MODULE 5

SECURITY IN THE CLOUD

- Security Overview
- Cloud Security Challenges
- Security -as-a-Service
- Security Governance
- Risk Management
- Security Monitoring
- Security Architecture Design
- Data Security
- Application Security
- Virtual Machine Security.

Defining cloud security

- It is a set of control-based technologies & policies adapted to stick to regulatory compliances, rules & protect data, application and cloud technology infrastructure.

Security Overview

- Cloud service providers are leveraging virtualization technologies combined with self-service capabilities for computing resources via the Internet.
- In these service provider environments, virtual machines from multiple organizations have to be co-located on the same physical server in order to maximize the efficiencies of virtualization.

- Cloud service providers must learn from the managed service provider (MSP) model and ensure that their customers’ applications and data are secure if they hope to retain their customer base and competitiveness.
- Today, enterprises are looking toward cloud computing horizons to expand their on-premises infrastructure
- But most cannot afford the risk of compromising the security of their applications and data.

- Security in cloud concerns how resources should be protected in the Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) environments
- It offers security “best practices” for service providers and enterprises that are in moving into the cloud computing space.

- **Software-as-a-Service** is a model of software deployment in which an application is licensed for use as a service provided to customers on demand.
- On-demand licensing and use relieves the customer of the burden of equipping a device with every application to be used.
- Gartner predicts that 30% of new software will be delivered via the SaaS model by 2010.

- **Platform-as-a-Service** is an outgrowth of the SaaS application delivery model.
- With the PaaS model, all of the facilities required to support the complete life cycle of building and delivering web applications and services are available to developers, IT managers, and end users entirely from the Internet, without software downloads or installation.
- PaaS is also sometimes known as “cloudware.”

- PaaS offerings include workflow facilities for application design, application development, testing, deployment, and hosting
- As well as application services such as team collaboration, web service integration and marshalling, database integration, security, scalability, storage, persistence, state management, application versioning, application instrumentation, and developer community facilitation.
- These services are provisioned as an integrated solution over the web.

- **Infrastructure-as-a-Service** is the delivery of computer infrastructure (typically a platform virtualization environment) as a service.
- These “virtual infrastructure stacks” are an example of the **everything-as-a-service** trend and share many of the common characteristics.
- Rather than purchasing servers, software, data center space, or network equipment, clients buy these resources as a fully outsourced service.

- Inspired by the IT industry’s move toward SaaS, in which software is not purchased but rented as a service from providers, IT-as-a-Service
- (ITaaS) is being proposed to take this concept further, to bring the service model right to your IT infrastructure.
- The modern IT organization must run itself as a separate operation and become more strategic in operational decisions.

- **Anything-as-a-Service (XaaS),** which is also a subset of cloud computing.
- XaaS broadly encompasses a process of activating reusable software components over the network. The most common and successful example is Software-as-a-Service.
- The growth of “as-a-service” offerings has been facilitated by extremely low barriers to entry (they are often accessible for free or available as recurring charges on a personal credit card).

Cloud security Challenges

- **Physical Security** – In Cloud you can not provide physical security
- **Shared Resources** – In public Cloud you are sharing resources
  - When in a shared environment you dont have any knowledge or control of where the resources run.
- **Vendor Lock-in** is another challenge
  - When choosing cloud-based services, its important to check to see how easy it would be to migrate from that service to another one.
  - For example, is your data stored in a format that is easy to export to a different system?
- **Integrity of data**
  - Data integrity means ensuring that data is identically maintained during any operation (such as transfer, storage, or retrieval).
  - Ensuring the integrity of the data really means that it changes only in response to authorized transactions.

- **Access to Log** –Security managers need to make sure to negotiate access to the providers logs as part of any service agreement
- **Frequent Update of application** –Cloud applications undergo constant feature additions, and users must keep up to date with application improvements to be sure they are protected.
- **Data Compliance** – The data owner is still fully responsible for compliance.
- **Isolation of Virtual Machines (VM's)** – Since the virtual machines of multiple IT firms can run in co-located environment, there must be mechanisms to ensure isolation of co-located VM's.

