CITRA

الهيئة العامة للاتصالات وتقنية المعلومات

COMMUNICATION & INFORMATION TECHNOLOGY REGULATORY AUTHORITY

Subscribers Guide to Cloud Services

State of Kuwait

V1.5

Communication and Information Technology Regulatory Authority

Table of Contents

Subject	Page
Introduction	3
Cloud Computing Overview	3
Cloud Services Available for Government Entities	6
Responsibilities of Subscribed Government Entities as Per the Cloud Regulatory Framework	8
Cloud Services Available for the Private Sector	12
Responsibilities of Subscribed Private Sector Entities as Per the Cloud Regulatory Framework	13
Cloud Services Available for Individuals	17
Responsibilities of Individual Subscribers as Per the Cloud Regulatory Framework	18
Related Documents	22

Introduction

Under its establishment law No. 37 of 2014 and amended by law No. 98 of 2015 the Communication and Information Technology Regulatory Authority (CITRA) is authorized to issue regulations, policies and regulatory guidelines for the telecommunication and information technology sectors to achieve comprehensive development in the State of Kuwait. As a result, CITRA initiated the Cloud Regulatory Framework to regulate cloud services in the State of Kuwait. CITRA initiated this document to support the Cloud Regulatory Framework by guiding subscribers from government entities, private sector, and individuals to the benefits of cloud services and their responsibilities.

This guide aims to highlight the concepts of cloud computing in general and its services that subscribers can benefit from, as well as to clarify other important aspects related to regulating the offered cloud such as their: data classification and protection, cybersecurity, their protection as subscribers, and clarifying their responsibilities in accordance with the Cloud Regulatory Framework.

Cloud Computing Overview

Cloud computing made a revolution in the advancement and technical development of communication and information technology. Governments, private sectors, and individual subscribers around the world have transformed to cloud computing due to the many advantages it provides in various fields, whether it was administrative or technical, which contributes in facilitating business procedures and making them easily available through a simple network connection from anywhere. For example, but not limited to, it became possible to conduct business meetings electronically over the network, and it also became possible to complete many transactions electronically. These transactions are available to individuals and institutions online using smart devices (for example, but not limited to, smart phones, smart TVs, computers).

This chapter highlight general information on cloud computing, such its characteristics, deployment models, and service models.

Terms and definitions in this document are as defined by the National Institute of Standards and Technology (NIST), Cloud First Policy and the Cloud Regulatory Framework, and can be reviewed through CITRA's website (www.citra.gov.kw).

Characteristics of Cloud Computing

1. **On-Demand Self-service:** the subscriber can provide computing capabilities, such as the time zone of the server time and network storage, as needed automatically without the need to request it from the service provider.
2. **Wide network access:** services and capabilities are available over the network and can be accessed through fixed and portable multimedia such as mobile phones, desktop and tablet computers, and laptops.
3. **Resource pooling:** computing resources are collected for the service provider to serve a number of subscribers at the same time. This process is accomplished by activating the multi-tenant model, which in turn allocates and reallocates those resources to each subscriber as needed. The multi-tenant model also includes computing resources, insulating the operations and data of each subscriber from the rest of the subscribers, as well as ensuring that unauthorized access to the data of each government agency from other parties is prohibited. Examples of resource pooling include storage, processing, memory, network capacity, and virtual computers.
4. **Flexibility and speed:** This feature enable subscribers to provide resources according to their need quickly, smoothly and automatically (in some cases) in order to rapidly expand or shrink the size and bandwidth of resources in proportion to the need of the subscriber. Resources for the subscriber appear as unlimited and can be allocated in any quantity and at any time.
5. **Service Measurement:** Cloud systems automatically control the usage and improvement of resources by activating the measurement feature available in cloud systems in proportion to the type of service, for example: storage, processing, bandwidth, and active user accounts. The use of resources can also be monitored, controlled and reported, providing transparency with respect to the service provided to both the service provider and the subscriber who use those services.

Cloud Deployment Models

The subscriber can choose the following cloud deployment models that suit the sensitivity, confidentiality, and security requirements of its protected and classified data according to the Data Classification Policy, the Cloud Regulatory Framework, and data privacy bylaw issued by the Communications and Information Technology Regulatory Authority (CITRA).

1. **Public Cloud:** The cloud infrastructure is provided to be used by the public. It may be owned, managed, and operated by a business, academic, or government entity, or a combination of them, and can be located on the service provider's website / center.

2. **Private Cloud:** Cloud infrastructure is provided for exclusive use by one entity/company that includes multiple users (for example: sectors and departments managed by that entity/company) and operated by the entity/company itself, or a third party (such as cloud service provider), or both, and its physical location may be inside or outside the entity's/company's headquarters. The entity/company itself manages the

data movement process. In this case, the development of solutions takes a longer time because all the publishing and testing processes need to be implemented within the entity/company.

