

**10th November, 2022**

**College of science and technology**

**Department of information technology**

**Group members:**

1. **DUSHIMIMANA Claude 219013371**
2. **NDAGIJIMANA Joseph 219002979**
3. **SHUMBUSHO Emile 219000157**

**CLOUD COMPUTING GROUP ASSIGNMENT**

**Summary of the Book: Cloud Security and Privacy chap: 2, 3, 4, 5, 7 and 8**

**Chap 2: WHAT IS CLOUD COMPUTING?**

CLOUD COMPUTING DEFINITION

**Our definition of cloud computing is based on five attributes:**

**Multitenancy**: (shared resources) unlike previous computing models, which assumed dedicated resources (i.e., computing facilities dedicated to a single user or owner), cloud computing is based on a business model in which resources are shared (i.e., multiple users use the same resource) at the network level, host level, and application level.

**Massive scalability**: although organizations might have hundreds or thousands of systems, cloud computing provides the ability to scale to tens of thousands of systems, as well as the ability to massively scale bandwidth and storage space.

**Elasticity:** Users can rapidly increase and decrease their computing resources as needed, as well as release resources for other uses when they are no longer required.

**Pay as you go:** Users pay for only the resources they actually use and for only the time they require them. Self-provisioning of resources Users self-provision resources, such as additional systems (processing capability, software, storage) and network resources.

**Relevant Technologies in Cloud Computing**

Cloud computing isn’t so much a technology as it is the combination of many preexisting technologies.

These technologies hey have come together to create a technical ecosystem for cloud computing.

**Cloud access devices** the range of access devices for the cloud has expanded in recent years. Home PCs, enterprise PCs, network computers, mobile phone devices, custom handheld devices, and custom static devices (including refrigerators) are all online.

**Browsers and thin clients** Users of multiple device types can now access applications and information from wherever they can load a browser.

**Data centers and server farms** Cloud-based services require large computing capacity and are hosted in data centers and server farms. These distributed data centers and server farms span multiple locations and can be linked via internetworks providing distributed computing and service delivery capabilities.

**The Traditional Software Model**

Traditional software applications are based on a model with large, upfront licensing costs and annual support costs. Increasing the number of users can raise the base cost of the package due to the need for additional hardware server deployments and IT support.

**The Cloud Services Delivery Model**

As we noted earlier, a cloud services delivery model is commonly referred to as an SPI and falls into three generally accepted services

1. **The Software-As-a-Service Model**

Traditional methods of purchasing software involved the customer loading the software onto his own hardware in return for a license fee.

The customer could also purchase a maintenance agreement to receive patches to the software or other support services.

In a SaaS model, the customer does not purchase software, but rather rents it for use on a subscription or pay-per-use model

**Key benefits of a SaaS model include the following:**

* SaaS enables software vendors to control and limit use, prohibits copying and distribution, and facilitates the control of all derivative versions of their software.
* Applications delivery using the SaaS model typically uses the one-to-many delivery approach, with the Web as the infrastructure.
* A typical SaaS deployment does not require any hardware and can run over the existing Internet access infrastructure.

The single most important architectural difference between the traditional software model and the SaaS model is the number of tenants the application supports.

1. **The Platform-As-a-Service Model**

PaaS solutions are development platforms for which the development tool itself is hosted in the cloud and accessed through a browser. With PaaS, developers can often build web applications without installing any tools on their computer, and can then deploy those applications without any specialized system administration skills

1. **The Infrastructure-As-a-Service Model**

In the traditional hosted application model, the vendor provides the entire infrastructure for a customer to run his applications. Often, this entails housing dedicated hardware that is purchased or leased for that specific application. The IaaS model also provides the infrastructure to run the applications, but the cloud computing approach makes it possible to offer a pay-peruse model and to scale the service depending on demand.

**Features available for a typical IaaS system include:**

**Scalability** The ability to scale infrastructure requirements, such as computing resources, memory, and storage (in near-real-time speeds) based on usage requirements.

**Pay as you go** the ability to purchase the exact amount of infrastructure required at any specific time

**Best-of-breed technology and resources** Access to best-of-breed technology solutions and superior IT talent for a fraction of the cost.

**Cloud Deployment Models**

**A public cloud** is hosted, operated, and managed by a third-party vendor from one or more data centers. The service is offered to multiple customers (the cloud is offered to multiple tenants) over a common infrastructure

**Private clouds** differ from public clouds in that the network, computing, and storage infrastructure associated with private clouds is dedicated to a single organization and is not shared with any other organizations

**A hybrid cloud** environment consisting of multiple internal and/or external providers is a possible deployment for organizations. With a hybrid cloud, organizations might run non-core applications in a public cloud, while maintaining core applications and sensitive data in-house in a private cloud

**CHAP3: INFRASTRUCTURE SECURITY**

**Infrastructure Security at network level**

However, if you choose to use public cloud services, changing security requirements will require changes to your network topology. You must address how your existing network topology interacts with your cloud provider’s network topology. There are four significant risk factors in this use case:

