UNIT 5

SECURITY IN THE CLOUD

Security, Cloud Security Challenges, Infrastructure Security: Network, Host and Application level, Data security and Storage, Security Management in the cloud, Data Privacy, Life cycle of Data, Key Privacy concerns in cloud and Disaster Recovery.

SECURITY :- In the computer industry, the term **security** or the phrase **computer security** --refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Most computer security measures involve **data encryption** and **passwords**.

•**Data encryption** is the translation of data into a form that is unreadable without a deciphering mechanism.

•A **password** is a secret word or phrase that gives a user access to a particular program or system.

CLOUD COMPUTING SECURITY CHALLENGES:-

- Cloud computing opens up a new world of opportunities for businesses, but mixed in with these opportunities are numerous security challenges that need to be considered and addressed prior to committing to a cloud computing strategy.
- Cloud computing security challenges fall into three broad categories:

•**Data Protection:** Securing your data both at rest and in transit

•**User Authentication:** Limiting access to data and monitoring who accesses the data

•**Disaster and Data Breach Contingency Planning**

1. Data Protection

- Implementing a cloud computing strategy means placing critical data in the hands of a third party, so ensuring the data remains secure both at rest (data residing on storage media) as well as when in transit is of paramount importance.
- Data needs to be encrypted at all times, with clearly defined roles when it comes to who will be managing the encryption keys.
- In most cases, the only way to truly ensure confidentiality of encrypted data that resides on a cloud provider's storage servers is for the client to own and manage the data encryption keys.

2. User Authentication

- Data resting in the cloud needs to be accessible only by those authorized to do so, making it critical to both restrict and monitor who will be accessing the company's data through the cloud.
- In order to ensure the integrity of user authentication, companies need to be able to view **data access logs and audit** trails to verify that only authorized users are accessing the data.
- These access logs and audit trails additionally need to be secured and maintained for as long as the company needs or legal purposes require.

Bamuengine.com

- As with all cloud computing security challenges, it's the responsibility of the customer to ensure that the cloud provider has taken all necessary security measures to protect the customer's data and the access to that data.

3. **Contingency Planning**

- With the cloud serving as a single centralized repository for a company's mission-critical data, the risks of having that data compromised due to a data breach or temporarily made unavailable due to a natural disaster are real concerns.
- Much of the liability for the disruption of data in a cloud ultimately rests with the company whose mission-critical operations depend on that data, although liability can and should be negotiated in a contract with the services provider prior to commitment.
- A comprehensive security assessment from a neutral third-party is strongly recommended as well.
- Companies need to know how their data is being secured and what measures the service provider will be taking to ensure the integrity and availability of that data should the unexpected occur.
- Additionally, companies should also have contingency plans in place in the event their cloud provider fails or goes bankrupt.
- Can the data be easily retrieved and migrated to a new service provider or to a non-cloud strategy if this happens? And what happens to the data and the ability to access that data if the provider gets acquired by another company?

INFRASTRUCTURE SECURITY

Securing an organization's core IT infrastructure at

- The network Level
- The host Level and
- Application Levels

From the Threats and Vulnerabilities.

NOTE:-Infrastructure security is different from IAAS security.

INFRASTRUCTURE SECURITY: THE NETWORK LEVEL

- With private clouds, there are no new attacks, vulnerabilities, or changes in risk specific to this topology that information security personnel need to consider.
- Although our organization's IT architecture may change with the implementation of a private cloud, our current network topology will probably not change significantly.
- To use public cloud services, changing security requirements will require changes to our network topology. We must address how our existing network topology interacts with our cloud provider's network topology

Bamuengine.com

There are four significant risk factors in this use case:

1) Ensuring the confidentiality and integrity of our organization's data-in-transit to and from our public cloud provider

2) Ensuring proper access control (authentication, authorization, and auditing) to whatever resources we are using at our public cloud provider.

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

4) Replacing the established model of network zones and tiers with domains.

1) Ensuring Data Confidentiality and Integrity

- Some resources and data previously confined to a private network are now exposed to the Internet, and to a shared public network belonging to a third-party cloud provider.
- **An example** of problems associated with this risk factor is an Amazon Web Services (AWS) security vulnerability reported in December 2008
- Although use of HTTPS (instead of HTTP) would have mitigated the integrity risk, users not using HTTPS (but using HTTP) did face an increased risk that their data could have been altered in transit without their knowledge.

2) Ensuring Proper Access Control

- Network resources are put in public cloud, face many risks to its data.
- Ability to audit the operation of our cloud provider's network in non-existent.
- We will have decreased access to relevant network-level logs and data, and a limited ability to thoroughly conduct investigations and gather forensic data.
- **An example** of the problems associated with this risk factor is the issue of reused (reassigned) IP addresses.
- Cloud providers do not sufficiently "age" IP addresses when they are no longer needed for one customer.
- A customer can't assume that network access to its resources is terminated upon release of its IP address. There is necessarily a lag time between the change of an IP address in DNS and the clearing of that address in DNS caches. There is a similar lag time between when physical (i.e., MAC) addresses are changed in ARP (Address Resolution protocol) tables and when old ARP addresses are cleared from cache; an old address persists in ARP caches until they are cleared. This means that even though addresses might have been changed, the (now) old addresses are still available in cache, and therefore they still allow users to reach these supposedly non-existent resources. The issue of "non-aged" IP addresses and unauthorized network access to resources does not apply only to routable IP addresses (i.e., resources intended to be reachable directly from the Internet). The issue also applies to cloud providers' internal networks for customer use and the assignment of non-routable IP addresses

Bamuengine.com

- Although our resources may not be directly reachable from the Internet, for management purposes our resources must be accessible within the cloud provider's network via private addressing. (Every public/Internet facing resource also has a private address.) Other customers of our cloud provider may not be well intentioned and might be able to reach our resources internally via the cloud provider's networks.

3) Ensuring the Availability of Internet-Facing Resources

Reliance on network security has increased because an increased amount of data or an increased number of organizational personnel now depend on externally hosted devices to ensure the availability of cloud-provided resources. Consequently, the three risk factors enumerated in the preceding section must be acceptable to your organization.

a) <u>BGP(Broader Gateway Protocol) Prefix hijacking:</u>

→**Prefix hijacking** provides a good example of this risk factor

- Prefix hijacking involves announcing an autonomous system address space that belongs to someone else without her permission. Such announcements often occur because of a configuration mistake, but that **misconfiguration** may still affect the availability of your cloud-based resources.
- In addition to misconfigurations, there are **deliberate attacks** as well.
- Although prefix hijacking due to deliberate attacks is far less common than misconfigurations; it still occurs and can block access to data.
- Probably the best known example of such a misconfiguration mistake occurred in February 2008 when Pakistan Telecom made an error by announcing a dummy route for YouTube to its own telecommunications partner, PCCW, based in Hong Kong. The intent was to block YouTube within Pakistan because of some supposedly blasphemous videos hosted on the site. The result was that YouTube was *globally* unavailable for two hours.

b) **<u>DNS attacks</u>** are another example of problems associated with this risk factor. In fact, there are several forms of DNS attacks to worry about with regard to cloud computing.

