# UNIT V

This unit identifies current security concerns about cloud computing environments and describes the methodology for ensuring application and data security and compliance integrity for those resources that are moving from on-premises to public cloud environments. It focuses on why and how these resources should be protected in the Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) environments and offers security "best practices" for service providers and enterprises. let's review the concepts of the three major cloud computing service provider models.

**Software-as-a-Service**

It is a model of software deployment in which an application is licensed for use as a service provided to customers on demand

**Platform-as-a-Service**

With the PaaS model, all of the facilities required to support the complete life cycle of building and delivering web applications and services are available to developers, IT managers, and end users entirely from the Internet, without software downloads or installation.

**Infrastructure-as-a-Service**

It is the delivery of computer infrastructure as a service. Rather than purchasing servers, software, data center space, or network equipment, clients buy these resources as a fully outsourced service.

**IT-as-a-Service (ITaaS)** is being proposed to bring the service model right to your IT infrastructure. Many organizations are in the process of transforming their IT departments into self-sustaining cost-center operations, treating internal users as if they were customers. Many large IT organizations have adopted the Information Technology Infrastructure Library (ITIL) framework to help with this transformation. The adoption of IT-as-a-Service can help enterprise IT functions focus on strategic alignment with business goals.

There are some key financial benefits in moving to an ITaaS model, such has not having to incur capital costs; having a transparent, monthly pricing plan; scalability; and reasonable costs of expansion. Operational benefits of ITaaS include increased reliability because of a centralized infrastructure, which can ensure that critical services and applications are monitored continually; software flexibility, with centrally maintained products that allow for quick rollout of new functionalities and updates; and data security.

## Cloud Security Challenges

With the cloud model, we lose control over physical security. In a public cloud, we are sharing computing resources with other companies. In a shared pool outside the enterprise, we don't have any knowledge or control of where the resources run. Simply because you share the environment in the cloud, may put your data at risk of seizure.

Storage services provided by one cloud vendor may be incompatible with another vendor's services. For instance, Amazon's "Simple Storage Service" [S3] is incompatible with IBM's Blue Cloud, or Google, or Dell.

If information is encrypted while passing through the cloud, who controls the encryption/decryption keys? Is it the customer or the cloud vendor? It should be ensured that the customer, control encryption/decryption keys, just as if the data were still resident on your own servers.

Data integrity means ensuring that data is identically maintained during any operation (such as transfer, storage, or retrieval). Ensuring the integrity of the data really means that it changes only in response to authorized transactions.

Choice of development tool should have a security model embedded in it to guide developers during the development phase and restrict users only to their authorized data when the system is deployed into production.

As more and more mission-critical processes are moved to the cloud, SaaS suppliers will have to provide log data in a real-time, straightforward manner, probably for their administrators as well as their customers' personnel.

Cloud applications undergo constant feature additions, and users must keep up to date with application improvements to be sure they are protected. The speed at which applications will change in the cloud will affect both the SDLC and security.

Security needs to move to the data level, so that enterprises can be sure their data is protected wherever it goes. Sensitive data is the domain of the enterprise, not the cloud computing provider. One of the key challenges in cloud computing is data-level security. Those who adopt cloud computing must remember that it is the responsibility of the data owner, not the service provider, to secure valuable data.

Some countries have strict limits on what data about its citizens can be stored and for how long, and some banking regulators require that customers' financial data remain in their home country.

Government policy will need to change in response to both the opportunity and the threats that cloud computing brings. This will likely focus on the off-shoring of personal data and protection of privacy, whether it is data being controlled by a third party or off-shored to another country.

Security managers will need to work with their company's legal staff to ensure that appropriate contract terms are in place to protect corporate data and provide for acceptable service-level agreements.

The dynamic and fluid nature of virtual machines will make it difficult to maintain the consistency of security and ensure the auditability of records. The ease of cloning and distribution between physical servers could result in the propagation of configuration errors and other vulnerabilities.

Enterprises are often required to prove that their security compliance is in accord with regulations, standards, and auditing practices, regardless of the location of the systems at which the data resides.

Operating system and application files are on a shared physical infrastructure in a virtualized cloud environment and require system, file, and activity monitoring to provide confidence and auditable proof to enterprise customers that their resources have not been compromised or tampered with.

