to the following:

- Ensuring the availability of physical protection requirements for the data centers affiliated with the Cloud supplier,
- Adoption of a set classification of data according to its sensitivity as the Company is required to hold the responsibility of its data classification,with the need for their conducting of periodical review of this classification,
- Identifying the data to be transferred to the Cloud in accordance with the approved data classification of the Company, while taking into consideration the risks arising from placing data classified as sensitive on the public or hybrid Cloud,

- Ensuring the supply of the Company with what indicates the separation of the data of the Company from the data of any other Cloud consumer or the supplier's data,
- Identifying the party responsible for making back-up copies of the data, and the storage mechanism and locations,
- Taking adequate steps to mitigate the security risks arising from the transfer of data on the Cloud,
- Identifying the nature and scope of the risks resulting from the loss of the Company's data, and mitigating these risks through:
    - Dissemination of data and applications in various locations,
    - Abidance with the best practices in business continuity and disaster recovery.
- Data (whether stored or transferred) and back-up copies of these data, most specifically the sensitive ones, must be subject to adequate deciphering controls, such as the following:
    - Placing detailed policies and procedures to regulate the deciphering keys in terms of their creation, storage, use, termination of its expiration, renewal , and archiving. Such policies and procedures shall be reviewed periodically,
    - Adequately reviewing the details related to the deciphering algorithms, the length of the deciphering keys, and data influxes by experts to identify possible weaknesses,
    - Ensuring that the secret keys used in deciphering are created and managed safely; for instance, the Hardware Security Mode (HSM),
    - Ensuring the existence of adequate controls to manage the deciphering keys and digital certifications,
    - Placing adequate security arrangements, such as the devices' security unit and other tools used for deciphering, on separate security networks to control access to it cautiously in a way that it cannot be accessed on the Subnets used by other companies dealing with the Cloud supplier or on the one that the supplier's employees might use,
    - That the deciphering keys used in deciphering the Company's data are unique and allocated for the Company's data only, and not to be used for the data of other companies that deal with the supplier.

- In case of the usage of the process of tokenization which aims at minimizing the amount of data, especially the sensitive ones, and which the Company might share with the Cloud supplier, and at guaranteeing that only authorized parties can have access to the Company's data when utilizing the Cloud supplier; the following should be taken into consideration:

  - Conducting a meticulous assessment of the risks, especially the ones related to the solutions used for the tokenization process, and identifying the unique characteristics used for accessing data,
  - Ensuring the inability of the Cloud supplier from retrieving data that are tokenized through his access to the system of the tokenization.

- The procedures for processing violations and other events of negative impact on the Cloud Computing services,
- Periodically conducting penetration tests of systems related to the services assigned to the cloud supplier, most specifically the operating systems on the virtual environment of the cloud and in cooperation with the supplier, considering their exposure to many risks due to the sharing of the Cloud consumers of physical components,
- Conducting vulnerability scanning periodically on the systems and softwares related to the services assigned to the Cloud supplier to reveal the weakness points and to treat gaps, in coordination with the supplier proactively to avoid the possibility of exposing these systems to risk.

2.8 Access Management

2,8,1 Management of the consumer's access and separation of duties

When the Cloud supplier has the ability to access and manage the systems or software related to the service assigned to him, the Company must take into consideration the following:

- Ensuring that the Cloud supplier implements its standard policies in management of access,

- Separation in the duties of consumers of systems and softwares, especially for sensitive and critical roles,
- Recording the access of consumers to the systems or softwares in the access log files belonging to the Cloud supplier, and reviewing them at least on an annual basis,
- Controlling access to the service, public accounts, and the accounts of the administrators of the systems affiliated with the Company, and which exist with the Cloud supplier through setting access management controls for consumers; most specifically the ones with privileged accounts, and recording the activities conducted on these systems to review them,
- The developers affiliated with the Cloud supplier shall not have any access right to the live environment of the company that exists on the Cloud.

2. 8.2 Active Access to Data

It is vital that the Company is able to access effectively its data related to the services assigned to the Cloud supplier, and which exist on the infrastructure of the Cloud; therefore, the company must see to the following:

- Ensuring the ability of accessing data as agreed upon with the Cloud supplier,
- Guaranteeing the lack of restrictions on the number of Company's requests for access or attainment of data,
- Guaranteeing that data are not stored in countries and locations that may prevent the effective access of the Company to its data.