- Not only vulnerabilities in the DNS protocol and in implementations of DNS, but also there are fairly widespread **DNS cache poisoning (DNS Spoofing)** attacks whereby a DNS server is tricked into accepting incorrect information.
- Variants of this basic cache poisoning attack include redirecting the target domain's name server (NS), redirecting the NS record to another target domain, and responding before the real NS (called **DNS forgery**).

c) A final example of problems associated with this third risk factor is **denial of service (DoS) and distributed denial of service (DDoS) attacks**

- Although DoS/DDoS attacks are not new and are not directly related to the use of cloud computing, the issue with these attacks and cloud computing is an increase in an organization's risk at the network level because of some increased use of resources external to your organization's network

Bamuengine.com

- When using IaaS, the risk of a DDoS attack is not only external (i.e., Internet-facing). There is also the risk of an internal DDoS attack through the portion of the IaaS provider's network used by customers (separate from the IaaS provider's corporate network). That internal (non-routable) network is a shared resource, used by customers for access to their non-public instances (e.g., Amazon Machine Images or AMIs) as well as by the provider for management of its network and resources (such as physical servers).

4) Replacing the Established Model of Network Zones and Tiers with Domains

- The established isolation model of network zones and tiers no longer exists in the public IaaS and PaaS clouds.
- For years, network security has relied on zones, such as intranet versus extranet and development versus production, to segregate network traffic for improved security. This model was based on exclusion
- Only individuals and systems in specific roles have access to specific zones. Similarly, systems within a specific tier often have only specific access within or across a specific tier. For example, systems within a presentation tier are not allowed to communicate directly with systems in the database tier, but can communicate only with an authorized system within the application zone.
- SaaS clouds built on public IaaS or PaaS clouds have similar characteristics. However, a public SaaS built on a private IaaS (e.g., Salesforce.com) may follow the traditional isolation model, but that topology information is not typically shared with customers.
- The traditional model of network zones and tiers has been replaced in public cloud computing with "security groups," "security domains" or "virtual data centers" that have logical separation between tiers but are less precise and afford less protection than the formerly established model.
- For example, the security groups feature in AWS allows your virtual machines (VMs) to access each other using a virtual firewall that has the ability to filter traffic based on IP address (a specific address or a subnet), packet types (TCP, UDP, or ICMP), and ports (or a range of ports).
- Domain names are used in various networking contexts and application-specific naming and addressing purposes, based on DNS.
- **In the established model** of network zones and tiers, not only were development systems logically separated from production systems at the network level, but these two groups of systems were also physically separated at the host level (i.e., they ran on physically separated servers in logically separated network zones). With cloud computing, however, this separation no longer exists.
- The cloud computing model of separation by domains provides logical separation for addressing purposes only.
- There is no longer any "required" physical separation, as a test domain and a production domain may very well be on the same physical server. Furthermore, the former logical network separation no longer exists; logical separation now is at the host level with both domains running on the same physical server and being separated only logically by VM monitors (hypervisors).

Bamuengine.com

INFRASTRUCTURE SECURITY: THE HOST LEVEL

1. SAAS and PAAS Host Security
2. IAAS Host Security

a) Virtualization software Security
b) Securing virtual servers
c) Virtual Server security
d) Threats to the hypervisor

1) SaaS and PaaS Host Security

- 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.
- In the context of SaaS (e.g., Salesforce.com, Workday.com) or PaaS (e.g., Google App Engine, Salesforce.com's Force.com) cloud services, **host security is opaque (Not Transparent)** to customers and the responsibility of **securing the hosts is relegated** to the CSP.
- To get assurance from the CSP on the security hygiene of its hosts, the vendor to share information under a **non-disclosure agreement (NDA)**or share the information via a controls assessment framework such as **SysTrust or ISO 27002.**
- Since virtualization is a key enabling technology that improves host hardware utilization, among other benefits, it is common for CSPs to employ virtualization platforms, including Xen and VMware hypervisors, in their host computing platform architecture.
- **Note: Xen** is the fastest and most secure infrastructure virtualization solution available today supporting wide range of OS. Using this thin s/w layer known as XEN hypervisor inserted between the Server's H/w and OS. It provides an abstract layer that allows the physical server to run 1 or more virtual servers.
- In short, if we are a SaaS or a PaaS customer, we are relying on the CSP to provide a secure host platform on which the SaaS or PaaS application is developed and deployed by the CSP host security responsibilities in SaaS and PaaS services are transferred to the CSP.

2) IaaS Host Security

- Unlike PaaS and SaaS, IaaS customers are primarily responsible for securing the hosts provisioned in the cloud.
- Almost all IaaS services available today employ virtualization at the host layer host security in IaaS should be categorized as follows:

a) Virtualization software Security
b) Securing virtual servers

Bamuengine.com

c) Virtual Server security

d) Threats to the hypervisor

a) <u>Virtualization software security</u>

- The software layer that sits on top of bare metal and provides customers the ability to create and destroy virtual instances.
- Virtualization at the host level can be accomplished using any of the virtualization models, including OS-level virtualization (Solaris containers, BSD jails, Linux-VServer), paravirtualization (a combination of the hardware version and versions of Xen and VMware), or hardware-based virtualization (Xen,VMware,Microsoft Hyper-V).
- It is important to secure this layer of software that sits between the hardware and the virtual servers.
- In a public IaaS service, customers do not have access to this software layer; it is managed by the CSP only.
- Since the CSP manages the virtualization software that sits on top of the hardware, customers will have neither visibility nor access to this software.
- Hardware or OS virtualization enables the sharing of hardware resources across multiple guest VMs without interfering with each other so that you can safely run several operating systems and applications at the same time on a single computer.
- For the purpose of simplicity, assumption is made that IaaS services are using **"bare metal hypervisor"** technologies (also known **as type 1 hypervisors** : is a hypervisor that runs directly on H/w and the hosts guest OS), such as VMware ESX, Xen, Oracle VM, and Microsoft's Hyper-V.
- These hypervisors support a variety of guest OSs, including Microsoft Windows, various Linux "flavors," and Sun's OpenSolaris.
- Given that hypervisor virtualization is the essential ingredient that guarantees compartmentalization and isolation of customer VMs from each other in a multitenant environment, it is very important to protect the hypervisors from unauthorized users.
- A new arms race between hacker and defender (CSP) in the realm of virtualization security is already underway.
- Since virtualization is very critical to the IaaS cloud architecture, any attack that could compromise the integrity of the compartments will be catastrophic to the entire customer base on that cloud.
- **Example:** A recent incident at a tiny UK-based company called Vaserv.com exemplifies the threat to hypervisor security. By exploiting a zero-day vulnerability in HyperVM, a virtualization application made by a company called Lxlabs, hackers destroyed 100,000 websites hosted by Vaserv.com.
- CSPs should institute the necessary security controls, including restricting physical and logical access to hypervisor and other forms of employed virtualization layers.

