Enterprises’ Guide to Cloud Computing Services

Issued by

Communication and Information Technology Commission

Version 3
Contents

1. Introduction .................................................................................................................. 1

2. Overview of Cloud Computing.................................................................................... 2

3. Examples of Cloud Computing in Common Business Operations................................. 4
   3.1. Storage services ........................................................................................................ 4
   3.2. Remote IT services ..................................................................................................... 5
   3.3. Productivity platforms ............................................................................................... 6
   3.4. Professional software platforms ............................................................................... 7

4. Implications of Cloud Computing Regulations in Saudi Arabia ...... 9
   4.1. Information security .................................................................................................... 9
   4.2. Data protection ......................................................................................................... 12
   4.3. Customer protection .................................................................................................. 12
Exhibits

Exhibit 2.1: Essential characteristics of Cloud Computing ........................................ 3
Exhibit 3.1: Overview of Cloud storage services .............................................................. 5
Exhibit 3.2: Overview of remote IT services offered over the Cloud .............................. 6
Exhibit 3.3: Overview of a productivity platform provided as Platform-as-a-Service (PaaS) over Cloud ......................................................................................................................... 7
Exhibit 3.4: Overview of a professional software platform provided over Cloud ..... 8
Exhibit 4.1: Data security classification levels for enterprises .............................. 10
1. Introduction

Pursuant to the Telecommunications Act, the Bylaw and the Communications and Information Technology Commission (the “Commission”) Ordinance, the Commission is the authority in charge or regulating Information and Communications Technology (ICT) sector in the KSA.

To create a favourable environment for provision and development of Cloud Computing services in Saudi Arabia, the Commission has adopted a Regulatory Framework on Cloud Computing. Its text lays down certain general rules and obligations/rights of each side (i.e. Cloud Service Providers -CSPs-, customers and users), while allowing substantial room for different commercial and technical solutions.

This Guide aims to provide business customers and enterprises with a basic understanding of Cloud Computing services, as well as with examples and information on the new Regulatory Framework’s provisions and implications.

The Guide contains the following sections:

- Overview of Cloud Computing
- Examples of Cloud Computing in Common Business Operations
- Implications of Cloud Computing Regulations in Saudi Arabia

1 KSA: Kingdom of Saudi Arabia
2. Overview of Cloud Computing

The concept of ‘Cloud Computing’ has emerged over recent years as a genuine paradigm shift in the use of ICT services by organizations and individuals. Solid demand and supply have converged on an understanding of what Cloud Computing implies, which is now widely accepted in the industry. Put simply, Cloud Computing allows customers to utilize remote computing resources, which are available on demand and can be rapidly scaled up or down according to a task’s needs. In a way, Cloud Computing is analogous to the manner in which power (e.g., electricity or gas) networks are used today, where instead of producing power individually, customers simply draw it as needed from a centralized location.

The commonly sought characteristics that distinguish a Cloud Computing service from traditional IT services are reflected in the following service provision aspects:

- Availability of services on-demand
- Access to services over a network connection
- Utilization of pooled computer resources
- Rapid provisioning (and de-provisioning) times
- Minimal interaction (i.e. formalities) to setup new services

These are commonly referred to as the five essential characteristics of Cloud Computing and are further explained below, through reliance on the terminology used by the U.S. National Institute of Standards and Technology (NIST):
1. On-demand self-service: Customers have the ability to provision computing capabilities, such as server time and network storage, on an "as needed" basis, without requiring human interaction with the service provider.

2. Broad network access: Capabilities are accessed over the network through standard mechanisms that promote use by different platforms such as mobile phones, tablets, laptops, and workstations.

3. Resource pooling: Provider's computing resources are pooled to serve multiple customers, with different physical and virtual resources dynamically assigned and reassigned according to customer demand.

4. Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand.

5. Measured service: Cloud systems automatically control and optimize resource use. Resource usage can be monitored, controlled, and reported, providing transparency for both provider and customer of the utilized service.

Exhibit 2.1: Essential characteristics of Cloud Computing

Cloud Computing services are already used in common business transactions by most enterprises, even if they may not always be aware of it. This section aims to highlight the ubiquitous nature of such Cloud services in business life today, through some examples of Cloud Computing services enterprises are most familiar with, including:

- Storage services
- Remote IT services
- Productivity platforms
- Professional software platforms.