2.9 Monitoring Security Events and Log Files

For the purposes of monitoring security events that the services assigned to the Cloud supplier may be exposed to, the Company shall ensure that there are adequate detection mechanisms in the network, systems, and applications of the supplier to analyze the activities that might impact the security and stability of the assigned service.The Company usually maintains log files that document the events which occur to its data and applications, and since the log files of the

service exist with the supplier, the Company must guarantee its obtaining of unrestricted authorities to access these records. Accordingly, the Company must see to the following:

- Providing what is needed to monitor and analyze the log files related to the assigned services automatically,
- Reviewing the events log files continually per the importance of the event and documenting the process,
- Reviewing, auditing, and maintaining access records to ensure that only authorized consumers have the access to data,
- Guaranteeing the attainment of the log files of security events of all services assigned to the Cloud supplier.

2.10 Business Continuity Management

The Company shall take all necessary arrangements to ensure the continuity of its business that is related to the services assigned to the Cloud supplier in case any disaster, failure, or sudden interruption occurs to these services, provided that these arrangements shall include at least the following:

- Setting a business continuity and disaster recovery plans, and testing them in cooperation with the supplier, as well as agreeing with the supplier upon contracting on what is related to the requirements and liabilities of the supplier in relation to the planning of business continuity, provided that such shall include: the recovery time objective and recovery point objective,
- Ensuring that the crisis management team affiliated with the Company fully realizes the recovery plan from the supplier's disasters,
- Looking into the possibility and impact of an unexpected interruption to the services assigned on the Company's business continuity,
- Ensuring that back-up copies of data and software are maintained in a substitute site, and testing the retrieval of back-up copies,
- Setting a contingency plan where the company documents a substitute supplier of the current supplier, and the arrangements to be followed in case the contract with the

current supplier is terminated suddenly, or if he cannot meet his commitments for any reason.

2.11 Change Management

Some risks may occur when changes are made to the Cloud Computing environment, and to avoid such risks the Company must take into consideration the following:

- Agreeing and arranging with the Cloud supplier on the method to be used for notifying the Company of the changes that occur on the Cloud Computing environment, and of its ability to review these changes to make it easier for the Company to supervise these changes,
- Ensuring the monitoring of the main changes that may affect the stability and security of the operation environment in the Cloud, and revealing erroneous or unauthorized changes,
- Agreeing with the cloud supplier on the arrangements regarding the management of change, which include the procedures for requesting, approving, and notification of change, in addition to the contingency procedures, standard changes, and the roles and responsibilities of the management of the change,
- Identifying the mechanism for conducting the testing of the preapproved changes.

2.12 Data Sovereignty

- Before the Company places its data in the Cloud supplier's country, it should look into the following:
    - Regulatory requirements of the supplier's country,
    - Political, economic, and social conditions of the supplier's country,
    - Diplomatic relations, governmental policies, and legal requirements in the supplier's country,
    - Events and disasters that may limit the ability of the supplier in providing his services.

- The Company must not enter into arrangements for engaging the Cloud suppliers in countries whose laws allow for immediate and forceful access to their data and information.
- The Company must set contractually obliging requirements that force the Cloud supplier to notify it in case he is legally obliged in the data center's country to disclose the Company's data to a third party, so that the Company may take necessary arrangements to guarantee the safety of the Company's data.

2.13 Termination Plan

The Company must have a specific and documented plan to ensure its ability to terminate the agreements of utilizing Cloud Computing services without disruption to providing its services or affecting its compliance with instructions and legislations issued by the Central Bank; therefore, the Company must see to the following:

- Setting plans and arrangements for termination, that are understood, documented, and tested fully and periodically with the cooperation of the Company and the Cloud supplier,
- Identifying the mechanism for transfer to the substitute supplier or return to the Company's system as well as maintaining the business continuity,
- A specific mechanism for the retrieval and deletion of data related to the Company and of all records and documents from the systems of the Cloud supplier upon the termination of the contract with the cloud supplier, wherever stored including the sites of back-up copies plus the data- storage media on the internet,
- Monitoring risks and considering the arrangements that might be taken in case the Cloud supplier stops functioning,
- Setting special arrangements to ensure the obtaining of the Company's data or their transfer to a substitute supplier in case the supplier fails to meet their liabilities or in case of terminating the contract with them for any reason, and obliging the current supplier to cooperate with the substitute supplier or the Company to complete the transfer process.