• Ensuring the confidentiality and integrity of your organization’s data-in-transit to and from your public cloud provider

• Ensuring proper access control (authentication, authorization, and auditing) to whatever resources you are using at your public cloud provider

• Ensuring the availability of the Internet-facing resources in a public cloud that are being used by your organization, or have been assigned to your organization by your public cloud providers

• Replacing the established model of network zones and tiers with domains

**Network-Level Mitigation**

If your organization is large enough to afford the resources of a private cloud, your risks will decrease—assuming you have a true private cloud that is internal to your network. In some cases, a private cloud located at a cloud provider’s facility can help meet your security requirements but will depend on the provider capabilities and maturity.

You can reduce your confidentiality risks by using encryption; specifically, by using validated implementations of cryptography for data-in-transit. Secure digital signatures make it much more difficult, if not impossible, for someone to tamper with your data, and this ensures data integrity.

Availability problems at the network level are far more difficult to mitigate with cloud computing—unless your organization is using a private cloud that is internal to your network topology. Even if your private cloud is a private (i.e., non-shared) external network at a cloud provider’s facility, you will face increased risk at the network level. A public cloud faces even greater risk.

**Infrastructure Security: The Host Level**

When reviewing host security and assessing risks, you should consider the context of cloud services delivery models (SaaS, PaaS, and IaaS) and deployment models (public, private, and hybrid).

n, the fact that the clouds harness the power of thousands of compute nodes, combined with the homogeneity of the operating system employed by hosts, means the threats can be amplified quickly and easily call it the “velocity of attack” factor in the cloud. More importantly, you should understand the trust boundary and the responsibilities that fall on your shoulders to secure the host infrastructure that you manage. And you should compare the same with providers’ responsibilities in securing the part of the host infrastructure the CSP manages.

**SaaS and PaaS Host Security**

In general, CSPs do not publicly share information related to their host platforms, host operating systems, and the processes that are in place to secure the hosts, since hackers can exploit that information when they are trying to intrude into the cloud service.

Both the PaaS and SaaS platforms abstract and hide the host operating system from end users with a host abstraction layer.

One key difference between PaaS and SaaS is the accessibility of the abstraction layer that hides the operating system services the applications consume. In the case of SaaS, the abstraction layer is not visible to users and is available only to the developers and the CSP’s operations staff, where PaaS users are given indirect access to the host abstraction layer in the form of a PaaS application programming interface (API) that in turn interacts with the host abstraction layer.

In summary, host security responsibilities in SaaS and PaaS services are transferred to the CSP. The fact that you do not have to worry about protecting hosts from host-based security threats is a major benefit from a security management and cost standpoint.

**IaaS Host Security**

Unlike PaaS and SaaS, IaaS customers are primarily responsible for securing the hosts provisioned in the cloud.

**Virtualization Software Security**

CSPs should institute the necessary security controls, including restricting physical and logical access to hypervisor and other forms of employed virtualization layers. IaaS customers should understand the technology and security process controls instituted by the CSP to protect the hypervisor. This will help you to understand the compliance and gaps with reference to your host security standard, policies, and regulatory compliances. However, in general, CSPs lack transparency in this area and you may have no option but to take a leap of faith and trust CSPs to provide an “isolated and secured virtualized guest OS.”

**Threats to the hypervisor**

The integrity and availability of the hypervisor are of utmost importance and are key to guaranteeing the integrity and availability of a public cloud built on a virtualized environment.

**Virtual Server Security**

Customers of IaaS have full access to the virtualized guest VMs that are hosted and isolated from each other by hypervisor technology. Hence customers are responsible for securing and ongoing security management of the guest VM.

Some of the new host security threats in the public IaaS include:

• Stealing keys used to access and manage hosts (e.g., SSH private keys)

• Attacking unpatched, vulnerable services listening on standard ports (e.g., FTP, NetBIOS, SSH)

• Hijacking accounts that are not properly secured (i.e., weak or no passwords for standard accounts)

• Attacking systems that are not properly secured by host firewalls

• Deploying Trojans embedded in the software component in the VM or within the VM image (the OS) itself

Securing the virtual server in the cloud requires strong operational security procedures coupled with automation of procedures. Here are some recommendations:

• Use a secure-by-default configuration.

• Track the inventory of VM images and OS versions that are prepared for cloud hosting.

• Protect the integrity of the hardened image from unauthorized access

• Safeguard the private keys required to access hosts in the public cloud.

**Infrastructure Security: The Application Level**

Since the browser has emerged as the end user client for accessing in-cloud applications, it is important for application security programs to include browser security into the scope of application security. Together they determine the strength of end-to-end cloud security that helps protect the confidentiality, integrity, and availability of the information processed by cloud services.

