AN OVERVIEW ON THE GLOBAL GOVERNMENTAL EFFORTS ON FOSTERING THE USE OF CLOUD COMPUTING

31/12/2020
EXECUTIVE SUMMARY

1. OVERVIEW OF THE CLOUD MARKET
   1.1. Private Cloud Services
   1.2. Public Cloud Services
   1.3. Community Cloud Services
   1.4. Hybrid Cloud Services
   1.5. Types of Cloud Computing
   1.6. Key Benefits of Cloud

2. WORLDWIDE PUBLIC CLOUD SERVICES MARKET OPPORTUNITY
   2.1. Cloud Ecosystem
   2.2. Global Cloud Drivers
   2.3. ITU Initiatives

3. CLOUD REGULATORY FRAMEWORKS
   3.1. United States
   3.2. United Kingdom
   3.3. South Korea
   3.4. Saudi Arabia

4. DATA SOVEREIGNITY/DATA PROTECTION AND GOVERNANCE POLICIES
   4.1. United States
   4.2. European Union
   4.3. Australia
   4.4. Saudi Arabia

5. CLOUD-FIRST STRATEGIES
   5.1. United States
   5.2. United Kingdom
   5.3. Japan
   5.4. The Nordics
   5.5. Benelux
   5.6. Germany
   5.7. Bahrain
   5.8. Saudi Arabia

6. GOVERNMENT CLOUD MODELS
   6.1. United Kingdom
   6.2. United States
   6.3. Japan
   6.4. Australia
   6.5. Saudi Arabia

7. CONCLUDING REMARKS

REFERENCES
Cloud adoption has been growing rapidly in the recent years due to key benefits such as cost savings, scalability, security, ease of deployment. The growth in cloud adoption also brings about its own set of challenges like data privacy and security. Cloud services are often classified as regulated approaches by government bodies for data privacy and security especially for Government/Semi-Government and vital sectors. Communications and Information Technology Commission (CITC) has taken purposeful measures to bring in policy frameworks for cloud services to encourage healthy development of the cloud ecosystem in the Kingdom of Saudi Arabia (the Kingdom or KSA).

The International Telecommunication Union (ITU) has been undertaking many initiatives around standardization of cloud services since 2010 by developing the technology vocabulary, reference architecture, information security controls and end-to-end resource management. A lot of emphasis has been given on the way the data is stored on cloud and the way it is handled by the cloud service providers.
CITC and the Ministry of Communications and Information Technology (MCIT) have taken timely measures in bringing cloud services under the ambit of regulations. CITC’s Cloud Computing Regulatory Framework (CCRF) that was published in February 2018 touches upon several key cloud regulatory areas on the registration of cloud service providers. The CCRF was updated and republished in December 2020, as the new version shows more enablement for cloud service providers by rearranging the cloud service provider’s registration levels, aligning with data and cybersecurity requirements, and creating a special track for providers classified as SMEs. For example, the CCRF clearly outlines the data classes for customer data, regulations for the protection of customer data, customer protection, content filtering, and commissioning of powers. The usage of cloud services in the public sector is directly governed by the ‘Cloud First Policy’ published by MCIT in October 2020. These measures put the Kingdom ahead of a number of developing markets.

Cloud services have been directly brought under rigorous data privacy laws such as the 'CLOUD Act [1]' of the US government, the United Kingdom's "Data Protection Act[2]", the European Union's General Data Protection Regulation (GDPR) [3], the 'Australia Privacy Act [4], and Saudi Arabia's NDMO National Data Governance Interim Regulation [24]. The cloud policy landscape is also shifting towards the 'Cloud First Policies' and the Government Cloud or Community Cloud deployment policy frameworks, which are already in effect in countries such as the US, UK, Japan, Germany, and in countries such as KSA, UAE and Bahrain within the region.
Over the past decade, cloud computing has become a significant alternative to IT sourcing for organizations all over the world. An increasing number of infrastructure and software services are being supplied in the cloud.

Cloud services are fundamentally about an alternative solution composition, delivery, and consumption model — one that can be applied to IT industry offerings but also, much more broadly, to services from many other industries, including entertainment, energy, financial services, health, manufacturing, retail, and transportation as well as the government and education sectors.

The cloud model goes well beyond prior online delivery approaches — combining efficient use of multitenant (shared) resources, radically simplified "solution" packaging, self-service provisioning, highly elastic and granular scaling, quick to deploy, flexible pricing, virtual and online — to make offerings dramatically easier to deploy and cheaper to consume. The cloud services are typically deployed under four models and comes in three main types\(^1\). The models being private cloud, public cloud, community cloud and hybrid cloud. The types are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Applications as a Service (SaaS).

### 1.1. Private Cloud Services

Private cloud services are shared within a single enterprise or an extended enterprise — with restrictions on access and level of resource dedication and defined-/controlled by the enterprise; can be onsite or offsite; and can be managed by a third-party or in-house staff. In a private cloud that is managed by in-house staff, "vendors (cloud service providers)" are equivalent to the IT departments/shared service departments within enterprises/groups. In this utilization model, where standardized services are jointly used within the enterprise/group, business departments, offices, and employees are the "service users." Key benefits offered by private cloud services include better control over their data, security risks being relatively lower through using firewalls specific to the business requirements. However, building a private cloud could lead to very high up-front costs, ongoing maintenance costs and separate costs for securing their cloud infrastructure, and may lead to lack of disaster recovery options.

---

Public cloud services are shared among unrelated enterprises and consumers; open to a largely unrestricted universe of potential users; and designed for a market, not a single enterprise. Public cloud services are known to deliver better scalable and reliable services cost-effectively, lowering up-front costs, and better disaster recovery capabilities. On the flip side, factors such as cyber security threats, limited flexibility in terms of configuration and security, inability to meet certain data privacy and compliance requirements are cited as the usual challenges of the public cloud services. There are thousands of Public cloud applications that are currently available across the world that can be consumed online.
1.3. Community Cloud Services

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared and aligned interests (e.g., mission, cybersecurity requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or a combination of these. The physical location may be on or off premise. The CSP guarantees the Service Level Agreements (SLAs) and uptime and also manages the data redundancy. This model offers a “plug and play” model which allows for faster timelines for deployment of new solutions. A common form of community Cloud for the Public sector is a Government-owned community Cloud, which is often cited as “G-Cloud” or “Government Cloud”. This is a Cloud typically fully owned by a Government, and provisioned for the exclusive use of Governmental authorities. Operations for this Cloud could be done by a Governmental authority, a third party (e.g. a CSP) or a combination of these. It is typically located inside the country, mainly to protect data sovereignty.

1.4. Hybrid Cloud Services

The term "hybrid cloud services" is used to describe the consolidated coordination/management of multiple cloud services. Hybrid cloud services include "public/public," "public/private," and "private/private" combinations. The service has proven to be very effective in scenarios where the enterprise workloads change frequently or dynamically and for separating critical workloads from less-sensitive workloads. The hybrid service model is also beneficial for organizations interested in making incremental move to the cloud and for businesses requiring temporary processing capacity needs. However, on the flip side, the need to keep a track of multiple platforms and vendors, requires more complex IT management skills to manage both the public and private cloud environments and the associated costs. Moreover, the security risks associated with Public Clouds are known to be the usual challenges of the hybrid cloud services. A multi-Cloud approach, a similar model, is a composition of two or more distinct cloud infrastructures but without necessarily connectivity or orchestration between them. Such approach is globally encouraged.
Cloud services can be broadly grouped into the following three types:

- **IaaS.** Infrastructure as a Service (IaaS) are highly scalable and automated compute resources. IaaS allows businesses to purchase compute resources on-demand and when needed rather than having to make an outright hardware purchase. IaaS delivers compute infrastructure, including servers, network, operating systems, and storage, through virtualization technology. These public cloud services are typically provided to the organization through a dashboard or an Application Programming Interface (API), giving clients complete visibility into the usage.

- **SaaS.** Software as a Service (SaaS), represents the most commonly used delivered services for businesses. SaaS services are Internet-delivered applications, which are managed by a third-party vendor on behalf of the users. These days majority of SaaS applications run directly through web browsers and they do not require app downloads or installations. SaaS vendors take the responsibility of managing all potential technical issues, such as data, middleware, servers, and storage ensuring streamlined maintenance and support.