Third Chapter: Standards Related to Cloud Computing

Considering the challenges faced by companies which may obstruct their adoption of the Cloud Computing technology, and seeking to enable companies from using this technology safely and in a way that reduces their exposure to incurred risks; companies shall assume all necessary procedures to protect themselves from these risks through the use of world- wide common security standards which support the Cloud Computing technology and through which companies can protect the safety and confidentiality of data while utilizing the Cloud supplier. These standards provide many benefits including the following:

- Solidifying the compatibility of the Company's systems with any other systems, which makes the transfer from one Cloud supplier to another simpler,
- Ensuring that the Company and Cloud suppliers follow the best practices in this regard,
- Standards are deemed an effective mean that enables companies from comparing between Cloud suppliers to select the best supplier,
- The use of standards offers an easier path for regulatory compliance.

There are various standards related to the security of Cloud Computing technology that have been issued lately, including the ISO/IEC 27017 and ISO/IEC 27018, which provide more detailed guidelines to both the Companies and the Cloud suppliers. In addition, there are many general standards for information technology that can be applied upon the use of Cloud Computing technology as these standards are not limited to Cloud Computing in particular, yet, they are general and can be applied on the cloud Computing environment. Therefore, the Company and Cloud supplier should lend importance to these standards as they offer guidelines and recommendations, in details, for the Company and the supplier. We note in particular the following standards classified into various topics as listed below in Table (3):

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

Topics	Standards
Governance, Risk Management and Compliance	• 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)
Operational and Commercial Processes	• SSAE 16 • ISO/IEC 27000
Role Management	• LDAP, SAML 2.0, OAuth 2.0, WS-Federation, OpenID Connect, SCIM • XACML • PKCS, X.509, OpenPG
Data and Information Management	• HTTPS, SFTP, VPN using IPSec or SSL • OASIS KMIP • US FIPS 140-2
Privacy Policies	• ISO/IEC 27018
Networks' Security and Safety	• ISO/IEC 27033 or FIPS199/200 standards
Security controls on the Infrastructure	• ISO/IEC 27002 • ISO/IEC 27017 & ISO/IEC 27018

Safety Conditions in the Service Level Agreement	• 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 • CWE list • CSA STAR registry • PCI DSS • FedRAMP program
Termination procedures	• ISO/IEC 19086

The Instructions and Circulars of the Central Bank Appendix

Instructions and circulars issued by the Central Bank in relation to the outsourcing of licensed banks operating in the kingdom have been compiled for the purpose of regulating the process of utilizing Cloud Computing services in the Kingdom :

1- The Instructions on the Governance and Management of Information and Related Technology no (65/2016) dated on 25/10/2016:

- Item (3/C): "Upon signing of outsourcing agreements with others to provide the human resources, services, programs, and information technology infrastructure for the purpose of conducting the bank's operations, banks shall ensure the other's commitment to the implementation of the items of these instructions whether fully or partially and to a degree adequate with the importance and nature of the bank's operations, services, programs, and infrastructure provided before and during the contracting period. This does not exempt the Board and senior executive management from final responsibility of achieving the regulatory requirements including the auditing requirements mentioned in Item (9) below. The period of effectiveness of these instructions or the contracting period shall be deemed

the period through which the currently contracted companies must regularize their conditions, whichever is nearer."