**Application-Level Security Threats**

It has been a common practice to use a combination of perimeter security controls and network- and host-based access controls to protect web applications deployed in a tightly controlled environment, including corporate intranets and private clouds, from external hackers. Web applications built and deployed in a public cloud platform will be subjected to a high threat level, attacked, and potentially exploited by hackers to support fraudulent and illegal activities.

**DoS and EDoS**

Additionally, you should be cognizant of application-level DoS and DDoS attacks that can potentially disrupt cloud services for an extended time. These attacks typically originate from compromised computer systems attached to the Internet (routinely, hackers hijack and control computers infected by way of viruses/worms/malware and, in some cases, powerful unprotected servers).

Apart from disrupting cloud services, resulting in poor user experience and service-level impacts, DoS attacks can quickly drain your company’s cloud services budget.

**End User Security**

You, as a customer of a cloud service, are responsible for end user security tasks—security procedures to protect your Internet-connected PC—and for practicing “safe surfing.” Protection measures include use of security software, such as anti-malware, antivirus, personal firewalls, security patches, and IPS-type software on your Internet-connected computer.

**Who Is Responsible for Web Application Security in the Cloud?**

Depending on the cloud services delivery model (SPI) and service-level agreement (SLA), the scope of security responsibilities will fall on the shoulders of both the customer and the cloud provider.

**Customer-Deployed Application Security**

PaaS developers need to get familiar with specific APIs to deploy and manage software modules that enforce security controls. Furthermore, given that the API is unique to a PaaS cloud service, developers are required to become familiar with platform-specific security features— available to them in the form of security objects and web services for configuring authentication and authorization controls within the application.

**Public Cloud Security Limitations** Customers evaluating the public cloud should keep in mind that there are limitations to the public cloud when it comes to support for custom security features.

Chap 4: **DATA SECURITY AND STORAGE**

**Aspects of Data Security**

With regard to data-in-transit, the primary risk is in not using a vetted encryption algorithm. Although this is obvious to information security professionals, it is not common for others to 61 understand this requirement when using a public cloud, regardless of whether it is IaaS, PaaS, or SaaS. It is also important to ensure that a protocol provides confidentiality as well as integrity (e.g., FTP over SSL [FTPS], Hypertext Transfer Protocol Secure [HTTPS], and Secure Copy Program [SCP])—particularly if the protocol is used for transferring data across the Internet.

Whether the data an organization has put into the cloud is encrypted or not, it is useful and might be required (for audit or compliance purposes) to know exactly where and when the data was specifically located within the cloud.

The risk posed by data eminence in cloud services is that an organization’s data can be inadvertently exposed to an unauthorized party—regardless of which cloud service you are using (SaaS, PaaS, or IaaS).

**Data Security Mitigation**

If prospective customers of cloud computing services expect that data security will serve as compensating controls for possibly weakened infrastructure security, since part of a customer’s infrastructure security moves beyond its control and a provider’s infrastructure security may (for many enterprises) or may not (for small to medium-size businesses, or SMBs) be less robust than expectations, you will be disappointed. Although data-in-transit can and should be encrypted, any use of that data in the cloud, beyond simple storage, requires that it be decrypted.

So, what should you do to mitigate these risks to data security? The only viable option for mitigation is to ensure that any sensitive or regulated data is not placed into a public cloud (or that you encrypt data placed into the cloud for simple storage only).

**Provider Data and Its Security**

In addition to the security of your own customer data, customers should also be concerned about what data the provider collects and how the CSP protects that data

**Storage**

For data stored in the cloud (i.e., storage-as-a-service), we are referring to IaaS and not data associated with an application running in the cloud on PaaS or SaaS. The same three information security concerns are associated with this data stored in the cloud (e.g., Amazon’s S3) as with data stored elsewhere: confidentiality, integrity, and availability.

**Confidentiality** When it comes to the confidentiality of data stored in a public cloud, you have two potential concerns. First, what access control exists to protect the data? Access control consists of both authentication and authorization.

**Integrity** In addition to the confidentiality of your data, you also need to worry about the integrity of your data. Confidentiality does not imply integrity; data can be encrypted for confidentiality purposes, and yet you might not have a way to verify the integrity of that data.

**Availability** Assuming that a customer’s data has maintained its confidentiality and integrity, you must also be concerned about the availability of your data.

Chap 5: **IDENTITY AND ACCESS MANAGEMENT**

**IAM Definitions** To start, we’ll present the basic concepts and definitions of IAM functions for any service:

**Authentication** is the process of verifying the identity of a user or system (e.g., Lightweight Directory Access Protocol [LDAP] verifying the credentials presented by the user, where the identifier is the corporate user ID that is unique and assigned to an employee or contractor).

**Authorization** is the process of determining the privileges the user or system is entitled to once the identity is established.

**Auditing** In the context of IAM, auditing entails the process of review and examination of authentication, authorization records, and activities to determine the adequacy of IAM system controls, to verify compliance with established security policies and procedures (e.g., separation of duties), to detect breaches in security services (e.g., privilege escalation), and to recommend any changes that are indicated for countermeasures.