Bamuengine.com

- IaaS customers should understand the technology and security process controls instituted by the CSP to protect the hypervisor. This will help to understand the compliance and gaps with reference to the host security standard, policies, and regulatory compliances. However, in general, CSPs lack transparency in this area and we may have no option but to take a leap of faith and trust CSPs to provide an **"isolated and secured virtualized guest OS."**

b) **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.
- A vulnerable hypervisor could expose all user domains to malicious insiders.
- Furthermore, hypervisors are potentially susceptible to subversion attacks.
- Since virtualization layers within public clouds for the most part are proprietary and closed source (although some may employ a derivative of open source virtualization software such as Xen), the source code of software used by CSPs is not available for scrutiny by the security research community.

c) **Customer guest OS or virtual server security**

- The virtual instance of an operating system that is provisioned on top of the virtualization layer and is visible to customers from the Internet; e.g., various flavors of Linux, Microsoft, and Solaris. Customers have full access to virtual servers.
- Customers of IaaS have full access to the virtualized guest VMs that are hosted and isolated from each other by hypervisor technology.
- Customers are responsible for securing and ongoing security management of the guest VM.
- A public IaaS, such as Amazon's Elastic Compute Cloud (EC2), offers a web services API to perform management functions such as provisioning, decommissioning, and replication of virtual servers on the IaaS platform.
- These system management functions, when orchestrated appropriately, can provide elasticity for resources to grow or shrink in line with workload demand.
- The dynamic life cycle of virtual servers can result in complexity if the process to manage the virtual servers is not automated with proper procedures.
- From an attack surface perspective, the virtual server (Windows, Solaris, or Linux) may be accessible to anyone on the Internet, so sufficient network access mitigation steps should be taken to restrict access to virtual instances.
- Typically, the CSP blocks all port access to virtual servers and recommends that customers use port 22 (Secure Shell or SSH) to administer virtual server instances.
- The cloud management API adds another layer of attack surface and must be included in the scope of securing virtual servers in the public cloud.

Bamuengine.com

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.

d) **Securing virtual servers**

- 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. Isolate the decryption keys from the cloud where the data is hosted. Include no authentication credentials in your virtualized images except for a key to decrypt the file system key.
- Do not allow password-based authentication for shell access. Require passwords for sudo or role-based access (e.g., Solaris, SELinux).
- Run a host firewall and open only the minimum ports necessary to support the services on an instance.
- Run only the required services and turn off the unused services (e.g., turn off FTP, print services, network file services, and database services if they are not required).
- Install a host-based IDS such as OSSEC or Samhain.
- Enable system auditing and event logging, and log the security events to a dedicated log server.
- If you suspect a compromise, shut down the instance, snapshot your block volumes, and back up the root file system.
- Institute a process for patching the images in the cloud—both offline and instantiated images.
- Periodically review logs for suspicious activities.

INFRASTRUCTURE SECURITY: THE APPLICATION LEVEL

- Application-Level Security Threats
- DoS and EDoS
- End User Security
- Who Is Responsible for Web Application Security in the Cloud?
    - SaaS Application Security
    - PaaS Application Security
        - PaaS application container
        - Customer-Deployed Application Security
- IaaS Application Security

Application-Level Security Threats

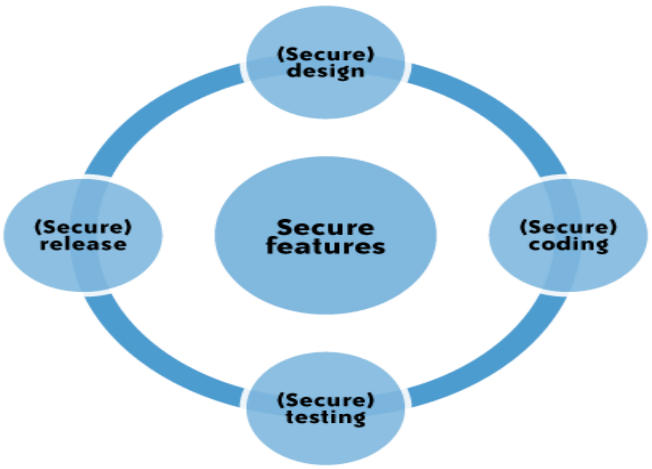
Bamuengine.com

- Designing and implementing applications targeted for deployment on a cloud platform will require that existing application security programs re-evaluate current practices and standards.
- The application security spectrum ranges from standalone single-user applications to sophisticated multiuser e-commerce applications used by millions of users.
- Web applications such as content management systems (CMSs), wikis, portals, bulletin boards, and discussion forums are used by small and large organizations.
- A large number of organizations also develop and maintain custom-built web applications for their businesses using various web frameworks.
- Few criminals attacked vulnerable websites because other attack vectors were more likely to lead to an advantage in unauthorized economic or information access.
- Advances in cross-site scripting (XSS) and other attacks have demonstrated that criminals looking for financial gain can exploit vulnerabilities resulting from **web programming errors as new ways to penetrate important organizations.**
- We will discussion only about the web application security: web applications in the cloud accessed by users with standard Internet browsers, such as Firefox, Internet Explorer, or Safari, from any computer connected to the Internet.
- 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.

- The existing threats exploit well-known application vulnerabilities including **cross-site scripting (XSS), SQL injection, malicious file execution**, and other vulnerabilities resulting from programming errors and design flaws.
- Armed with knowledge and tools, hackers are constantly scanning web applications for application vulnerabilities.
- They are then exploiting the vulnerabilities they discover for various **illegal activities including financial fraud, intellectual property theft, converting trusted websites into malicious servers serving client-side exploits, and phishing scams**.
- All web frameworks and all types of web applications are at risk of web application security defects, ranging from insufficient validation to application logic errors.
- 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.

Bamuengine.com

- In that threat model, web applications deployed in a public cloud (the SPI model) must be designed for an Internet threat model, and **security must be embedded into the Software Development Life Cycle (SDLC)**as in figure.