Security-as-a-Service(SECaas)

- **Security as a service (SECaaS)** is an outsourced service where a third party handles and manages security of a company.
- The simplest example of security as a service is using an anti-virus software over the Internet.
- Conventionally security is ensured in firms by installing virus protection software, spam filtering software, and other security tools on each machine or on the network or server in workplace, and keeping the software up-to-date.
- But security as a service allows you to use the same tools using only a web browser, making it direct and affordable.

Security-as-a-Service Offerings

- **Disaster recovery and business continuity.**
  - Tools that help to make sure that IT and operations are back in no time when disaster strikes.
- **Continuous monitoring.**
  - Tools that allow to manage risks continually by monitoring the security processes that are in place.
- **Data loss prevention.**
  - Tools that protect, monitor, and verify the security of all of your data, whether they are in storage or in use.

- **Email security.**
  - Protects your business from phishing, spam, and malicious attachments.
- **Encryption.**
  - Makes your data unreadable unless it is decoded using the right numerical and cryptographic ciphers.
- **Identity and access management.**
  - Provides authentication, access intelligence, and identify verification & user management tools.
- **Intrusion management.**
  - Detects unusual events and behaviors using pattern recognition technology.
  - These tools not only detect intrusions; they also help you manage them.

- **Network security.**
  - Tools and services that help you manage network access and protect, and monitor network services.
- **Security assessment.**
  - Audits the current security measures you have in place to see if these are compliant with industry standards.
- **Security information and event management.**
  - Tools that aggregate log and event information, which can be analyzed in real time to help you detect possible anomalies and intrusion.
- **Vulnerability scanning.**
  - Detects any vulnerability in your network or IT infrastructure.
- **Web security.**
  - Gives you protection for online applications that are accessed by the public in real-time

Security governance

- **Security Governance** is an attempt to emphasize that security needs to be managed and governed throughout the organization, not just in the IT department.
- Security governance is the collection of practices related to supporting, defining, and directing the security efforts of an organization.
- Security governance is closely related to and often intertwined with corporate and IT governance.

Security Governance -principles

- **Establish organization wide information security.**
  - Top-level management should ensure that information security serves overall business objectives and should establish responsibility and accountability throughout the organization.
- **Adopt a risk-based approach.**
  - Security governance, including allocation of resources and budgets, should be based on the risk appetite of an organization.
- **Set the direction of investment decisions.**
  - Information security investments are intended to support organizational objectives.

- **Ensure conformance with internal and external requirements.**
  - External requirements include mandatory legislation and regulations, standards leading to certification, and contractual requirements.
  - Internal requirements comprise broader organizational goals and objectives.
  - Independent security audits are the accepted means of determining and monitoring conformance.
- **Foster a security-positive environment for all stakeholders.**
  - Security governance should be responsive to stakeholder expectations, keeping in mind that various stakeholders can have different values and needs.
- **Review performance in relation to business outcomes.**
  - Governance executives should mandate reviews of a performance measurement program for monitoring, audit, and improvement that links information security performance to business performance.

Security Governance-Desired Outcomes

- **Strategic alignment**:
  - Information security strategy and policy be aligned with business strategy.
- **Risk management**:
  - Involves mitigating risks and reducing or preventing potential impact on information resources.

Security Governance-Desired Outcomes

- **Resource management**:
  - Key goal of information security governance is to align information security budgets with overall enterprise requirements
- **Value delivery**:
  - Resources expended on information security be constrained within overall enterprise resource objectives and should achieve optimum value.
- **Performance measurement**:
  - The enterprise needs metric against which to judge information security policy to ensure that organizational objectives are achieved.

Risk management in cloud

Risk management in cloud

- Cloud-based information systems are exposed to threats that can have adverse effects on organizational operations, organizational assets, individuals, and other organizations.
- Malicious entities can exploit both known and unknown vulnerabilities to compromise the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by those systems.
- The differences in methods and responsibilities for securing different combinations of service and deployment models present a significant challenge for cloud Consumers.

How it is done..

