Module 2

Cloud security

Customer responsibilities

The following are the responsibilities of customers from an IAM perspective:

User provisioning

- User provisioning methods are typically unique to the SaaS provider. Customers need to understand the preferred method, lag time to activate users, and user attributes that are supported by the SaaS service.
- Most often the provisioning process is manual and may involve uploading spreadsheets or documents in XML format. Almost all SaaS providers support bulk upload of user identities, as that's the most common use case for provisioning users.
- Some SaaS providers may support just-in-time provisioning where user identities are created on the fly using a provisioning request (sometimes SPML-employed) that is usually triggered by user activity such as the user clicking on a hyperlink that is unique to the user identity.

Profile management

- As part of the provisioning process, customers may have the ability to create user profiles that play a role in user authorization.
- User profiles such as user and manager are an approach to assigning entitlements to users within the SaaS application.
- Admittedly, these are not sophisticated features and will require customers to understand the flexibility and management of the profiles.

SaaS IAM capability evaluation

- Customers are responsible for evaluating the support for IAM features such as SSO (using identity federation) by CSPs. SAML is the de facto standard for federating identities and is now supported by large SaaS providers (among them Google and Salesforce.com).

- However, not all providers are supporting SAML 2.0, and some may support only SAML 1.1.
- For example, Salesforce.com supports SAML 1.1 while Google Apps supports SAML 2.0. Hence, it is important to understand what federation protocols are supported by which providers and the integration requirements to federate and support SSO.

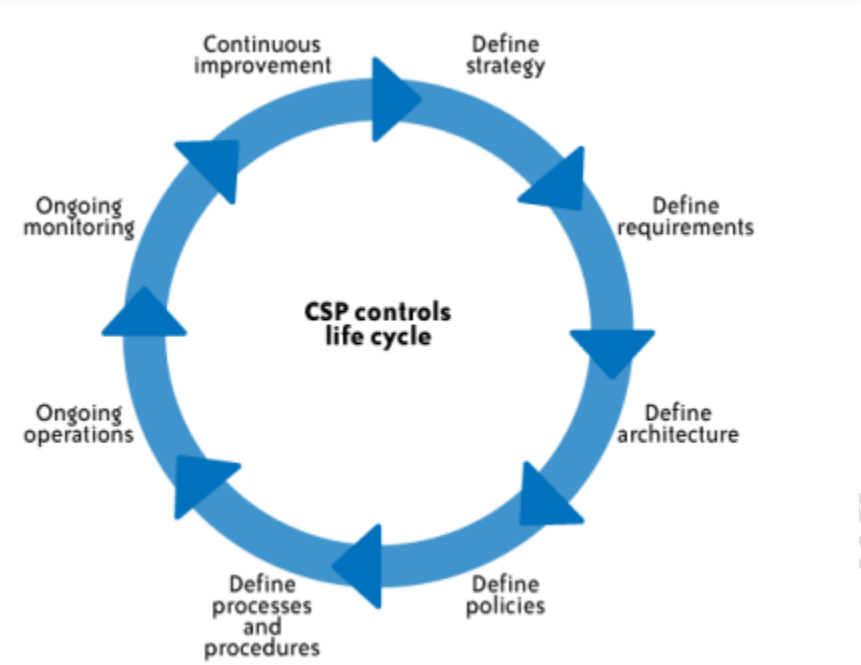
Investigation support

- Logs and audit trails are also often needed to investigate incidents. For example, PCI DSS requires the provider to "provide for timely forensic investigation" if the service provider suffers a breach.
- Since the SaaS provider's logs are internal and are not necessarily accessible externally or by customers, monitoring (let alone investigation) is difficult.
- Since access to logs is required for PCI compliance and may be requested by auditors and regulators make sure to negotiate access to the provider's logs as part of any service agreement.

Compliance management

- Although the same security concerns companies already have within their own networks—securing the network, hardware, applications, and data—apply for companies outsourcing their data with SaaS, trust and transparency exacerbate the situation in cloud computing.
- When compliance with government regulations such as SOX, the GrammLeach-Bliley Act (GLBA), and HIPAA and with industry standards such as PCI DSS come into the scope of the data hosted in SaaS, it could be challenging to meet those demands.
- In general, customers of SaaS services are responsible for compliance management, although the provider hosts the data.
- Make an effort to understand the access control, logging, reporting, and auditing capabilities offered by SaaS providers and assess whether those controls are adequate to meet compliance management requirements.