**IAM Architecture and Practice**

The directory interacts with IAM technology components such as authentication, user management, provisioning, and federation services that support the standard IAM practice and processes within the organization.

The IAM processes to support the business can be broadly categorized as follows:

**User management:** Activities for the effective governance and management of identity life cycles.

**Authentication management:** Activities for the effective governance and management of the process for determining that an entity is who or what it claims to be.

**Authorization management:** Activities for the effective governance and management of the process for determining entitlement rights that decide what resources an entity is permitted to access in accordance with the organization’s policies.

**Access management:** Enforcement of policies for access control in response to a request from an entity (user, services) wanting to access an IT resource within the organization.

**Data management and provisioning:** Propagation of identity and data for authorization to IT resources via automated or manual processes.

**Monitoring and auditing**: Monitoring, auditing, and reporting compliance by users regarding access to resources within the organization based on the defined policies.

**IAM processes support the following operational activities**:

* **Provisioning**: This is the process of on-boarding users to systems and applications. These processes provide users with necessary access to data and technology resources.
* **Credential and attribute management:** These processes are designed to manage the life cycle of credentials and user attributes— create, issue, manage, revoke—to minimize the business risk associated with identity impersonation and inappropriate account use. Credentials are usually bound to an individual and are verified during the authentication process.
* **Entitlement management:** Entitlements are also referred to as authorization policies. The processes in this domain address the provisioning and deprovisioning of privileges needed for the user to access resources including systems, applications, and databases. Proper entitlement management ensures that users are assigned only the required privileges (least privileges) that match with their job functions.
* **Compliance management:** This process implies that access rights and privileges are monitored and tracked to ensure the security of an enterprise’s resources.
* **Identity federation management:** Federation is the process of managing the trust relationships established beyond the internal network boundaries or administrative domain boundaries among distinct organizations.
* **Centralization of authentication (authN) and authorization (authZ)**: A central authentication and authorization infrastructure alleviates the need for application developers to build custom authentication and authorization features into their applications.

**IAM Standards and Specifications for Organizations**

The following IAM standards and specifications will help organizations implement effective and efficient user access management practices and processes in the cloud. These sections are ordered by four major challenges in user and access management faced by cloud users:

1. How can I avoid duplication of identity, attributes, and credentials and provide a single sign-on user experience for my users? SAML.

2. How can I automatically provision user accounts with cloud services and automate the process of provisioning and de-provisioning? SPML.

3. How can I provision user accounts with appropriate privileges and manage entitlements for my users? XACML.

4. How can I authorize cloud service X to access my data in cloud service Y without disclosing credentials? Oath.

**Open Authentication (Oath**)

OAuth is an emerging authentication standard that allows consumers to share their private resources (e.g., photos, videos, contact lists, bank accounts) stored on one CSP with another CSP without having to disclose the authentication information (e.g., username and password). OAuth is an open protocol and it was created with the goal of enabling authorization via a secure application programming interface (API)—a simple and standard method for desktop, mobile, and web applications

**IAM Standards, Protocols, and Specifications for Consumers**

The following protocols and specifications are oriented toward consumer cloud services, and are not relevant from an enterprise cloud computing standpoint.

**Open ID** is an open, decentralized standard for user authentication and access control, allowing users to log on too many services with the same digital identity. a single sign-on user experience with services supporting Open ID.

**Information cards** Information cards are another open standard for identity on the Web. The standard itself is directed by the Information Card Foundation, whose steering members include representatives from Google, Microsoft, PayPal, Oracle Novell, and Equifax.

**Open Authentication (OATH)** OATH is a collaborative effort of IT industry leaders aimed at providing an architecture reference for universal, strong authentication across all users and all devices over all networks.

The goal of this initiative is to address the three major authentication methods:

• Subscriber Identity Module (SIM)-based authentication (using a Global System for Mobile Communications/General Packet Radio Service [GSM/GPRS] SIM)

• Public Key Infrastructure (PKI)-based authentication (using an X.509v3 certificate)

• One-Time Password (OTP)-based authentication

**Open Authentication API** (OpenAuth) OpenAuth is an AOL-proprietary API that enables third-party websites and applications to authenticate AOL and AOL Instant Messenger (AIM) users through their websites and applications.

**Enterprise identity provider**

In this architecture, cloud services will delegate authentication to an organization’s IdP. In this delegated authentication architecture, the organization federates identities within a trusted circle of CSP domains.

Here are the specific pros and cons of this approach:

**Pros**

Organizations can leverage the existing investment in their IAM infrastructure and extend the practices to the cloud. For example, organizations that have implemented SSO for applications within their data center exhibit the following benefits:

• They are consistent with internal policies, processes, and access management frameworks.

• They have direct oversight of the service-level agreement (SLA) and security of the IdP.

• They have an incremental investment in enhancing the existing identity architecture to support federation

. **Cons**

By not changing the infrastructure to support federation, new inefficiencies can result due to the addition of life cycle management for non-employees such as customers.