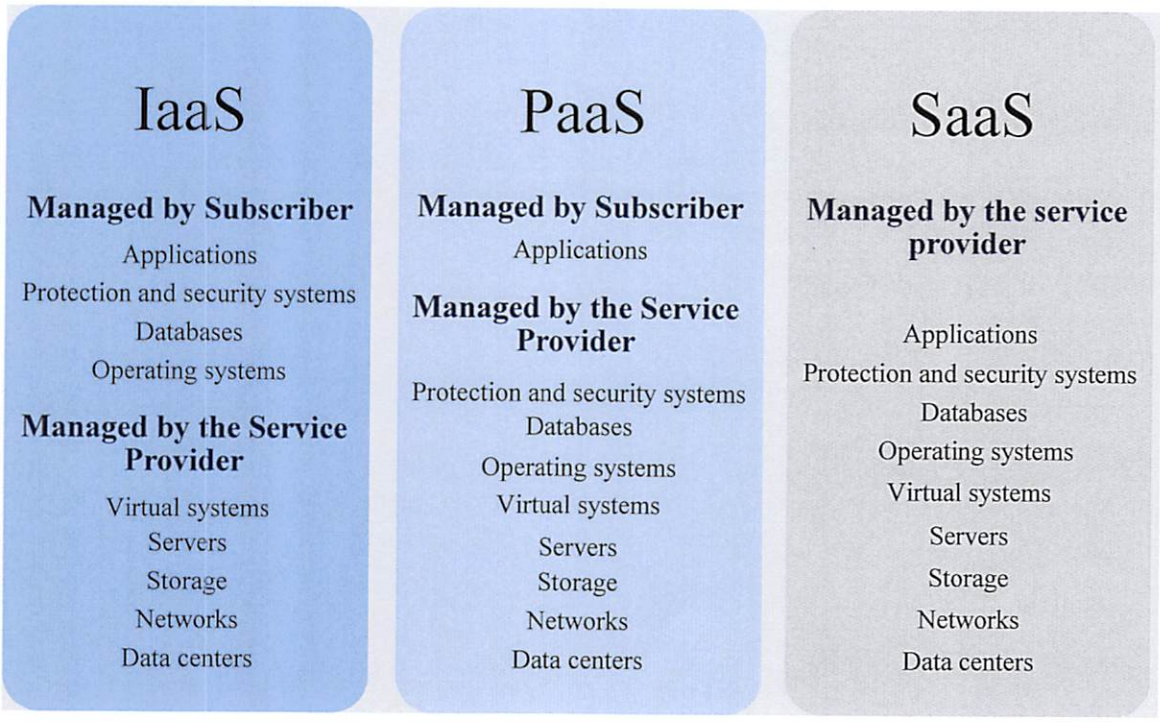
3. **Community Cloud:** Cloud infrastructure is provided for exclusive use by a specific group of users who belong to entities/companies that have shared / compatible interests (for example, entity/company roles and responsibilities, cybersecurity requirements, and compliance considerations). It may be owned, managed, and operated by one or more of the entities/companies included in that group, or a third party (service provider), or both, and its physical location may be inside or outside the entity's/company's headquarters. The service provider manages the data movement process (to fulfill the service level agreement (SLA) between the service provider and the entity/company). As this model supports accelerated installation and immediate operation mechanisms, this speeds up the process of publishing new solutions.

4. **Hybrid Cloud:** The infrastructure for this type of cloud is a combination of two or more cloud infrastructures mentioned (private, community, or public) where each infrastructure remains unique by itself and its characteristics but is linked with each other with measured and standardized technology, or proprietary technology that enables the connection between each cloud infrastructure, applications, and data transmission. For example: A private cloud platform may be converted to a public platform for load balancing purposes between linked cloud platforms.

Cloud Service Models

1. **Software as a Service (SaaS):** A software distribution model in which the service provider hosts applications and makes them available to the subscribers via the Internet. Examples include, but not limited to: applications, Web services, virtual machines, and customer relationship management systems (CRM).
2. **Platform as a Service (PaaS):** In this model, the service provider provides the environment that includes both hardware and software tools required to develop applications by the subscriber over the Internet. The service provider hosts the hardware and software on its own infrastructure, thus exempting the subscribers from purchasing infrastructure to install new ICT solutions. Some examples include, but are not limited to: application development, databases, middleware, test tools and developer tools.
3. **Infrastructure as a Service (IaaS):** In this model, the service provider hosts infrastructure components that make up a data center such as servers, storage, network devices, and the subscribers' virtualization layer. The user (the subscriber) does not manage or control the main cloud infrastructure, but rather controls the operating system, storage, applications, and some protection systems. These include, but are not limited to: mainframes, storage, load balancers and virtual machines.

The following chart illustrates the responsibilities of the service provider and the participants based on each service model:



Cloud service models and their management responsibilities

Cloud Services Available for Government Entities

This chapter highlights some of the cloud services that government entities can benefit from, for example, but not limited to storage, IT systems, productivity platforms, enterprise applications, government cloud, and social media platforms.

1. Storage

Cloud provides data and information storage and processing services for everyone and are easily accessible across a variety of smart devices such as mobile phones, desktops and laptops.

Government entities have a large amount of data; therefore, their storage needs are growing rapidly. Due to the sensitivity of some of government entities' data; data loss or breaches can cause significant harm to these entities; thus, data security and storage locations are important factors to government entities. Processing and storing government entities' data may take a long time depending on the entities' work procedures and data sensitivity. In addition, government entities need to archive some data that may be outdated but must be preserved for years even if not being used. As a result, government entities require large and highly secure storage spaces that are easily accessible and can be processed according to entities' defined access controls and other security and access requirements. Traditional solutions are often expensive, as the entities allocate large budgets in order to establish, manage and expand their data centers in order to preserve their data.