3.1. Storage services

Cloud storage services are perhaps the most common type of Cloud services in usage today. They allow enterprise customers to upload and securely store their data in storage space of a centralized datacentre where such capacities are allocated for account holders. Almost all of these services offer enterprises a certain amount of free storage per employee, up to a certain capacity (e.g., 50 GB). Higher capacities are generally available on a monthly paid subscription, as a stand-alone service or part of a package.

Such Cloud storage services, when compared to traditional file storage on physical media or in a business customer’s on-site servers, have the benefit of allowing continuous and immediate securitized access, over multiple fixed or mobile devices, by different people in a company. At the same time, they virtually eliminate the risk of data loss or a security breach, as the protection of Cloud content is professionally handled by the CSP operating the Cloud datacentre. Last but not least, they can help reduce a company’s investment and operating expenses for in-house IT equipment, upgrades, personnel and training, and they are scalable, i.e., business customers pay for the storage they actually need and can adjust it regularly and easily, without any risk of significantly over- or underinvesting in storage capacity.
### Service description

- **Service type:**
  - Storage
- Uploading and storing of files to a cloud server
- Files are accessible across different devices

### How it works

<table>
<thead>
<tr>
<th>How it works</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service type:</strong> Storage</td>
</tr>
<tr>
<td><strong>Uploading and storing of files to a cloud server</strong></td>
</tr>
<tr>
<td><strong>Files are accessible across different devices</strong></td>
</tr>
</tbody>
</table>

**Exhibit 3.1: Overview of Cloud storage services**

### 3.2. Remote IT services

Most of the IT services that enterprises would traditionally manage internally can now be moved to the Cloud and managed by the CSP. Due to the elasticity and rapid deployment characteristics of Cloud services, enterprises can shift costs of maintaining a large in-house IT operation, throughout the year, to having a lightweight IT operation in the Cloud that can be scaled up or down with demand, thus resulting in cost savings. For enterprises wishing to maintain full direct control of their software and data, many large CSPs offer Infrastructure-as-a-Service (IaaS), which allows their customers to utilize remote servers in the CSPs’ datacentres, making it possible for any business to run its IT remotely, on the Cloud.
3.3. **Productivity platforms**

Another example of Cloud services is the provision of productivity platforms for enterprises. These types of service leave server management in the hands of the CSP, and offer customers a platform on which professional grade software applications can be developed by Cloud customers. This allows enterprises to focus on developing various applications tailored to their specific needs, while the necessary computing resources are handled by the CSP. Cloud-based productivity platforms also facilitate project management and collaboration across different departments and teams.
### 3.4. Professional software platforms

Professional software platforms are increasing in popularity among enterprises in recent years. These Cloud services focus on offering an increased flexibility for traditional productivity software, such as word processing, spreadsheet software, or database management or customer relationship management (CRM) software. They generally rely on a monthly subscription model, in line with the measured service characteristics of the Cloud services, with software being rented from the CSP instead of having to be purchased by the Customer.

For example, a variety of Cloud solutions can allow a small or medium enterprise to use affordable CRM software and CRM tools that reside in the Cloud, together with that enterprise’s customer data, and can be easily accessed from that enterprise through the Internet. CRM solutions offered through the Cloud allow such a customer to automate and synchronize many aspects of customer interaction, such as marketing, sales, customer service, and support, in combination with other tools (e.g., analytics and Cloud-based teleconferencing) typically available in the same service package.

Such Cloud-based business solutions have the benefit of always incorporating the latest productivity features and security updates in the software instead of necessitating the purchase of a new version every few years, which would need to be installed on all customer devices separately and would require a full synchronization of data and procedures across the company.
### Exhibit 3.4: Overview of a professional software platform provided over Cloud

<table>
<thead>
<tr>
<th>Service description</th>
<th>How it works</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service type:</strong></td>
<td></td>
</tr>
<tr>
<td>Professional</td>
<td><img src="image" alt="Diagram" /></td>
</tr>
<tr>
<td>Software Platform</td>
<td>User A</td>
</tr>
<tr>
<td></td>
<td>User B</td>
</tr>
<tr>
<td></td>
<td>Software</td>
</tr>
<tr>
<td><strong>Traditional</strong></td>
<td></td>
</tr>
<tr>
<td>productivity</td>
<td></td>
</tr>
<tr>
<td>software offered</td>
<td></td>
</tr>
<tr>
<td>over the cloud,</td>
<td></td>
</tr>
<tr>
<td>allowing universal</td>
<td></td>
</tr>
<tr>
<td>access, and</td>
<td></td>
</tr>
<tr>
<td>collaboration</td>
<td></td>
</tr>
</tbody>
</table>
4. Implications of Cloud Computing Regulations in Saudi Arabia

As commented previously, the Commission has issued a Regulatory Framework on Cloud Computing, which defines general rules and obligations/rights of each side involved in a Cloud contract (i.e. CSP and Cloud customer).

