ARYA INSTITUTE OF ENGINEERING & TECHNOLOGY, KUKAS, Jaipur

Lecture Notes

Branch : CSE Sem. : VII Subject : Cloud Computing

Topic : Cloud Security Unit : IV Lecture No.

## ★ Cloud Computing Security Fundamentals-

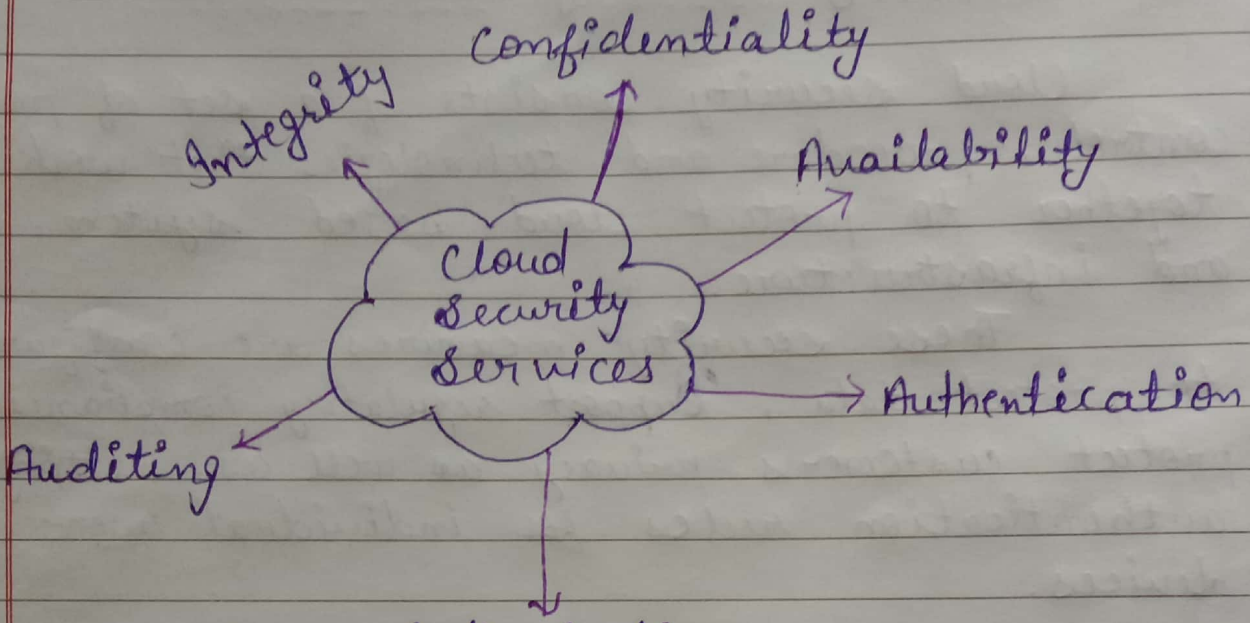
Cloud security consists of a set of policies, controls, procedure and technologies that work together to protect cloud based system, data and infrastructure.

These security measures are configured to protect data, support regulatory compliance & protect customer's privacy as well as setting authentication rules for individual users and devices.

### Importance of cloud computing security-

→ Ensure proper protection of data & information.
→ Manage people, roles & identities.
→ Ensure effective gournance, risk & compliance processes.
→ Understand security requirements of the exit process.
→ Ensure cloud network & connection are secure.
→ Manage security terms in the cloud SLA
→ Enforce privacy policy.
→ Assess security provision for cloud application.

## ★ Cloud Security Services -




We have two models for security - (I) CIA (II) AAA

### I CIA Model -

- **Confidentiality** - confidentiality refers to protecting information from being accessed by unauthorized parties. In other words, only the people who are authorized to do so can gain access to sensitive data.

  The failure on confidentiality of data known as data breach, typically can't be remedied.

In cloud we use "Identity and Access Management (IAM)" to define the resource accessibility permission. In IAM, we can define users, groups, roles and policies. IAM also helps to manage the API access using access keys

and secret keys. Similarly, we have a keystone in openstack to define users, groups, roles & policies.

- **Integrity** - Integrity refers to ensuring the authenticity of information - that information is not altered and that the source of the information is genuine. It maintains the accuracy, consistency and trustworthiness of data over its entire life cycle.