Cloud provides ideal low-cost solutions if compared to traditional systems and provides solutions to all issues mentioned in the previous paragraph, as cloud storage guarantees that data and information stored will never be lost nor damaged, will always be available to be accessed easily by the entities' authorized personnel, and automated (dynamic) resources allocation as needed. Usually, the service provider provides free storage spaces (as per the contract between the service provider and government entity and the service level agreement) to the entity's employees for their personal or professional use.

2. IT Systems

Nowadays, by migrating to cloud, government entities can manage their IT systems remotely and no longer need to manage them internally using the traditional way. Thus, government entities can significantly reduce cost spent on traditional data center hardware and equipment, their management, to a small cost that depends on the entity's use of cloud.

Entities requiring full control of their software and applications as well as their data can use the infrastructure-as-a-Service (IaaS) model provided by the service provider, where the service provider in this model provides the cloud environment that constructs a data center that enables government entities to deploy their applications and programs, store their data and manage them completely.

3. Productivity Platforms

The service provider provides the Platform-as-a-Service (PaaS) model to government entities which enables them to develop their applications and software without worrying about cloud resources needed for this platform. This service enables government entities to focus on developing different applications and software that fulfill their needs.

4. Enterprise Applications

The service provider provides enterprise applications to government entities (e.g. CRM applications, word processing, charts and visual presentations applications). These applications are available to subscribers for a monthly subscription fee, this model reliefs government entities from the many costs associated with purchasing and hosting these applications on their data centers. These applications are fully managed by the service provider (in accordance with the Software-as-a-Service (SaaS) model) so that subscribers are exempted from managing them. These applications enable government entities to focus on improving the quality of the services they provide to individuals, institutions and other government entities and other aspects related to their mandates and commitments.

5. Government Cloud

The Integration between government entities and public sector institutions in the State of Kuwait became an urgent necessity as part of the government's digital transformation, for many purposes, including but not limited to: facilitating communication between entities and enabling them to facilitate and simplify services provided to the public and to fulfill their commitments. Cloud provides these capabilities for government entities, as they can fully or partially manage and operate a government cloud by contracting with service providers.

Government cloud provides a secure platform through which various government services are provided to citizens and residents of the country easily, enable government entities to integrate with each other effectively while taking into account all aspects of information

security and confidentiality, as entities can choose the services they are willing to share and integrate, through the government cloud, with other entities, and entities can isolate some processes and data that they consider sensitive and should not be integrated or shared with other government entities within the government cloud.

6. Social Media Platforms

Social media platforms have become an integral part of our daily lives, and since they are considered as cloud services that are available to subscribers; they provide government entities subscribers with the necessary computing platforms to enable them to socialize with citizens and residents as well as companies, institutions, and other entities. Subscribers of these entities can upload photos, videos, opinions, polls, articles, or advertisements related to official government decisions or services they provide that interests the public.

Responsibilities of Subscribed Government Entities as Per the Cloud Regulatory Framework

The Cloud Regulatory Framework defined the general regulations and controls implied by contracts between cloud service providers and the subscribers. For public sector subscribers, it is important to know their implications from using cloud services regarding Information Security and Data Classification, Data Protection, and Subscribers Protection.

1. Information Security and Data Classification

Information security indicates required measures to protect against data breaches, and it is the responsibility of:

- The cloud service provider by using renown international standards to protect their cloud environment and ensure its confidentiality, safety and availability, as well complying with the commitments associated with the service model they provide to the subscriber (IaaS, PaaS, SaaS) as detailed in the "Cloud Service Providers Regulations and Commitments" document.

- The cloud subscriber by:

1. Choosing the appropriate service provider, which is accredited by CITRA, utilize the security features they provide, and ensure the service provider's capability to enable the subscriber to comply with the laws and regulations enforced in the State of Kuwait.

2. Knowing their responsibilities and commitments related to the service model they wish to subscribe to, and to review the responsibilities of the service provider in this regard, as the usage of cloud generates shared responsibilities between the subscriber and the service provider that depends on the contracted service models contracted (IaaS, PaaS, SaaS), which has been detailed in the Cloud Regulatory Framework, and in the Cloud Service Providers Regulations and Commitments documents.

3. Complying with Cloud Regulatory Framework regulations related to classifying data into 4 tiers depending on its sensitivity and ensuring compliance with required security levels.

The security measures required to protect subscribers' data become stricter as the tier of classification of such data increases (and therefore the level of information security required increases as well). Subscribers may have to encrypt their data and increase this level of encryption as the data classification tier increases, and the subscriber may have to maintain backups of this data in addition to any other security requirements from the subscriber or the service provider. Data that falls under the fourth tier of classification (for example but not limited to: encryption key or highly sensitive information available to government entities such as military information, international negotiations or those related to homeland security), requires special handling and the subscriber decides how to it should be handled.

CITRA has the right to adjust the tiers of classification and their security requirements, or issue regulations related to information security to accommodate the classification tiers mentioned in the Cloud Regulatory Framework in the future as it deems appropriate.

The Cloud Regulatory Framework defined data classification as "to classify (or place or arrange) data to appropriate security tiers based on its sensitivity to determine the best ways to process and protect the data from risks." and put its responsibility on the data owner.

In this context, the subscriber must know their subscriber's content and data sensitivity and classify them before migrating to cloud (Refer to the Cloud Regulatory Framework).