- **PaaS.** Platform as a Service (PaaS), provides cloud components of software platforms mainly for application development. PaaS provides a framework for the developer community so that they can use it to create specialized applications. Under this delivery model, servers, storage, and networking may be managed by the enterprise or a third-party provider, while the developers can maintain management of the applications. The delivery model of PaaS is similar to that of SaaS. However, instead of delivering the software over the internet, PaaS provides a platform via a web browser allowing developers to create applications with no bearing on operating system, software updates, storage, or infrastructure.
1.6. Key Benefits of Cloud

**Cost Reduction.**

Cloud services drive operational efficiencies and reduce IT costs. This feature means that companies will not be required to make large upfront capital expenditure on purchasing and maintaining equipment, platforms, or applications, thus having the potential to drive down the CAPEX costs. It also removes costs associated with datacenter hardware, facilities, and utilities when scaling up IT infrastructure. Organizations will also be able to minimize costs associated with maintaining large IT teams to handle data center operations. Besides, use of services offered by hyperscale service providers promises very high uptime which means companies will be able to reduce downtime costs.

**Scalability.**

Scalability is one of the top advantages of public cloud services. Companies of different sizes and belonging to various industries have their unique IT needs. Further, depending upon the nature of the business and the local market dynamics, organizations may require efficiently and quickly scaling up or scaling down their IT operations and this is where public cloud services could play a major role. Thus, Public Cloud services are ideal for businesses with growing or fluctuating IT requirements. For example, organizations experiencing rapid growth in IT requirements may embrace public cloud services without investing in physical infrastructure. Scalable solutions such as cloud can minimize the risks associated with operational issues and provide access to skilled resources for professional solutions without a need for up-front investments.

**Data Security.**

Cyber security is one of the major concerns for organizations of all sizes and industries. Cyber-attacks can adversely affect organizations’ revenue, customer loyalty, and brand image. Cloud services are known to offer advanced security features that guarantee the security of data stored on the cloud. As such, cloud service providers implement baseline protections for their platforms and the data through authentication, access control, and encryption. Several organizations using public cloud services supplement these protections with added security measures to support data protection and tighten access to sensitive information on the cloud.
**Disaster Recovery.**

Besides data security, data loss is a major concern for the majority of organizations. Storing data in the cloud makes it always available having no bearing on the end-point equipment such as laptops, PCs, or mobile devices. Usage of cloud-based services, data recovery becomes almost certain in all kinds of emergency scenarios, including natural disasters, power outages, or cyberattacks. Thus, cloud infrastructure helps in the prevention of losses associated with the loss of valuable data. If companies rely on the traditional on-premises approach, all their data will be stored locally, on a local datacenter or office computers. Despite best efforts, organizations may realize that it is almost impossible to recover their locally stored data on datacenters or computers. However, cloud stored data, provides very high levels of accessibility, and recoverability as long as there is reliable connectivity.

**Control.**

Public cloud services also offer a very high level of control over privileged data by allowing organizations to decide on user access policies. Cloud offers organizations with complete visibility and control over user data and ensures that the right employee gains the right level of access to the right set of data. This feature also drives process efficiencies and productivity. It also allows employees to collaborate effectively without having to worry about version control.
Enterprises’ continuing strategic focus on digital innovation and transformation, to remain competitive in their industries, will be the key driver of cloud growth. Most of these initiatives (and resulting digital innovations) will deploy cloud technologies and solutions to power them, making digital transformation the number one driver of cloud spending in the foreseeable future. The major cloud platforms — and their expanding solution ecosystems — are becoming the "launchpad" for virtually all tech innovation. This development of tech innovation comes from the key public cloud suppliers, making it virtually impossible for enterprises (and developers) to seek an advantage not to embrace the public cloud.

The accelerating migration of enterprise application providers to the SaaS model also brings their customer bases along with them to the public cloud. Additionally, the expansion of cloud-related managed services and professionals allows organizations to more quickly and easily assess, adopt, integrate, and manage cloud services within their overall IT portfolio.

Increasing, intense competition among the major cloud service platform players has continued to drive down prices, raise support quality, and stimulate a tech innovation "arms race" that has dramatically benefitted technology ecosystem partners, enterprises, and consumers.

Over the past several years, the major public cloud services suppliers have introduced a steady stream of innovative new IT services, including a wide variety of AI-related services, blockchain services, IoT back-end services, AR/VR back-end services, robotics back-end services, encryption services, container services, serverless computing services, and even new computing hardware services Graphics Processing Unit (GPU), Field-Programmable Gate Array (FPGA), AI-optimized processors, and Quantum computers). The pace of IT innovation launches on public clouds will continue and, more likely, accelerate. As a result of this, developers seeking access to the latest IT innovations will likely find them on one or more of the major public cloud platforms.
Looking at the cloud market, the cloud ecosystem can be clustered into 5 clusters which include companies ranging from infrastructure providers to multi-cloud integration/management platforms.

- **Cloud Mega-platforms.** These are the big global providers of horizontal-/foundational cloud-based IT services.

- **App-centric Platforms.** Companies here are focused on providing platforms that support business solutions, services, and processes (usually ride on top of one or more cloud mega-platforms).

- **Industry Platforms.** These are industry-focused app-centric platforms, focused on delivering an ecosystem of data, services, and solutions to customers within a single industry or among related industries, which is a rapidly growing community. Most players are not traditional technology providers but leaders within an industry. However, traditional technology providers – especially those competing in the app-centric platform cluster also enter the industry platform world.

- **Multi-cloud Integration and Management Platforms.** This cluster includes companies that help enterprises integrate and manage across multiple clouds. As of now, this cluster is in a primordial state, consisting of a "soup" of diverse players up and down the stack, many of which are not yet platform-based: network connectivity players, managed service providers, global and regional systems integrators, distributors Value Added Resellers (VARs), and more.

- **Cloud-centric Infrastructure and Connectivity.** Every platform requires real hardware/infrastructure to function, in addition to connectivity infrastructure providers to provide cloud connectivity. Thus, this cluster includes infrastructure and network services providers.
Each country is at a different stage in its cloud journey. A country’s cloud maturity depends on several factors including but not limited to its network infrastructure, government initiatives, and digital literacy which are detailed below.

The key drivers affecting cloud adoption are:

- **Broadband Footprint.** Cloud infrastructure maturity heavily depends on the level of broadband infrastructure for organizations to access public cloud services. Thus, ICT regulators that are serious about developing cloud penetration are also focusing on expanding the footprint of broadband networks, especially fiber network (FTTx).

- **e-Government Initiatives.** The growing investments in digitizing economies or implementing e-government services is indirectly driving ICT investments.

- **Investments by Telecom Operators.** A number of telecom operators are building datacenter capacity traditionally for hosting and colocation services. However, telecom operators are slowly migrating that capacity for public cloud services through partnerships with hyperscale cloud service providers to ensure data localization.

- **Cloud-First Policies.** A number of countries worldwide, both developed and developing economies, have realized the need to have Cloud-First policies in place. Cloud-First policy aims to migrate from traditional IT solutions to cloud-based models to gain advantages such as enhanced agility, reliability, security and innovation. Cloud-First policies and strategies will significantly enhance the awareness levels of cloud services, thereby contributing to the accelerated adoption of cloud services by public and private organizations. For example, Saudi Arabia’s Ministry of Communications and Information Technology (MCIT) has unveiled its official Cloud-First Policy in October 2020 [5]. The policy is aimed at encouraging public sector migration from traditional IT solutions to cloud-based models. Other countries implementing similar policies in the region include UAE [6] and Bahrain [7].
• **G-Cloud Policies.** Progress countries have realized the importance of Cloud First approach within the government sector and have started implementing Government Cloud (G-cloud) services. This approach is a form of "community cloud", to serve the cloud requirements of government authorities, departments, and close associates securely, cost-effectively, and efficiently. Countries such as the UK, Belgium, and Estonia have a functional G-Cloud service in place. Saudi Arabia has already announced its plans to launch G-Cloud through its National Information Center (NIC) through MCIT's Cloud-First policy.

**In addition to cybersecurity, key inhibitors affecting cloud adoption include:**

• **Lack of Skillset.** Lack of skills relevant to supporting cloud services has been highlighted as a key inhibitor for the cloud adoption in several services. Governments in several countries are taking deliberate measures to develop the digital skillsets required to provide new age services including cloud. However, there is a lot of work remaining to be done in this direction and retaining skilled labor will also emerge as a key challenge.

• **Data Privacy Concerns.** Most of the countries worldwide, both from the developed and emerging economies, already have overarching data privacy laws or industry specific data privacy laws for sectors such as banking and finance, government, retail, and healthcare.