For integrity there are multiple types of encryption for storage, where data is stored and for data transit we can use SSL. If we want to implement an additional layer of security, we can use "Aws cloudHSM" module as well. In Openstack the integrity starts with the bootstrap level and goes up until the file level.

- **Availability** - Availability denotes that the information is available to the authorized user. If it isn't available to authorized users, again it will incur a loss. Information has value if right people can access it at the right time.

For availability, Aws offers many services that ensure the service availability at different

layers. We have -
Route 53 as DNS,
Elastic load Balancing (ELB) &
autoscaling.

All three services ensure that you have the service available in case of DDOS attack as well. Availability of the application or solution also depends on how it is designed and deployed.

II AAA Model-

Authentication- Authentication refers to confirmation that a user who is requesting a service is a valid user. It is accomplished via the presentation of an identity and credentials.
For ex. passwords, one-time tokens, digital signatures, phone no. etc.

In Aws, we have IAM for user identity. Here we can define users and groups. IAM enables you to define the password-based authentication & key based authentication for users. We can also enable multi-factor authentication (MFA) for users.

ARYA INSTITUTE OF ENGINEERING & TECHNOLOGY, KUKAS, Jaipur
Lecture Notes
Branch : ..... Sem. : ..... Subject : .....
Topic : ..... Unit ..... Lecture No. .....

**Authorization-** Once the user is authenticated, there must be some authority defined for the user to access the data so that he can perform the required action. Basically, here we define the access policies and roles for users. Users with read permission should not be able to modify the data.

For authorization, AWS uses IAM roles & ;policies. There are many predefined user roles for different services.

We can also define custom roles. For ex suppose we have an EC2 instance, that need to access the Simple Storage Service (S3) resource and cloudwatch logs. Here we can also define a custom role of an EC2 instance which grant access to the S3 bucket and cloudwatch logs and binds the role with EC2 instances.

**Auditing-** Auditing does the accounting of user activity on data. Here all the activities of users are monitored and captured including session duration login time, updation etc.

AWS provides CloudTrail to log all the action or activity for AWS services. Apart from this, it provides Virtual Private Cloud (VPC) logs and ELB logs, which can be stored in the S3 bucket or can be transferred to Cloudwatch logs. Openstack provides a telemetry service called ceilometer to store & manage logs.

Name of Lecturer .....

## ★ Cloud Security Design Principles-

The NCSC (National Cyber Security Centre) published some cloud security principles in 2016. These principles are designed to give guidance to cloud service providers in order to protect their customers.

① Data in transit protection- User data which is transitioning between networks should be protected against any interference.

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

③ Separation between users- If a user of a service is compromised by malicious s/w, this should not affect the service or data of another users.

④ Governance Framework- A security Governance framework shoud be followed by the service provider, in order to internally coordinate its management of the service.

⑤ Operational Security- In order to prevent & detect attacks, the service must be operated securely. Adequate security shouldn't require complex or expensive processes.

ARYA INSTITUTE OF ENGINEERING & TECHNOLOGY, KUKAS, Jaipur
Lecture Notes
Branch : ..... Sem. : ..... Subject : .....
Topic : ..... Unit ..... Lecture No. .....

(6) Personnel security - Service provider personel should be thoroughly screened, followed by in-depth training to reduce the liklihood of accidental or malicious compromise.

(7) Secure development - Services shoud be designed with security in mind. Nexor is proud to follow a secure by design approach.

(8) Supply chain security The service provider shoud ensure that their supply chain adhers to all of the same security principles.

(9) Secure user management - Your service provider should ensure that you have the relevant tools to securely manage the use of their services. Management interfaces prevent unauthorized access to your data, making them a vital part of the security barrier.

(10) Identity and authentication - Access to the service interfaces should only be granted to specific individuals and should all be guarded by adequate authentication measures - two party authentication if possible.

(11) External interface protection - Any external or less trustworthy service interfaces must be identified and defended appropriately.

(12) Secure service administration - If a cloud service is compromised through its administration system, important company data could be stolen or manipulated. It is vital that these services are secure.

(13) Audit information for users - A service provider should supply their customers with the audit recorded needed to monitor the service & who is able to access your data. This is important as it gives you a means to identify inappropriate or malicious activity.