- Attachment no (6) of the instructions (Policies' system) of outsourcing: "Adoption of a general policy for utilizing resources in general and information technology resources in particular. Such resources, whether owned by the bank (in-sourcing) or owned by others (outsourcing), must take into consideration the instructions, systems, and laws. Moreover, they should emulate the best internationally accepted practices in this regard, and shall take into consideration the production process site (on-site, off-site, near-site, off-shore). It should also take into consideration and follow the requirements of monitoring service levels, activating the audit right by trusted and neutral third parties, and achieving the business continuity requirements and protection controls essential to meet the confidentiality and credibility requirements, in addition to the requirements of efficiency and effectiveness in employing resources."
- Attachment no (8): the services, programs, and information technology infrastructure, hosting and the physical and environmental security of the main servers rooms and telecommunications rooms as well as power supply; physical and environmental security controls shall be provided according to the following at minimum:
    - Rooms and the building's infrastructure design must be distant and protected from potential threats of floods, water and sewage leakage; whether below or at the end of the building near the roofs or any other exposed location. The rooms' size should be adequate and meet the current bank's requirements while taking into consideration the possible future expansion.
    - The location of the room and the building in general should not be of limited access (whether by the nature of the geographical location or in virtue of the exclusive contractual agreements) to all telecommunications companies and different suppliers.
    - The main servers rooms, telecommunications rooms such as (Routers, Switches, etc.), and the rooms for supplying electricity shall enjoy physical and environmental protection whereby they are surrounded by reinforced concrete walls without windows, and isolated from the electromagnetic waves that might negatively affect the computer's data. They should also be served with a robust

back-up entrance for use by individuals upon emergencies. The room must also be in terms of design served by electricity outlets and fire- fighting appliances such as FM 200 per related international and domestic specifications . The room must also be on a raised floor and should contain highly sensitive smoke, water, heat, and humidity detectors. In addition, recorded televised monitoring and fairly distributed cooling on all of the room's space to protect the appliances from high heat and humidity shall be provided, while providing appliances to remove dust from the room. The entrance must be controlled and monitored so as unauthorized personnel may not be able to enter while taking into consideration not to place any signs that can show others the direction to the location of these sensitive rooms in the bank without authorized attendants.

- The servers and telecommunications rooms must be supplied by a multi- source power outlet where transfer between them is automatic, i.e. providing UPS batteries in addition to power generators at an adequate capacity to operate the appliances and operations of the bank (at least the sensitive ones) in the case of an outage in the main power source.
- The requirements of the General Directorate of Civil Defense and the Jordan Standards and Metrology Organization must be taken into consideration (wherever necessary).
- All mentioned above stands for the back-up servers, power and telecommunications rooms (Disaster recovery sites).

2- Business Continuity Plan Circular no (10/1/9943) dated on 17/8/2014

- Item (11): "Taking into consideration that agreements signed with external suppliers regarding the technical support of services in general and critical services in particular shall include their responsibilities in providing the necessary support within the service level agreement's attached conditions. Such conditions must guarantee availability at the highest degree and details in all circumstances and in proportion to the banks requirements regarding their business continuity plans in that respect."

- Item (12) " that the outsourcing policies of banks shall take into consideration the necessity of the availability of a dependable business continuity plan of others, with a confirmation by a neural independent party conducted annually at least. Such plans must guarantee availability and confidentiality of the data and operations of the bank upon the occurrence of any emergency that might cause disruption to the supply of these services. This rule should be observed as an important standard when choosing service suppliers. The contracts and agreements signed with suppliers must reflect these requirements and current suppliers should be contacted to regularize their condition on that accord."

3- The Internal Control and Supervision Systems Instructions no (35/2007) dated on 10/6/2007

- Item (9/E) " The quality of services rendered by external parties and the mechanism of presenting them in terms of maintaining the terms of confidentiality, punctuality, availability, credibility; such conditions must be controlled through duly document agreements.

4- The Circular on the Principles of E-Banking Risks Management no (10/1/3344) dated on 21/3/2005

- Item (First/3): " The board and senior management must work on establishing a system and mechanism for the management of services contracted with external parties (outsourcing relationships) for the purpose of supporting the process for presenting the e-banking services and continuing to develop it."

5- Instructions for Conducting Banks' Activities via Electronic Means no (8/2001) dated on 26/7/2001:

- Item (7): "The necessity of 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, RuedigerZarnekow, 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, RajnikantPalwe, 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**. "The Methods of Utilizing the Cloud Computing Applications in Rendering the Information Services in the United Arab Emirates** , College of Islamic and Arabic Studies in Dubai 3/2014