**Chap 7: PRIVACY**

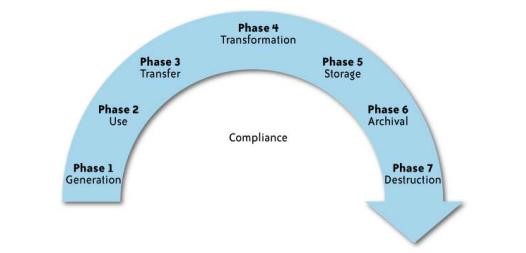
**What Is Privacy?**

The concept of privacy varies widely among (and sometimes within) countries, cultures, and jurisdictions. It is shaped by public expectations and legal interpretations; as such, a concise definition is elusive if not impossible. Privacy rights or obligations are related to the collection, use, disclosure, storage, and destruction of personal data (or personally identifiable information—PII). At the end of the day, privacy is about the accountability of organizations to data subjects, as well as the transparency to an organization’s practice around personal information.

What Is the Data Life Cycle?

Personal information should be managed as part of the data used by the organization. It should be managed from the time the information is conceived through to its final disposition.

Protection of personal information should consider the impact of the cloud on each of the following phases as detailed in Figure 7-1.



The components within each of these phases are:

Generation of the information

Ownership: Who in the organization owns PII, and how is the ownership maintained if the organization uses cloud computing?

Classification: How and when is PII classified? Are there limitations on the use of cloud computing for specific data classes?

Governance: Is there a governance structure to ensure that PII is managed and protected through its life cycle, even when it is stored or processed in a cloud computing environment?

Use

Internal versus external: Is PII used only within the collecting organization, or is it used outside the organization (e.g., in a public cloud)?

Third party: Is the information shared with third parties (e.g., subcontractors or CSPs)?

Appropriateness: Is the use of the information consistent with the purpose for which it was collected. Is the use within the cloud appropriate based on the commitments the organization made to the data subjects?

Discovery/subpoena: Is the information managed in the cloud in a way that will enable the organization to comply with legal requirements in case of legal proceedings?

Transfer

Public versus private networks: When information is transferred to a cloud is the organization using public networks, and is it protected appropriately? (PII should always be protected to address the risk level and legal requirements.)

Encryption requirements: Is the PII encrypted? Some laws require that PII will be encrypted when transmitted via a public network (and this will be the case when the organization is using a public cloud).

Access control: Are there appropriate access controls over PII when it is in the cloud?

Transformation

Derivation: Are the original protection and use limitations maintained when data is transformed or further processed in the cloud?

Aggregation: Is data in the cloud aggregated so that it is no longer related to an identifiable individual (and hence is no longer considered PII)?

Integrity: Is the integrity of PII maintained when it is in the cloud?

Storage

Access control: Are there appropriate controls over access to PII when stored in the cloud so that only individuals with a need to know will be able to access it?

Structured versus unstructured: How is the data stored to enable the organization to access and manage the data in the future?

Integrity/availability/confidentiality: How are data integrity, availability, and confidentiality maintained in the cloud?

Encryption: Several laws and regulations require that certain types of PII should be stored only when encrypted. Is this requirement supported by the CSP?

Archival

Legal and compliance: PII may have specific requirements that dictate how long it should be stored and archived. Are these requirements supported by the CSP?

Off-site considerations: Does the CSP provide the ability for long-term off-site storage that supports archival requirements?

Media concerns: Is the information stored on media that will be accessible in the future? Is the information stored on portable media that may be more susceptible to loss? Who controls the media and what is the organization’s ability to recover such media from the CSP if needed?

Retention: For how long will the data be retained by the CSP? Is the retention period consistent with the organization’s retention period?

Destruction

Secure: Does the CSP destroy PII obtained by customers in a secure manner to avoid potential breach of the information?

Complete: Is the information completely destroyed? Does the destruction completely erase the data, or can it be recovered?

What Are the Key Privacy Concerns in the Cloud?

Privacy advocates have raised many concerns about cloud computing. These concerns typically mix security and privacy. Here are some additional considerations to be aware of:

Access: Data subjects have a right to know what personal information is held and, in some cases, can make a request to stop processing it.

Compliance: What are the privacy compliance requirements in the cloud? What are the applicable laws, regulations, standards, and contractual commitments that govern this information, and who is responsible for maintaining the compliance?

Storage: Where is the data in the cloud stored? Was it transferred to another data center in another country? Is it commingled with information from other organizations that use the same CSP?

Retention: How long is personal information (that is transferred to the cloud) retained? Which retention policy governs the data? Does the organization own the data, or the CSP?

Destruction: How does the cloud provider destroy PII at the end of the retention period? How do organizations ensure that their PII is destroyed by the CSP at the right point and is not available to other cloud users?

Audit and monitoring: How can organizations monitor their CSP and provide assurance to relevant stakeholders that privacy requirements are met when their PII is in the cloud?