- We need to perform the following steps
  1. Risk assessment
     - Analyze cloud environment to identify potential vulnerabilities and shortcomings
     - The level of risk is estimated on the basis of the likelihood of an incident scenario, mapped against the estimated negative impact .
     - The likelihood of an incident scenario is given by a threat exploiting vulnerability with a given likelihood.

How it is done..

2. Risk treatment – Design mitigation policies and plans
    - Implement
    - Assess
    - Authorize
3. Risk control – Risk monitoring, surveying, reviewing, events, identifying policy, adjustments

Security Portfolio Management

- Security portfolio management is a fundamental component of ensuring efficient and effective operation of any information security program and organization.
- Lack of portfolio and project management discipline can lead to projects never being completed or never realizing their expected return.

- For every new project that a security team undertakes, the team should ensure that a project plan and project manager with appropriate training and experience is in place so that the project can be seen through to completion.
- Portfolio and project management capabilities can be enhanced by developing methodology, tools,and processes to support the expected complexity of projects that include both traditional business practices and cloud computing practices.

Secure Software Development Life Cycle (SecSDLC)

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

- **Phase 1**.Investigation: Define project processes and goals, and document them in the program security policy.
- **Phase 2.**Analysis: Analyze existing security policies and programs,analyze current threats and controls, examine legal issues, and perform risk analysis.
- **Phase 3**.Logical design: Develop a security blueprint, plan incident response actions, plan business responses to disaster, and determine the feasibility of continuing and/or outsourcing the project

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

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

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

Cloud security monitoring-What it is..?

- **Security Monitoring**, also referred to as "Security Information Monitoring (SIM)" or "Security Event Monitoring (SEM),"
  - involves collecting and analysing information to detect suspicious behavior or unauthorised system changes on your network, defining which types of behavior should trigger alerts, and taking action on alerts as needed.

Challenges of cloud security monitoring

- **Virtualization** poses challenges for monitoring in the cloud, and traditional configurations involving log management, log correlation, and event management tools, since
  - they are not routinely configured to adapt to dynamic environments where virtual machines may come and go in response to sharp increases or decreases in demand.
- **Visibility** can also be a concern when it comes to cloud monitoring.
  - due to lack of access to every layer in the cloud computing stack, and therefore cant gain full visibility to monitor for potential security flaws and vulnerabilities.

Challenges of cloud security monitoring

- **Shifts in security scope** is another common challenge when dealing with cloud environments
  - as assets and applications may move between systems which may not necessarily have the same level of security monitoring.

Security Architecture Design

- A security architecture framework should be established with consideration of processes , operational procedures, technology specifications, people and organizational management, and security program compliance and reporting.
- A security architecture document should be developed that defines security and privacy principles to meet business objectives.