### 2.3. ITU Initiatives

In April 2017, ITU published a document on “Overview of the ITU works on Cloud Computing” [8], presented by the head of department of The Postal and Electronic Communications Regulatory Authority (ARPCE) of Algeria. The document highlights the following areas for cloud computing standardization by ARPCE.

- **Security**
- **Portability**
- **QoS**
- **Data privacy**
- **Interoperability**
- **Integration**

As per the document, a series of technical Focus Group studies were carried out by ITU-T (standardization sector of ITU), and workshops have been conducted to evolve the cloud computing standards and increase its applications in diverse fields of industry.
The cloud computing services market is experiencing healthy double-digit growth globally. Different regions are currently at different maturity stages and sharing some security and data privacy related challenges of varying degrees. Policy makers worldwide are exploring options to address these challenges and thinking of putting policy frameworks on data classification, data handling, and working on data localization and data sovereignty laws. A few policy makers from the developed countries are also working on strategies to address "Cloud-First" and "Government Cloud" needs. These acts are serving as the overarching governing principles for the public cloud services in those countries. In summary, the key priorities of policy makers of public cloud services are as follows:

- To put in place data privacy regulations to provide a level of confidence to consumers about their personal data on the cloud.
- To make enterprises accountable and to put in place specific mechanisms and measures for dealing with the consumer data responsibly.
- To roll out 'Cloud-First' policies or strategies to create mutual opportunities for the local enterprises and cloud service providers. On one hand, this approach is expected to drive business agility and lower the cost of local enterprises’ operations. On the other hand, it will attract investments from both global and local cloud service providers.
- To create a conducive environment for the development of Government Clouds (G-Cloud).

Several international efforts in developing cloud computing regulatory frameworks and their evolution will follow.
3.1. United States

The United States has several industry-specific regulatory frameworks and state-level legislations that oversee data privacy.

In February 2018, the US government passed an act with far reaching provisions for the US government authorities, under the name 'Clarifying Lawful Overseas Use of Data' (CLOUD) Act [1]. The act is a continuation of the "USA Patriot Act [9]" and mutual legal assistance treaty (MLAT), with the EU, which allowed the US law enforcement agencies and their EU counterparts to source data from the communication service providers and the public cloud service providers in the interest of national security and security of their citizens.

The CLOUD Act states that, “A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.” In other words, by means of this act, the law enforcement agencies of the US government will be able to gain access to their resident's information even if it resides in another country, with which US has a "mutual" executive agreement with.

3.2. United Kingdom

The UK government's regulatory framework, in general, is relatively better evolved. Being one of the top countries in the European region, in terms of public cloud spending, the government has taken a proactive approach in streamlining the laws governing public cloud services.

BSA, which was originally founded as Business Software Alliance – now known as the Software Alliance, has published its "Global Computing Scorecard [10]" that measures the countries' preparedness for cloud adoption by taking a number of factors into consideration that include policy areas, privacy laws, cybersecurity laws, and broadband infrastructure. In 2018, the UK was ranked fourth in BSA's Global Computing Scorecard.

The country has improved its ranking over the previous years, by implementing the Data Privacy Act and the National Cyber Security Guidance [11]. The processing of personal data by UK businesses in the country is governed by the UK's Data Protection Act (DPA) of 2018 [12], which is the UK's implementation of the EU General Data Protection Regulation (GDPR).
The Data Protection Act, 2018

The GDPR provides certain provisions to individual member states to interpret and implement it. Although the Brexit discussions are ongoing, the UK took a measure to retain the requirements of GDPR through Part 2, Chapter 2 of the DPA 2018 [12], which should be read alongside the GDPR. By implementing this "applied GDPR", the UK imposed a similar regime of data protection on certain areas that do not fall under the typical scope of GDPR. One such area is data processing by public authorities; for example, the UK’s act lays down data processing regimes for law enforcement and intelligence agencies.

In April 2019, the UK passed an amendment [13] to UK data protection law to this effect in case the country leaves the EU without a deal¹. Through this amendment, the government hopes to attain a status quo situation in terms of the exchange of personal data between the UK and the EU to maintain the current economic relationships and ongoing security collaboration. The UK and the EU are said to have agreed to establish cooperation between the UK’s Information Commissioner’s Office (ICO) and the EU Data Protection Authorities.

In other words, with or without the imminent Brexit, the UK agrees to continue to share its personal data with the European Economic Area (EEA) states, EU and EEA institutions, and some other countries that EU has existing "adequacy" decisions on.

Both GDPR and DPA uses the term "processor" for the service providers such as cloud providers. However, not all the references to a processor necessarily mean a cloud provider. The DPA regulations clearly outline the conditions for data processors in the following situations:

NCSC’S Cloud Security Guidance

The UK’s National Cyber Security Center (NCSC) has released ‘Cloud Security Guidance’ [11] on how to configure, deploy, and use cloud services securely. It provides guidelines on identifying cloud services that are suitably secure for a given purpose of use. The following steps are suggested to help cloud users make the right decisions to identify a secure cloud environment.

¹ Without a Brexit deal with EU, in article 50 Treaty on European Union, EU law and other agreements would cease to apply to the established interactions between the UK and the rest of the EU. Additionally, UK interactions with non-EU countries, which until now have been governed by EU agreements with those countries, may need to be renegotiated.
1. **Understand business requirements.** Cloud users should understand the purpose for using cloud services. They should consider issues such as availability and connectivity and clearly identify the risks which would be unacceptable to the businesses.

2. **Understand information.** Users should identify the types of information that would be processed, stored or circulated using the cloud service and understand the legal and regulatory implications. For example, if personal data is to be stored or processed, then the Data Protection Act will come in to play.

3. **Determine relevant security principles.** The previous steps give the user a clear picture about how to determine which of the Cloud Security Principles are most relevant.

4. **Understand how the principles are implemented.** The user should evaluate cloud service claims to implement the security principles that they have identified as relevant since different approaches will result in different risks.

5. **Understand the level of assurance offered.** To check with the service provider if they could demonstrate the principles identified from step three have been implemented correctly. In this regard, users can have the service providers provide contracts or engage certified, and independent assessors to validate their claims.

6. **Identify additional mitigations that can be applied.** Users should think of any additional measures their organization can apply to help reduce risk associated with applications and information.

7. **Consider residual risks.** Having worked through the above steps, the user will be able to decide if any remaining risks are acceptable.

8. **Continue to monitor and manage the risks.** Once in use, users should periodically review whether the service still meets their business and security requirements.

The Cloud Security Guidance also released 14 Cloud Security Principles together with description, objective, and guidance on implementation of the principles. A detail of the principles has been furnished below.
1. **Data in transit protection.** User data transiting networks to be sufficiently protected against tampering and wiretapping.

2. **Asset protection and resilience.** User data, the underlined assets storing or processing it, should be protected against physical tampering, loss, or damage.

3. **Separation between users.** A malicious or compromised user of a service should not be able to affect the services or another user.

4. **Governance framework.** The service provider should have a security governance framework that coordinates and directs the management of its services and information on their assets.

5. **Operational security.** The service needs to be operated and managed securely in order to obstruct, detect or prevent attacks. At the same time, good operational security should not require complex, bureaucratic, time consuming, or expensive processes.

6. **Personnel security.** Wherever a service provider's staff has access to personal data, they should be trained to treat such data with high degree of confidence and trustworthiness. Regular screening, adequate training of staff reduces the likelihood of accidental or malicious compromise of personal data.

7. **Secure development.** Services should be designed and developed to identify and mitigate security threats. The areas that may not seem obvious sources of vulnerabilities may end up creating security issues that could compromise user data, disrupt service, or even enable malicious activity.

8. **Supply chain security.** The service provider should ensure that their supply chain sufficiently supports the security principles that the service promises to fulfill.

9. **Secure user management.** A service provider should make the necessary tools available to the users to securely avail the services. Management interfaces and procedures are essential part of the security barrier, preventing unauthorized access and alteration of resources, applications and data.
10. **Identity and authentication.** Access to service interfaces should be limited to authenticated and authorized users only.

11. **External interface protection.** All external or less trusted interfaces of the service should be identified and properly guarded.

12. **Secure service administration.** Systems used for service administration should provide very highly privileged access as their compromise would have significant impact on businesses.

13. **Audit information for users.** Users should be provided with audit records needed to monitor access to user service and the data held in it. The type of audit information available to users will provide them with the ability to detect and respond to inappropriate or malicious activity within reasonable timeframe.