Government entities that do not operate within sensitive sectors and do not own or deal with a large volume of personal data that falls under Tier 3 from the data classification, may decide on the adequacy of the security criteria available to Tier 1 and 2 (it should be noted that the subscriber can hold their content and data hosted on public cloud from being viewed by the public by using the available settings controlled by the subscriber) from the classification, and use it to host such data, although the natural option is to choose the third tier mentioned above. The subscriber should not over-classify their content and data, as most of this data falls under the first tier and some falls under the second tier, and less may fall under the third tier. Also, the less will fall into the fourth tire. In addition, the loss of tier 1 and 2 of data or content will not do much harm to the subscriber. The government entity classifies its data as Tier 3 and 4 based on its knowledge of the extent of the harm that may occur to it. if such data is compromised, especially if it intends to use cloud to process or store such data.

The Cloud Regulatory Framework gives the subscriber (not the service provider) the responsibility to choose the level of information security required that they deem appropriate for their on-cloud subscriber content and data, and security measures, or to choose the framework provided by the cloud service provider to protect the subscriber's data if it meets their specific needs, obligations, mandates, and security requirements.

The cloud service provider and subscriber should both know their responsibilities, which were detailed according to the contracted service model in the Cloud Regulatory Framework, and in Cloud Service Providers Regulations and Commitments document, as well as the following:

a. Cloud service provider responsibilities:
    1. Responsible for the security of their cloud environment and their available security controls.
    2. Responsible for providing the levels of security required by subscribers.
    3. Not responsible for monitoring the subscriber's content and data or determining their level of confidentiality.
    4. Not responsible for the damage caused by the negligence of subscribers resulting from not using the information security controls provided by the service provider.

b. Subscribers' responsibilities:
    1. Select the appropriate service provider (especially the ones authorized by CITRA) to ensure that they provide appropriate security standards and controls to protect their data or subscriber's content.
    2. Determine the level of information security appropriate to the nature of the workloads of the subscribed government entities, and the classification of available data related to the entities or individuals.
    3. Responsible for security controls, access controls, access rights, employee's usage authorizations, and other business procedures related to processing and usage of data and subscriber's content they own (if the service model is PaaS or SaaS)
    4. Compliance with the Cloud Regulatory Framework and its associated regulations and policies related to cloud computing, data classification and any cloud-related regulations or bylaws that may be issued by CITRA in the future. Also, subscribers must comply with Kuwait's laws relating to cybercrime, intellectual property rights and others.
    5. Cloud subscribers should be aware that the service provider will not be responsible or legally pursued for the subscribers' negligence regarding information security controls provided by the service provider, as the subscribers will be held responsible if they do not utilize all security controls provided by the service provider, including legal implications due to damage incurred due to the failure to fully utilize the security controls provided by the service provider.
    6. The compliance of their employees with the laws or internal regulations, especially if they are related to cloud services and require more strict procedures.

For individual subscribers, the Cloud Regulatory Framework classified their data at the second and third tier of classification, therefore this classification applies to employees working for government entities.

If the subscribed government entity considers that part or all of their data falls under Tier 4; Then, it is their responsibility to secure such data, by ensuring the application of all information security controls provided by the service provider are applied, as well as ensuring that the service provider can provide the necessary information security requirements to assist them in complying with the laws and regulations related to the use of cloud as mentioned above.

The Cloud Regulatory Framework obliges service providers to urgently notify their subscribers without delay if their information security has been compromised or whose data has been compromised or reviewed without authorization. If such data falls under Tier 3, the service provider must notify the relevant authorities as well.

Subscribers should consider the regulations of the Cloud Regulatory Framework and its associated policies and guidelines, especially the regulations related to the commitments of cloud service providers are non-binding and unenforceable and cannot be imposed on cloud service providers who are not located within the State of Kuwait and are not authorized by CITRA. The regulations of this framework and its associated policies and guidelines are applicable on cloud service providers located within the State of Kuwait and authorized by CITRA and own data centers with a cloud infrastructure and cloud operating environment within the country's borders.

2. Data Protection

The Cloud Regulatory Framework specifies controls for protecting personal and individual data by the cloud service provider by providing the suitable environment for the security requirements that the subscriber may request, as well as the commitment not to share them with other parties. The Cloud Regulatory Framework regulations are not limited to personal and individual data, but extends to all types of subscriber's data, including data that does not fall under personal information. The Cloud Regulatory Framework prohibits service providers from publishing subscribers' data, contents, or information to any third parties, unless required in accordance with the laws of the State of Kuwait, or by taking the subscriber's written consent.

Other examples of data available to government entities that require protection and do not fall under personal information include financial, medical, legal and human resources record or confidential documents available to the subscriber.

The ownership, accessibility and editing of the subscriber's content and data is an absolute right of the subscriber and the service provider is not entitled to view, transfer, erase or seize such data without the written permission of the data owner. Cloud service providers must enable subscribers to access, process, delete or edit their data as per the Cloud Regulatory Framework regulations.

3. Subscribers Protection

The Cloud Regulatory Framework outlined the minimum requirements for cloud computing contracts between subscribers (in this case government subscribers) and cloud service providers so that these contracts include the minimum protection requirements, and to protect subscribers from unfair contract terms.

The Cloud Regulatory Framework stated that the service provider must be transparent in their cloud contracts and indicate the services that will be provided to the subscriber, their service levels, contracts duration (if applicable), payment methods, service level agreements (SLA) details, and available security controls.

The framework outlined the commitments of service providers to compensate subscribers (through service balances) in the event of negligence by the service provider or their

employees, if such negligence resulted in harm to the subscriber or violation of the subscriber's privacy, data, or content. Especially if the subscriber has correctly implemented all required security controls of the subscribed service.

