UNIT – IV Cloud Administration and Security Management

Cloud security

- Different types of cloud computing service models provide different levels of security services. You get the least amount of built in security with an Infrastructure as a Service provider, and the most with a Software as a Service provider
- The Internet was designed primarily to be resilient; it was not designed to be secure. Any distributed application has a much greater attack surface than an application that is closely held on a Local Area Network. Cloud computing has all the vulnerabilities associated with Internet applications, and additional vulnerabilities arise from pooled, virtualized, and outsourced resources

- highlighted the following areas of cloud computing that they felt were uniquely troublesome:
- Auditing
- Data integrity
- e-Discovery for legal compliance
- Privacy l Recovery
- Regulatory compliance

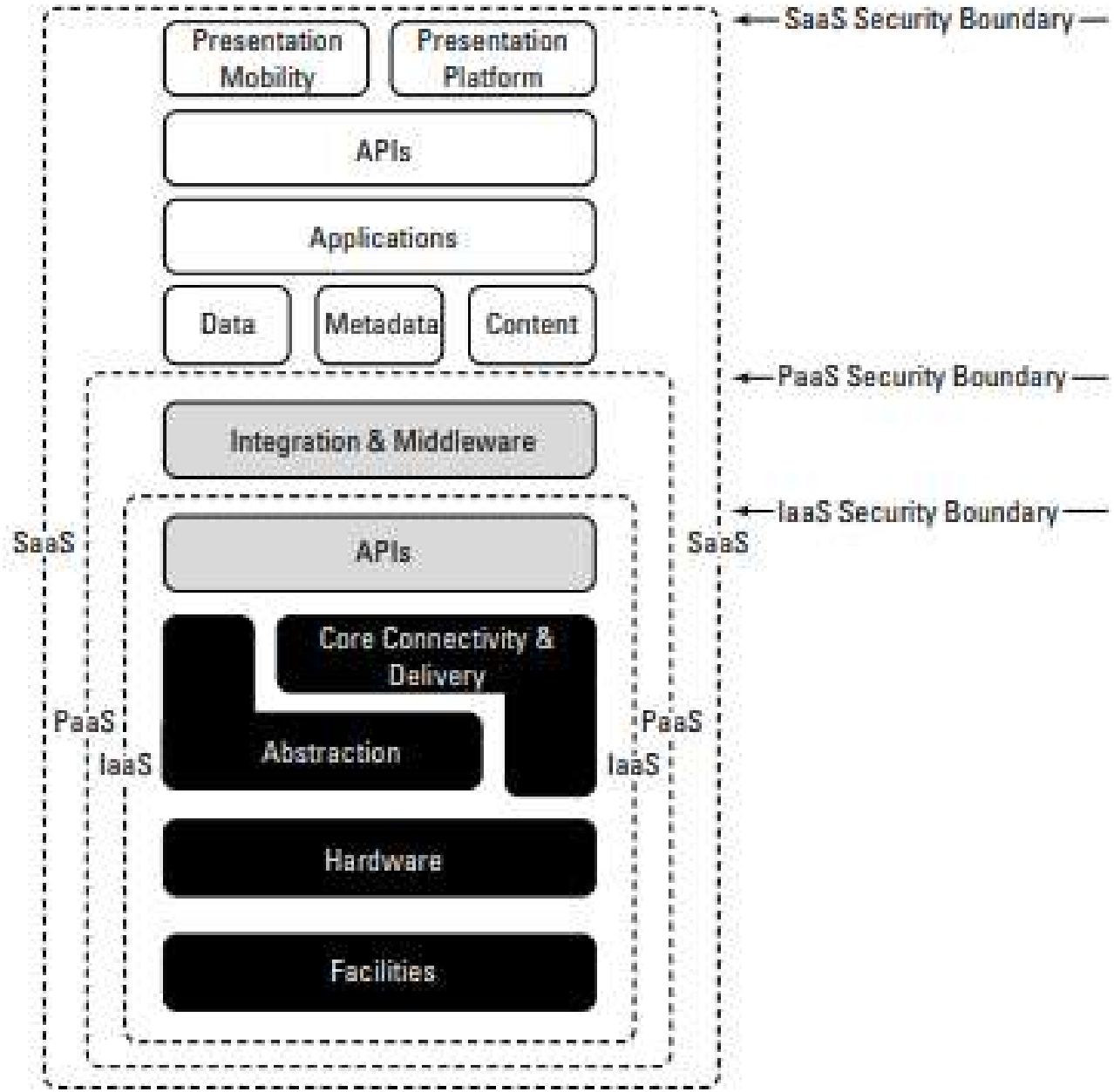
- Your risks in any cloud deployment are dependent upon the particular cloud service model chosen and the type of cloud on which you deploy your applications. In order to evaluate your risks, you need to perform the following analysis:
- 1. Determine which resources (data, services, or applications) you are planning to move to the cloud.
- 2. Determine the sensitivity of the resource to risk. Risks that need to be evaluated are loss of privacy, unauthorized access by others, loss of data, and interruptions in availability.
- 3. Determine the risk associated with the particular cloud type for a resource. Cloud types include public, private (both external and internal), hybrid, and shared community types.
- 4. Take into account the particular cloud service model that you will be using. Different models such as IaaS, SaaS, and PaaS require their customers to be responsible for security at different levels of the service stack.
- 5. If you have selected a particular cloud service provider, you need to evaluate its system to understand how data is transferred, where it is stored, and how to move data both in and out of the cloud.