Privacy breaches: How do you know that a breach has occurred, how do you ensure that the CSP notifies you when a breach occurs, and who is responsible for managing the breach notification process (and costs associated with the process)?

Who Is Responsible for Protecting Privacy?

There are conflicting opinions regarding who is responsible for security and privacy. Some publications assign it to providers; but although it may be possible to transfer liability via contractual agreements, it is never possible to transfer accountability.

History and experience have proven that data breaches have a cascading effect. When an organization loses control of users’ personal information, the users are responsible (directly or indirectly) for subsequent damages resulting from the loss.

The accountability model (discussed earlier in this chapter) is similar to discussions around privacy in outsourcing or subcontracting relationships, and the conclusion is similar:

Organizations can transfer liability, but not accountability.

Risk assessment and mitigation throughout the data life cycle is critical.

Knowledge about legal obligations and contractual agreements or commitments is imperative.

There are, however, many new risks and unknowns; thus, the overall complexity of privacy protection in the cloud represents a bigger challenge

Changes to Privacy Risk Management and Compliance in Relation to Cloud Computing

The following topics describe analysis of the potential impact of cloud computing on the key OECD and other common privacy principles.

Collection Limitation Principle This principle specifies that collection of personal data should be limited to the minimum amount of data required for the purpose for which it is collected. Any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject

Use Limitation Principle This principle specifies that personal data should not be disclosed, made available, or otherwise used for purposes other than those with the consent of the data subject, or by the authority of law.

Security Principle Security is one of the key requirements to enable privacy. This principle specifies that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.

Retention and Destruction Principle This principle specifies that personal data should not be retained for longer than needed to perform the task for which it was collected, or as required by laws or regulations. Data should be destroyed in a secure way at the end of the retention period.

Transfer Principle This principle specifies that data should not be transferred to countries that don’t provide the same level of privacy protection as the organization that collected the information.

Accountability Principle This principle states that an organization is responsible for personal information under its control and should designate an individual or individuals who are accountable for the organization’s compliance with the remaining principles.

Legal and Regulatory Implications

Across the globe, the legal and regulatory requirements for data privacy range from strictly enforced to non-existent, which can prove to be a daunting challenge for multinational companies or those serving customers from multiple jurisdictions. Some programs such as the OECD Guidelines‡ and the European Union Data Protection Directive§ are principle-based, where personal data processing is not permitted, except as directed in the statutes, whereas in countries such as the United States, certain types of processing are restricted, but activities are generally considered lawful unless specifically prohibited by applicable state and federal regulations. The jurisdiction of these laws is determined differently in different countries and states. Some of the laws are based on the location of the organization, some on the physical location of the data center, and some on the location of the data subjects. The only universal consistency is that the law has not caught up with the technology.

To further compound the challenge of processing personal data in a global environment, some requirements are conflicting. For example, compliance with the U.S. Federal Rules of Civil Procedure (FRCP) can breach the EU Directive. Differing attitudes on privacy have been the force behind countless cross-jurisdictional legal battles, international trade barriers, and longstanding political disputes.

In the next section, we will describe the implications of cloud computing on compliance with various privacy regulations. The scope is limited to aspects that are different in a public cloud environment, because many resources are available to help understand the full extent of the requirements.

U.S. Laws and Regulations

The U.S. regulatory environment is a complex combination of sector-specific federal privacy laws, statespecific laws, and other laws and regulations that can have a significant privacy impact on cloud computing environments.

Federal Rules of Civil Procedure

Rule 26‖ of the FRCP requires that parties involved in a civil lawsuit have a duty to disclose to the other party all information that will be used to support its claims or defenses. This includes electronically stored information (ESI), which creates a challenge in a cloud environment.

USA Patriot Act

At a high level, the challenge with the Patriot Act can be viewed as location, location, location. Exactly where is your data physically, and therefore whose government policies will your data be subject to? What law enforcement (including intelligence) practices, or perhaps conversely, privacy regulations, is the location of your data and your CSP required to abide by?

Electronic Communications Privacy Act

Fundamental to addressing all cloud computing risks (including those related to privacy) is the contractual agreement with the provider. It is absolutely critical for users to have a thorough understanding of the terms and conditions—from both a legal and a technical perspective. Agreements should clearly describe the services provided, limitations, liabilities, and rights of each party.

FISMA

The first thing to note when discussing the U.S. Federal Information Security Management Act of 2002 (FISMA) is that the act requires only U.S. federal agencies to develop, document, and implement an agency-wide information security program.

International Laws and Regulations

The international regulatory environment is driven by two approaches: one represented by EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (EU Directive), that was the model used by countries in Europe as well as Canada, and another reflected by the APEC Privacy Framework. The two approaches have a different privacy impact on cloud computing environments.

EU Directive

The most significant difference between the EU and U.S. legislation is the notion of personal privacy. In Europe, privacy is considered a basic human right and cannot be divorced from one’s personal freedom.