14. **Secure use of the service.** The security of cloud services and the data held within them can be undermined if the user does not use services poorly. Thus, users should have certain responsibilities when handling data to ensure it is adequately protected.

On similar lines, the Cloud Security Guidance provides guidelines on data separation measures and deployment models and responsibilities of IaaS service users. NCSC has laid down 13 IaaS principles, along with recommendations and the risk management guidance for the service providers.

### 3.3. South Korea

South Korea had passed an act on the Development of Cloud Computing and Protection of its Users [14] in 2015, to implement policies that facilitate development and use of cloud computing, security and data privacy issues that may arise with a growing utilization of cloud computing in South Korea.

**The act consists of the following chapters.**

<table>
<thead>
<tr>
<th></th>
<th>Chapter Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>General provisions</td>
</tr>
<tr>
<td>2</td>
<td>Creation of basis for the development of cloud computing</td>
</tr>
<tr>
<td>3</td>
<td>Facilitating use of cloud computing services</td>
</tr>
<tr>
<td>4</td>
<td>Enhancement of reliability of cloud computing services and protection of users</td>
</tr>
<tr>
<td>5</td>
<td>Supplementary provisions</td>
</tr>
<tr>
<td>6</td>
<td>Penalty provisions</td>
</tr>
</tbody>
</table>
The act stipulates the establishment of master plans and implementation plans for cloud computing, research and development activities, fostering skilled professionals, implementing pilot projects, and setting up a cloud datacenter to help the Korean government to support the promotion of cloud computing. The Act also mandates the adoption of cloud services in the public sector. Cloud services option is accorded the first priority while implementing national informatization projects. The Act also mandates certain permissions and authorization processes for the cloud computing equipment, mostly when the computing equipment is provided to promote cloud computing utilization in the private sector.

The Act also establishes certain rules for user protection. It mandates cloud service providers to notify incidents, user information leakage, and service termination to users. The 'Ministry of Science, ICT, and Future Planning' gives the users of cloud services the right to know the country where their data is being stored. Additionally, the Act prohibits sharing of user information with a third party without the user's consent or using it for a purpose other than the one stated initially.

While Korea's Personal Information Protection Act (PIPA) [15] and the Network Act [16], which are responsible for promoting cybersecurity and protecting personal information and enhancing data security on IT networks, the Cloud Act provides strict data protection standards within the context of cloud computing. In recent years, the Financial Security Institute published a guideline on the utilization of cloud computing for financial companies. The Ministry of Interior and Safety (MIS) has also published a guideline for public institutions on the utilization of cloud services offered by the private sector. The Korea Internet & Security Agency (KISA) also mandates the cloud service providers to obtain Korea Information Security Management System (K-SIMS) certification. The certification assesses an enterprise or organization's information security management system if it is properly established, managed, and operated. As part of the process, Korea Internet & Security Agency (KISA) or an assessment body appointed by the Ministry of Science and ICT (MSIT) conducts a certification audit.

3.4. Saudi Arabia

CITC set forth the Cloud Computing Regulatory Framework (CCRF) [17], and it clearly outlines the roles and responsibilities of the cloud service providers and the users of different nature, namely individual customers, government agencies, and enterprises. This framework and other related policies and regulations shows that Saudi Arabia is one of the early adopters amongst the majority of countries which issued specific-fit regulations for cloud computing and also clearly describes the governance of responsibility between the CSP and the customer.
In addition, the Guide for Cloud Service Providers [18] lays down the registration requirements for the service providers, which is defined as "any company or corporation engaged, in whole or in part, in the provision of Cloud Services in the Kingdom of Saudi Arabia, which exercises direct or effective control over datacenters or other critical Cloud System infrastructure hosted in the Kingdom and used in whole or in part for the provision of Cloud Services, and shall use telecommunications infrastructure (including international infrastructure) through operators licensed by CITC". The registration requirements include providing a description of the intended services, a description of the cloud systems designed to use, and submission of documents certifying compliance with the technical standards or requirements. Depending upon the type of customers the service providers intend to target their services, the following standards have been set for the Cloud Service Providers (CSPs) in the Kingdom.

Table 1 – Minimum Standards / Requirements for CSPs [18]

<table>
<thead>
<tr>
<th>CSP Class</th>
<th>Minimum Standards / Requirements</th>
</tr>
</thead>
</table>
| Class (A) | • ISO/IEC 27001  
• ISO/IEC 27017  
• ISO/IEC 27018 (or ISO/IEC 27701)  
• Constructed Facility Certificate Tier 2 or above (or ISO/IEC 27001 for the datacenters) |
| Class (B) | Minimum Standards / Requirements of Class (A), plus:  
• Constructed Facility and Operational Sustainability Certificate Tier 3 or above  
• CSA STAR Certification (CSA STAR LEVEL 2) |
| Class (C) | Minimum Standards / Requirements of Class (B), plus:  
The CSP must coordinate with CITC in order to get the final approvals in accordance with policies and regulation in the Kingdom. |

CSPs are also required to provide a description of intended operations, list of licenses held, documentation to be provided in Arabic and English. The CCRF also defines the customer data classes so that the relevant data classes can be brought under the purview of the information security regulations.
## Table 2 – Data Classification [17]

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Top Secret**         | Data shall be classified as “Top Secret”, if unauthorized access to or disclosure of such data or its content adversely and exceptionally affects in a way that is difficult to resolve:  
  - National interest including violations of conventions and treaties, adverse damage to the reputation of the country, diplomatic relations and political affiliations, operational efficiency of the security or intelligence operations of military forces, national economy, national infrastructure and Government functions, and/or  
  - The Kingdom’s government entities functionality causing damage to the national interest, and/or  
  - Individuals’ health and safety at massive scale and privacy of Protected Individual personnel, and/or  
  - Catastrophic damage to the environment or natural resources |
| **Secret**             | Data shall be classified as “Secret”, if unauthorized access to or disclosure of such data or its content adversely affects:  
  - Affects national interest such as damage to the reputation of the country, diplomatic relations, operational efficiency of the security or intelligence operations of military forces, national economy, national infrastructure. Government functions, or the investigation of major cases such as terrorism funding and/or  
  - Financial loss that leads to bankruptcy or inability of organizations to perform their duties or major loss of competitive abilities or combination thereof, and/or  
  - Causes significant harm or injury impacting life of individuals  
  - Causes long-term damage to the environment or natural resources |
| **Confidential**       | Data shall be classified as “Confidential” data, if unauthorized access to or disclosure of such data or its content causes:  
  - Contained negative affect on the Kingdom’s government entities’ operations, the Kingdom’s economy, and/or  
  - Damage to any entity’s assets and limited loss to its financial and competitive status, and/or  
  - Negative effect on individual’s interests  
  - Contained damage in the short-term to the environment or natural resources |
| **Public**             | Data shall be classified as “Public”, if unauthorized access to or disclosure of such data or its content has no impact on:  
  - National Interest, or  
  - Organizations, or  
  - Individuals, or  
  - Environment |
| **Government Related Data** | Government Related Data: to be classified as received from any government entity based on the levels above:  
  - Other: Not covered by what is mentioned above.  
  - Acts, regulations, policies, and decisions issued by the National Data Management Office or the sector regulators supervising the customer  
  - must be taken into consideration.  