(14) Secure use of service - you have a responsibility to ensure the service is used properly, to ensure your data is kept safe & protected.

ARYA INSTITUTE OF ENGINEERING & TECHNOLOGY, KUKAS, Jaipur
Lecture Notes
Branch : ..... Sem. : ..... Subject : .....
Topic : ..... Unit ..... Lecture No. .....

## ★ Cloud Security Policy Implementation -

Cloud s/w security requirements are a function of policies such as system security policies, s/w policies and information system policies. Cloud providers also have to satisfy regulations & directives such as -

FISMA - (Federal Information Security Management Act) - is one of the most important regulations for federal data security standard & guidelines.

Gramm-Leach-Bliley Act - (GLA or GLBA) - Financial modernization Act. It is a US federal law that requires financial institutions to explain how they share & protect their customers' private information.

Sarbanes-Oxley Act - federal law that established sweeping auditing & financial regulations for public companies.

HIPAA - Health Insurance Portability & Accountability Act - with the goal of protecting the privacy of sensitive patient information.

For proper secure cloud s/w implementation, these issues have to be accounted for during the s/w development life cycle & through an effective cloud s/w security policy.

Name of Lecturer : .....

* Implementation Issues-
→ Access controls
→ Data Protection
→ Confidentiality
→ Integrity
→ Identification & Authentication
→ Communication security
→ Accountability.

For the high level policy functional requirements the following activities should result-

→ Derive the detailed functional requirements -
Ex- The server should return public-access web-pages to any browser that requests those pages.

→ Identity the related constraint requirements-
Ex- The server should return restricted web pages only to browsers that are acting as proxies for user with authorized privileges sufficient to access those web pages.

→ Derive the functional security requirements-
Ex- The server must authenticate every browser that requests access to a restricted web page.

→ Identify the related negative requirements-
Ex- The server must not return a restricted web page to any browser that it can't authenticate.

ARYA INSTITUTE OF ENGINEERING & TECHNOLOGY, KUKAS, Jaipur

Lecture Notes

Branch : ..... Sem. : ..... Subject : .....

Topic : ..... Unit..... Lecture No. .....

## ★ Cloud Computing Security Challenges-

① Lack of visibility & control – Relating to both public & hybrid cloud environment, the loss of overall service visibility and the associated lack of control can be a problem.

② Data Breaches and Downtime - Despite the fact that generally speaking enterprise-grade cloud services are more secure than legacy architecture, there is still a potential cost in the form of data breaches and downtime.

③ Vendor lock-In - Sometimes, a company may find themselves locked into a certain cloud provider. Vendor lock-in can become an issue in cloud computing because it is very difficult to move database once they are set up.

④ Lack of Transparency- When a user buys a cloud services, the service provider will not be provided with a full service description, detailing exactly how the platform works & the security processes the vendor operates.

This lack of service transparency makes it hard for customers to intelligently evaluate whether their data is being stored & processed securely all at times.

⑤ Insecure Interface and APIs - Cloud vendors provide their customers with a range of Application Programming Interfaces (APIs), which the customer uses to manage the cloud service. Unfortunately, not every API is entirely secure.

⑥ Insufficient Due Diligence - For companies that lack the internal resources to fully evaluate the implication of cloud adoption, then the risk of deploying a platform that is ineffective & even insecure is real.

⑦ Denial of Service (DoS) attacks - DoS attacks are attack meant to disable a machine or n/w, making it inaccessible to its intended users.

ARYA INSTITUTE OF ENGINEERING & TECHNOLOGY, KUKAS, Jaipur

Lecture Notes

Branch : ..... Sem. : ..... Subject : .....

Topic : ..... Unit ..... Lecture No. .....