Dos and EDoS:-(Denial of Service and Economic Denial of Sustainability)

- Application-level DoS and DDoS attacks typically originate from **compromised computer** systems attached to the Internet.
- Application-level DoS attacks could manifest themselves as high-volume **web page reloads, XML web services requests (over HTTP or HTTPS), or protocol-specific requests supported by a cloud service**.
- Since these malicious requests blend with the legitimate traffic, it is extremely difficult to selectively filter the malicious traffic without impacting the service as a whole.
- Apart from disrupting cloud services, resulting in poor user experience and service-level impacts, DoS attacks **can quickly drain our company's cloud services** budget.
- DoS attacks on pay-as-you-go cloud applications will result in a dramatic increase in your cloud utility bill: **increased use of network bandwidth, CPU, and storage consumption**.
- This type of attack is also being characterized as ***economic denial of sustainability (EDoS)***
- The low barriers for small and medium-size enterprises to adopt cloud computing for legitimate use are also leveling the field for hackers. Using hijacked or exploited cloud accounts, hackers will be able to link together computing resources to achieve massive amounts of computing without any of the capital infrastructure costs.

End User Security: -

- We, 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 our Internet-connected computer.
- The new mantra of "**the browser is your operating system**" appropriately conveys the message that browsers have become the ever-present"operating systems" for consuming cloud services.

Bamuengine.com

- All Internet browsers routinely suffer from software vulnerabilities that make them vulnerable to end user security attacks.
- Hence, our recommendation is that cloud customers take appropriate steps to protect browsers from attacks.
- To **achieve end-to-end security in a cloud**, it is essential for customers to maintain good browser hygiene. The means keeping the browser (e.g.,Internet Explorer, Firefox, Safari) patched and updated to mitigate threats related to browser vulnerabilities.
- Currently, although browser security add-ons are not commercially available, users are encouraged to frequently check their browser vendor's website for security updates, use the auto-update feature, and install patches on a timely basis to maintain end user security.

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**.
- The key is to understand what our security responsibilities are versus those of the CSP.
- In that context, recent security surveys have highlighted the fact that **lack of transparency** in security controls and practices employed by CSPs is a barrier to cloud adoption.
- Cloud customers **do not have the transparency** required in the area of software vulnerabilities in cloud services. This prevents customers from managing the operational risk that might come with the vulnerabilities.
- By treating their software as proprietary, CSPs are impeding security researchers from analyzing the software for security flaws and bugs.
- Due to this lack of transparency, customers are left with no choice but to trust their CSPs to disclose any new vulnerability that may affect the confidentiality, integrity, or availability of their application.
- The following sections discuss the web application security in the context of the SPI cloud service delivery model:-
- **SaaS Application Security**
- **PaaS Application Security**
- **IaaS Application Security**

SaaS Application Security:-

- The SaaS model dictates that the provider manages the entire suite of applications delivered to users.
- Therefore, SaaS providers are largely responsible for securing the applications and components they offer to customers.
- Customers are usually responsible for operational security functions, including user and access management as supported by the provider.

Bamuengine.com

- It is a common practice for prospective customers, usually under an NDA, to request information related to the provider's security practices.
- This information should encompass
- **Design**
- **Architecture**
- **Development**
- **Black-and white-box application security testing, and**
- **Release management.**
- Some customers go to the extent of hiring independent security vendors to perform penetration testing (black-box security testing) of SaaS applications (with consent from the provider) to gain assurance independently.
- However, penetration testing can be costly and not all providers agree to this type of verification.
- Extra attention needs to be paid to the authentication and access control features offered by SaaS CSPs. Usually that is the only security control available to manage risk to information.
- Example: Web based administration user interface tool Google DOC
- Additional controls should be implemented to manage privileged access to the SaaS administration tool, and enforce segregation of duties to protect the application from insider threats. In line with security standard practices, customers should implement a strong **password policy**—one that forces users to choose strong passwords when authenticating to an application
- It is a common practice for SaaS providers to commingle their customer data (structured and unstructured) in a **single virtual data store** and rely on data tagging to enforce isolation between customer data.
- In that multitenant data store model, where encryption may not be feasible due to key management and other design barriers, data is tagged and stored with a unique customer identifier.
- So the customers should understand the virtual data store architecture and the preventive mechanisms the SaaS providers use to guarantee the compartmentalization and isolation required in a virtual multitenant environment.

PaaS Application Security

- PaaS vendors broadly fall into the following two major categories:
- Software vendors (e.g., Bungee, Etelos, GigaSpaces, Eucalyptus)
- CSPs (e.g., Google App Engine, Salesforce.com's Force.com, Microsoft Azure, Intuit QuickBase) Organizations evaluating a private cloud may utilize PaaS software to build a solution for internal consumption it is recommended that organizations evaluating PaaS software perform a risk assessment and apply the software security standard similar to acquiring any enterprise software.

Bamuengine.com

- **By definition**, a PaaS cloud (public or private) offers an integrated environment to design, develop, test, deploy, and support custom applications developed in the language the platform supports.
- PaaS application security **encompasses two software layers**:

- Security of the PaaS platform itself (i.e., runtime engine)
- Security of customer applications deployed on a PaaS platform

- PaaS CSPs (e.g., Google, Microsoft, and Force.com) are responsible for securing the platform software stack that includes the runtime engine that runs the customer applications.
- Since PaaS applications may use third-party applications, components, or web services, the third-party application provider may be responsible for securing their services.

Customer-Deployed Application Security

- PaaS developers need to get familiar with specific APIs to deploy and manage software modules that enforce security controls, developers are required to become familiar with platform-specific security features—available to them in the form of security objects
- No consistent API in cloud, **example** Google App Engine supports only Python and Java, and Salesforce.com'sForce.com supports only a proprietary language called Apex.
- The lack of an API standard has ramifications for both security management and portability of applications across the cloud.
- Developers should expect CSPs to offer a set of security features, including user authentication, single sign-on (SSO) using federation, authorization (privilege management), and SSL or TLS support, made.

IaaS Application Security

- IaaS cloud providers (e.g., Amazon EC2, GoGrid, and Joyent) treat the applications on customer virtual instances as a black box, and therefore are completely agnostic to the operations and management of the customer's applications customers have full responsibility for securing their applications deployed in the IaaS cloud, customers should not expect any application security assistance from CSPs other than basic guidance and features related to firewall policy that may affect the application's communications with other applications, users, or services within or outside the cloud.
- Web applications deployed in a public cloud must be designed for an Internet threat model, embedded with standard security countermeasures against common web vulnerabilities
- Customers are solely responsible for keeping their applications and runtime platform patched to protect the system from malware and hackers scanning for vulnerabilities to gain unauthorized access to their data in the cloud
- Developers writing applications for IaaS clouds must implement their own features to handle authentication and authorization

Bamuengine.com

- Any custom implementations of Authentication, Authorization, and Accounting (AAA) features can become a weak link if they are not properly implemented, and you should avoid them when possible.
- Customers of IaaS clouds are responsible for all aspects of their application security and should take the steps necessary to protect their application to address application-level threats in a multitenant and hostile Internet environment.