<table>
<thead>
<tr>
<th>Customer Data Classification</th>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
</table>
|                              | Top Secret | Data shall be classified as “Top Secret”, if unauthorized access to or disclosure of such data or its content adversely and exceptionally affects in a way that is difficult to resolve:  
  - National interest including violations of conventions and treaties, adverse damage to the reputation of the country, diplomatic relations and political affiliations, operational efficiency of the security or intelligence operations of military forces, national economy, national infrastructure and Government functions, and/or  
  - The Kingdom’s government entities functionality causing damage to the national interest, and/or  
  - Individuals’ health and safety at massive scale and privacy of Protected Individual personnel, and/or  
  - Catastrophic damage to the environment or natural resources |
|                              | Secret | Data shall be classified as “Secret”, if unauthorized access to or disclosure of such data or its content adversely affects:  
  - Affects national interest such as damage to the reputation of the country, diplomatic relations, operational efficiency of the security or intelligence operations of military forces, national economy, national infrastructure. Government functions, or the investigation of major cases such as terrorism funding and/or  
  - Financial loss that leads to bankruptcy or inability of organizations to perform their duties or major loss of competitive abilities or combination thereof, and/or  
  - Causes significant harm or injury impacting life of individuals  
  - Causes long-term damage to the environment or natural resources |
|                              | Confidential | Data shall be classified as “Confidential” data, if unauthorized access to or disclosure of such data or its content causes:  
  - Contained negative affect on the Kingdom’s government entities’ operations, the Kingdom’s economy, and/or  
  - Damage to any entity’s assets and limited loss to its financial and competitive status, and/or  
  - Negative effect on individual’s interests  
  - Contained damage in the short-term to the environment or natural resources |
|                              | Public | Data shall be classified as “Public”, if unauthorized access to or disclosure of such data or its content has no impact on:  
  - National Interest, or  
  - Organizations, or  
  - Individuals, or  
  - Environment |
|                             | Non Government Data | Government Related Data: to be classified as received from any government entity based on the levels above:  
  - Other: Not covered by what is mentioned above.  
  - Acts, regulations, policies, and decisions issued by the National Data Management Office or the sector regulators supervising the customer  
  - must be taken into consideration. |
It also mandates the CSPs to inform both the customers and CITC about any data breaches that might have taken place. Moreover, the CCRF requires the CSPs "to inform their Cloud Customers, upon their request, of any insurance coverage that those CSPs have for any civil liability to those Cloud Customers". Also, CCRF requires CSPs to adopt internal rules and policies on business continuity, disaster recovery, and risk management. Further, CCRF lays down customer data protection regulations that the CSPs are required to comply with. One of the essential provisions that was offered to empower customers is as follows: "CSPs shall grant Cloud Customers the right and the technical capability to access, verify, correct or delete their Customer Data in a way that does not conflict with The National Data Management Office (ND-MO)'s regulations related to personal data".

CCRF also provides instances of "unlawful infringement of content". One of the key provisions is: "CSPs must refer to any third parties, except for the component authorities, complaining against Unlawful Content or Infringing Content on their Cloud System to the competent authorities in the Kingdom, only if they decide not to resolve such complains directly according to provision 3-5-5". CCRF also provides regulations on mandatory content under "Cloud Contracts". Besides, the CCRF protects customers against unfair cloud contract terms. Thus, CCRF is certainly a good starting point from CITC's point of view to cover all the key areas of the cloud regulatory framework. CITC is planning to update the CCRF to suit the changing competitive and market dynamics.
Data protection legislation is seen as a way for governments to react to the mounting number of security breaches. Regulations are a way for the government bodies to take back the control of sensitive use data. Governments are enforcing stringent data protection policies to mandate companies to take the highest possible measures to secure their customers’ data privacy and protection. Companies are also taking these regulations seriously as data breaches have had serious consequence to their brand reputation and loss of trust of their customers. On the flipside, regulatory compliance is becoming a time consuming and expensive proposition for a few organizations. It requires them to update their internal policies and upgrade their cyber security infrastructure. Another major concern for organizations is the massive fines that they might have to incur in the event of non-compliance.

4.1. United States

In the US, there is no common law or regulation on data privacy which is applicable to all states or industries at federal level. Every state has its own separate law for ensuring data privacy in its jurisdiction. Some of the well-known laws passed by the US government are as follows [19]:

- **Family Educational Rights and Privacy Act (FERPA).** Enacted in 1974, this law refers to the privacy of student immunizations and other school health records

- **Children’s Online Privacy Protection Act (COPPA).** which protects children’s data and also protects the online privacy of children under the age of thirteen

- **Consumer Privacy Bill of Rights.** These are processes and procedures that organizations should put in place to handle consumer information.

- **Fair Information Practice Principles (FIPPs).** These are processes and procedures that organizations should put in place to handle consumer information.
HIPAA. One of the most important industry specific regulation is the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule [20], which ensures the data privacy of individuals. The HIPAA Privacy Rule are a set of national standards that safeguard patients' personal information and health care transaction records maintained by healthcare providers. It protects the privacy of personal health information and sets restrictions on the dissemination and use of individual health information without patients' authorization. The Privacy Rule provides patients with rights to access and edit their health information.

However, the most comprehensive regulations of all being California Consumer Privacy Act (CCPA), which was approved by the California State Governor on 28 June 2018 [21]. The act which went into effect from 1st January 2020 is expected to set new standards of data protection for the State of California and for the country as a whole. California is home to a very large percentage of mid-sized and large enterprises including several multinational companies, which necessitated a strict law on data privacy.

Under the California Consumer Privacy Act (CCPA), the Data Sovereignty rules and regulations for cloud service providers in USA are highlighted below:

**Encryption of Data.** Cloud is being used to store data, which can be easily accessed over the internet for frequent use. This data also involves Personally Identifiable Information (PII) which is highly regulated by the CCPA. The PII can be broadly defined as any information related to an individual, right from his name, to location data, to employment information and much more. Encryption of such critical information is the first and most critical step for a cloud service provider to ensure.

**Clear Visibility and Classification of Data.** There is huge amount of data on the cloud. It is crucial for cloud service providers to ensure that the data is properly sorted and arranged so that the content can be classified based on its sensitivity which gives the controller a good understanding of which information can be placed on a sanctioned cloud and which on an unsanctioned cloud¹. A sanctioned cloud contains data in applications that are supported by the business and information technology teams.

**Ability to Monitor and Control.** Under this regulation a cloud service provider (referred to as "processor") is mandated to provide full control to customers (referred to as "controller") of their data. This also involves providing con-

---

¹-A sanctioned cloud handles workload with confidential business data. These services serve organizational cloud security standards to ensure the protection of industrial data, which is stored online. Unsanctioned cloud services are the ones that enable an individual to work with industry data on any public or unsecure online platform.
trollers with the authority to block unauthorized access of data by the processor.

- **Digital Rights Management (DRM).** Under this regulation the cloud service provider is bound to secure customer data even if the data is moved out of the organization. However, as per the business needs, information sharing is a common practice across organizations. To ensure the sovereignty of this data, digital rights management provides the right encryption and digital signatures to documents.

- **Collection of Audit and Log Data.** This regulation enforces the cloud service provider to support compliance assessment as per any other compliance law. This regulation is crucial for the customers as it is important for them to understand who accessed their sensitive cloud data, when and specifically what data elements were accessed.

### 4.2. European Union

Data Sovereignty rules and regulations for cloud service providers in European Union (EU) fall under General Data Protection Regulation (GDPR) [3] and they are as follows.

- **Cloud provider to store data in European Economic Area (EEA).** Data on the cloud can be stored anywhere depending on the location of the data center. However, under GDPR, the cloud service provider must ensure that the data is stored locally in the EEA by setting up a local data center.

- **Retention of Data on Cloud.** Personal data which is being stored on a cloud should not be kept for longer than the predefined period. Therefore, data should be effectively deleted when the retention period expires. However, it is also important for the cloud service provider to consider as to how backups are secured and how retention is managed for storing data locally following the geographic jurisdiction of the GDPR.

- **Data Portability Rights to the Controller.** The controller should be provided with the right of data portability by the cloud service provider so that the controller can retrieve the data in a structured, commonly used and machine-readable format to provide it to a data subject or another controller.

- **Breach Response and Coordination.** The cloud service provider must clearly define the procedure which will be followed in event of a breach in the system. All protocols must be clearly indicated in the contract.
Data Protection Impact Assessment (DPIA). The cloud service provider is subject to third party risk management assessment of any organization who is in a contract with them.

Visibility Regarding Metadata and Data Minimization. A cloud service provider needs to specify what level of protection it would provide for metadata, who would have the ownership rights of the metadata, the intended uses of metadata and the rights of the controller to opt out of collection or distribution of metadata.

Transparency on the IT Security Standards. The cloud service provider should comply with the IT security standards of the customer and, if need be, they should be able to extend the privacy measures or certifications.

4.3. Australia

Data Sovereignty rules and regulations for cloud service providers are provided in Australia's Privacy Act 1988 [4]. Although it is one of the oldest data privacy acts, a few regulations were added subsequently to make it relevant for the recent global technology developments. Those added regulations are Privacy Regulations, 2013 [22] and Privacy Amendment (Notifiable Data Breaches) Act of 2017 [23]. The key regulatory provisions under Australia's Privacy Act are as follows:

- Cloud providers must notify as to what personal information will be collected from the customer and state the intended disclosure arrangements, including any offshore storage destinations intended to be used.

- It is mandatory for cloud providers to provide access to the personal information upon request by a customer and at the same time take reasonable steps to correct any discrepancy in personal data on request.