## ★ Cloud Computing Security Architecture-

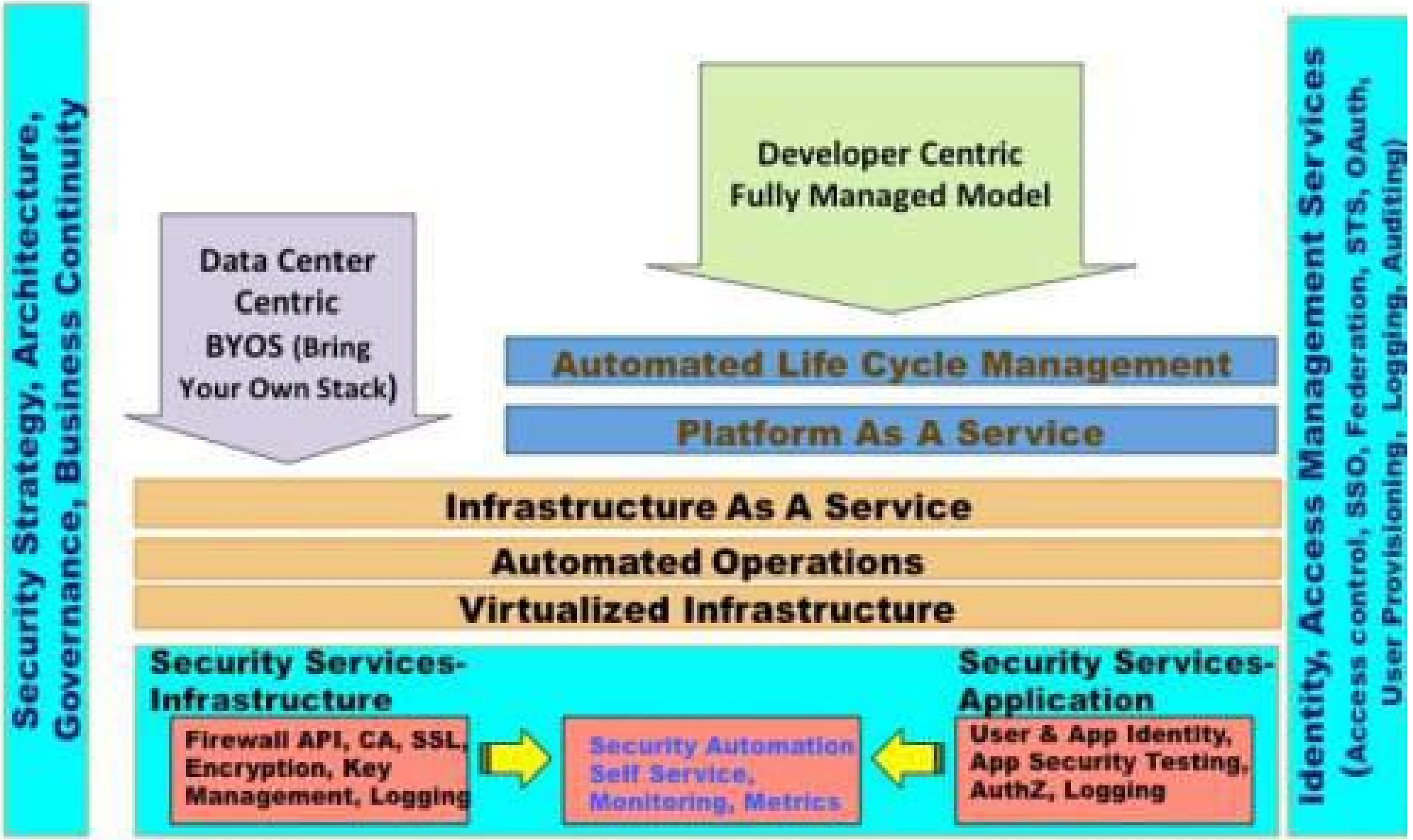
The Open Security Alliance (OSA) defines security architecture as-

"the design artifacts that describes how the security controls (security countermeasures) are positioned, and how they relate to the overall IT architecture. These controls serve the purpose to maintain the system's quality attributes, among them confidentiality, integrity, availability, accountability & assurance"

The Information security society switzerland (ISSS) describes security architecture as-

"A cohesive security design, which addresses the requirements (ex- authentication, authorization etc.) and in particular the risk of a particular environment / scenario and specifies what security controls are to be applied where. The design should be reproducible"

# High Level Cloud Architecture – Security services



The following are cloud security best practices to mitigate risk to cloud services:

Architect for security-as-a-services- Application deployments in the cloud involve orchestration of multiple services including automation of DNS, load balancer, network QoS etc. Security automation falls in the same category which includes automation of firewall policies between cloud security zones, provisioning of certificates (for SSL), virtual machine system configuration, privileged accounts and log configuration.