DATA SECURITY AND STORAGE

Several aspects of **data security**, including:

• Data-in-transit

• Data-at-rest

• Processing of data, including multitenancy

• Data lineage

• Data provenance

• Data remanence

Three information security concerns associated with the data storage in the cloud are:

- Confidentiality
- integrity, and
- availability.

Aspects of Data Security:-

Data-in-transit:-

➢ With regard to data-in-transit, the primary risk is in not using a vetted encryption algorithm. It is also important to ensure that a protocol provides confidentiality as well as integrity --particularly if the protocol is used for transferring data across the Internet. Merely encrypting data and using a non-secured protocol can provide confidentiality, but does not ensure the integrity of the data

Data-at-rest:-

➢ Although using encryption to protect data-at-rest might seem obvious, the reality is not that simple. If we are using an IaaS cloud service for simple storage, encrypting data-at-rest is possible—and is strongly suggested.

➢ Encrypting data-at-rest that a PaaS or SaaS cloud-based application is using as a compensating control is not always feasible. Data-at-rest used by a cloud-based application is generally not encrypted, because encryption would prevent indexing or searching of that data. Both PAAS and SAAS use a multi-tenancy architecture for sorting and accessing data. So, the data when processed or stored by cloud application is commingled with other user's data (Google BigTable). Although applications are often designed with features such as data tagging to prevent unauthorized access to commingled data, unauthorized access is still possible through some exploit of application vulnerability.

Bamuengine.com

➢ Although some cloud providers have their applications reviewed by third parties or verified with third-party application security tools, data is not on a platform dedicated solely to one organization.

➢ Although an organization's **data-in-transit** might be encrypted during transfer to and from a cloud provider, and its **data-at-rest** might be encrypted if using simple storage , an organization's data is definitely not encrypted if it is processed in the cloud. For any application to process data, that data ***must be unencrypted***.

Data lineage:-

➢ Whether the data an organization has put into the cloud is encrypted or not, it is useful and might be required to know exactly where and when the data was specifically located within the cloud. **For example,** the data might have **been transferred** to a cloud provider, (AWS), on **date x1 at time y1** and **stored** in a bucket on Amazon's S3 in **example1.s3.amazonaws.com**, then **processed** on **date x2 at time y2** on an instance being used by an organization on Amazon's Elastic Compute Cloud (EC2) in **ec2-67-202-51-223.compute-1.amazonaws.com**, then **restored** in another bucket on AS3,**example2.s3.amazonaws.com**, before being brought back into the organization for **storage in an internal data warehouse** belonging to the marketing operations group on **date x3 at time y3.**

➢ Following the path of data (mapping application data flows or data path visualization) is known as ***data lineage****, and it is important for an auditor's assurance.*

Data provenance:-

➢ Even if data lineage can be established in a public cloud, for some customers there is an even more challenging requirement and problem: **proving data provenance** —not just proving the integrity of the data, but the more specific provenance of the data. Important difference between the **two terms**.

➢ ***Integrity of data*** *refers to data that has not been changed in* an unauthorized manner or by an unauthorized person.

➢ ***Provenance means*** *not only that the* data has integrity, but also that it is computationally accurate; that is, the data was accurately calculated.

➢ For example, consider the following financial equation: SUM((((2*3)*4)/6)−2) = $2.00

➢ With that equation, the expected answer is $2.00. If the answer were different, there would be an integrity problem. Of course, the assumption is that the $2.00 is in U.S. dollars, but the assumption could be incorrect if a different dollar is used with the following associated assumptions:

- The equation is specific to the Australian, Bahamian, Barbadian, Belize, Bermudian, Brunei, etc dollar.
- The dollar is meant to be converted from another country's dollars into U.S. dollars.
- The correct exchange rate is used and the conversion is calculated correctly and can be proven.

➢ In this example, if the equation satisfies those assumptions, the equation has integrity but not provenance.

Bamuengine.com

Data remanence:-

➢ **Data remanence** is the residual representation of data that has been in some way nominally erased or removed. This residue may be due to data being left intact by a nominal delete operation, or through physical properties of the storage medium. Data remanence may make inadvertent disclosure of sensitive information possible, should the storage media be released into an uncontrolled environment. The risk posed by data remanence in cloud services is that an organization's data can be inadvertently exposed to an unauthorized party—regardless of which cloud service we are using (SaaS, PaaS, or IaaS)

INFORMATION SECURITY CONCERNS WITH 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.

➢ **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.

1.What access control exists to protect the data?

2. Howis the data that is stored in the cloud actually protected?

1.What access control exists to protect the data?

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.

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).

But these access control issues are not unique to all CSPs

2. 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.

encryption algorithm and key strength varies between cloud providers

Examples: EMC's MozyEnterprise does encrypt a customer's data. AWS S3 does *not encrypt a customer's data*

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

Bamuengine.com

Encryption is of **two types: Symmetric and Asymmetric** **Symmetric**is often used in data store security due to its speed and computational efficiency to handle encryption of large volumes of data

Following diagram state the Symmetric and Asymmetric –With Email

Figure is related to email, the same concept (i.e., a single shared, secret key) is used in data storage encryption.