Compliance and Audit Security Recommendations.



1. **Define strategy**

- As a CSP undertakes to build out or take a fresh look at its service offerings, the CSP should clearly define its business strategy and related risk management philosophy. What market segments or industries does the CSP intend to serve?
- This strategic decision will drive the decision of how high the CSP needs to "set the bar" for its controls. This is an important decision, as setting it too low will make it difficult to meet the needs of new customers and setting it too high will make it difficult for customers to implement and difficult for the CSP to maintain in a cost-effective manner.
- A clear strategy will enable the CSP to meet the baseline requirements of its customers in the short term and provide the flexibility to incorporate necessary changes while resisting unnecessary or potentially unprofitable customization.

2. **Define requirements**

- Having defined its strategy and target client base, the CSP must define the requirements for providing services to that client base.
- What specific regulatory or industry requirements are applicable? Are there different levels of requirements for different sets of clients?

- The CSP will need to determine the minimum set of requirements to serve its client base and the incremental industry-specific requirements.
- For example, the CSP will need to determine whether it supports all of those requirements as part of a base product offering or whether it offers incremental product offerings with additional capabilities at a premium, now or in a future release.

3. Define architecture

- Driven by its strategy and requirements, the CSP must now determine how to architect and structure its services to address customer requirements and support planned growth.
- As part of the design, for example, the CSP will need to determine which controls are implemented as part of the service by default and which controls (e.g., configuration settings, selected platforms, or workflows) are defined and managed by the customer.

4. Define policies

- The CSP needs to translate its requirements into policies. In defining such policies, the CSP should draw upon applicable industry standards
- The CSP will also need to take a critical look at its staffing model and ensure alignment with policy requirements.

5. Define processes and procedures

- The CSP then needs to translate its policy requirements into defined, repeatable processes and procedures—again using applicable industry standards and leading practices guidance. Controls should be automated to the greatest extent possible for scalability and to facilitate monitoring.

6. Ongoing operations

- Having defined its processes and procedures, the CSP needs to implement and execute its defined processes, again ensuring that its staffing model supports the business requirements.

7. Ongoing monitoring

- The CSP should monitor the effectiveness of its key control activities on an ongoing basis with instances of non-compliance reported and acted upon. Compliance with the relevant internal and external requirements should be realized as a result of a robust monitoring program.

8. Continuous improvement

- As issues and improvement opportunities are identified, the CSP should ensure that there is a feedback loop to guarantee that processes and controls are continuously improved as the organization matures and customer requirements evolve.

Changing provider's reasons

1. Pricing

- Prices are constantly changing, and they don't always trend downward. Some providers may woo customers with attractively low rates, only to increase those costs after the first year contract expires.
- Some providers charge for certain services such as 24/7 support, while other providers may include such perks in their monthly service packages at no additional cost. These additional charges can add up over time, making some providers more expensive than they initially appear.
- When considering the cost of your service provider, compare apples to apples rather than apples to oranges. When reviewing your current plan, be sure that any new quotes are truly comparable.
- Make sure the details are the same, from storage and services to speeds and contracts. More often than not, businesses get excited about what appears to be a cheaper plan and may leave their current provider, only to be disheartened when they realize the new provider isn't as great or as cheap as they'd hoped.
- Keep in mind that switching providers are often a fair amount of work and time, the cost savings provided by switching providers should be significant enough to justify the transition.

2. Security Issues

- According to industry professionals, providers who do not prioritize security at every level put their client's data at serious risk.
- The **rise of ransomware** is proof that bad actors will stop at nothing to get a hold of your organization's critical data.
- If you feel that your provider isn't taking your security seriously it's time to switch. The security of your data is paramount and could have significant impacts on your bottom line and reputation if mishandled.

- Having an SLA that includes details about your security requirements is key to establishing a clear understanding from the get-go.

3. Problems with Your Service Level Agreement (SLA)

- Some service providers fail to provide SLAs. **SLAs are key to protecting both the client and provider**, they create peace of mind for both parties, establish clear and measurable guidelines for the relationship and provide recourse for unmet obligations.
- It is highly recommended that your organization request an SLA from your provider, if they are unable to meet this request, I would suggest considering a different provider.
- An SLA protects both parties and establishes a legal contract, I would be suspicious of a provider that doesn't want an SLA or at least doesn't give you a darn good reason for why they don't want one.
- If you do have an SLA with your provider but find that it doesn't meet your changing needs or you find issues with the current agreement, suggest making changes. If these changes can't be accommodated, changing providers is a viable option.