CITRA invites subscribers to review the Cloud Regulatory Framework and its associated policies and guidelines available on CITRA's website (https://citra.gov.kw) for more information.

Cloud Services Available for the Private Sector

This chapter highlights some of the cloud services that the private sector can benefit from, for example, but not limited to storage, IT systems, productivity platforms, enterprise applications, and social media platforms.

1. Storage

Cloud provides data and information storage and processing services for everyone and are easily accessible across a variety of smart devices such as mobile phones, desktops and laptops. Cloud storage guarantees that data and information stored will never be lost nor damaged, will always be available as per the service level agreement (SLA) provided by the service provider when registering or subscribing for this service.

In this context, private sector companies contract with service providers to provide cloud storage spaces for their employees, thereby exempting private sector companies from costs associated with purchasing and managing data centers for this type of services.

2. IT Systems

Nowadays, by migrating to cloud, companies can manage their IT systems remotely and no longer need to manage them internally using the traditional way. Thus, companies can significantly reduce cost spent on traditional data center hardware and equipment, their management, to a small cost that depends on the company's use of cloud.

Companies requiring full control of their software and applications as well as their data can use the infrastructure-as-a-Service (IaaS) model provided by the service provider, where the service provider in this model provides the cloud environment that constructs a data center that enables companies to deploy their applications and programs, store their data and manage them completely.

3. Productivity Platforms

The service provider provides the Platform-as-a-Service (PaaS) model to private sector companies which enables them to develop their applications and software without worrying about cloud resources needed for this platform. This service enables these companies to focus on developing different applications and software that fulfill their needs.

4. Enterprise Applications

The service provider provides enterprise applications to private sector companies (e.g., CRM applications, word processing, charts and visual presentations applications). These applications are available to subscribers for a monthly subscription fee, this model reliefs these companies from the many costs associated with purchasing and hosting these applications on their data centers. These applications are fully managed by the service

provider (in accordance with the Software-as-a-Service (SaaS) model) so that subscribers are exempted from managing them.

Small and Medium Enterprises can benefit from these services, which relieves them from purchasing and managing these applications in full and enabling them to focus on their economic growth and other business management aspects.

5. Social Media Platforms

Social media platforms have become an integral part of our daily lives, and since they are considered as cloud services that are available to subscribers; they provide private sector subscribers and entrepreneurs with the necessary computing platforms to enable them to socialize with their customers, or subscribers. Subscribers from these companies can upload photos, videos, opinions, polls, articles, or promotional and marketing materials related to their products and services and share them with other individuals and other subscribers.

Responsibilities of Subscribed Private Sector Entities as Per the Cloud Regulatory Framework

The Cloud Regulatory Framework defined the general regulations and controls implied by contracts between cloud service providers and the subscribers. For private sector and entrepreneur subscribers, it is important to know their implications from using cloud services regarding Information Security and Data Classification, Data Protection, and Subscribers Protection.

1. Information Security and Data Classification

Information security indicates required measures to protect against data breaches, and it is the responsibility of:

- The cloud service provider by using renown international standards to protect their cloud environment and ensure its confidentiality, safety, and availability, as well complying with the commitments associated with the service model they provide to the subscriber (IaaS, PaaS, SaaS) as detailed in the "Cloud Service Providers Regulations and Commitments" document.

- The cloud subscriber by:

1. Choosing the appropriate service provider, which is accredited by CITRA, utilize the security features they provide, and ensure the service provider's capability to enable the subscriber to comply with the laws and regulations enforced in the State of Kuwait.

2. Knowing their responsibilities and commitments related to the service model they wish to subscribe to, and to review the responsibilities of the service provider in this regard, as the usage of cloud generates shared responsibilities between the subscriber and the service provider that depends on the contracted service models contracted (IaaS, PaaS, SaaS), which has been detailed in the Cloud Regulatory Framework, and in the Cloud Service Providers Regulations and Commitments documents.

3. Complying with Cloud Regulatory Framework regulations related to classifying data into four tiers depending on its sensitivity and ensuring compliance with required security levels.

The security measures required to protect subscribers' data become stricter as the tier of classification of such data increases (and therefore the level of information security required increases as well). Subscribers may have to encrypt their data and increase this level of encryption as the data classification tier increases, and the subscriber may have to maintain backups of this data in addition to any other security requirements from the subscriber or the service provider. Data that falls under the fourth tier of classification (for example but not limited to: encryption key or highly sensitive information available to private sector companies), requires special handling and the subscriber decides how to it should be handled.

CITRA has the right to adjust the tiers of classification and their security requirements, or issue regulations related to information security to accommodate the classification tiers mentioned in the Cloud Regulatory Framework in the future as it deems appropriate.

The Cloud Regulatory Framework defined data classification as "to classify (or place or arrange) data to appropriate security tiers based on its sensitivity to determine the best ways to process and protect the data from risks." and put its responsibility on the data owner.

In this context, the subscriber must know their subscriber's content and data sensitivity and classify them before migrating to cloud (Refer to the Cloud Regulatory Framework).