- Cloud Security Alliance (CSA; http://www.cloudsecurity alliance.org/) cloud computing stack model, which shows how different functional units in a network stack relate to one another.
- this model can be used to separate the different service models from one another. CSA is an industry working group that studies security issues in cloud computing and offers recommendations to its members.

Security service boundary

- The CSA functional cloud computing hardware/software stack is the Cloud Reference Model.
- IaaS is the lowest level service, with PaaS and SaaS the next two services above. As you move upward in the stack, each service model inherits the capabilities of the model beneath it, as well as all the inherent security concerns and risk factors.
- IaaS supplies the infrastructure; PaaS adds application development frameworks, transactions, and control structures; and SaaS is an operating environment with applications, management, and the user interface.
- As you ascend the stack, IaaS has the least levels of integrated functionality and the lowest levels of integrated security, and SaaS has the most.
- each different type of cloud service delivery model creates a security boundary at which the cloud service provider's responsibilities end and the customer's responsibilities begin.
- Any security mechanism below the security boundary must be built into the system, and any security mechanism above must be maintained by the customer.
- As you move up the stack, it becomes more important to make sure that the type and level of security is part of your Service Level Agreement

The CSA Cloud Reference Model with security boundaries shown



- In the SaaS model, the vendor provides security as part of the Service Level Agreement, with the compliance, governance, and liability levels stipulated under the contract for the entire stack.
- For the PaaS model, the security boundary may be defined for the vendor to include the software framework and middleware layer. In the PaaS model, the customer would be responsible for the security of the application and UI at the top of the stack.
- The model with the least built-in security is IaaS, where everything that involves software of any kind is the customer's problem.

Security Responsibilities by Service Model

Model Type	Infrastructure Security Management	Infrastructure Owner	Infrastructure Location	Trust Condition
Hybrid	Both vendor and customer	Both vendor and customer	Both on- and off-premises	Both trusted and untrusted
Private/Community	Customer	Customer	On- or off-premises	Trusted
Private/Community	Customer	Vendor	Off- or on-premises	Trusted
Private/Community	Vendor	Customer	On- or off-premises	Trusted
Private/Community	Vendor	Vendor	Off- or on-premises	Trusted
Public	Vendor	Vendor	Off-premises	Untrusted