ARYA INSTITUTE OF ENGINEERING & TECHNOLOGY, KUKAS, Jaipur
Lecture Notes
Branch : ..... Sem. : ..... Subject : .....
Topic : ..... Unit..... Lecture No. .....

**Implement sound identity, accessmanagement architecture & practice-** Cloud access controls architecture should address all aspects of user & access management lefecycles for both end users and privileged users - user provisioning & deprovisioning, authentication, federation, authorization & auditing. A sound architecture will enable reusability of identity and access services for all use cases in public, private & hybrid cloud models.

**Leverage APIs to automate safeguards-** Any new security services should be deployed with an API (REST/SOAP) to enable automation. APIs can help automate firewall policies, configuration hardening and access control at the time of application deployment.

**Always encrypt or mask sensitive data -** To protect sensitive data from unauthorized access, we should encrypt or mask the data.

**Do not rely on an IP address for authentication services-** IP addresses in clouds are ephemeral (for short duration of time) in nature so you cannot solely rely on them for enforcing nlw access control.

Log, log, log - Applications should centrally log all security events that will help create an end-to-end transaction view with non-repudiation characteristics. In the event of a security incident, logs and audit trails are the only reliable data leveraged by forensic engineers to investigate & understand how an application was exploited. Clouds are elastic and logs are ephemeral hence it is critical to periodically migrate log files to a different cloud or to the enterprise data center.

Continuously monitor cloud services - Monitoring is an important function given that prevention controls may not meet all the enterprise standards. Security monitoring should leverage logs produced by cloud services, APIs & hosted cloud applications to perform security event correlation

ARYA INSTITUTE OF ENGINEERING & TECHNOLOGY, KUKAS, Jaipur

Lecture Notes

Branch : ..... Sem. : ..... Subject : .....

Topic : ..... Unit ..... Lecture No. .....

## * Legal issues in Cloud Computing -

Cloud computing can help your business reduce costs as you don't have to invest in h/w and other physical infrastructure, your data is stored on a secure location and you only pay for what you use - there are no licensing fees associated with cloud computing. still there are some legal issues, which are -

① **Data location** - Many service provider contracts explicitly outline the right to maintain customer data on any of their sites, regardless of the origin of the data. Maintaining data across multiple geographical locations provides a greater level of security, it does raise issues in relation to export control and needs to be addressed directly within the contract, legislating against extraterritorial storage.

② **Privacy and Confidentiality** - In many cases, data collected for a specific purpose may only be used for that specific purpose.

For ex. student information stored in college databases typically may only be outsourced to designated vendors with legitimated interests in the data.

③ **Data Security** - The main privacy /data security issue relating to the cloud is "data breach".

Name of Lecturer : .....

Data breach may be in the generic sense defined as the loss of unencrypted electronically stored information. A data breach can cause loss to both the provider as well as the customer in numerous ways: with identity theft & chances of debit / credit card fraud to the customer, & financial harm, loss of customer, loss of reputation etc.

(4) **Intellectual Property Rights** - Intellectual property rights differ from one country to another, so it is not very clear what intellectual property laws will apply in the cloud computing environment. Make sure you are aware of the regulations & rights from the country you store your intellectual work. The provider you choose should know how to protect intellectual property it store & how to avoid potential infringement pitfalls.

(5) **Service Level Agreements** - Guarantees for the service provision need to be detailed to provide for the minimum amount of uptime, the process & the timescale associated with correcting downtime.

(6) Third party access issues - Third-party involvement could be a risk. All third parties using a multi-tenant shared cloud are using the same administration interface, so make sure multi-factor authentication & enhanced security is present.

## Business Continuity & Disaster Recovery in Cloud Computing:

Business continuity planning (BCP) and disaster recovery planning (DRP) involve the preparation, testing, and updating of the actions required to protect critical business processes from the effects of major system and network failures.

BCP comprises scoping and initiating the planning, conducting a business impact assessment (BIA), and developing the plan. DRP includes developing the DRP processes, testing the plan, and implementing the disaster recovery procedures.