To establish zones of trust in the cloud, the virtual machines must be self-defending, effectively moving the perimeter to the virtual machine itself. Enterprise perimeter security (i.e., firewalls, demilitarized zones [DMZs], network segmentation, intrusion detection and prevention systems [IDS/IPS], monitoring tools, and the associated security policies) only controls the data that resides and transits behind the perimeter.

## Software-as-a-Service Security

There are seven security issues

***Privileged user access***

- Inquire about who has specialized access to data, and about the hiring and management of such administrators.

***Regulatory compliance***

- Make sure that the vendor is willing to undergo external audits and/or security certifications.

***Data location***

- Does the provider allow for any control over the location of data?

***Data segregation***

- Make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals.

***Recovery***

- Find out what will happen to data in the case of a disaster. Do they offer complete restoration? If so, how long would that take?

***Investigative support***

- Does the vendor have the ability to investigate any inappropriate or illegal activity?

***Long-term viability***

- What will happen to data if the company goes out of business? How will data be returned, and in what format?

To address the security issues listed above along with others mentioned earlier in the chapter, SaaS providers will need to incorporate and enhance security practices used by the managed service providers and develop new ones as the cloud computing environment evolves.

## Security Governance

Security governance is the mechanism through which organizations can ensure effective management of security in the Cloud. To address governance, the level of risk and complexity of each cloud deployment must be taken into consideration. Public Cloud has highest risk due to lack of security control, multi-tenancy, data management, limited SLA and lack of common regulatory controls. Private Cloud has least risk due to single ownership and strong shared mission goals and legal/regulatory requirements. Risks in hybrid cloud dependent upon combined models. Combination of private/community is lowest risk, while combination of public is greatest risk. Security Governance Framework can be established with standard quality management cycle of continuous improvement. The outcome of the effective framework would be strategic alignment, value delivery, risk management and performance measurement.

A security steering committee should be developed whose objective is to focus on providing guidance about security initiatives and alignment with business and IT strategies. A charter for the security team is typically one of the first deliverables from the steering committee. This charter must clearly define the roles and responsibilities of the security team and other groups involved in performing information security functions.

By following guidelines, a security governance framework is expected to be established in the cloud provider's organization.

**Start with your people:** Awareness must be created among all employees about significance of security, how it can affect the goodwill of organization and what they can and must do.

**Audit compliance:** It is required to make a horizontal audit compliance framework that provides a view across all business units and combines the respective information streams.

**Identity and access management (IAM):** Insider threats can be overcome by a strict Identity and Access Management solution that will allow IT managers to track privileged access to sensitive data and also allow them to assign or revoke these privileges.

**Security information and event management (SIEM):** Combines security incident and security event management to ensure a complete view of the organization's security posture.

**Look for guidance but ensure your own security:** Cloud Security Alliance (CSA) provides good security guidance for cloud computing. Use standards as guidance and develop your own security policies to build security governance framework

**Governance framework solution:** Build a framework by using Business Service Management (BSM) solution that has drill-down functionality to all IT governance, risk and compliance (GRC) and security elements.

## Risk Management

It is necessary to identify, control and eliminate/ minimizing uncertain events or threats which many affect system resources. This system includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review

Effective risk management entails

- identification of technology assets
- identification of data and its links to business processes, applications, and data stores
- assignment of ownership and custodial responsibilities

A formal risk assessment process should be created that allocates security resources linked to business continuity.

Effective risk management entails identification of technology assets; identification of data and its links to business processes, applications, and data stores; and assignment of ownership and custodial responsibilities. Actions should also include maintaining a repository of information assets. Owners have authority and accountability for information assets including protection requirements, and custodians implement confidentiality, integrity, availability, and privacy controls. A formal risk assessment process should be created that allocates security resources linked to business continuity.

## Risk Assessment

A formal information security risk management process should proactively assess information security risks as well as plan and manage them on a periodic or as-needed basis. More detailed and technical security risk assessments in the form of threat modeling should also be applied to applications and infrastructure. It can help the product management and engineering groups to be more proactive in designing and testing the security of applications and systems and to collaborate more closely with the internal security team. Threat modeling requires both IT and business process knowledge, as well as technical knowledge of how the applications or systems under review work.