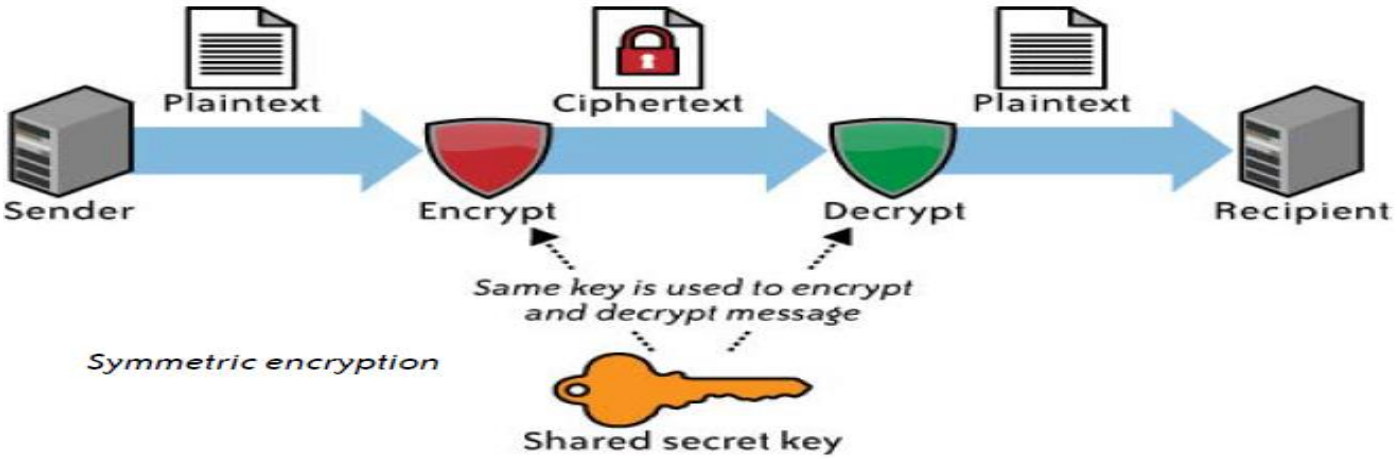
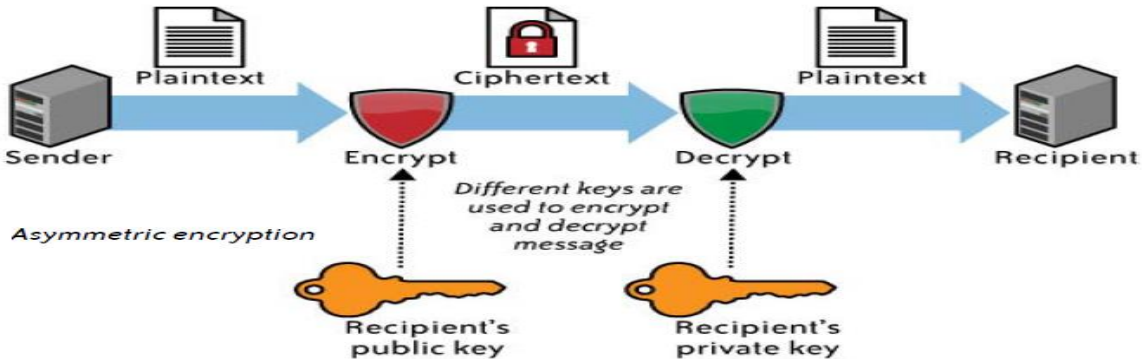


Figure is related to email, the same concept (i.e., a public key and a private key) is *not* used in data storage encryption.



The next consideration about the **key length** used.

With symmetric encryption, the longer the key length (i.e., the greater number of bits in the key), the stronger the encryption.

Although long key lengths provide more protection, they are also more computationally intensive, and may strain the capabilities of computer processors.

The key lengths should be a minimum of 112 bits for Triple DES (Data Encryption Standard) and 128-bits for AES (Advanced Encryption Standard) Finally about **the key management**.

we have the expertise to manage our own keys. It is not recommended that we entrust a cloud provider to manage our keys—at least not the same provider that is handling our data.

This means additional resources and capabilities are necessary. That being said, proper key management is a complex and difficult task.

Integrity:-

In addition to the confidentiality of our data, we also need to worry about the integrity of our data.

Bamuengine.com

Confidentiality does not imply integrity; data can be encrypted for confidentiality purposes, and yet we may 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** (as opposed to a streaming symmetric algorithm) in **cipher block chaining** (CBC) mode, and to include a **one-way hash function.** 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 reload 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.

Availability: -

Assuming that a customer's data has maintained its confidentiality and integrity, we must also be concerned about the **availability** of our data.

There are currently **three major** threats in this regards—none of which are new to computing, but all of which take on increased importance in cloud computing because of increased risk.

First threat –network-based attacks

Second threat –CSP's own availability

Third threat –Data Backup

Network based attacks –Secure protocol usage, DOS, DDOS, DNS Forgery etc

CSP's own availability

No CSPs offer the sought-after "five 9s" (i.e., 99.999%) of uptime.

Table shows, there is a considerable difference between five 9s and three 9s

Examples

- Outage occurrence
- Data loss

Bamuengine.com

Percentage of uptime

	Total downtime (HH:MM:SS)		
Availability	**Per day**	**Per month**	**Per year**
99.999%	00:00:00.4	00:00:26	00:05:15
99.99%	00:00:08	00:04:22	00:52:35
99.9%	00:01:26	00:43:49	08:45:56
99%	00:14:23	07:18:17	87:39:29

Data Backup:-

- 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, 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."
- However, "data that is maintained within running instances on Amazon EC2, or within Amazon S3 and Amazon SimpleDB, is all customer data and therefore AWS does not perform backups

SECURITY MANAGEMENT IN THE CLOUD:--

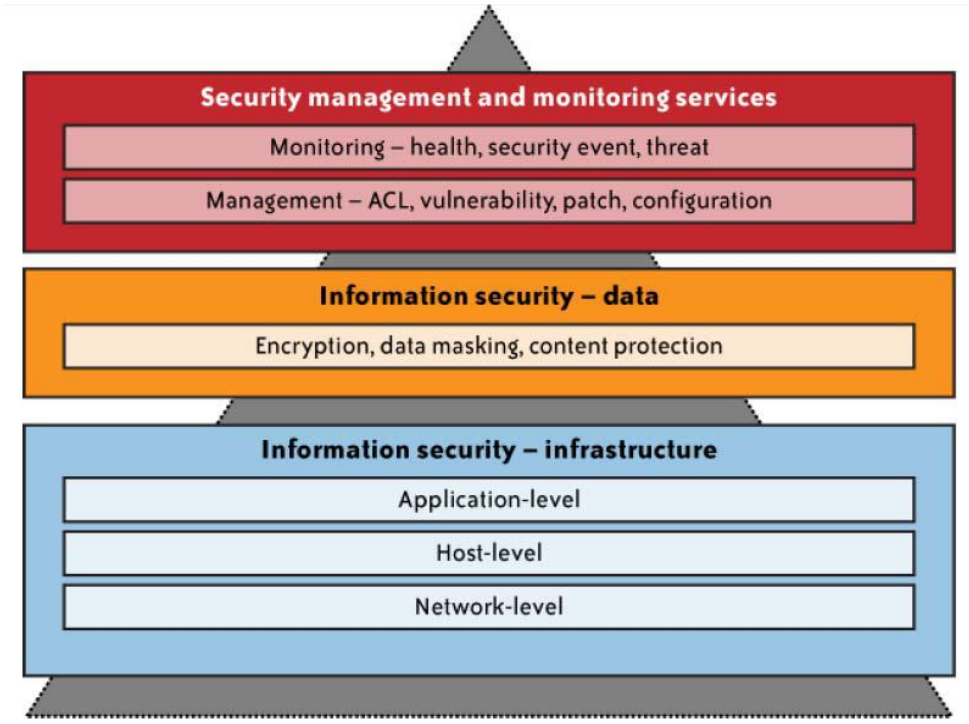
The cloud services delivery model will create islands of virtual perimeters as well as a security model with responsibilities shared between the customer and the cloud service provider (CSP). This **shared responsibility** model will **bring new security management challenges** to the organization's IT operations staff. With that in mind, the first question that should be answered by a chief information security officer**(CISO)** is whether they have an adequate **transparency** from cloud services to manage the shared responsibilities and implementation of security management processes (preventive and detective controls) to assure the business that the data in the cloud is appropriately protected. The answer to this question **has two parts:**