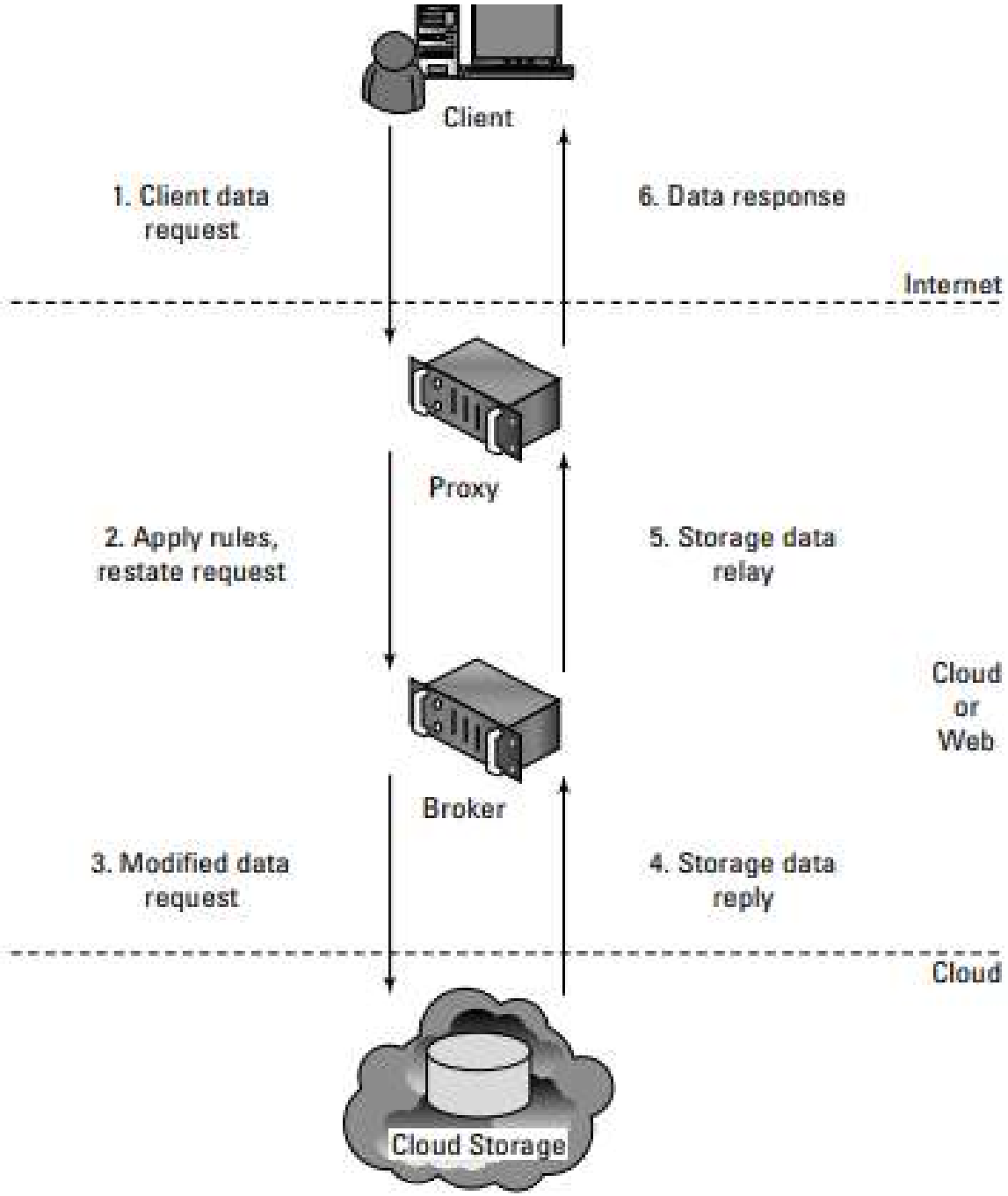
Securing Data

- Securing data sent to, received from, and stored in the cloud is the single largest security concern that most organizations should have with cloud computing. As with any WAN traffic, you must assume that any data can be intercepted and modified. These are the key mechanisms for protecting data mechanisms:
- Access control
- Auditing
- Authentication
- Authorization

Brokered cloud storage access

- The problem with the data you store in the cloud is that it can be located anywhere in the cloud service provider's system: in another datacenter, another state or province, and in many cases even in another country.
- With other types of system architectures, such as client/server, you could count on a firewall to serve as your network's security perimeter; cloud computing has no physical system that serves this purpose.
- Therefore, to protect your cloud storage assets, you want to find a way to isolate data from direct client access.
- In one scheme, two services are created: a broker with full access to storage but no access to the client, and a proxy with no access to storage but access to both the client and broker.

- when a client makes a request for data, here's what happens:
- 1. The request goes to the external service interface (or endpoint) of the proxy, which has only a partial trust.
- 2. The proxy, using its internal interface, forwards the request to the broker.
- 3. The broker requests the data from the cloud storage system.
- 4. The storage system returns the results to the broker.
- 5. The broker returns the results to the proxy.
- 6. The proxy completes the response by sending the data requested to the client.


Client
1. Client data request
6. Data response
Internet
Proxy
2. Apply rules, restate request
5. Storage data relay
Cloud or Web
Broker
3. Modified data request
4. Storage data reply
Cloud
Cloud Storage

- **Encryption**
- Strong encryption technology is a core technology for protecting data in transit to and from the cloud as well as data stored in the cloud. It is or will be required by law.
- The goal of encrypted cloud storage is to create a virtual private storage system that maintains confidentiality and data integrity while maintaining the benefits of cloud storage: ubiquitous, reliable, shared data storage.
- Encryption should separate stored data (data at rest) from data in transit.