As regards enterprise customers in particular, the Regulatory Framework has a number of important practical implications related to:

- Information security
- Data protection
- Customer protection

4.1. Information security

Information security refers to the protection of information systems against unauthorized access, use, disclosure, disruption, modification or destruction, primarily by third parties. In other words, it relates to a CSP’s obligation to use appropriate industry standards to protect its Cloud System and confidentiality, integrity and availability of the systems generally under its control and a customer's obligation to protect its content by selecting a qualified CSP and appropriately using the security features offered by the CSP. It is the customer’s responsibility to ensure that it implements all security features required under the Regulatory Framework, which classifies data into 4 levels, depending on their level of sensitivity (from 1- least sensitive, to 4- top secret), and other law or regulation. The customer should ensure that the CSP it selects offers the necessary security features to enable the customer to comply.

The higher the level of security for the customer's content, the stricter the information security requirements to secure the content. The customer may be required to use features such as strong encryption mechanisms, back-ups, multi-factor authentication, virtual private networking and other security features provided by either the customer or the CSP. Level 4 data, such as State secrets, are subject to separate rules and generally fall outside the scope of Cloud regulation by the Commission.
An enterprise’s data will normally fall into one of the first three levels, according to the criteria set out in the table below:

<table>
<thead>
<tr>
<th>Level</th>
<th>Type</th>
<th>Indicative Examples</th>
</tr>
</thead>
</table>
| **Level 1**    | Non-sensitive content                        | ▶ Company websites  
▶ Companies’ published accounts and reports  
▶ Commercial brochures  
▶ Marketing materials                                                                 |
| **Level 2**    | Sensitive content                            | ▶ Non-published financial information  
▶ Relevant commercial information (Sales, customers, product costs, etc.)  
▶ Personnel information with personal data (e.g. salaries, performance, etc.)  
▶ Business plans  
▶ Company emails (unless the company operates in a sensitive sector) |
| **Level 3**    | Particularly sensitive content or subject to sector-specific confidentiality obligations | ▶ Information relating to banking and financial transactions  
▶ Medical records  
▶ Security information  
▶ Customer information of certain regulated public utilities  
▶ Company’s secret know-how whose disclosure would cause serious damage |

*Exhibit 4.1: Data security classification levels for enterprises*

Typical enterprises, which operate in non-sensitive sectors and are not handling large volumes of sensitive personal or regulated data, may well decide that Level 1 protection is sufficient for them, even if the ‘default option’ for enterprises is Level 2 (see discussion below). Indeed, Level 1 data are not necessarily accessible to the broad public – this will depend on settings under the Cloud Customer’s control – but their loss or breach would not normally cause significant or any harm to the Cloud Customer concerned. The choice between Level 2 or Level 3 will depend on the expected impact of any loss or breach of the data a company intends to store or process in the Cloud.

It is important to understand that, in principle, it is up to each business customer of Cloud services and not the CSP to select the information security level among those listed in the above table, which best matches that customer’s specific needs and security requirements. Responsibility for security and compliance is shared by CSPs and their customers. CSPs are responsible for the security of their Cloud System.
and the proper operation of the security features they provide. Customers are responsible for security and compliance with respect to their content and operations in the cloud. Accordingly, customers are fully responsible for selecting a qualified CSP, for ensuring that their content is adequately protected in the CSP’s Cloud System by using the security features required by law or regulation or otherwise offered by the CSP, and for ensuring that they do not transfer any Level 3 content outside the KSA unless permitted by KSA law or regulation. CSPs will not be responsible or liable for the acts or omissions of their customers or the customers of other CSPs who use their Cloud System. The customer is solely responsible for its failure to fully implement the security features provided by the CSP, including all security features required by law or regulation, including responsibility for any damages caused by such failure or that could have been prevented by proper use of all security features.

It is also up to customers to comply with any rules they are bound under, for example, any applicable internal corporate policies, instructions from management or sector-specific regulation (e.g., for banks and financial institutions, hospitals etc.). CSPs do not have an obligation or even the capability to monitor their customers’ data and content, let alone assess independently whether these are confidential or secret.