4. Our Needs Are Not Being Met

- Whether your needs aren't being met because your needs have changed or simply your provider isn't meeting the needs discussed in your contract, a change of provider should be considered.
- Discuss with your provider and re-iterate your needs, if they're still not able to meet them (depending on the importance and severity of the problem) you may need to change providers immediately.
- If your needs have changed and your current provider is unable to meet these new demands you may need to bring in a second provider to assist with these new needs or switch providers entirely.
- For example, not all providers offer **platform as a service (PaaS)** or Disaster **Recovery as a Service** (DRaaS). These are highly valuable services, if you aren't considering them now you may require them in the future, it's important to choose a provider that offers a wide portfolio of services, supporting your business as it expands and evolves.

5. Simple, Quick Installation

One of the major benefits of cloud-based offerings is that there is no installation; it is all running through the existing browser. No long installers, files to open and save, or slow desktop run speeds. A customer expects that once they make the purchase, within a matter of a few minutes the product should be operational.

Changing provider's expectations

1. **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.
- CSPs generally use weak authentication mechanisms (e.g., username + password), and the authorization ("access") controls available to users tend to be quite coarse and not very granular.
- For large organizations, this coarse authorization presents significant security concerns unto itself. Often, the only authorization levels cloud vendors provide are administrator authorization (i.e., the owner of the account itself) and user authorization (i.e., all other authorized users)—with no levels in between (e.g., business unit administrators, who are authorized to approve access for their own business unit personnel).
- Second potential concern: how is the data that is stored in the cloud actually protected? For all practical purposes, protection of data stored in the cloud involves the use of encryption.
- So, is a customer's data actually encrypted when it is stored in the cloud? And if so, with what encryption algorithm, and with what key strength? It depends, and specifically, it depends on which CSP you are using.
- For example, EMC's MozyEnterprise does encrypt a customer's data. However, AWS S3 does not encrypt a customer's data. Customers are able to encrypt their own data themselves prior to uploading, but S3 does not provide encryption.
- If a CSP does encrypt a customer's data, the next consideration concerns what encryption algorithm it uses.

- Not all encryption algorithms are created equal.
- Cryptographically, many algorithms provide insufficient security. Only algorithms that have been publicly vetted by a formal standards body (e.g., NIST) or at least informally by the cryptographic community should be used.
- Any algorithm that is proprietary should absolutely be avoided.
- Note that we are talking about symmetric encryption algorithms here. Symmetric encryption (see Figure 1) involves the use of a single secret key for both the encryption and decryption of data.
- Only symmetric encryption has the speed and computational efficiency to handle encryption of large volumes of data.
- It would be highly unusual to use an asymmetric algorithm for this encryption use case. (See Figure) Although the example in Figure 2 is related to email, the same concept (i.e., a single shared, secret key) is used in data storage encryption.