- **Auditing and compliance**
- Logging is the recording of events into a repository; auditing is the ability to monitor the events to understand performance.
- Logging and auditing is an important function because it is not only necessary for evaluation performance, but it is also used to investigate security and when illegal activity has been perpetrated.
- Logs should record system, application, and security events, at the very minimum.
- Logging and auditing are unfortunately one of the weaker aspects of early cloud computing service offering

IAM (Identity and Access Management)

- IAM Definitions
  - Authentication
  - Authorization
  - Auditing
- **Authentication** is the process of verifying the identity of a user or system (e.g., Lightweight Directory Access Protocol [LDAP] verifying the credentials presented by the user, where the identifier is the corporate user ID that is unique and assigned to an employee or contractor).
- Authentication usually denotes a more robust form of identification.

- **Authorization** is the process of determining the privileges the user or system is entitled to once the identity is established.
- In the context of digital services, authorization usually follows the authentication step and is used to determine whether the user or service has the necessary privileges to perform certain operations—in other words, authorization is the process of enforcing policies.
- **Auditing** In the context of IAM, auditing entails the process of review and examination of authentication, authorization records, and activities to determine the adequacy of IAM system controls, to verify compliance with established security policies and procedures (e.g., separation of duties), to detect breaches in security services , and to recommend any changes that are indicated for countermeasures

Identity and presence protocol standards,

- **LDAP :**The Lightweight Directory Access Protocol (LDAP) is an open-source protocol not associated with any specific vendor, although it does provide the basis for Microsoft's Active Directory.
- LDAP was established as an industry standard in the 1990s and is among the oldest identity and access management protocols.
- It runs above the TCP/IP stack and is most often used in modern organizations as a tool to handle authentication for on-premise applications.

SAML

- **SAML :** The Security Assertion Markup Language (SAML) protocol is most often used in systems employing the Single Sign-On (SSO) method of access control.
- In SSO, one set of credentials allows users to access multiple applications.
- This method is most beneficial when users must move between applications during sessions. Instead of requiring individual logins for each application, SSO makes use of data already authenticated for the session to streamline the switch between applications. The resulting increase in efficiency helps prevent bottlenecks in the authorization process.

OpenID

- OpenID is an open, decentralized standard for user authentication and access control, allowing users to log on to many services with the same digital identity—i.e., a single sign-on user experience with services supporting OpenID.
- As such, it replaces the common logon process that uses a logon username and password, by allowing a user to log on once and gain access to the resources of multiple software systems.
- OpenID is primarily targeted for consumer services offered by Internet companies including Google, eBay, Yahoo!, Microsoft, AOL, BBC, PayPal, and so on.

Information cards

- Information cards are another open standard for identity on the Web. The standard itself is directed by the Information Card Foundation, whose steering members include representatives from Google, Microsoft, PayPal, Oracle Novell, and Equifax.
- The Foundations states that its mission is "to reduce the instance of identity theft by securing digital identities in place of traditional logons and passwords."
- The goal of this standard is to provide users with a safe, consistent, phishing-resistant user interface that doesn't require a username and password.
- People can use an information card digital identity across multiple sites for convenience without compromising their login information
- .The Information Cards Protocol is designed for use in high-value scenarios, such as banking, where phishing resistance and support for secure authentication mechanisms such as smart cards are critical business requirements.

Open Authentication (OATH)

- OATH is a collaborative effort of IT industry leaders aimed at providing an architecture reference for universal, strong authentication across all users and all devices over all networks.
- The goal of this initiative is to address the three major authentication methods:
  - • Subscriber Identity Module (SIM)-based authentication (using a Global System for Mobile Communications/General Packet Radio Service [GSM/GPRS] SIM)
  - • Public Key Infrastructure (PKI)-based authentication
  - • One-Time Password (OTP)-based authentication

Open Authentication API (OpenAuth)

- OpenAuth is an AOL-proprietary API that enables third-party websites and applications to authenticate AOL and AOL Instant Messenger (AIM) users through their websites and applications.
- Using this authentication method, an AIM- or AOL-registered user can log on to a third-party website or application and access AOL services or new services built on top of AOL services.
- According to AOL, the OpenAuth API provides the following features:
- • A secure method to sign in. User credentials are never exposed to the websites or applications the user signs into.
- • A secure method to control which sites are allowed to read private or protected content. • Automatic granting of permissions only if the user selects Allow Always on the Consent page.
- • A prompt for user consent when the website or application attempts to read any private or protected content (e.g., separate consent requests to allow Buddy List information, to send IMs, to read albums).
- • Access to other non-AOL websites without the need to create a new user account at each site that supports AOL OpenAuth APIs.