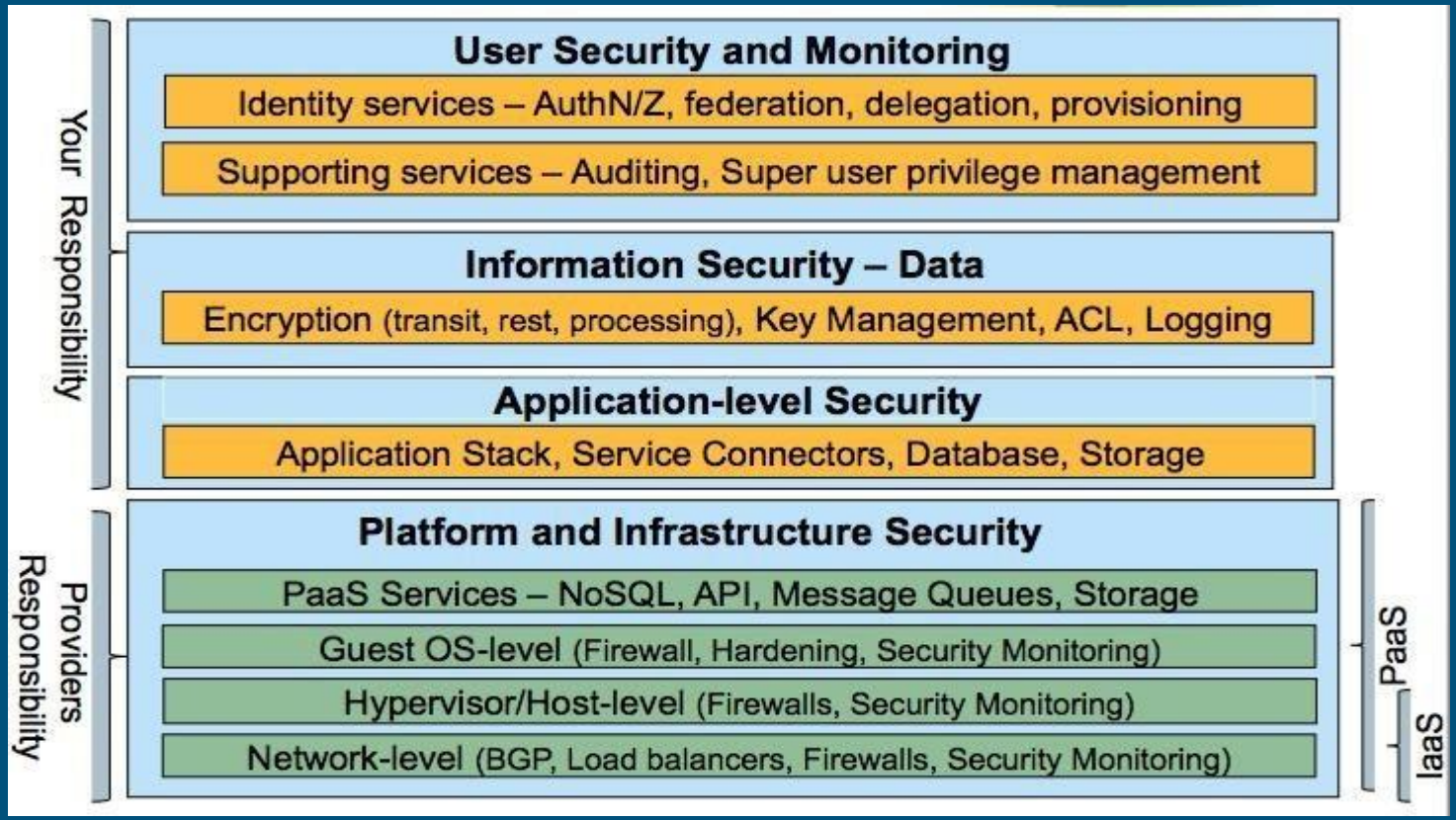
- Documentation is required for management controls and metrics specific to asset classification and control, physical security, system access controls, network and computer management, application development and maintenance, business continuity, and compliance.
- A design and implementation program should also be integrated with the formal system development life cycle to include a business case, requirements definition, design, and implementation plans.