## Security Monitoring

Centralized security information management systems should be used to provide notification of security vulnerabilities and to monitor systems continuously through automated technologies to identify

potential issues. They should be integrated with network and other systems monitoring processes (e.g., security information management, security event management, security information and event management, and security operations centers that use these systems for dedicated 24/7/365 monitoring). Management of periodic, independent third-party security testing should also be included.

The types and sophistication of threats and attacks for a SaaS organization require a different approach to security monitoring than traditional infrastructure and perimeter monitoring. The organization may thus need to expand its security monitoring capabilities to include application- and data-level activities. This may also require subject-matter experts in applications security and the unique aspects of maintaining privacy in the cloud. Without this capability and expertise, a company may be unable to detect and prevent security threats and attacks to its customer data and service stability.

## Secure Software Development Life Cycle (SecSDLC)

It involves identifying specific threats and the risks they represent, followed by design and implementation of specific controls to counter those threats and assist in managing the risks they pose to the organization and/or its customers. The SecSDLC must provide consistency, repeatability, and conformance. The SDLC consists of six phases which are listed below:

1. **Investigation:** Define project processes and goals, and document them in the program security policy.

2. **Analysis:** Analyze existing security policies and programs, analyze current threats and controls, examine legal issues, and perform risk analysis.

3. **Logical design:** Develop a security blueprint, plan incident response actions, plan business responses to disaster, and determine the feasibility of continuing and/or outsourcing the project.

4. **Physical design:** Select technologies to support the security blueprint, develop a definition of a successful solution, design physical security measures to support technological solutions, and review and approve plans.

5. **Implementation:** Buy or develop security solutions. At the end of this phase, present a tested package to management for approval.

6. **Maintenance:** Constantly monitor, test, modify, update, and repair to respond to changing threats.

In the SecSDLC, application code is written in a consistent manner that can easily be audited and enhanced; core application services are provided in a common, structured, and repeatable manner; and

framework modules are thoroughly tested for security issues before implementation and continuously retested for conformance through the software regression test cycle. Additional security processes are developed to support application development projects such as external and internal penetration testing and standard security requirements based on data classification. Formal training and communications should also be developed to raise awareness of process enhancements.

## Security Architecture Design

A security architecture framework should be established with consideration of processes, operational procedures, technology specifications, people and organizational management, and security program compliance and reporting.

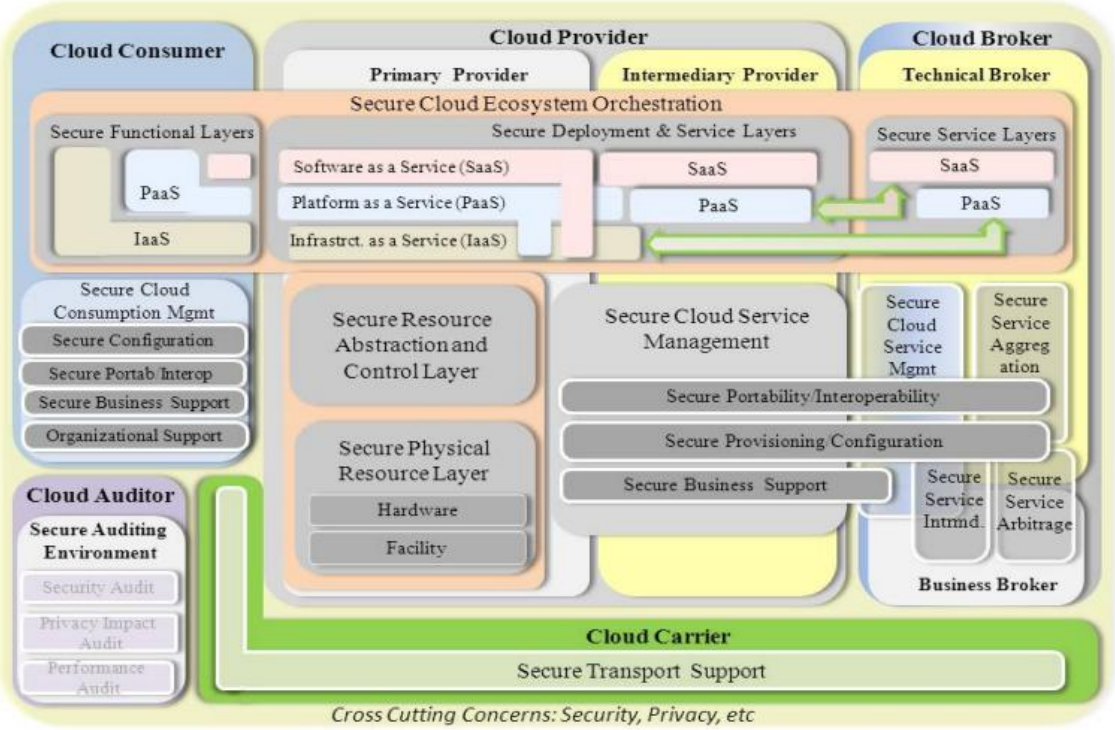
A security architecture document should be developed that defines security and privacy principles to meet business objectives. Documentation is required for management controls and metrics specific to asset classification and control, physical security, system access controls, network and computer management, application development and maintenance, business continuity, and compliance.