- It is the sole responsibility of a cloud provider to take reasonable steps to secure customer personal data from misuse, interference or loss and from unauthorized access, modification or disclosure, and also take care of any security breaches that might occur offshore.

- When dealing with disclosure of personal data outside of Australia, the cloud provider must take necessary steps to ensure the overseas recipient does not breach the data privacy regulations of that region.

- It is the cloud provider's reasonability to remove or de-identify personal information that is no longer needed for the purpose for which it was collected.
In the past couple of years, relevant government authorities, i.e. CITC, NDMO and The National Cybersecurity Authority (NCA), took an initiative to classify data, set its governance and set cybersecurity requirements for cloud computing for the goal of protecting national security and interests, data sovereignty, and to safeguard public’s personal data and also to govern roles and responsibilities amongst authorities and individuals. Such policies and regulations allow also data sharing and prevent data duplication while protecting authorities and their data.

The first version of CITC’s CCRF contained a four-level Costumer Content Classification based on information security; Level 1 included non-sensitive customer content of individuals or private sector companies, not subject to any sector-specific restrictions on the outsourcing of data and gradually into Level 4 which included highly sensitive or secret Customer Content belonging to relevant governmental agencies or institutions. In December 2020, version 3 of the CCRF was announced [17]. It included Data Classification which in line with NDMO’s National Data Governance Interim Regulations (NDGIR) that was published in June 2020 [24]. The NDGIR sets the policies and regulations required for data classification, data sharing, and data privacy. It also demonstrates the relationship and interdependencies of Data-specific policies and regulations within data lifecycle; data creation, data storage, data transfer, data usage, and data retirement. It also includes a number of key principles and has classified data into 4 classifications which is mostly mentioned in Table 2 above.

In 2020, the NCA has published the Cloud Cybersecurity Controls (CCC) which builds on the Essential Cybersecurity Controls (ECC) that was made public in 2018 [25, 26]. The CCC was written on the perspective of two stakeholders, namely CSPs and Cloud Service Tenants (CSTs). The regulation aims to set the minimum cloud cybersecurity requirements for both stakeholders. It includes 4 main domains and 24 subdomains. The main domains are: Cybersecurity Governance, Cybersecurity Defense, Cybersecurity Resilience, and Third party Cybersecurity.

In addition, building on HRH the Crown Prince of Saudi Arabia’s two initiatives to boost cybersecurity that were announced during the Global Cybersecurity Forum in February 2020, a partnership has been built between NCA and ITU to develop a practical cooperation that focuses on constructing a global program to protect children in cyberspace revolving around the development of best practices, policies and programs by driving the adoption by teachers, families and other decision makers [27]. According to NCA, the second initiative focuses on empowering women in cybersecurity. It pivots on stepping up efforts to encourage and support women in cybersecurity and enabling them to obtain the education and qualification necessary to allow them to participate effectively in building the cybersecurity sector and to assume leadership positions within it [28].
With the realization of benefits offered by the cloud services, both enterprises and governments alike, in the developed economies, are considering Cloud-First strategies as an alternative for the traditional in-house do-it-yourself (DIY) investments. Cloud-First policies are being formulated to drive operational efficiencies, save on IT budgets, derive benefits out of scalability, and ensure data back-up and recovery. Simultaneously, the adoption of cloud services brings its own cybersecurity and data privacy compliance requirements, which are to be addressed for an efficient implementation of a cloud-first policy.

5.1. United States

The US is recognized as a leader in Cloud and released a Cloud First policy as early as 2011, recognizing the potential to address inefficiencies in the Federal Government’s IT environment and to promote innovation.

The Office of Management and Budget (OMB) has pledged to update the Government’s legacy Federal Cloud Computing Strategy [29]. As part of this decision, the Administration has developed a new strategy to accelerate the adoption of cloud-based solutions, known as "Cloud Smart". This is with reference to the Report submitted to the President on Federal IT Modernization, released in 2017 in accordance with Executive Order 13800. The strategy sets out clear guidelines for identifying services to move to the Cloud and provisioning Cloud services effectively. These efforts were supported by a Government Cloud computing community and resources such as a centralized online storefront. Among other things, the policy aimed to ensure that agencies considered potential security benefits of Cloud alongside any potential vulnerabilities.

The Federal Cloud Computing Strategy establishes a Cloud First principle with the purpose of helping the Federal Government in reaching the level of productivity that the private sector is realizing through Cloud computing. It requires
5.2. United Kingdom

Agencies to evaluate safe and secure Cloud Computing options before making any new investments. Similar principles were subsequently considered or implemented by a number of other countries internationally like UK and Bahrain. The Cloud Smart strategy is formulated on three pillars: security, procurement, and workforce. These three elements will be used for IT modernization in order to provide improved return on investments, enhanced security, and higher quality services to the US residents and its citizens.

Analysis by the Government Accountability Office (GAO) has documented the growth of Cloud adoption at seven agencies, finding that the number of Cloud services increased from 21 to 101 between 2012 and 2014, achieving savings of around $96 million [30], based on analysis of just a minority of the services used.

More recently, the US President signed an Executive Order on cybersecurity mandating that federal systems move to the Cloud.

In the UK, a Cloud First Policy was published in 2013 [31] to mandate that central Government agencies consider and fully evaluate potential Cloud solutions before considering other options. This approach was also strongly recommended across the wider public sector. To support this policy, the Government created G-Cloud, which consists of a series of framework agreements [32] with suppliers, to streamline procurement; and an online store where public bodies can search for services covered by these agreements.

There has been a strong focus on promoting cloud computing as part of broader digital society in the UK. However, there is potential to further promote awareness of cloud and its benefits, and to help stakeholders address concerns or uncertainty about security in the cloud.

In March 2017, the Government published its Digital Strategy 2017 [33], including objectives that should help create an enabling environment for Cloud:

- Building world-class digital infrastructure and connectivity
- Improving digital skills and inclusion
The Asian Cloud Computing Association (ACCA) ranked Japan in the fourth place in cloud market in Asia and Oceania in their Cloud Readiness Index [34], being ranked among the top Asian markets for almost all categories used in the rankings, including broadband quality and intellectual property protection. Japan is also recognized as a global leader in fostering innovation and digitalization and is ranked second by the BSA for its policy environment in relation to cloud specifically [10]. The country benefits from advanced connectivity, as successive broadband plans in the country resulted in comprehensive fiber-to-the-home deployment, while the ACCA has noted recent amendments to the Act on the Protection of Personal Information (APPI) [35] and the establishment of a new central data protection regulator as positive developments.

The Japanese government began to examine Cloud adoption for the public sector with the “KASUMIGASEKI Cloud”, proposed in 2009 as a private Cloud to be used throughout the public sector in the future [36]. The initiative has led to annual rollouts of new Government Cloud services and is reported to have “played a prominent role in growing Japan’s Cloud market”.

For example, a Platform as a Service (PaaS) service called “Government Shared Platform” (GSP) was introduced in March 2013 and 23 information systems were consolidated and transferred onto GSP by March 2015. The expected savings in 2015 was a 24% reduction of total cost for the transferred systems, expected to reach €47 million per year after 2022 when its development is expected to be completed [37].

In 2017, the Japanese authorities issued the updated version of the “Declaration to be the World’s Most Advanced IT Nation” [38], which reviews the implementation of a reform to government information systems for the purpose of halving the number of central government systems and lowering operating costs by
thirty percent. The number of systems will be reduced to 894 by FY 2018 (sixty-two percent less than in FY 2012) while operating costs will be reduced by 110.4 billion yen per year by 2021 (twenty-nine percent less than in FY 2013). This includes a Cloud-by-default principle like the Cloud first policy implemented in the UK. They propose a Cloud-utilization count as a KPI to monitor progress and the amount of cost reduction as an outcome KPI. They also propose the implementation and monitoring of the progress of other initiatives involving Cloud adoption in municipalities, education, the health sector, forest land registers, and forest management. These initiatives along with potential new ones are positive steps towards fostering the adoption of Cloud services in the public administration more extensively.

There are no legally binding data localization requirements in Japan, but some guidelines (for example the MIC guidelines for the medical industry) require private information processing operators to store data within the country.

The Japanese government issues a periodic review of their “Declaration to be the World’s Most Advanced IT Nation” that covers the evolution and implementation of several initiatives related to ICT including the migration of national and local government services to cloud. Publishing this information helps raise awareness about Cloud and its benefits.