In the case of individual customers, the Regulatory Framework establishes a presumption that any information these customers store or process is Level 1 information. The corresponding default option for private sector legal persons, such as companies, other corporate entities, associations or organisations that are incorporated or have a Customer Address in the Kingdom is Level 2.

If the customers in question consider that part or the whole of any such content is sensitive and are ready to pay for any added security measures required for such higher levels, they must secure that information accordingly. Because CSPs do not monitor or review the customer’s content, it is the customer's responsibility to ensure that it is using all required security features depending on the content level. Customers should ensure that their CSP can provide them with all the necessary features to help the customer ensure compliance before placing content in the cloud.

Customers should bear in mind, however, that obligations for CSPs under the Regulatory Framework may be difficult, and sometimes impossible, to enforce against CSPs that are not registered in the KSA, in line with the relevant provisions of the Regulatory Framework on Cloud computing. An obligation for such a registration exists only for CSPs that have a datacentre or other essential Cloud infrastructure in the territory of the Kingdom.
The Regulatory Framework requires CSPs to notify their affected customers in case of an information leakage or security breach. If such an incident concerns Level 3 content or is significant, CSPs also have an obligation to notify the Commission as well.

The Regulatory Framework further allows customers to request information about the CSPs’ insurance coverage in order to be able to assess their exposure to risk and decide on their own insurance coverage.

### 4.2. Data protection

Data protection refers to the protection of, first and foremost, personal data or other personally identifiable information of individuals. Put simply, it can be interpreted as the CSP’s obligation to not share customer data with others.

As there are no general and comprehensive rules on personal data protection in the Kingdom, the Regulatory Framework addresses this issue in a Cloud context, by introducing a set of minimum data protection rights that CSPs need to respect. Moreover, the scope of these rules in the Regulatory Framework is not limited to personal data of individuals but covers all types of customer data, including business information that would not normally qualify as ‘personal data’.

Examples of such business data protected as customer data under the Regulatory Framework include Cloud customers’ prices, data on their personnel, product or customer lists, their financial, audit and security data, and their business and product development data, even if such data or other information are in public domain, unless the Cloud Customer has agreed otherwise.

The Regulatory Framework explicitly prohibits the dissemination of Cloud customers’ content or data to third parties, unless this is required under the laws of the Kingdom, or the customer provides his express prior consent.

The Regulatory Framework also requires CSPs to grant their customers the right and technical possibility to access, verify, modify or delete their data that are stored on the Cloud.

### 4.3. Customer protection

The Regulatory Framework has defined a minimum set of customer protection rules for Cloud contracts. These do not protect individual customers only, but all types of Cloud customers that consume Cloud services, thus also including enterprises.
Under these rules, CSPs have an obligation to provide clear and transparent information in their contracts for potential customers, such as a description of the service, conditions of use and applicable payment terms. The Regulatory Framework gives Cloud customers the right to retrieve their data stored in the CSP’s system, if the Cloud contract is terminated.

Furthermore, the Regulatory Framework limits the CSPs’ right to exclude their liability unreasonably or to impose unfair contract terms related, for instance, to loss of, or damage to, customer’s data, quality of service degradations such as service unavailability, or data breaches. However, CSPs may fully exclude certain damages and losses, including indirect, incidental and consequential damages and loss of revenue or profits. CSPs may further limit or exclude liability in situations where the customer has failed to use recommended practices for data security, data durability (e.g. redundant storage), and service availability (e.g. utilization of recommended high availability solutions). CSPs may limit liability to service credits for certain performance failures and may also limit their total liability to a reasonable maximum amount associated with fees paid related to particular content or services affected by a material breach. For example, a CSP may limit liability to the trailing six months’ service fees paid by the customer related to affected content, or may provide a service credit associated with service disruptions that are outside the standard service terms or service level agreements. Such credits would be based on the type and duration of the service disruption, including whether the customer had properly architected its services to provide for high availability. A limitation of liability should be considered reasonable if it is consistent with limitations of liability commonly agreed upon by CSPs and their customers worldwide. Notwithstanding the foregoing or the liability-related provisions in the Regulatory Framework, CSPs and customers who are not individual consumers (e.g. companies, organizations and governmental agencies) can negotiate whatever liability-related provisions they choose.

Enterprises wishing to obtain more details on their rights and obligations under the Regulatory Framework and other information on Cloud Computing in the Kingdom are invited to consult the Commission’s website.