Availability Management

- Cloud services are not immune to outages, and the severity and scope of impact to the customer can vary based on the outage situation.
- Similar to any internal IT-supported application, business impact due to a service outage will depend on the criticality of the cloud application and its relationship to internal business processes.
- In the case of business-critical applications where businesses rely on the continuous availability of service, even a few minutes of service outage can have a serious impact on your organization's productivity, revenue, customer satisfaction, and service-level compliance.
- Furthermore, depending on the severity of the incident and the scope of the affected infrastructure, outages may affect all or a subset of customers.
- During a cloud service disruption, affected customers will not be able to access the cloud service and in some cases may suffer degraded performance or user experience.
- For example, when a storage service is disrupted, it will affect the availability and performance of a computing service that depends on the storage service.

SaaS Availability Management

- By virtue of the service delivery and business model, SaaS service providers are responsible for business continuity, application, and infrastructure security management processes.
- This means the tasks your IT organization once handled will now be handled by the CSP.
- for example, if a marketing application is considered critical and has a high department's availability expectation based on the SaaS provider's SLA?

- In some cases, SaaS vendors may not offer SLAs and may simply address service terms via terms and conditions.
- For example, Salesforce.com does not offer a standardized SLA that describes and specifies performance criteria and service commitments.
- However, another CRM SaaS provider, NetSuite, offers the following SLA clauses:
- Uptime Goal—NetSuite commits to provide 99.5% uptime with respect to the NetSuite application, excluding regularly scheduled maintenance times.
- Scheduled and Unscheduled Maintenance—Regularly scheduled maintenance time does not count as downtime. Maintenance time is regularly scheduled if it is communicated at least two full business days in advance of the maintenance time. Regularly scheduled maintenance time typically is communicated at least a week in advance, scheduled to occur at night on the weekend, and takes less than 10–15 hours each quarter
- NetSuite hereby provides notice that every Saturday night 10:00pm–10:20pm Pacific Time is reserved for routine scheduled maintenance for use as needed..

Customer Responsibility

- Customers should understand the SLA and communication methods (e.g., email, RSS feed, website URL with outage information) to stay informed on service outages.
- When possible, customers should use automated tools such as Nagios or Siteuptime.com to verify the availability of the SaaS service.
- Customers of cloud services should note that a multitenant service delivery model is usually designed with a "one size fits all" operating principle, which means CSPs typically offer a standard SLA for all customers.
- Thus, CSPs may not be amenable to providing custom SLAs if the standard SLA does not meet your service-level requirements. However, if you are a medium or large enterprise with a sizable budget, a custom SLA may still be feasible.

SaaS Health Monitoring

- The following options are available to customers to stay informed on the health of their service:
- • Service health dashboard published by the CSP. Usually SaaS providers, such as Salesforce.com, publish the current state of the service, current outages that may impact customers, and upcoming scheduled maintenance services on their website (e.g., http://trust.salesforce.com/trust/status/).
- • The Cloud Computing Incidents Database (CCID). (This database is generally community supported, and may not reflect all CSPs and all incidents that have occurred.)
- • Customer mailing list that notifies customers of occurring and recently occurred outages.
- • Internal or third-party-based service monitoring tools that periodically check SaaS provider health and alert customers when service becomes unavailable (e.g., Nagios monitoring tool).
- • RSS feed hosted at the SaaS service provider.

PaaS Availability Management

- The customer is responsible for managing the availability of the customer developed application and third-party services, and the PaaS CSP is responsible for the PaaS platform and any other services supplied by the CSP.
- For example, Force.com is responsible for the management of the AppExchange platform, and customers are responsible for managing the applications developed and deployed on that platform.
- PaaS application availability depends on the robustness of your application, the PaaS platform on which the application is built, and third-party web services components.

- In cases where the PaaS platform enforces quotas on compute resources (CPU, memory, network I/O), upon reaching the thresholds the application may not be able to respond within the normal latency expectations and could eventually become unavailable.
- For example, the Google App Engine has a quota system whereby each App Engine resource is measured against one of two kinds of quotas: a billable quota or a fixed quota.