5.4. The Nordics

Overall, the Nordic countries have exhibited a proactive approach to creating an enabling policy environment for cloud, through a combination of international collaboration and country-specific initiatives, as set out below. Along with Norway’s Cloud Computing Strategy [39] and the Nordic cooperation, both of which explicitly target an objective of increasing public sector cloud adoption, other Nordic countries such as Denmark include cloud computing initiatives in their e-government strategy.

**Denmark’s Digital Strategy 2016-2020 [34]** This includes an initiative for cloud computing in the public sector, including issuing updated legal guidelines based on the European GDP describing the possibilities available for the authorities regarding to cloud computing, and which addresses the assessment and management of security risks. The guidelines are with regards to
collection of data, storage and usage of data, and ways to handle sensitive personal data and confidential data. Authorities will control who has access to sensitive data on the public and businesses. Denmark is advanced in the rollout of independent cloud-based applications and has seen successful implementations with cost savings for the public sector of 50%-80% from specific cloud initiatives.

5.5. Benelux

Countries in the Benelux region (a politico-economic union of three European countries: Belgium, the Netherlands, and Luxembourg) exhibit a policy environment generally supportive of cloud although some data localization requirements exist across the Benelux. In 2012, the Dutch Ministry of the Interior and Kingdom Relations issued a policy note on “The Netherlands iStrategy” [41] explaining the intention to eliminate fragmented IT infrastructure and develop government-wide infrastructure that should be based on the concept of cloud computing.

In Belgium, the G-Cloud [42] was born as a hybrid Cloud combining services in public Cloud environments and national data centers based on a joint initiative of several public institutions and implemented by the “Cloud Governance Board”. An expanding range of services is made available via an online marketplace, including IaaS, PaaS and SaaS services from various vendors.

In Luxembourg, government representatives meet the Luxembourg information and communications technology (ICT) sector representatives yearly. After the last meeting, the latter have praised the government’s efforts and progress in the digital sector, such as the development of the fintech sector, the adoption of an open data philosophy, the implementation of projects such as the Luxembourg digital skills bridge as well as the evolution of the Infrachain initiative.

5.6. Germany

Initial e-government projects, such as 'BundOnline' and the National e-government strategy started as early as 1998. However, Germany has not opted thus far to explicitly promote or prioritize Cloud adoption in the public sector. There are two main barriers for the adoption of a public cloud by the German public administration:
5.7. Bahrain

In the Middle East region, Kingdom of Bahrain is among the countries to announce its "Cloud First Policy" in 2017 [7]. Bahrain's Information and eGovernment Authority (iGA) has announced the use of cloud computing to achieve cost reduction, increased security, increased productivity, and to develop excellent citizen services. The policy provides guidance to all government authorities in Bahrain as they move towards a common cloud operating environment, with the purpose of achieving the following.

- **Reduction in cost for both hardware and platforms.** Outsourcing government services to cloud computing results in reductions of large capital outlays for infrastructure and maintenance costs. Up to date, best of class solutions also become available to government agencies through cloud provisioning.

The German Regulation on the Award of Public Contracts (updated in 2009) promotes a technology-neutral approach to all procurement, subject to some limited exceptions.

One example of public administration use of Cloud is the marketplace ‘www.govCloud.de’, created by municipal Cloud computing providers to offer tailor-made Cloud services for public authorities in the areas of finance, construction, traffic and health, among others. Another innovative initiative has been the go Berlin project, which has provided citizens with online services through a Cloud based marketplace.

German authorities have pushed for the development of a more secure environment at a European level, as they state in their current digital strategy “We must develop a European data region policy based on common principles (e.g., data security and informational autonomy). Trust in the digital environment is weakened whenever there is any concern that basic rights, such as the protection of personal data by the service provider, are not being observed”.

5.7. **Bahrain**

In the Middle East region, Kingdom of Bahrain is among the countries to announce its "Cloud First Policy" in 2017 [7]. Bahrain's Information and eGovernment Authority (iGA) has announced the use of cloud computing to achieve cost reduction, increased security, increased productivity, and to develop excellent citizen services. The policy provides guidance to all government authorities in Bahrain as they move towards a common cloud operating environment, with the purpose of achieving the following.

- **Reduction in cost for both hardware and platforms.** Outsourcing government services to cloud computing results in reductions of large capital outlays for infrastructure and maintenance costs. Up to date, best of class solutions also become available to government agencies through cloud provisioning.
Improved manageability and productivity of ICT solutions. Government ICT resiliency and security is improved and made consistent with upgrades to both hardware and software being managed by the service provider.

Improved manageability and productivity of ICT solutions. Government ICT resiliency and security is improved and made consistent with upgrades to both hardware and software being managed by the service provider.

Better integration between services. More effective collaboration is enabled as agencies are able to share resources across institutions, improving efficiency, and enabling creativity in delivering public services.

Operational continuity and business recovery. With centralized and redundant data storage and backups, business recovery and data retrieval during times of crisis becomes faster and more cost effective.

Greater budget control. A ‘pay for what you use’ model allows government agencies to purchase as much or as little resource as needed, and only when needed. Cloud scalability results in systems usage being dialed up or down as it is required. Transparency of the utility-based pricing structure sets spending caps and alerts to assist in budget control.

Greater agility. Cloud computing streamlines development, support and hosting of ICT solutions, resulting in improved service performance and faster deployment of services. It reduces the amount of ICT infrastructure required to be built and owned by government agencies, shifting the focus from management of infrastructure to delivery of services.

Bahrain's Cloud-First Policy clearly sets out operational framework for the implementation of cloud-based solution development, which includes:

1. Application migration criteria  
2. Cloud security principles  
3. Security framework  
4. Mitigation and back-up  
5. Data Sovereignty
The Cloud-First Policy also lays down the Open Data policy for the government authorities. As per the policy, the government entities should endorse the open data principle, and technically feasible and economically reasonable, make non-restricted data available to other government agencies and the public through the cloud. In keeping with this principle and policy, government agencies should likewise manage their data assets to promote openness and use for the public good. Additionally, each stakeholder's roles and responsibilities, involved in the policy implementation, have been listed.

5.8. Saudi Arabia

In October 2020, the Ministry of Communications and Information Technology published the Kingdom's Cloud First Policy which is in effect on the date of publication [5].

This policy is intended to accelerate the pace at which governmental authorities are migrating from traditional IT solutions to cloud solutions and accelerate the adoption of cloud computing services in the Kingdom, which will serve as a key pillar in supporting and driving the digital transformation in the Kingdom, and the Kingdom's Vision 2030. The policy covers all government authorities with some exclusions, and these authorities are required to consider cloud computing options when making new IT investment decisions in line with a clearly defined decision tree that caters for technical, security and commercial requirements, with the goal of achieving the following:

- Increase quality of service by using more agile, innovative solutions in the Government services sector (e-services).
- Reduce total cost of ownership by improving IT utilization, aggregating demand and removing duplications in Governmental IT spend.
- Improve cyber security robustness by using accredited platforms with best-in-class cybersecurity standards by leveraging CSPs’ expertise in this domain.
- Enable interoperability amongst authorities.
6. Government Cloud Models

The awareness levels among the government authorities are growing across the world. The potential advantages including scalability, cost benefits, increased efficiencies, and most data localization features are already well realized by some mature economies. The Government Cloud model has started picking up among the emerging markets. However, government authorities will also be required to be cognizant of the some of the inherent challenges that comes along the way such as disaster recovery which necessitates the need to co-locate servers in different locations, loss of data control, potential data security threats, and limitations with regards to the connectivity speeds. Some instances of the successful implementations of Government Cloud services are discussed in this section.

6.1. United Kingdom

The UK government's G-Cloud service was implemented to ensure seamless procurement of IT services by all central government agencies leveraging cloud infrastructure. The service was launched in 2012 and has gone through several framework adjustments to include more services and vendors.

G-Cloud is mandatory for central government agencies, however other public sector entities were encouraged to adhere to the same practice. To facilitate G-Cloud implementation, framework agreements with local and global suppliers was created to enable seamless procurement process. Solutions and services from these suppliers are available on an online portal called Digital Marketplace. The portal allows easy search and purchase of services available in the G-Cloud frameworks agreement without necessity for new tender process.