A design and implementation program should also be integrated with the formal system development life cycle to include a business case, requirements definition, design, and implementation plans. Technology and design methods should be included, as well as the security processes necessary to provide the following services across all technology layers:

- Authentication
- Authorization
- Availability
- Confidentiality
- Integrity
- Accountability
- Privacy

The creation of a secure architecture provides the engineers, data center operations personnel, and network operations personnel a common blueprint to design, build, and test the security of the applications and systems. Design reviews of new changes can be better assessed against this architecture to assure that they conform to the principles described in the architecture, allowing for more consistent and effective design reviews.

NIST introduced the security architecture reference model which contains the responsibilities of security controls throughout the cloud life cycle. The level of involvement for each actor in implementing security components is considered for each environment (service deployment model). Architectural Components and Sub-Components are deployed with security characteristics and technical brokers are assisting to get secure Cloud Service Management.




## Data Security

Security will need to move to the data level so that enterprises can be sure their data is protected wherever it goes. It can also force encryption of certain types of data, and permit only specified users to access the data. It can provide compliance with the Payment Card Industry Data Security Standard (PCIDSS).

There are complex data security challenges in the cloud:

- The need to protect confidential business, government, or regulatory data
- Cloud service models with multiple tenants sharing the same infrastructure
- Data mobility and legal issues relative to such government rules as the EU Data Privacy Directive
- Lack of standards about how cloud service providers securely recycle disk space and erase existing data
- Auditing, reporting, and compliance concerns
- Loss of visibility to key security and operational intelligence that no longer is available to feed enterprise IT security intelligence and risk management

Traditional models of data security have focused on network-centric and perimeter security, frequently with devices such as firewalls and intrusion detection systems. But this approach does not provide sufficient protection against APTs, privileged users, or other insidious types of security attacks. Any data-centric approach must incorporate encryption, key management, strong access controls, and security

intelligence to protect data in the cloud and provide the requisite level of security. By implementing a layered approach that includes these critical elements, organizations can improve their security posture more effectively and efficiently.

The strategy should incorporate a blueprint approach that addresses compliance requirements and actual security threats. Best practices should include securing sensitive data, establishing appropriate separation of duties between IT operations and IT security, ensuring that the use of cloud data conforms to existing enterprise policies, as well as strong key management and strict access policies. Protecting your data in the cloud is also done by implementing:

- Access control lists to define the permissions attached to the data objects
- Storage encryption to protect against unauthorized access at the data center (especially by malicious IT staff)
- Transport level encryption to protect data when it is transmitted
- Firewalls to include web application firewalls to protect against outside attacks launched against the data center
- Hardening of the servers to protect against known, and unknown, vulnerabilities in the operating system and software
- Physical security to protect against unauthorized physical access to data

## Application Security

Cloud providers ensure that applications available as a service via the cloud (SaaS) are secure by specifying, designing, implementing, testing and maintaining appropriate application security measures in the production environment. This is where the security features and requirements are defined and application security test results are reviewed. Application security processes, secure coding guidelines, training, and testing scripts and tools are typically a collaborative effort between the security and the development team.