- Security services included in different layers are

1. Authentication
2. Authorization
3. Availability
4. Confidentiality
5. Integrity
6. Accountability
7. Privacy

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

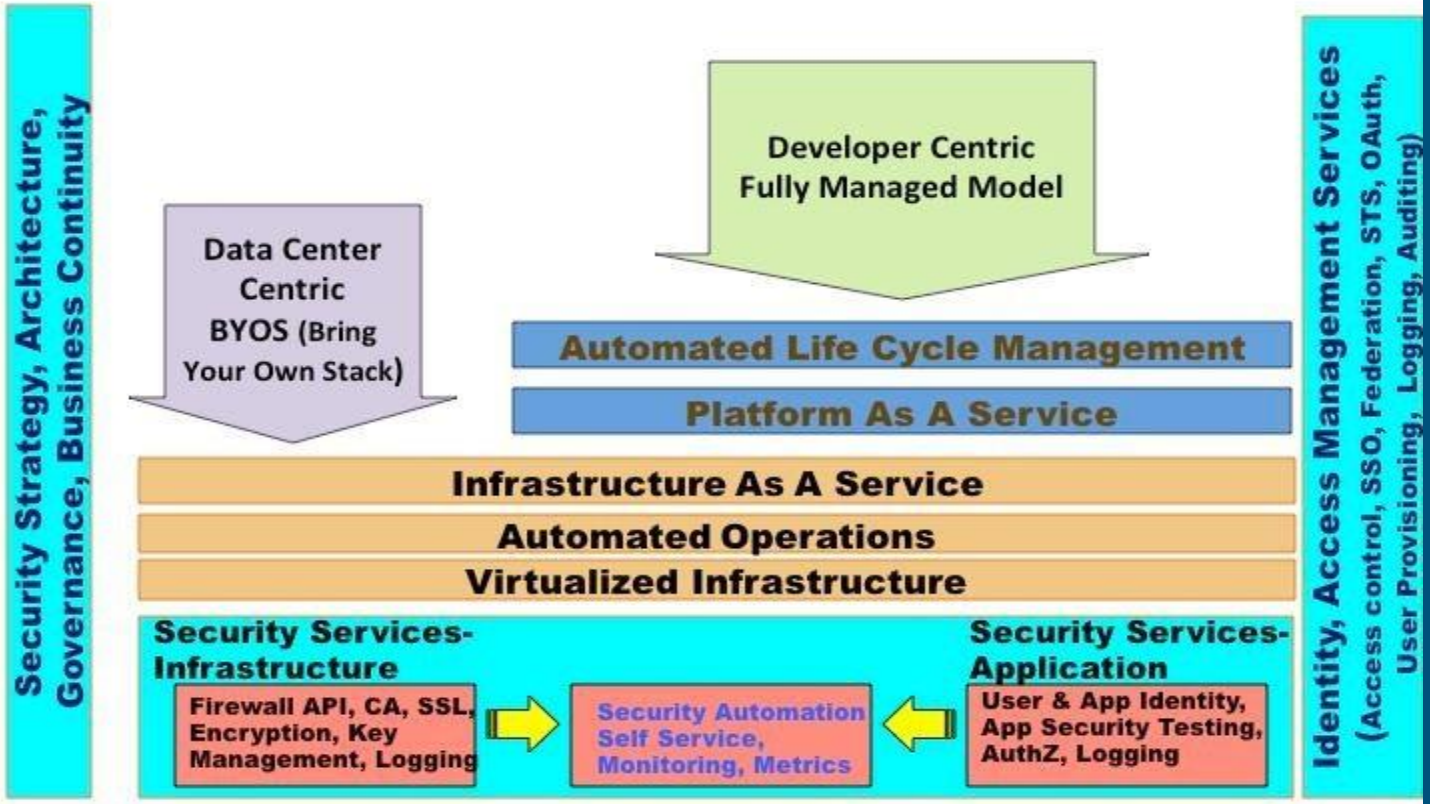
The figure below highlights the layers, within a cloud service, that are secured by the provider versus the customer.



Cloud security architecture-plan

- As a first step, architects need to understand what security capabilities are offered by cloud platforms (PaaS, IaaS).
- The figure below illustrates the architecture for building security into cloud services.

High Level Cloud Architecture – Security services



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

- **Architect for security-as-a-service:** Ultimately this will mitigate threats due to human errors, improve operational efficiency and embed security controls into the cloud applications.
- **Implement sound identity, access management architecture and practice** : Scalable cloud bursting and elastic architecture will rely less on network based access controls and warrant strong user access management architecture.

- A sound architecture will enable reusability of identity and access services for all use cases in public, private and hybrid cloud models
- **Leverage APIs to automate safeguards**
- **Always encrypt or mask sensitive data** : Today's private cloud applications are candidates for tomorrow's public cloud deployment.
- Hence architect applications to encrypt all sensitive data irrespective of the future operational model.

- **Do not rely on an IP address for authentication services :** IP addresses in clouds are ephemeral in nature so you cannot solely rely on them for enforcing network access control.
- Employ certificates (self-signed or from a trusted CA) to enable SSL between services deployed on cloud.
- **Log, Log, Log –** Applications should centrally log all security events that will help create an end-to-end transaction view with non-repudiation characteristics.

- **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 and hosted cloud applications to perform security event correlation.

Data Security

- Traditional models of data protection have often focused on network-centric and perimeter security, frequently with devices such as firewalls and intrusion detection systems.
- But this approach does not provide sufficient protection against APTs(Advanced Persistent Threats), privileged users, or other insidious types of security attacks.