Private sector companies and entrepreneurs that do not operate within sensitive sectors and do not own or deal with a large volume of personal data that falls under Tier 3 from the data classification, may decide on the adequacy of the security criteria available to Tier 1 and Tier 2 (it should be noted that the subscriber can hold their content and data hosted on public cloud from being viewed by the public by using the available settings controlled by the subscriber) from the classification, and use it to host such data, although the natural option is to choose the third tier mentioned above. The subscriber should not over-classify their content and data, as most of this data falls under the first and second tiers and some falls under the third tier, and less may fall under the fourth tier. In addition, the loss of tier 1 and tier 2 data or content will not do much harm to the subscriber. The company classifies its data as Tier 3 and 4 based on its knowledge of the extent of the harm that may occur to it if such data is compromised, especially if it intends to use cloud to process or store such data.

The Cloud Regulatory Framework gives the subscriber (not the service provider) the responsibility to choose the level of information security required that they deem appropriate for their on-cloud subscriber content and data, and security measures, or to choose the framework provided by the cloud service provider to protect the subscriber's data if it meets their specific needs, obligations, mandates, and security requirements.

The cloud service provider and subscriber should both know their responsibilities, which were detailed according to the contracted service model in the Cloud Regulatory Framework, and in Cloud Service Providers Regulations and Commitments document, as well as the following:

a. Cloud service provider responsibilities:
   1. Responsible for the security of their cloud environment and their available security controls.
   2. Responsible for providing the levels of security required by subscribers.
   3. Not responsible for monitoring the subscriber's content and data or determining their level of confidentiality.
   4. Not responsible for the damage caused by the negligence of subscribers resulting from not using the information security controls provided by the service provider.

b. Subscribers' responsibilities:
   1. Select the appropriate service provider (especially the ones authorized by CITRA) to ensure that they provide appropriate security standards and controls to protect their data or subscriber's content.
   2. Determine the level of information security appropriate to the nature of the workloads of the subscribed government entities, and the classification of available data related to the entities or individuals.
   3. Responsible for security controls, access controls, access rights, employee's usage authorizations, and other business procedures related to processing and usage of data and subscriber's content they own (if the service model is PaaS or SaaS)
   4. Compliance with the Cloud Regulatory Framework and its associated regulations and policies related to cloud computing, data classification and any cloud-related regulations or bylaws that may be issued by CITRA in the future. Also, subscribers must comply with Kuwait's laws relating to cybercrime, intellectual property rights and others.
   5. Cloud subscribers should be aware that the service provider will not be responsible or legally pursued for the subscribers' negligence regarding information security controls provided by the service provider, as the subscribers will be held responsible if they do not utilize all security controls provided by the service provider, including legal implications due to damage incurred due to the failure to fully utilize the security controls provided by the service provider.
   6. The compliance of their employees with the laws or internal regulations, especially if they are related to cloud services and require more strict procedures.

For individual subscribers, the Cloud Regulatory Framework classified their data at the second and third tiers of classification, therefore this classification applies to employees working for private sector companies and entrepreneur.

If the subscribed private sector company considers that part or all of their data falls under Tier 4, then, it is their responsibility to secure such data, by ensuring the application of all information security controls provided by the service provider are applied, as well as ensuring that the service provider can provide the necessary information security requirements to assist them in complying with the laws and regulations related to the use of cloud as mentioned above.

The Cloud Regulatory Framework obliges service providers to urgently notify their subscribers without delay if their information security has been compromised or whose data

has been compromised or reviewed without authorization. If such data falls under Tier 3, the service provider must notify the relevant authorities as well.

Subscribers should take into account the regulations of the Cloud Regulatory Framework and its associated policies and guidelines, especially the regulations related to the commitments of cloud service providers are non-binding and unenforceable and cannot be imposed on cloud service providers who are not located within the State of Kuwait and are not authorized by CITRA. The regulations of this framework and its associated policies and guidelines are applicable on cloud service providers located within the State of Kuwait and authorized by CITRA and own data centers with a cloud infrastructure and cloud operating environment within the country's borders.

2. Data Protection

The Cloud Regulatory Framework specifies controls for protecting personal and individual data by the cloud service provider by providing the suitable environment for the security requirements that the subscriber may request, as well as the commitment not to share them with other parties. The Cloud Regulatory Framework regulations are not limited to personal and individual data, but extends to all types of subscriber's data, including data that does not fall under personal information. The Cloud Regulatory Framework prohibits service providers from publishing subscribers' data, contents, or information to any third parties, unless required in accordance with the laws of the State of Kuwait, or by taking the subscriber's written consent.

Other examples of data available to private sector and entrepreneurs that require protection and do not fall under personal information include commercial data related to products and services, marketing data, or data related to information security.

The ownership, accessibility and editing of the subscriber's content and data is an absolute right of the subscriber and the service provider is not entitled to view, transfer, erase or seize such data without the written permission of the data owner. Cloud service providers must enable subscribers to access, process, delete or edit their data as per the Cloud Regulatory Framework regulations.

3. Subscribers Protection

The Cloud Regulatory Framework outlined the minimum requirements for cloud computing contracts between subscribers (in this case private sector subscribers) and cloud service providers so that these contracts include the minimum protection requirements, and to protect subscribers from unfair contract terms.

The Cloud Regulatory Framework stated that the service provider must be transparent in their cloud contracts and indicate the services that will be provided to the subscriber, their service levels, contracts duration (if applicable), payment methods, service level agreements (SLA) details, and available security controls.

The framework outlined the commitments of service providers to compensate subscribers (through service balances) in the event of negligence by the service provider or their employees, if such negligence resulted in harm to the subscriber or violation of the subscriber's privacy, data, or content. Especially if the subscriber has correctly implemented all required security controls of the subscribed service.