External penetration testers are used for application source code reviews, and attack and penetration tests provide an objective review of the security of the application as well as assurance to customers that attack and penetration tests are performed regularly.

Since many connections between companies and their SaaS providers are through the web, providers should secure their web applications by following Open Web Application Security Project (OWASP) guidelines for secure application development and locking down ports and unnecessary commands on Linux, Apache, MySQL, and PHP (LAMP) stacks in the cloud, just as you would on-premises. LAMP is an open-source web development platform, also called a web stack that uses Linux as

the operating system, Apache as the web server, MySQL as the relational database management system RDBMS, and PHP as the object-oriented scripting language. Perl or Python is often substituted for PHP.

The following security risks within the application and business environment is critical for addressing the full scope of security and privacy issues

- **Loss of governance –** Because the organization may not have direct control of the infrastructure, trust in the provider and its own ability to provide proper security is paramount
- **Compliance risk** – The cloud provider impacts the organization's ability to comply with regulations, privacy expectations and industry standards, because data and systems may exist outside the organization's direct control.
- **Isolation failure** – Multi-tenancy and resource sharing are defining characteristics of the cloud. It is entirely possible for competing companies to be using the same cloud services, in effect running their workloads shoulder-to-shoulder. Keeping memory, storage and network access separate is essential.
- **Data protection** – Because the organization relinquishes direct control over data, it relies on the provider to keep that data secure, and when it is deleted, ensure that it is permanently destroyed.
- **Management interface and role-based access** – Cloud applications are accessed and managed through the Internet, and involve deep and extensive control. The risk associated with a security breach is therefore increased and proper access authorization must be carefully considered.

## Virtual Machine Security

Firewalls, intrusion detection and prevention, integrity monitoring, and log inspection can all be deployed as software on virtual machines to increase protection and maintain compliance integrity of servers and applications as virtual resources move from on-premises to public cloud environments.

To facilitate the centralized management of a server firewall policy, the security software loaded onto a virtual machine should include a bidirectional stateful firewall that enables virtual machine isolation and location awareness, thereby enabling a tightened policy and the flexibility to move the virtual machine from on-premises to cloud resources. Integrity monitoring and log inspection software must be applied at the virtual machine level.

The security issues related with managing images, virtual machine monitoring, networking, integrity, confidentiality, privacy and availability.

**Managing images**

VMs images contain information of files, processes and memory blocks of the guest OS. Images are kept in offline at an image repository. Even in offline, they are vulnerable to the theft and code injection. The administrator of image repository risks hosting and distributing malicious images. Images

should converge to a steady state by performing scans for worms and other virus. Otherwise infected VMs can sporadically disseminate malware. Another issue is VM sprawl, it is the possibility of having the number of VMs continuously growing while most of them are idle or never back sleep in turn wasting resources. A cloud user risks running vulnerable, malicious, out-of-date /unlicensed images stored at insecure, unadministrated repository.

**Monitoring VMs**

One of the VMM vulnerability is, VM escape refers to the case of gaining access of VMM through a VM, which is capable of attacking VMs monitored by the same VMM. In the virtualization environment, one could be capable of gaining access to VMMs or VMs. Hyper VM was once exploited without the knowledge of the provider, resulting in the destruction of many websites. The ease of cloning and distributing VMs throughout cloud servers can propagate errors and make raise to other vulnerabilities.

**Networking**

Vulnerabilities in the DNS servers affect cloud. Incorrect virtualization may allow the user to access the sensitive portions of the underlying infrastructure, disclosing sensitive knowledge of the real network or resources from other users. Virtualization software may also have vulnerabilities that enable network based VM attacks. VMs are likely to be copied or moved to other servers via network links, enabling quick deployments, but also quick spread of vulnerable configurations and images theft. A template image may retain original owner information may leak sensitive information like secret key cryptographic salt values.

**Integrity, Confidentiality and Privacy**

VM hopping is a term used to refer malicious gain of access to another VM belonging to a different cloud user, which may happen due to VMM isolation failure. Thus integrity, confidentiality and privacy properties are compromised by such attacks. By exploiting VM relocation, one can gain the access to get plain text passwords in memory dumps of VM. The availability is also compromised because attacker can stop the services or ruin boot configurations so that VMs fixed.