Customer Responsibility

- Customer Responsibility Considering all of the variable parameters in availability management, the PaaS application customer should carefully analyze the dependencies of the application on the third-party web services (components) and outline a holistic management strategy to manage and monitor all the dependencies.
- The following considerations are for PaaS customers
- PaaS platform service levels Customers should carefully review the terms and conditions of the CSP's SLAs and understand the availability constraints.
- Third-party web services provider service levels When your PaaS application depends on a third-party service, it is critical to understand the SLA of that service. For example, your PaaS application may rely on services such as Google Maps and use the Google Maps API to embed maps in your own web pages with JavaScrip
- Network connectivity parameters for the network (Internet)-connecting PaaS platform with third-party service providers The parameters typically include bandwidth and latency factors.

PaaS Health Monitoring

- The following options are available to customers to monitor the health of their service:
- • Service health dashboard published by the CSP
- • CCID (this database is generally community-supported, and may not reflect all CSPs and all incidents that have occurred) • CSP customer mailing list that notifies customers of occurring and recently occurred outages
- • RSS feed for RSS readers with availability and outage information
- • Internal or third-party-based service monitoring tools that periodically check your PaaS application, as well as third-party web services that monitor your application (e.g., Nagios monitoring tool)

IaaS Availability Management

- Managing your IaaS virtual infrastructure in the cloud depends on five factors:
- • Availability of a CSP network, host, storage, and support application infrastructure. This factor depends on the following:
  - CSP data center architecture, including a geographically diverse and fault-tolerance architecture.
  - Reliability, diversity, and redundancy of Internet connectivity used by the customer and the CSP.
  - Reliability and redundancy architecture of the hardware and software components used for delivering compute and storage services
  - Availability management process and procedures, including business continuity processes established by the CSP.
  - Web console or API service availability. The web console and API are required to manage the life cycle of the virtual servers. When those services become unavailable, customers are unable to provision, start, stop, and deprovision virtual servers.
  - SLA. Because this factor varies across CSPs, the SLA should be reviewed and reconciled, including exclusion clauses.

IaaS Health Monitoring

- The following options are available to IaaS customers for managing the health of their service:
- Service health dashboard published by the CSP.
- CCID (this database is generally community-supported, and may not reflect all CSPs and all incidents that have occurred).
- CSP customer mailing list that notifies customers of occurring and recently occurred outages.
- • Internal or third-party-based service monitoring tools (e.g., Nagios) that periodically check the health of your IaaS virtual server. For example, Amazon Web Services (AWS) is offering a cloud monitoring service called CloudWatch.
- This web service provides monitoring for AWS cloud resources, including Amazon's Elastic Compute Cloud (EC2). It also provides customers with visibility into resource utilization, operational performance, and overall demand patterns, including metrics such as CPU utilization, disk reads and writes, and network traffic.
- • Web console or API that publishes the current health status of your virtual servers and network

Security Patch Management

- Security patch management is a vital threat management element in protecting hosts, network devices, and applications from unauthorized users exploiting a known vulnerability.
- Patch management processes follow a change management framework and feeds directly from the actions directed by your vulnerability management program.
- Security patch management mitigates risk to your organization by way of insider and outsider threats.
- Hence, SaaS providers should be routinely assessing new vulnerabilities and patching the firmware and software on all systems that are involved in delivering the *aaS service to customers.

- The scope of patch management responsibility for customers will have a low-to-high relevance in the order of SaaS, PaaS, and IaaS services—that is,
- customers are relieved from patch management duties in a SaaS environment, whereas they are responsible for managing patches for the whole stack of software (operating system, applications, and database) installed and operated on the IaaS platform. Customers are also responsible for patching their applications deployed on the PaaS platform.

Security Configuration Management

- Security configuration management is another significant threat management practice to protect hosts and network devices from unauthorized users exploiting any configuration weakness.
- Security configuration management is closely related to the vulnerability management program and is a subset of overall IT configuration management.
- Protecting the configuration of the network, host, and application entails monitoring and access control to critical system and database configuration files, including OS configuration, firewall policies, network zone configuration, locally and remotely attached storage, and an access control management database.
- configuration management from a customer responsibility perspective has a low-to-high relevance in the order of SaaS, PaaS, and IaaS services—that is,

- SaaS and PaaS service providers are responsible for configuration management of their platform, whereas IaaS customers are responsible for configuration management of the operating system, application, and database hosted on the IaaS platform.
- Customers are also responsible for configuration management of their applications deployed on the PaaS platform.