A disaster is a rapidly occurring or unstoppable event that can cause loss of life, or damage. A DRP is a comprehensive statement of consistent actions to be taken before, during, and after a disruptive event that causes a significant loss of information systems resources.

Specific areas that can be addressed by cloud providers include the following:

- Protecting an organization from a major computer services failure
- Providing extended backup operations during an interruption
- Providing the capability to implement critical processes at an alternate site
- Guaranteeing the reliability of standby systems through testing and simulations
- Returning to the primary site and normal processing within a time frame that minimizes business loss by executing rapid recovery procedures.
- Minimizing the decision-making required by personnel during a disaster
- Proving an organized way to make decisions if a disruptive event occurs
- Minimizing the risk to the organization from delays in providing service

## Disaster Recovery Planning:

The DRP should address all information processing areas of the company:

- Cloud resources being utilized
- LANs, WANs, and servers
- Telecommunications and data communication links
- Workstations and workspaces
- Applications, software, and data
- Media and records storage
- Staff duties and production processes

**Recovery Time Frame Requirements Classification:**

| RATING CLASS | RECOVERY TIME FRAME REQUIREMENTS |
|---|---|
| AAA | Immediate recovery needed; no downtime allowed |
| AA | Full functional recovery required within four hours |
| A | Same-day business recovery required |
| B | Up to 24 hours downtime acceptable |
| C | 24 to 72 hours downtime acceptable |
| D | Greater than 72 hours downtime acceptable |

**Disaster Recovery Plan Testing:** The major reasons to test a disaster recovery plan are summarized as follows:

- To inform management of the recovery capabilities of the enterprise
- To verify the accuracy of the recovery procedures and identify deficiencies
- To prepare and train personnel to execute their emergency duties
- To verify the processing capability of the alternate backup site or cloud provider

**Management Roles:** The plan should also detail the roles of senior management during a disaster:

- Remaining visible to employees and stakeholders
- Directing, managing, and monitoring the recovery
- Rationally amending business plans and projections
- Clearly communicating new roles and responsibilities
- Monitoring employee morale ν Providing employees and family with counselling and support
- Re-establishing accounting processes, such as payroll, benefits, and accounts payable
- Re-establishing transaction controls and approval limits

## Business Continuity Planning:

A BCP is designed to keep a business running, reduce the risk of financial loss, and enhance a company's capability to recover promptly following a disruptive event. The four principle components of a BCP are as follows:

- **Scope and plan initiation —** Creating the scope and other elements needed to define the plan's parameters
- **Business impact assessment (BIA) —** Assisting the business units in understanding the impact of a disruptive event. This phase includes the execution of a vulnerability assessment.
- **Business continuity plan development —** Using information collected in the BIA to develop the actual business continuity plan. This process includes the areas of plan implementation, plan testing, and on-going plan maintenance.
- **Plan approval and implementation —** Obtaining the final senior management sign-off, creating enterprise wide awareness of the plan, and implementing a maintenance procedure for updating the plan as needed.

**BIA:** A key element of the BCP process is conducting a BIA. The purpose of a BIA is to create a document that outlines what impact a disruptive event would have on the business. The impact might be financial (quantitative) or operational (qualitative), such as the inability to respond to customer complaints. A vulnerability assessment is often part of the BIA process. A BIA has three primary goals:

**Criticality prioritization —** Every critical business unit process must be identified and prioritized, and the impact of a disruptive event must be evaluated.

**Downtime estimation —** The BIA is used to help estimate the maximum tolerable downtime (MTD) that the business can withstand and still remain viable; that is, what is the longest period of time a

critical process can remain interrupted before the company can never recover? The BIA process often determines that this time period is much shorter than expected.
**Resource requirements —** The resource requirements for the critical processes are also identified at this time, with the most time-sensitive processes receiving the most resource allocation.

A BIA generally involves four steps:

1. Gathering the needed assessment materials
2. Performing the vulnerability assessment
3. Analyzing the information compiled
4. Documenting the results and presenting recommendations

**Using the Cloud for BCP/DRP:** Proper design of a cloud-based IT system that meets the requirements of a BCP and DRP should include the following:

- Secure access from remote locations
- A distributed architecture with no single point of failure
- Integral redundancy of applications and information
- Geographical dispersion

**RISK MANAGEMENT:** RM is the identification, analysis, control, and minimization of loss that is associated with events. RM's main function is to mitigate risk. Mitigating risk means reducing risk until it reaches a level that is acceptable to an organization. The risk management process minimizes the impact of threats realized and provides a foundation for effective management decision making. As defined in NIST SP 800-30, risk management is composed of three processes:

- Risk assessment
- Risk mitigation
- Evaluation and assessment

The RM task process has several elements, primarily including the following: performing a risk analysis; including the cost-benefit analysis of protections; and implementing, reviewing, and maintaining protections.