1. What security controls must the customer provide over and above the controls inherent in the cloud platform, and
2. How must an enterprise's security management tools and processes adapt to manage security in the cloud

As a customer of the cloud, we should start with the exercise of understanding the trust boundary of our services in the cloud. We should understand all the layers we own, touch, or interface with in the cloud service—network, host, application, database, storage, and web services including identity services as shown in figure . We also need to understand the scope of IT system management and monitoring responsibilities that fall on our shoulders, including access, change, configuration, patch, and vulnerability management. Although we may be transferring some of the operational responsibilities to the provider, the

Bamuengine.com

level of responsibilities will vary and will depend on a variety of factors, including the **service delivery model**(SPI), **provider service-level agreement** (SLA), and **provider-specific capabilities** to support the extension of our internal security management processes and tools. Mature IT organizations are known to employ security management frameworks, such as **ISO/ IEC 27000 and the Information Technology Infrastructure Library** (ITIL) service management framework. These industry standard management frameworks provide guidance for planning and implementing a governance program with sustaining management processes that protect information assets. A key tenet of ITIL, and one that is applicable to cloud computing, is that organizations (people, processes) and information systems are constantly changing. Management frameworks such as ITIL will help with the continuous service improvement that is necessary to align and realign IT services to changing business needs.



Given the dynamic characteristics of cloud computing services, the activities present within the security management processes must be continually revised to remain current and effective. The goal of the ITIL Security Management framework is **divided into two parts**:

1. Realization of security requirements

Security requirements are usually defined in the SLA as well as in other external requirements, which are specified in underpinning contracts, legislation, and internally or externally imposed policies.

2. Realization of a basic level of security

This is necessary to guarantee the security and continuity of the organization and to reach simplified service-level management for information security management. Well-established security management processes are also aligned with an organization's IT policies and standards, with the goal of protecting the confidentiality, integrity, and availability of information.

Security Management Standards

Bamuengine.com

the standards that are relevant to security management practices in the cloud are **ITIL and ISO/IEC 27001 and 27002.**

ITIL:-

The **Information Technology Infrastructure Library** (ITIL) is a set of best practices and guidelines that define an integrated, process-based approach for managing information technology services.

ITIL can be applied across almost every type of IT environment including cloud operating environment.

ITIL seeks to ensure that effective information security measures are taken at strategic, tactical, and operational levels. Information security is considered an iterative process that must be controlled, planned, implemented, evaluated, and maintained.

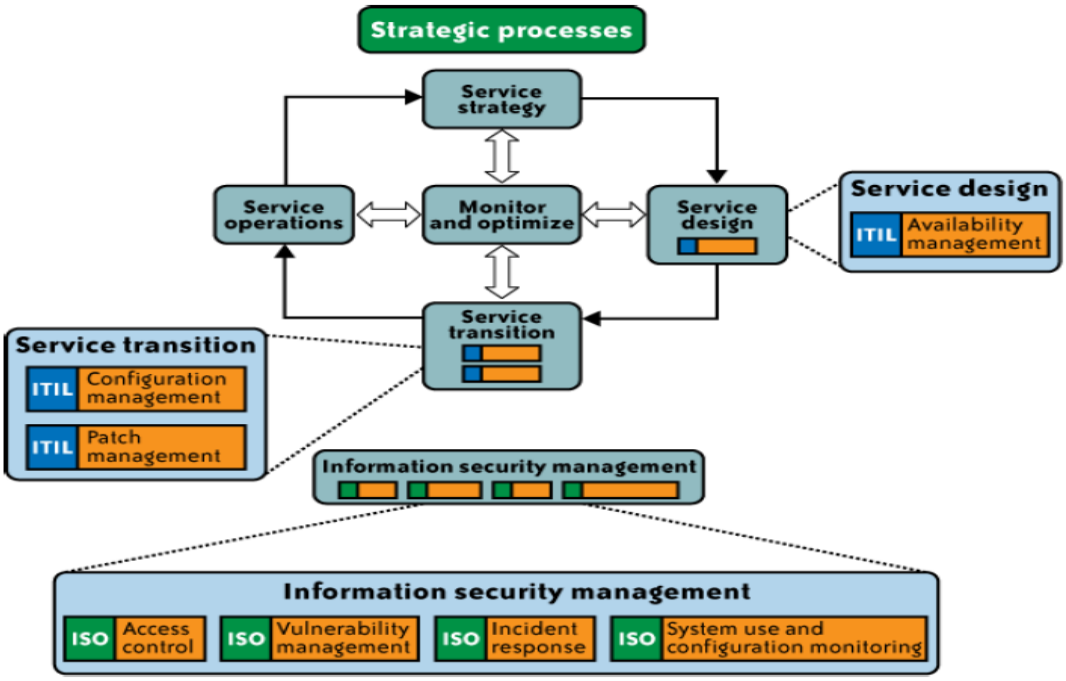
ITIL breaks information security down into:

Policies :- The overall objectives an organization is attempting to achieve

Processes :- What has to happen to achieve the objectives

Procedures:- Who does what and when to achieve the objectives

Work instructions:- Instructions for taking specific actions



The ITIL life cycle in a enterprise

Figure illustrates the ITIL life cycle in a enterprise. Security management disciplines are represented by relevant ISO and ITIL functions.

The ITIL-process security management is based on the code of practice for information security management also known as **ISO/IEC 17799:2005.**

The ITIL security management process has relationships with almost all other ITIL processes.

the most obvious relationships will be to the **Service-level management process, Incident management process, and Change management process**, since they greatly influence the state of security in the system (server, network, or application).

Bamuengine.com

ITIL also is related **to ISO/IEC 20000** as that's the first international standard for IT Service Management (ITSM).

ISO 27001/27002:-

ISO/IEC 27001 formally defines the mandatory requirements for an Information Security Management System (ISMS).

It is also a certification standard and uses **ISO/IEC 27002** to indicate suitable information security controls within the ISMS.

since **ISO/IEC 27002** is merely a code of practice/guideline rather than a certification standard, organizations are free to select and implement controls as they see fit.