CITRA invites subscribers to review the Cloud Regulatory Framework and its associated policies and guidelines available on CITRA's website (https://citra.gov.kw) for more information.

Cloud Services Available for Individuals

This chapter highlights some of the cloud services used by individuals, for example, but not limited to storage, IT systems, entertainment platforms, social media platforms, and productivity platforms.

1. Storage

Cloud provides data and information storage and processing services for everyone and are easily accessible across a variety of smart devices such as mobile phones, desktops, and laptops. Cloud storage guarantees that data and information stored will never be lost nor damaged, will always be available as per the service level agreement (SLA) provided by the service provider when registering or subscribing for this service.

In this context, cloud storage providers offer free storage space for subscribers with a specific capacity determined by the service provider, and the subscriber can increase this storage capacity as needed for a monthly or annual subscription fees, this subscription may be individual or within a package that includes other services.

2. IT Systems

Nowadays, due to the flexibility and widespread usage of cloud computing, the use of personal information technology systems, which were offered to businesses and companies only, is now available to use by individual subscribers. Perhaps the most common examples of these systems are e-mail, calendars, digital books and music libraries.

Taking the example of e-mail, the cloud service provider provides all the operating requirements of its e-mail platform (servers and necessary infrastructure), and individual subscriber creates an account on this platform and uses the service provider's servers without having to install the email server on their personal computer, or smart device. The subscriber can read, send, and process e-mails with ease and minimal cost.

Similarly, other email-based examples such as calendars, notebooks, digital books, and music libraries that enable individual subscribers to benefit from these cloud services, due to the cost efficiency of cloud computing, which enabled service providers to manage IT systems more professionally to include a larger segment of subscribers and provide them with more services.

3. Entertainment Platforms

Millions of people use online entertainment platforms daily, including videos and movies live streaming websites, mobile gaming platforms, and various entertainment applications available on these individuals' smart devices. These platforms are often hosted on cloud, as these platforms exempt the subscriber from the need to provide complex devices for access and enjoyment of those platforms (for examples but not limited to satellite receivers

and other traditional broadcasting services). The subscriber uses smart devices available with an internet subscription (such as a laptop, smartphone, or smart TVs) to log-in and enjoy the services of those platforms available on cloud.

Taking the example of video live streaming websites hosted on cloud, users of these websites view the entertainment content available by registering on these websites either free of charge or according to a monthly subscription provided by the service provider within a range of privileges. These websites may be in the form of an application that can be downloaded on subscribers' smart devices. In this case, the subscriber does not need to use satellite receivers as is done in traditional methods, nor does they need much storage space to store this content, but rather watch it as a live stream from the website or the application directly.
Some video gaming platforms and other entertainment applications follow the same methodology, where the subscriber downloads the application on their smart device, then access the application platform hosted on cloud and enjoy the entertainment services provided without the need to provide the necessary infrastructure to operate these games.

4. Social Media Platforms

Social media platforms have become an integral part of our daily lives, and since they are considered as cloud services that are available to subscribers; they provide individual subscribers with the necessary computing platforms to enable them to socialize with each other. Subscribers can upload photos, videos, opinions, polls, articles and share them with each other.

5. Productivity Platforms

Perhaps the most common of these platforms are the ones for editing and processing documents of all kinds, programming, and application development via cloud computing. The subscriber "rents", rather than purchasing, these applications from service providers for a fee. These applications have continuous updates in terms of productivity platforms and information security, unlike older applications that are fully purchased for a period and then the subscriber needs to purchase their new versions after a few years. The cloud service provider usually provides these applications in addition to other related services, such as storage and IT systems services mentioned above within a package, this package may also include other services.

Responsibilities of Individual Subscribers as Per the Cloud Regulatory Framework

The Cloud Regulatory Framework defined the general regulations and controls implied by contracts between cloud service providers and the subscribers. For individual subscribers, it is important to know their implications from using cloud services regarding Information Security and Data Classification, Data Protection, and Subscribers Protection.

1. Information Security and Data Classification

Information security indicates required measures to protect against data breaches, and it is the responsibility of:

- The cloud service provider by using renown international standards to protect their cloud environment and ensure its confidentiality, safety, and availability, as well complying with the commitments associated with the service model they provide to the subscriber (IaaS, PaaS, SaaS) as detailed in the "Cloud Service Providers Regulations and Commitments" document.

- The cloud subscriber by:

1. Choosing the appropriate service provider, which is accredited by CITRA, utilize the security features they provide, and ensure the service provider's capability to enable the subscriber to comply with the laws and regulations enforced in the State of Kuwait.

2. Knowing their responsibilities and commitments related to the service model they wish to subscribe to, and to review the responsibilities of the service provider in this regard, as the usage of cloud generates shared responsibilities between the subscriber and the service provider that depends on the contracted service models contracted (IaaS, PaaS, SaaS), which has been detailed in the Cloud Regulatory Framework, and in the Cloud Service Providers Regulations and Commitments documents.

3. Complying with Cloud Regulatory Framework regulations related to classifying data into four tiers depending on its sensitivity and ensuring compliance with required security levels.