APEC Privacy Framework

The Asia Pacific Economic Corporation (APEC) Privacy Framework, similar to the OECD Privacy Guidelines, is established as best practices for organizations operating within these economic areas. Unlike the EU Directive, these guidelines are not mandatory, and as such they may be adopted by participating economies as part of their laws.

**Chap 8: AUDIT AND COMPLIANCE**

AUDIT AND COMPLIANCE refers to the internal and external processes that an organization implements to:

* Identify the requirements with which it must abide and whether those requirements are driven by business objectives, laws and regulations, customer contracts, internal corporate policies and standards, or other factors
* Put into practice policies, procedures, processes, and systems to satisfy such requirements
* Monitor or check whether such policies, procedures, and processes are consistently followed

**Governance, Risk, and Compliance (GRC)**

CSPs are typically challenged to meet the requirements of a diverse client base. To build a sustainable model, it is essential that the CSP establish a strong foundation of controls that can be applied to all its clients. In that regard, the CSP can use the concept of GRC that has been adopted by several leading traditional outsourced service providers and CSPs.

**Programmatic approach to compliance:**

**Risk assessment**

This approach begins with an assessment of the risks that face the CSP and identification of the specific compliance regimes/requirements that are applicable to the CSP’s services. The CSP should address risks associated with key areas such as appropriate user authentication mechanisms for accessing the cloud, encryption of sensitive data.

**Key controls**

Key controls are then identified and documented to address the identified risks and compliance requirements. These key controls are captured in a unified control set that is designed to meet the requirements of the CSP’s customers and other external requirements. The CSP drives compliance activities based on its key controls rather than disparate sets of externally generated compliance requirements.

**Monitoring**

Monitoring and testing processes are defined and executed on an ongoing basis for key controls. Gaps requiring remediation are identified with remediation progress tracked. The results of ongoing monitoring activities may also be used to support any required external audits.

**Reporting**

Metrics and key performance indicators (KPIs) are defined and reported on an ongoing basis. Reports of control effectiveness and trending are made available to CSP management and external customers, as appropriate.

**Continuous improvement**

Management improves its controls over time—acting swiftly to address any significant gaps identified during monitoring and taking advantage of opportunities to improve processes and controls.

**Risk assessment—new IT projects and systems**

The CSP performs a risk assessment as new IT projects, systems, and services are developed to identify new risks and requirements, to assess the impact on the CSP’s current controls, and to determine whether additional or modified controls and monitoring processes are needed.

**Benefits of GRC for CSPs**

CSPs must adhere to a variety of IT process control requirements including external requirements and internal requirements. As we examine these requirements, we find numerous points of intersection. By combining compliance efforts to address all these requirements and taking a more uniform and strategic approach, increased efficiencies and compliance can be attained. Instead of performing control review and testing cycles separately, control language and testing can be structured to address the needs of multiple sets of requirements.

**GRC approach helps a CSP to:**

* Reduce risks through a structured risk management approach
* Improve monitoring of IT compliance
* Improve security
* Rationalize compliance requirements and control assessment processes
* Reduce the burden of compliance monitoring and testing

**Additional control objectives may be applicable depending on the nature of the services offered by the CSP.**

* Asset management, access control

***Data protection/segregation/encryption***

to provide logical segregation of CSP customers’ data To enable customer classification of sensitive data To enable protection of data commensurate with risk and defined information classifications

* Information systems acquisition, development, and maintenance

***Encryption standards***

To enable encryption of sensitive data using consistent mechanisms

To enable access to current and archived data regardless of which keys were used for encryption

* Communications and operations management

***Logging***

To securely provide audit logs of relevant actions (e.g., user activity, configuration changes) for internal or external review

To periodically review higher-risk audit events with appropriate action taken where required

* Access control

***Authentication to the cloud***

To provide authentication mechanisms commensurate with the associated risk

To strictly limit CSP administrative access to customer data, including IT and customer support personnel

* Compliance

***Monitoring/compliance function***

To provide ongoing monitoring of compliance with policies, procedures, and standards

To provide proactive risk identification and mitigation

**Additional Key Management Control Objectives**

Where encryption is used, effective key management controls are critically important to help ensure the confidentiality and availability of sensitive data. Here are the relevant key management control objectives.