**Strategies to Mitigate Cloud Risk:** While the list of implied security and compliance considerations for cloud migration is extensive, the benefits gained easily outweigh these risks if they are managed properly. Utilize these methods to mitigate cloud migration risk:

1. **Data Encryption at Rest:** Encryption at rest protects data that is not in use or in transit. As data at rest is typically protected by firewalls and monitoring, it can be tempting to believe that is secure without encryption. However, if the password of an authorized user is compromised, the privacy of this data is no longer secure. When sensitive data is moved to a third-party cloud provider, the risk of unauthorized access increases. Data encryption at rest minimizes this risk by ensuring data security even if unauthorized access via stolen credentials occurs.
2. **Two-Factor Authentication (2FA):** By combining a password with a second authentication component such as a one-time password generated by a personal PIN, IT executives can add an important extra layer of security to their cloud hosted environments. Not only is two-factor

authentication much more secure than just relying on username/password combinations, it is also supports ease-of-use from an end user perspective. Like data encryption at rest, 2FA also nicely complements industry and government compliance mandates.

3. **Eliminate Shared Accounts:** As with other web-based services, sharing cloud platform credentials with coworkers is common practice. While most professionals don't think twice about employing a shared account model with services that require multiple cooks in the kitchen, it can be a recipe for cloud disaster. Even if it's more convenient/cost-effective than requiring a unique account for each user, sharing cloud accounts injects unnecessary risk into cloud operations. To maintain accountability and preserve data auditability and integrity, cloud services accounts should not be shared between users for any reason.
4. **Insist on a well-defined shared responsibility model:** Whether it's for Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS), a well-defined and reciprocal shared responsibility agreement with each cloud services provider is critical to mitigating the risks associated with cloud-hosted services. Additionally, ensure that everyone on your staff (whether they are full-time employees or consultants) is crystal clear about the various shared responsibility models in use by your various cloud providers. As the complexity of enterprise cloud environments continue to increase, implementing the methods outlined above will continue to increase in importance to mitigate the inherent risk associated with the cloud.
5. **Use Standardized Cloud Assessment Questions:** In addition, having a set of up-to-date cloud provider assessment questions that are representative of your organization's cyber security and compliance goals is important as well. With cloud services coming in all shapes and sizes, asking a standardized set of questions to each potential vendor will help you establish a comparison baseline to understand which cloud provider/service will be best for your business's needs.

## Common threats to cloud computing:

**Eavesdropping —** Data scavenging, traffic or trend analysis, social engineering, economic or political espionage, sniffing, dumpster diving, keystroke monitoring, and shoulder surfing are all types of eavesdropping to gain information or to create a foundation for a later attack. Eavesdropping is a primary cause of the failure of confidentiality.

**Fraud —** Examples of fraud include collusion, falsified transactions, data manipulation, and other altering of data integrity for gain.

**Theft —** Examples of theft include the theft of information or trade secrets for profit or unauthorized disclosure, and physical theft of hardware or software.

**Sabotage —** Sabotage includes denial-of-service (DoS) attacks, production delays, and data integrity sabotage.

**External attack —** Examples of external attacks include malicious cracking, scanning, and probing to gain infrastructure information, demon dialing to locate an unsecured modem line, and the insertion of a malicious code or virus.

**Logon Abuse**: Logon abuse can refer to legitimate users accessing services of a higher security level that would normally be restricted to them. Unlike network intrusion, this type of abuse focuses primarily on those users who might be legitimate users of a different system

or users who have a lower security classification. Masquerading is the term used when one user pretends to be another user, such as an attacker socially engineering passwords from an Internet Service Provider (ISP).