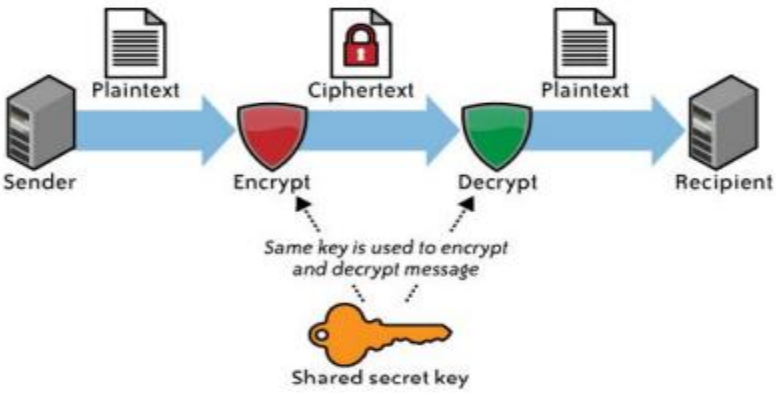


fig 1

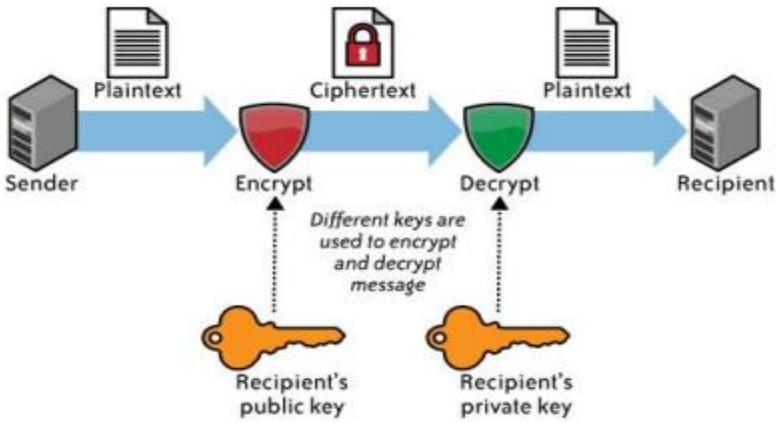


fig 2

2. 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.
- Encryption alone is sufficient for confidentiality, but integrity also requires the use of message authentication codes (MACs).
- The simplest way to use MACs on encrypted data is to use a block symmetric algorithm
- Another aspect of data integrity is important, especially with bulk storage using IaaS. Once a customer has several gigabytes (or more) of its data up in the cloud for storage, how does the customer check on the integrity of the data stored there?
- There are IaaS transfer costs associated with moving data into and back down from the cloud,*as well as network utilization (bandwidth) considerations for the customer's own network.
- What a customer really wants to do is to validate the integrity of its data while that data remains in the cloud—without having to download and reupload that data.
- This task is even more difficult because it must be done in the cloud without explicit knowledge of the whole data set.
- Customers generally do not know on which physical machines their data is stored, or where those systems are located. Additionally, that data set is probably dynamic and changing frequently.
- Those frequent changes obviate the effectiveness of traditional integrity insurance techniques.
- **What is needed instead is a proof of retrievability—that is, a mathematical way to verify the integrity of the data as it is dynamically stored in the cloud.**

3. Availability

- Assuming that a customer's data has maintained its confidentiality and integrity, you must also be concerned about the availability of your data
- . There are currently three major threats in this regard—none of which are new to computing, but all of which take on increased importance in cloud computing because of increased risk.
- The first threat to availability is network-based attacks
- The second threat to availability is the CSP's own availability. No CSPs offer the sought-after "five 9s" (i.e., 99.999%) of uptime. A customer would be lucky to get "three 9s" of uptime.

- A number of high-profile cloud provider outages have occurred. For example, Amazon's S3 suffered a 2.5-hour outage in February 2008 and an eight-hour outage in July 2008.
- In addition to service outages, in some cases data stored in the cloud has actually been lost. For example, in March 2009, "cloud-based storage service provider Carbonite Inc. filed a lawsuit charging that faulty equipment from two hardware providers caused backup failures that resulted in the company losing data for 7,500 customers two years ago.
- A larger question for cloud customers to consider is whether cloud storage providers will even be in business in the future.
- In February 2009, cloud provider Coghead suddenly shut down, giving its customers fewer than 90 days (nine weeks) to get their data off its servers—or lose it altogether.
- Finally, prospective cloud storage customers must be certain to ascertain just what services their provider is actually offering.
- Cloud storage does not mean the stored data is actually backed up. Some cloud storage providers do back up customer data, in addition to providing storage.
- However, many cloud storage providers do not back up customer data, or do so only as an additional service for an additional cost.
- For example, "data stored in Amazon S3, Amazon SimpleDB, or Amazon Elastic Block Store is redundantly stored in multiple physical locations as a normal part of those services and at no additional charge

IaaS Cloud Solutions

- Iaas is also known as **Hardware as a Service (HaaS)**. It is one of the layers of the cloud computing platform. It allows customers to outsource their IT infrastructures such as servers, networking, processing, storage, virtual machines, and other resources. Customers access these resources on the Internet using a pay-as-per use model.
- In traditional hosting services, IT infrastructure was rented out for a specific period of time, with pre-determined hardware configuration.
- The client paid for the configuration and time, regardless of the actual use. With the help of the IaaS cloud computing platform layer, clients can dynamically scale the configuration to meet changing requirements and are billed only for the services actually used.
- IaaS cloud computing platform layer eliminates the need for every organization to maintain the IT infrastructure.

- IaaS is offered in three models: public, private, and hybrid cloud. The private cloud implies that the infrastructure resides at the customer-premise.
- In the case of public cloud, it is located at the cloud computing platform vendor's data center, and the hybrid cloud is a combination of the two in which the customer selects the best of both public cloud or private cloud.