One key objective of implementing G-Cloud was to ensure 50% of government's IT spending was driven by cloud services. So, to ensure compliance, in 2013, the UK government created the Cloud First policy, which was geared towards priority consideration for cloud IT procurement unless it could be proven that other on-premise alternatives were more cost effective.
G-Cloud includes over 13,000 IaaS, PaaS, and SaaS cloud services from over 1,000 suppliers. Additionally, the digital marketplace was designed to provide equal opportunity and visibility to all suppliers be it an SME type or global enterprise, so undue advantage is not given to a set of suppliers. Government agencies are also shielded from extended vendor lock-in contracts; therefore, maximum of two-year contracts is allowed, this also helps spur healthy competition among suppliers.

By May 2019, total cloud spend via the digital marketplace was about $5.88bn. The cloud first policy has in no small measure driven rapid implementation digital transformation across the UK public sector, as cloud procurements are mandatory for central government agencies.

6.2. United States

Currently the US federal government is implementing a cloud computing strategy called Cloud Smart for all its agencies. It's a long-term strategic approach to drive cloud adoption across federal government agencies. Cloud smart is an update of an initial cloud policy created in 2010 called Cloud first. Cloud First allowed individual federal government agencies broad oversight in procuring cloud services, however, Cloud Smart offers specific guidelines that agencies must follow to procure cloud services. Among other objectives, Cloud Smart was implemented to ensure migration to secure cloud infrastructure. Also, the revised policy was targeted at driving cost savings and faster deployment of mission critical solutions. Essentially, this new policy rests on three key pillars i.e. security, procurement, and workforce.

- **Security.** The new cloud strategy emphasizes the importance of taking a risk-based approach to securing cloud environments through increased investments in data, network and physical layers respectively. Cloud smart is designed to improve and increase access to federal government information across various networks and platforms either remotely or off-premises. It is also expected to boost data privacy and integrity of systems through continuous monitoring to detect potential malicious activity.

- **Procurement.** Cloud smart is expected to support seamless procurement of cloud solutions from a central marketplace; hence guidelines have been recommended to support procurement through analytics and knowledge sharing.
Creation and implementation of regulation are two key drivers that have spurred growth of cloud services among government agencies in Japan. Prior to cloud policy implementation, there had been concerns around regular increase in total costs of managing government information systems and growing threats of cyber-attacks.

Therefore, the government proposed a policy to drive down cost and increase security of government data and infrastructure. The Japanese government was also keen on infrastructure integration and consolidation across the public sector. Major milestone for the government was to integrate and consolidate about 1,300 government information systems to about 850 by end of 2021.

Therefore, in 2009, the government began examining cloud adoption strategies for the public sector. The “New Strategy for Digital New Era” also known as the “KASUMIGASEKI Cloud” was proposed. The proposal was adopted in 2011, then launched in 2013 as the government shared platform (GSP). GSP is essentially a platform as a service cloud solution to consolidate all government information systems. Through GSP government agencies can access datacenter services including network, hardware, and software. Since GSP’s launch in 2013, there has been year on year system migration, integration and consolidation to meet expected milestone by 2021.

Key success factors of the GSP is extensive consultation and collaboration by all government agencies in creating a sustainable policy that aligns government goals and objective. By 2015, GSP had helped reduce government’s IT capital and operational expenditure by 24% [37].
In 2014, the Australian government created its cloud computing policy. One of the key objectives of the policy was to ensure digitization of government functions to enhance easier, faster and more secured access by citizens. The policy is also expected to create a roadmap through which government's IT infrastructure can be consolidated on the cloud. Cost reduction was another key objective, one strategy to ensure cost reduction was outsourcing all generic IT services to specialist cloud providers, hence allowing agencies manage only mission critical functions.

Furthermore, through the cloud computing policy government is expected to increase efficiency and agility, enhance flexibility and security and improve data storage. The policy provides stringent security requirements on managing public data to match Australia's cyber security requirements.

The purpose of the cloud computing policy was to drive uptake of cloud services in the public sector. However, in 2017, a new secure cloud strategy was created after series of consultations between government and private sector stakeholders. The new policy focuses on supporting ease of use of available cloud services and offers guideline to cloud adoption unlike the 2014 policy. Agencies will have autonomy in creating their own cloud strategy to fit requirements, however all implementations shall be guided by the following principles [43]:

- Make risk-based decisions when applying cloud security
- Design services for the cloud
- Use public cloud services as the default
- Use as much of the cloud as possible
- Avoid customization and use cloud services as they come
- Take full advantage of cloud automation practices
- Monitor the health and usage of cloud services in real time
In the second half of 2020, The Saudi Data and Artificial Intelligence Authority (SDAIA) has launched the official identity of the governmental cloud "DEEM", represented by the National Information Center (NIC) reflecting the hype of developments towards digital transformation [44, 45]. DEEM allows government and non-government authorities to have more freedom on focusing on enhancing their services much more efficiently and investing on their technical assets without worrying about the infrastructure and behind-the-senses operational responsibilities ensuring data security and efficient IT-related spending. So far, DEEM provides about 23 services focusing on digital infrastructure services, platforms’ services, programs’ services, and managed services to about 60 government and non-government entities [45].
Adoption of Cloud service in Saudi Arabia is growing, driven by national transformation efforts and governments policies. With increased adoption, maintaining users’ data privacy and ensuring cybersecurity are top priority for the government and cloud service providers. To that aim, CITC and other government agencies have introduced regulations and guidance for cloud usage and how users’ information is handled.

The Cloud related regulations in Saudi Arabia shows a certain level of maturity and commitment. CITC has managed to capture some of the key themes from the globally practiced cloud regulations in the form of 'Cloud Computing Regulatory Framework', and it has managed to provide written guidelines for 'Enterprises', 'Government Agencies', 'Cloud Service Providers', and 'Individual Customers'. The Ministry of Communications and Information Technology (MCIT) also has taken a timely decision to implement Government’s Cloud First policy and assigned the roles and responsibilities of different authorities and offices.

Public cloud providers and their users need to be aware of such regulations and policies to benefit from the advantages public cloud could achieve such as flexibility, efficiency and scalability, while reducing the risks of cyberattacks and privacy breaches.
REFERENCES

[1] CLOUD Act, US Congress, 2018

[2] Data Protection Act, UK Government, 2018
https://www.gov.uk/data-protection


[5] KSA Cloud First Policy, Ministry of Communications and Information Technology (MCIT), 2019

https://www.tra.gov.ae/userfiles/assets/QqQuIA0SR5C.pdf

[7] Bahrain’s Cloud First Policy, Information & eGovernment Authority (iGA), 2017


[9] United States’ Patriot Act, Department of Justice, 2001
https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

[10] BSA Global Cloud Computing Scorecard, The Software Alliance (BSA), 2018

https://www.ncsc.gov.uk/collection/cloud-security

[12] The Data Protection Act, UK Government, 2018

[13] Amendments to UK data protection law in the event the UK leaves the EU without a deal, UK Government, 2019

https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=35630&type=part&key=43

[15] Personal Information Protection Act (PIPA) and its amendments, Government of South Korea, 2014-2020
http://www.pipc.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000501881&fileSn=0

https://www.privacy.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000830762&fileSn=0


[18] Guide for Cloud Service Providers

https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

[21] California Consumer Privacy Act, State of California, 2018
http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81


https://sdaia.gov.sa/ndmo/Files/PoliciesEn.pdf


[26] Essential Cybersecurity Controls, 2018

[27] ITU and the National Cybersecurity Authority of Saudi Arabia launch a new global programme to keep children safe online, ITU, 2020

[28] Two global cybersecurity initiatives, NCA, 2020


https://www.gov.uk/guidance/government-cloud-first-policy


[34] The Cloud Readiness Index 2018, Asia Cloud Computing Association (ACCA), 2018
https://asiacloudcomputing.org/2018/04/16/the-cloud-readiness-index/

https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf

[36] Smart Cloud Strategy, Smart Cloud Study Group, Japanese Government, 2010


[38] Declaration to be the World’s Most Advanced IT Nation, Japanese Government, 2017
https://www.regjeringen.no/contentas-sets/4e30afec51734d458596e723c0bdea0e/cloud_computing_strategy.pdf

[40] A Stronger and More Secure Digital Denmark (Digital Strategy 2016-2020), Danish Government,
https://digst.dk/media/16165/ds_singlepage_uk_web.pdf

https://www.gov amsterdam.nl/documents/policy_notes/2012/03/30/the-netherlands-istrategy


[44] DEEM Cloud, SDAIA, 2020
https://sdaia.gov.sa/

[45] DEEM Cloud, NIC, 2020
https://nic.gov.sa/?Lang=en&page=SectionProducts
For More Information