**Inappropriate System Use:** This style of network abuse refers to the non-business or personal use of a network by otherwise authorized users, such as Internet surfing to inappropriate content sites (travel, pornography, sports, and so forth). As per the International Information Systems Security Certification Consortium (ISC) Code of Ethics and the Internet Advisory Board (IAB) recommendations, the use of networked services for other than business purposes can be considered abuse of the system. While most employers do not enforce extremely strict Web surfing rules, occasional harassment litigation may result from employees accessing pornography sites and employees operating private Web businesses using the company's infrastructure.

**Denial-of-Service (DoS) Attacks:** A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

**Session Hijacking Attacks:** Unauthorized access to a system can be achieved by session hijacking. In this type of attack, an attacker hijacks a session between a trusted client and network server. The attacking computer substitutes its IP address for that of the trusted client and the server continues the dialog, believing it is communicating with the trusted client. Highjacking attacks include IP spoofing attacks, TCP sequence number attacks, and DNS poisoning.

**Cloud SLA (Cloud Service-Level Agreement):** A cloud SLA (cloud service-level agreement) is an agreement between a cloud service provider and a customer that ensures a minimum level of service is maintained. It guarantees levels of reliability, availability and responsiveness to systems and applications, while also specifying who will govern when there is a service interruption.

A Service Level Agreement (SLA) is the bond for performance negotiated between the cloud services provider and the client. Earlier, in cloud computing all Service Level Agreements were negotiated between a client and the service consumer. Nowadays, with the initiation of large utility-like cloud computing providers, most Service Level Agreements are standardized until a client becomes a large consumer of cloud services. Service level agreements are also defined at different levels which are mentioned below:

- Customer-based SLA
- Service-based SLA
- Multilevel SLA

Few Service Level Agreements are enforceable as contracts, but mostly are agreements or contracts which are more along the lines of an Operating Level Agreement (OLA) and may not have the restriction of law. It is fine to have an attorney review the documents before

making a major agreement to the cloud service provider. Service Level Agreements usually specify some parameters which are mentioned below:

1. Availability of the Service (uptime)
2. Latency or the response time
3. Service components reliability
4. Each party accountability
5. Warranties

In any case, if a cloud service provider fails to meet the stated targets of minimums then the provider has to pay the penalty to the cloud service consumer as per the agreement. So, Service Level Agreements are like insurance policies in which the corporation has to pay as per the agreements if any casualty occurs. Microsoft publishes the Service Level Agreements linked with the Windows Azure Platform components, which is demonstrative of industry practice for cloud service vendors. Each individual component has its own Service Level Agreements. Below are two major Service Level Agreements (SLA) described:

**Windows Azure SLA –**Window Azure has different SLA's for compute and storage. For compute, there is a guarantee that when a client deploys two or more role instances in separate fault and upgrade domains, client's internet facing roles will have external connectivity minimum 99.95% of the time. Moreover, all of the role instances of the client are monitored and there is guarantee of detection 99.9% of the time when a role instance's process is not runs and initiates properly.

**SQL Azure SLA –** SQL Azure clients will have connectivity between the database and internet gateway of SQL Azure. SQL Azure will handle a "Monthly Availability" of 99.9% within a month. Monthly Availability Proportion for a particular tenant database is the ratio of the time the database was available to customers to the total time in a month. Time is measured in some intervals of minutes in a 30-day monthly cycle. Availability is always remunerated for a complete month. A portion of time is marked as unavailable if the customer's attempts to connect to a database are denied by the SQL Azure gateway.

**SLA Life Cycle:** SLA management should support the SLA Life Cycle. The management of SLAs requires interactions between many processes. Various stages must be considered. This lifecycle may be the following:

**The Product /Service Development stage (Marketing stage):** This stage consists in the identification of the customer needs and the network capacities. From that, service templates are prepared.

**The Negotiation & Sales stage:** where an SLA is negotiated with a customer. Resource reservation is also used to check with the planning if the SLA can be supported.

**The Provisioning stage:** This stage consists of there source provisioning (i.e. network and service provisioning) and the service activation.

**The Assurance stage:** which is in charge to monitor, validate and report the SLA, detect SLA violations and handle them

**The Assessment stage:** composed of two parts. Assessment with the Customer (to check its satisfaction and to identify evolution of its requirements) and internal operator assessment (to check the overall Service quality, key problems, …)