- IaaS provider provides the following services -

1. **Compute:** Computing as a Service includes virtual central processing units and virtual main memory for the Vms that is provisioned to the end- users.
2. **Storage:** IaaS provider provides back-end storage for storing files.
3. **Network:** Network as a Service (NaaS) provides networking components such as routers, switches, and bridges for the Vms.
4. **Load balancers:** It provides load balancing capability at the infrastructure layer.

PaaS Cloud Solutions

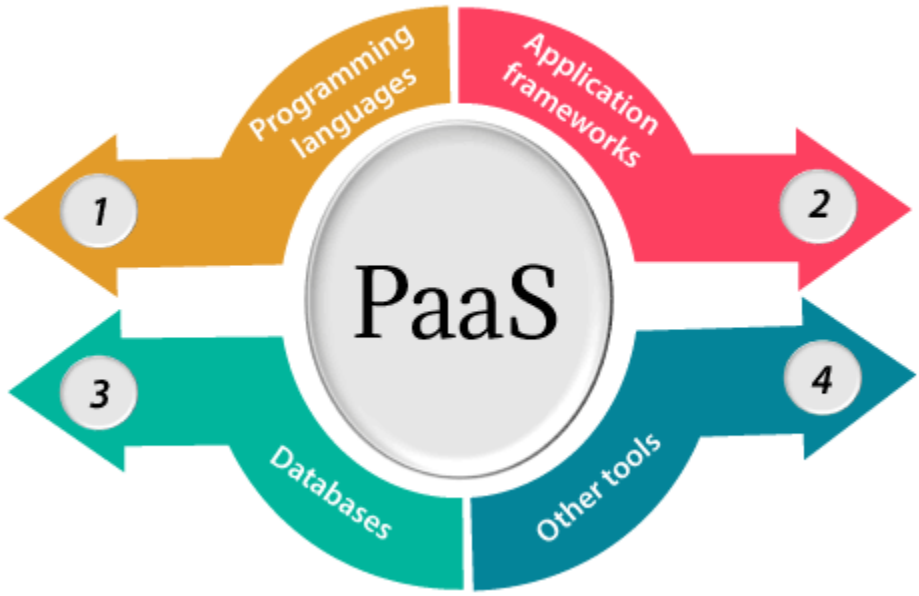
- Platform as a Service (PaaS) provides a runtime environment. It allows programmers to easily create, test, run, and deploy web applications. You can purchase these applications

from a cloud service provider on a pay-as-per use basis and access them using the Internet connection.

- In PaaS, back end scalability is managed by the cloud service provider, so end- users do not need to worry about managing the infrastructure.
- PaaS includes infrastructure (servers, storage, and networking) and platform (middleware, development tools, database management systems, business intelligence, and more) to support the web application life cycle.

Example: Google App Engine, Force.com, Joyent, Azure.

- PaaS providers provide the Programming languages, Application frameworks, Databases, and Other tools:



1. Programming languages

PaaS providers provide various programming languages for the developers to develop the applications. Some popular programming languages provided by PaaS providers are Java, PHP, Ruby, Perl, and Go.

2. Application frameworks

PaaS providers provide application frameworks to easily understand the application development. Some popular application frameworks provided by PaaS providers are Node.js, Drupal, Joomla, WordPress, Spring, Play, Rack, and Zend.

3. Databases

PaaS providers provide various databases such as ClearDB, PostgreSQL, MongoDB, and Redis to communicate with the applications.

4. Other tools

PaaS providers provide various other tools that are required to develop, test, and deploy the applications.

SaaS Cloud Solutions.

SaaS is also known as "**On-Demand Software**". It is a software distribution model in which services are hosted by a cloud service provider. These services are available to end-users over the internet so, the end-users do not need to install any software on their devices to access these services.

There are the following services provided by SaaS providers -

Business Services - SaaS Provider provides various business services to start-up the business. The SaaS business services include **ERP** (Enterprise Resource Planning), **CRM** (Customer Relationship Management), **billing**, and **sales**.

Document Management - SaaS document management is a software application offered by a third party (SaaS providers) to create, manage, and track electronic documents.

Example: Slack, Samepage, Box, and Zoho Forms.

Social Networks - As we all know, social networking sites are used by the general public, so social networking service providers use SaaS for their convenience and handle the general public's information.

Mail Services - To handle the unpredictable number of users and load on e-mail services, many e-mail providers offering their services using SaaS.