**Key management**

***Key generation practices***

Cryptographic keys are generated in accordance with industry standards, including:

* + Random or pseudorandom number generation
  + Prime number generation
  + Key generation algorithms
  + Hardware and software components
  + References to the key generation procedural documentation

***Key storage, backup, and recovery practices***

Asymmetric private keys and symmetric keys remain secret, and their integrity and authenticity are retained, including:

* Key separation mechanisms
* Hardware and software components
* References to key storage, backup, and recovery procedures
* Business continuity management documentation

***Key distribution practices***

Secrecy of asymmetric private keys, symmetric keys, and keying material, and the integrity and authenticity of all keys and keying material, are maintained during key distribution, including:

* + Initial key distribution processes
  + Subsequent key replacement processes
  + Key synchronization mechanisms
  + References to the key distribution procedural documentation

***Key use practices***

Cryptographic keys are used only for their intended purpose, including:

* + Business applications
  + Key separation mechanisms
  + Related crypto periods
  + References to the business and system description documentation

***Key destruction and archival practices***

All active instances of cryptographic keys are properly erased (destroyed) at the end of their designated crypto-periods and archived keys are handled appropriately, including:

* + Controls to maintain confidentiality, integrity, and authenticity
  + Mechanisms to prevent an archived key from being reinstalled
  + Inclusion of references to the business and system documentation

***Cryptographic hardware life cycle practices***

Access to cryptographic hardware is limited to properly authorized individuals, and the hardware is functioning properly. The description should include:

* + Controls for the device life cycle (e.g., shipping, inventory controls, installation, initialization, repair, and de-installation)
  + References to device documentation

***Certificate life cycle management***

Subscribers are properly identified and authenticated, and certificate request information is accurate and complete. Certificates are generated and issued securely and accurately. Upon issuance, complete and accurate certificates are available to subscribers and relying parties.

* Certificates are revoked based on authorized and validated certificate revocation requests.
* Certificates and certificate chains are properly verified.

**Control Considerations for CSP Users**

The following are illustrative control objectives of relevance to users of CSPs. Additional control objectives may be applicable depending on the nature of the services offered by the CSP.

* Access control

***Managing access to the cloud***

To restrict user access to cloud resources based on job function/responsibilities To properly administer users throughout the life cycle from hire, to role change, to termination

***Configuration management***

To clearly define responsibilities for configuration management between the CSP and CSP user to restrict access to change virtual system configurations and provide logging of any such changes

* Information systems acquisition, development, and maintenance

***Change management***

To clearly define responsibilities for infrastructure change management between the CSP and CSP user to ensure that administrative privileges are properly restricted To ensure that changes are properly documented, authorized, approved, tested, and implemented

***Application maintenance***

To clearly define responsibilities for application change management between the CSP and CSP user to ensure that administrative privileges are properly restricted To ensure that changes are properly documented, authorized, approved, tested, and implemented

**PCI DSS**

Companies that process credit card transactions are required to comply with the Payment Card Industry (PCI) Data Security Standard (DSS) as evidenced through third-party assessments and/or self-assessments depending on the volume of card processing activity. These requirements apply whether cardholder data is processed and stored by the company or by a third party.

PCI DSS contains the following set of 12 high-level requirements that are supported by a series of more detailed requirements:

* + Install and maintain a firewall configuration to protect cardholder data.
  + Do not use vendor-supplied defaults for system passwords and other security parameters.
  + Protect stored cardholder data.
  + Encrypt transmission of cardholder data across open, public networks.
  + Use and regularly update antivirus software.
  + Develop and maintain secure systems and applications.
  + Restrict access to cardholder data based on the business’s need to know.
  + Assign a unique ID to each person with computer access.
  + Restrict physical access to cardholder data.
  + Track and monitor all access to network resources and cardholder data.
  + Regularly test security systems and processes.
  + Maintain a policy that addresses information security.

**Auditing the Cloud for Compliance**

Auditing the Cloud for Compliance deals with two perspectives:

First, what your organization’s internal audit department’s expectations are for meeting requirements, and the expectations that your external auditors have with regard to meeting requirements.

Internal Audit Perspective

A programmatic approach to compliance is particularly important in a cloud computing environment as the impact of a control failure could be quite severe. The CSP cannot afford to wait until the annual external audit to determine whether controls have operated effectively during the past year, because of the increased potential for control failures impacting multiple customers. Key controls must be identified early on and proactively monitored so that any potential issues can be investigated and addressed in a timely manner.

External Audit Perspective

An external audit of the CSP will likely be required for customers to gain comfort in the effectiveness of the CSP’s controls. Historically, a variety of audit frameworks have been used to assess the controls of outsourced service providers, including CSPs. Some of the most common audit frameworks are summarized here and described in the section that follows. Although some CSPs have been completing such external audits for five or more years, an increasing number of CSPs are now initiating external audits for the first time in response to increasing market pressure.

**Audit framework**

***SAS 70***

Audit of controls based on control objectives and control activities (defined by the service provider). Auditor opinion on the design, operational status, and operating effectiveness of controls. Intended to cover services that are relevant for purposes of customers’ financial statement audits.

***SysTrust***

Audit of controls based on defined principles and criteria for security, availability, confidentiality, and processing integrity. Intended to apply to the reliability of any system.

***WebTrust***

Audit of controls based on defined principles and criteria for security, availability, confidentiality, processing integrity, and privacy. Intended to apply to online/e-commerce systems.

***ISO 27001***

Audit of an organization’s Information Security Management System (ISMS), as defined in a documented ISMS.