The security measures required to protect subscribers' data become stricter as the tier of classification of such data increases (and therefore the level of information security required increases as well). Subscribers may have to encrypt their data and increase this level of encryption as the data classification tier increases, and the subscriber may have to maintain backups of this data in addition to any other security requirements from the subscriber or the service provider. Data that falls under the fourth tier of classification (for example but not limited to: criminal record in case of individual subscribers, or security or military information in case of government entity subscribers), requires special handling and the subscriber decides how to it should be handled.

CITRA has the right to adjust the tiers of classification and their security requirements, or issue regulations related to information security to accommodate the classification tiers mentioned in the Cloud Regulatory Framework in the future as it deems appropriate.

The Cloud Regulatory Framework defined data classification as "to classify (or place or arrange) data to appropriate security tiers based on its sensitivity to determine the best ways to process and protect the data from risks." and put its responsibility on the data owner.

In this context, the subscriber must know their subscriber's content and data sensitivity and classify them before migrating to cloud (Refer to the Cloud Regulatory Framework and Data Classification Policy).

It should be noted that the subscriber can hold their content and data hosted on public cloud under the first and second tier from being viewed by the public by using the available

settings controlled by the subscriber. In addition, the loss of tier 1 data or content will not do much harm to the subscriber.

The Cloud Regulatory Framework gives the subscriber (not the service provider) the responsibility to choose the level of information security required that they deem appropriate for their on-cloud subscriber content and data, and security measures, or to choose the framework provided by the cloud service provider to protect the subscriber's data if it meets their specific needs, obligations, mandates, and security requirements.

The cloud service provider and subscriber should both know their responsibilities regarding information security, which are detailed as follows:

a. Cloud service provider responsibilities:
    1. Responsible for the security of their cloud environment and their available security controls.
    2. Responsible for providing the levels of security required by subscribers.
    3. Not responsible for monitoring the subscriber's content and data or determining their level of confidentiality.
    4. Not responsible for the damage caused by the negligence of subscribers resulting from not using the information security controls provided by the service provider.

b. Subscribers' responsibilities:
    1. Select the appropriate service provider (especially the ones authorized by CITRA) to ensure that they provide appropriate security standards and controls to protect their data or subscriber's content.
    2. Compliance with the Cloud Regulatory Framework and its associated regulations and policies related to cloud computing, data classification and any cloud-related regulations or bylaws that may be issued by CITRA in the future. Also, subscribers must comply with Kuwait's laws relating to cybercrime, intellectual property rights and others.
    3. Cloud subscribers should be aware that the service provider will not be responsible or legally pursued for the subscribers' negligence regarding information security controls provided by the service provider, as the subscribers will be held responsible if they do not utilize all security controls provided by the service provider, including legal implications due to damage incurred due to the failure to fully utilize the security controls provided by the service provider.
    4. Cloud subscribers should be aware that they will be legally pursued if they store data or subscriber's content that is seen as illegal by the laws of the State of Kuwait related to cybercrime or electronic transactions, or intellectual property, and they should refrain from such illicit acts to avoid sanctions stated by the law of the State of Kuwait.
    5. Compliance, where they should, with other unmentioned laws or commitments, such as internal laws and regulations of their employing entity, especially if their employing entity provides cloud services to them and require more strict procedures.

For individual subscribers, the Cloud Regulatory Framework classified their data at the second and third tiers of classification (Tier 2 & 3); If these subscribers consider part or all of their data falls under Tier 4, then, it is their responsibility to secure such data, by ensuring the application of all information security controls provided by the service provider are applied, as well as ensuring that the service provider can provide the necessary information security requirements to assist them in complying with the laws and regulations related to the use of cloud as mentioned above.

Subscribers should consider the regulations of the Cloud Regulatory Framework and its associated policies and guidelines, especially the regulations related to the commitments of cloud service providers are non-binding and unenforceable and cannot be imposed on cloud service providers who are not located within the State of Kuwait and are not authorized by CITRA. The regulations of this framework and its associated policies and guidelines are applicable on cloud service providers located within the State of Kuwait and authorized by CITRA and own data centers with a cloud infrastructure and cloud operating environment within the country's borders.

2. Data Protection

The Cloud Regulatory Framework specifies controls for protecting personal and individual data by the cloud service provider by providing the suitable environment for the security requirements that the subscriber may request, as well as the commitment not to share them with other parties. The Cloud Regulatory Framework prohibits service providers from publishing subscribers' data, contents or information to any third parties, unless required in accordance with the laws of the State of Kuwait, or by taking the subscriber's written consent.

The ownership, accessibility and editing of the subscriber's content and data is an absolute right of the subscriber and the service provider is not entitled to view, transfer, erase or seize such data without the written permission of the data owner. Cloud service providers must enable subscribers to access, process, delete or edit their data as per the Cloud Regulatory Framework regulations.

3. Subscribers Protection

The Cloud Regulatory Framework outlined the minimum requirements for cloud computing contracts between subscribers (in this case individual subscribers) and cloud service providers so that these contracts include the minimum protection requirements, and to protect subscribers from unfair contract terms.

The Cloud Regulatory Framework stated that the service provider must be transparent in their cloud contracts and indicate the services that will be provided to the subscriber, their service levels, contracts duration (if applicable), payment methods, service level agreements (SLA) details, and available security controls.

CITRA invites subscribers to review the Cloud Regulatory Framework and its associated policies and guidelines available on CITRA's website (https://citra.gov.kw) for more information.

Related Documents

1. Data Classification Policy
2. Cloud Computing Regulatory Framework
3. ICT Terms and Definitions