Debate: Customer Responsibility For Cloud Security

Session Leader: Ravindra Jugdav

19 June 2019

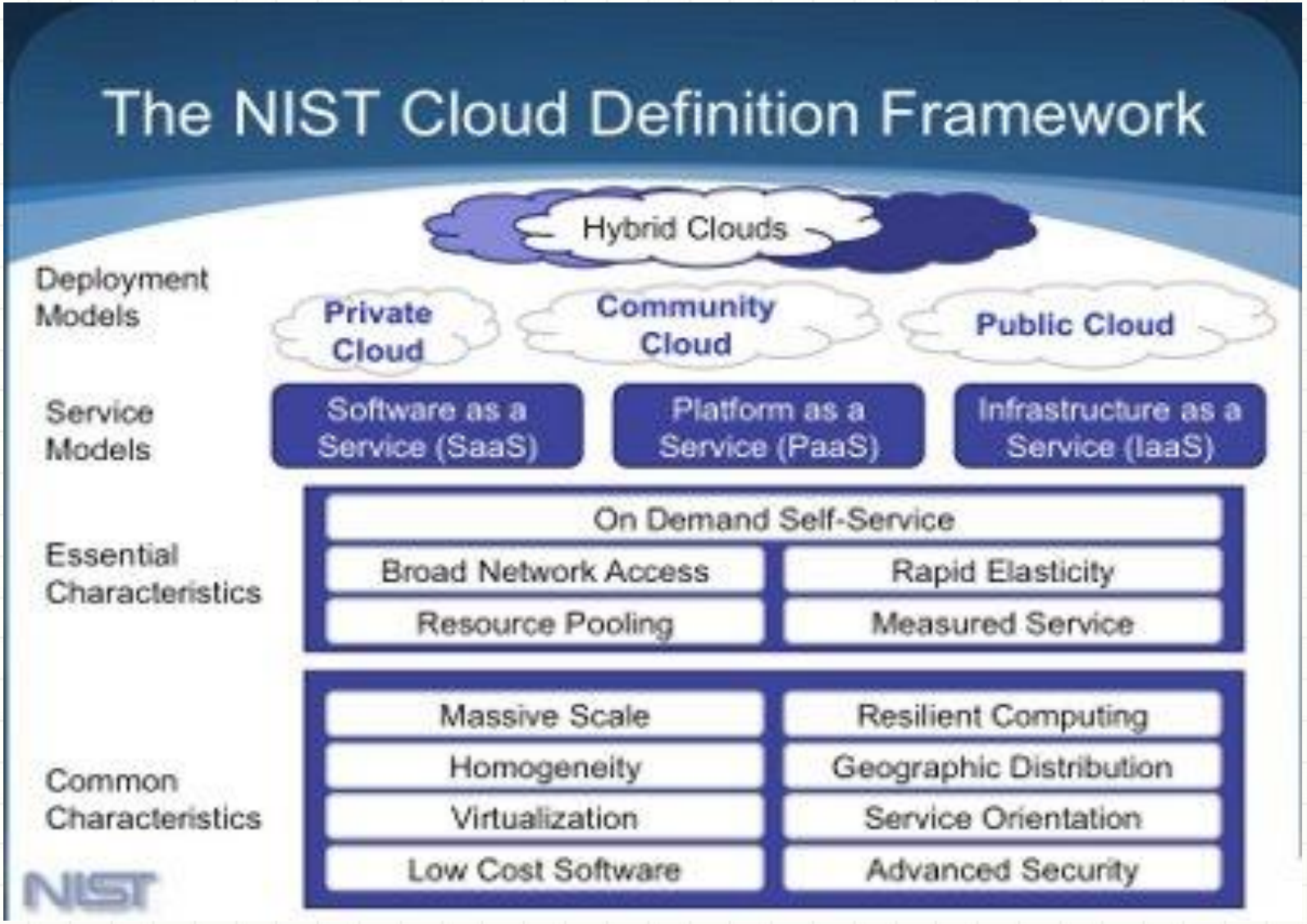
AGENDA

- Cloud Computing Overview
- The Various Cloud Models
- Shared Responsibility Model
- Customer's Responsibility and best practices for:
  - Identity and Access Management
  - Data Security / Encryption
  - Backup and Recovery
  - Operating System Security and Patching
  - Network Security