Security Management in the Cloud

After analyzing the management process disciplines across the ITIL and ISO frameworks, the following relevant processes are identified as the recommended security management focus areas for securing services in the cloud:

1. Availability management (ITIL)
2. Access control (ISO/IEC 27002, ITIL)
3. Vulnerability management (ISO/IEC 27002)
4. Patch management (ITIL)
5. Configuration management (ITIL)
6. Incident response (ISO/IEC 27002)
7. System use and access monitoring (ISO/IEC 27002)

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. Typically mix security and privacy

Some considerations to be aware of:

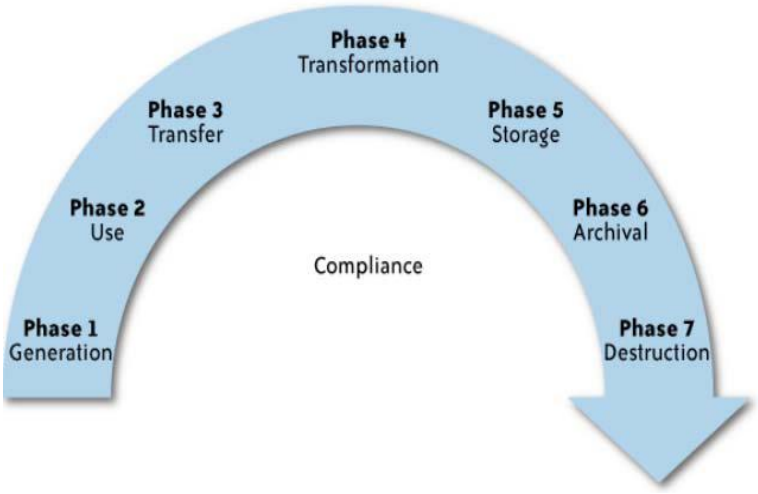
- Storage
- Retention
- Destruction
- Auditing, monitoring and risk management
- Privacy breaches

Bamuengine.com

- Who is responsible for protecting privacy?

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



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).

Bamuengine.com

• ***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?

The impact differs based on the specific cloud model used by the organization, the phase (Figure 7-1, shown earlier) of personal information in the cloud, and the nature of the organization. The following analysis provides some of these considerations; however, every organization should consider performing a Privacy Impact Assessment (PIA) before embarking on a cloud computing initiative that involves personal information.

Bamuengine.com

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. This is especially important with regard to marketing activities; in some jurisdictions, marketing activities are subject to additional regulations and are almost always addressed in the end user privacy policy for applicable organizations. In the cloud, the main concern is the organization's ability to provide the individual with access to all personal information, and to comply with stated requests. If a data subject exercises this right to ask the organization to delete his data, will it be possible to ensure that all of his information has been deleted in the cloud?

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? How are existing privacy compliance requirements impacted by the move to the cloud? Clouds can cross multiple jurisdictions; for example, data may be stored in multiple countries, or in multiple states within the United States. What is the relevant jurisdiction that governs an entity's data in the cloud and how is it determined?

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? Privacy laws in various countries place limitations on the ability of organizations to transfer some types of personal information to other countries. When the data is stored in the cloud, such a transfer may occur without the knowledge of the organization, resulting in a potential violation of the local law.

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? Who enforces the retention policy in the cloud, and how are exceptions to this policy (such as litigation holds) managed?

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? How do they know that the CSP didn't retain additional copies? Cloud storage providers usually replicate the data across multiple systems and sites—increased availability is one of the benefits they provide. This benefit turns into a challenge when the organization tries to destroy the data—can you truly destroy information

Bamuengine.com

once it is in the cloud? Did the CSP really destroy the data, or just make it inaccessible to the organization? Is the CSP keeping the information longer than necessary so that it can mine the data for its own use?

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)? If contracts include liability for breaches resulting from negligence of the CSP, how is the contract enforced and how is it determined who is at fault?

Disaster Recovery:

Disaster recovery plan involves two key metrics

Recovery Point Objective (RPO)

The recovery point objective identifies how much data you are willing to lose in the event of a disaster. This value is typically specified in a number of hours or days of data.

Recovery Time Objective (RTO)

The recovery time objective identifies how much downtime is acceptable in the event of a disaster. If your RTO is 24 hours, you are saying that up to 24 hours may elapse between the point when your system first goes offline and the point at which you are fully operational again.

Disasters in the Cloud

1. Backups and data retention
2. Geographic redundancy
3. Organizational redundancy

Disaster Management Monitoring

•Monitoring your cloud infrastructure is extremely important. You cannot replace a failing server or execute your disaster recovery plan if you don't know that there has been a failure.

•The trick, however, is that your monitoring systems cannot live in either your primary or secondary cloud provider's infrastructure. They must be independent of your clouds. If you want to enable automated disaster recovery, they also need the ability to manage your EC2 infrastructure from the monitoring site.

Monitor for failure at three levels:

- Through the provisioning API (for Amazon, the EC2 web services API)
- Through your own instance state monitoring tools
- Through your application health monitoring tools

Bamuengine.com

Load Balancer Recovery

•One of the reasons companies pay absurd amounts of money for physical load balancers is to greatly reduce the likelihood of load balancer failure. With cloud vendors such as GoGrid and in the future, Amazon you can realize the benefits of hardware load balancers without incurring the costs. Under the current AWS offering, you have to useless –reliable EC2 instances. Recovering a load balancer is simply a matter of launching a new load balancer instance from the AMI and notifying it of the IP addresses of its application servers. You can further reduce any downtime by keeping a load balancer running in an alternative availability zone and then re-mapping our static IP address up the failure of them a in load balancer.

Application Server Recovery

If you are operating multiple application servers in multiple availability zones, your system as a whole will survive the failure of any one instance or even an entire availability zone. You will still need to recover that server so that future failures don't affect your infrastructure.

Database Recovery

•Database recovery is the hardest part of disaster recovery in the cloud. Your disaster recovery algorithm has to identify where an uncorrupted copy of the database exists. This process may involve promoting slaves into masters, rearranging your backup management, and reconfiguring application servers.

•The best solution is a clustered database that can survive the loss of an individual database server without the need to execute a complex recovery procedure.

•Absent clustering, the best recovery plan is one that simply launches a new database instance and mounts the still functional EC2 volume formerly in use by the failed instance. When an instance goes down, however, any number of related issues may also have an impact on that strategy. The database could be irreparably corrupted by whatever caused the instance to crash. The volume could have gone down with the instance. The instance's availability zone (and thus the volume as well) could be unavailable. You could find yourself unable to launch new instances in the volume's availability zone.

Bamuengine.com