Data Security challenges in cloud.

- The need to protect confidential business, government, or regulatory data
- Cloud service models with multiple tenants sharing the same infrastructure
- Data mobility and legal issues relative to such government rules as the EU Data Privacy Directive
- Lack of standards about how cloud service providers securely recycle disk space and erase existing data

- Auditing, reporting, and compliance concerns
- Loss of visibility to key security and operational intelligence that no longer is available to feed enterprise IT security intelligence and risk management
- A new type of insider who does not even work for your company, but may have control and visibility into your data

Techniques for protecting data in the cloud

- Implement a data security strategy that provides a veritable firewall around the data itself for comprehensive protection.
- Robust access control and well protected key management.
- Stick to all kinds of regulations regarding data compliances - including data privacy, data clearing etc

Common cloud application security threats

- **Mis-configuration of application setup** is the single biggest threads to cloud security because data breaches tend to happen when services are accidentally exposed to the public internet.
- **Unauthorized access** to a website, server, service, or other system is also an area for great concern because once they are in, there is no telling what unauthorized users will do to create chaos.

Common cloud application security threats

- **Insecure APIs and interfaces** present easy opportunities for attackers to breach systems because they are the only asset(s) outside of the organizational boundary with a public IP address.
- **Account hijacking** is feared because so much sensitive data and resources is stored and accessed on devices shared by many different users and because keeping tabs on rogue employees is difficult.

Cloud application security -How they do it..

- The security features and requirements are defined and application security test results are reviewed.
- Application security processes, secure coding guidelines, training, and testing scripts and tools are built as a collaborative effort between the security and the development teams.
- External penetration testers are used for application source code reviews, and attack
- Penetration tests provide an objective review of the security of the application

Virtual machine security

- Virtual Machines are an important part of Cloud Computing.
- In the cloud environment, physical servers are consolidated to multiple virtual machine instances on virtualized servers.
- Majority of the cloud applications are run on VM's
- Hence Security of VM's is an important

Virtual machine security-How it is done.?

- Data center security teams replicate typical security controls for the data center at large to secure the virtual machines
- They can also advise their customers on how to prepare these machines for migration to a cloud environment when appropriate.

Virtual machine security-How it is done.?

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

Cyber attacks that are specific to VM migration

- **Spoofing:** – Mimicking a server to gain unauthorized access.
- **Thrashing:** – A sophisticated denial-of-service (DOS) attack.
  - The attacker deliberately disrupts the migration process at calculated intervals, so the migration is continually restarted over and over, consuming extra compute and network resources as a result.
- **Smash and Grab:** – Forcing a VM image, either at the source or destination server host, into a bad state for the purpose of disrupting operations or exfiltrating data.

- **Spoofing:** – Modern hypervisors should utilize the proper authentication protocols integrated within its migration process to prevent this class of attack.
- **Thrashing:** – Automated migration requests should be throttled to prevent network contention and avoid overloading a single host.
- **Smash and Grab:**
  - First, before initiating a migration, you should regularly create snapshots of the important VM images,
  - Second, many hypervisor toolstacks support customization of the migration process via scripts.
  - Third – hypervisor toolstack may delete the old VM image file after completion

Identity Access Management (IAM)

- Identity and access management is a critical function for every organization, and a fundamental expectation of SaaS customers is that the principle of least privilege is granted to their data.
- The principle of least privilege states that only the minimum access necessary to perform an operation should be granted, and that access should be granted only for the minimum amount of time necessary.

- The advent of cloud services and services on demand is changing the identity management landscape.
- Most of the current identity management solutions are focused on the enterprise and typically are architected to work in a very controlled, static environment.

- In the cloud environment, where services are offered on demand and they can continuously evolve, aspects of current models such as trust assumptions, privacy implications, and operational aspects of authentication and authorization, will be challenged.

- Meeting these challenges will require a balancing act for SaaS providers as they evaluate new models an management processes for IAM to provide end-to-end trust and identity throughout the cloud and the enterprise.
- Another issue will be finding the right balance between usability and security.
- If a good balance is not achieved, both business and IT groups may be affected by barriers to completing their support and maintenance activities efficiently.