NIST Definition of Cloud Computing

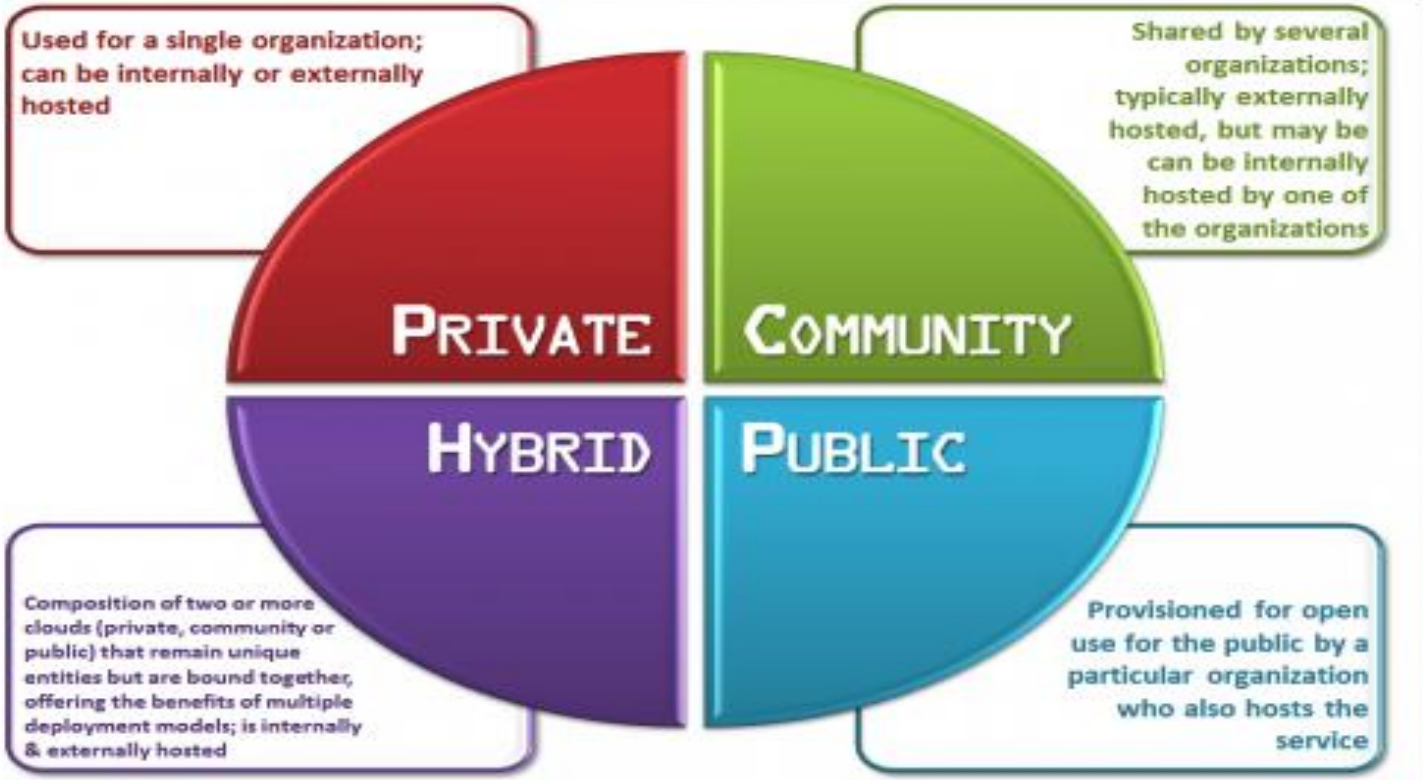
- A service delivery model that includes the following essential characteristics:
  - On-demand self-service – users can provision services on their own
  - Broad network access – service is available on any medium or device, including mobile
  - Resource pooling – multiple users and dynamic access to pooled resources
  - Rapid elasticity – resources can expand or contract as quickly as they are used or freed
  - Measured service – services are charged based on what is used

NIST Definition of Cloud Computing



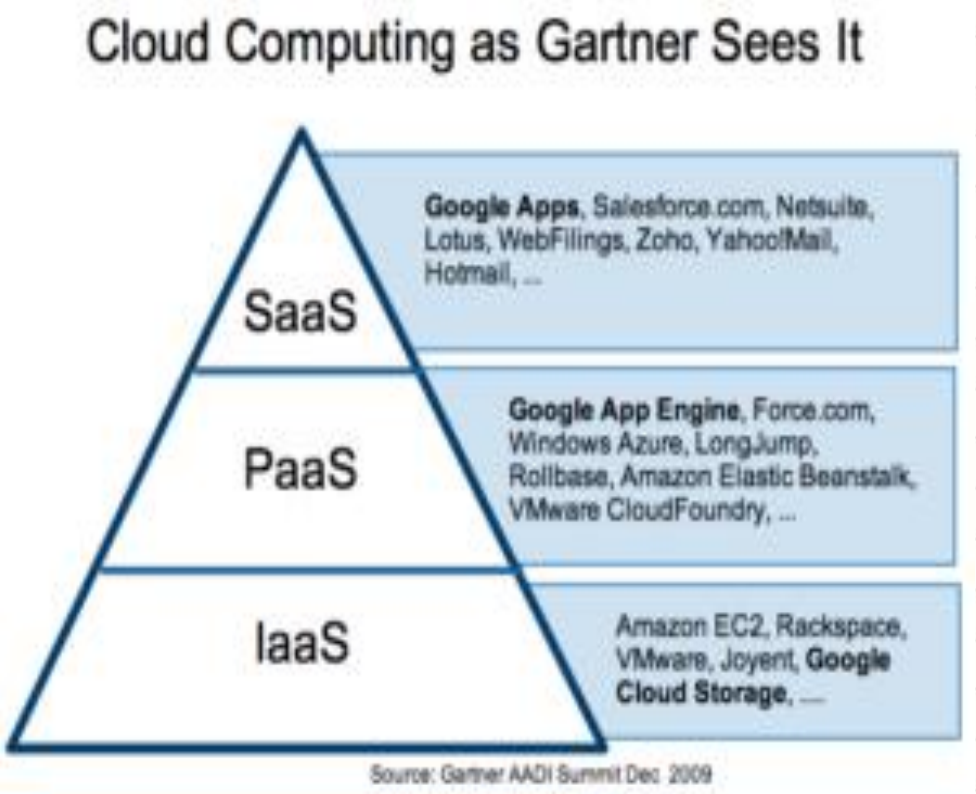
Types of Cloud

- Based on cloud location, we can classify Cloud as follows:



Gartner's View Of Cloud

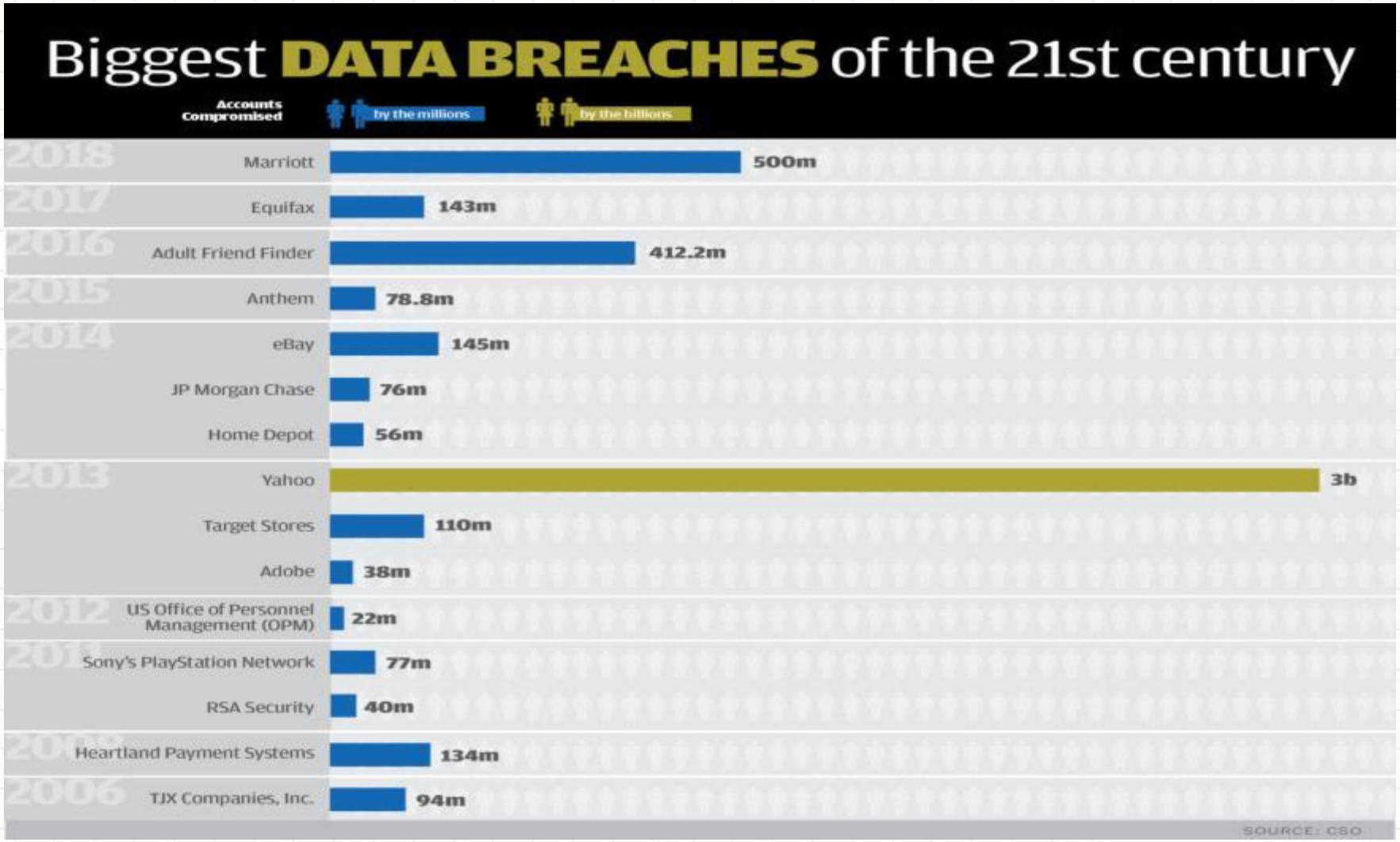
- Based on cloud location, Gartner classifies Cloud models as follows:



Aim of today's debate:

1. What key challenges do customers experience moving workloads and data into the Cloud?
2. Do customers have a responsibility for data that they store IN the cloud?
4. What is the Service Provider's responsibility for data OF the cloud?
3. How is data privacy ensured and how long can data stored and be transmitted?

Major Cloud Breaches in the 21st Century



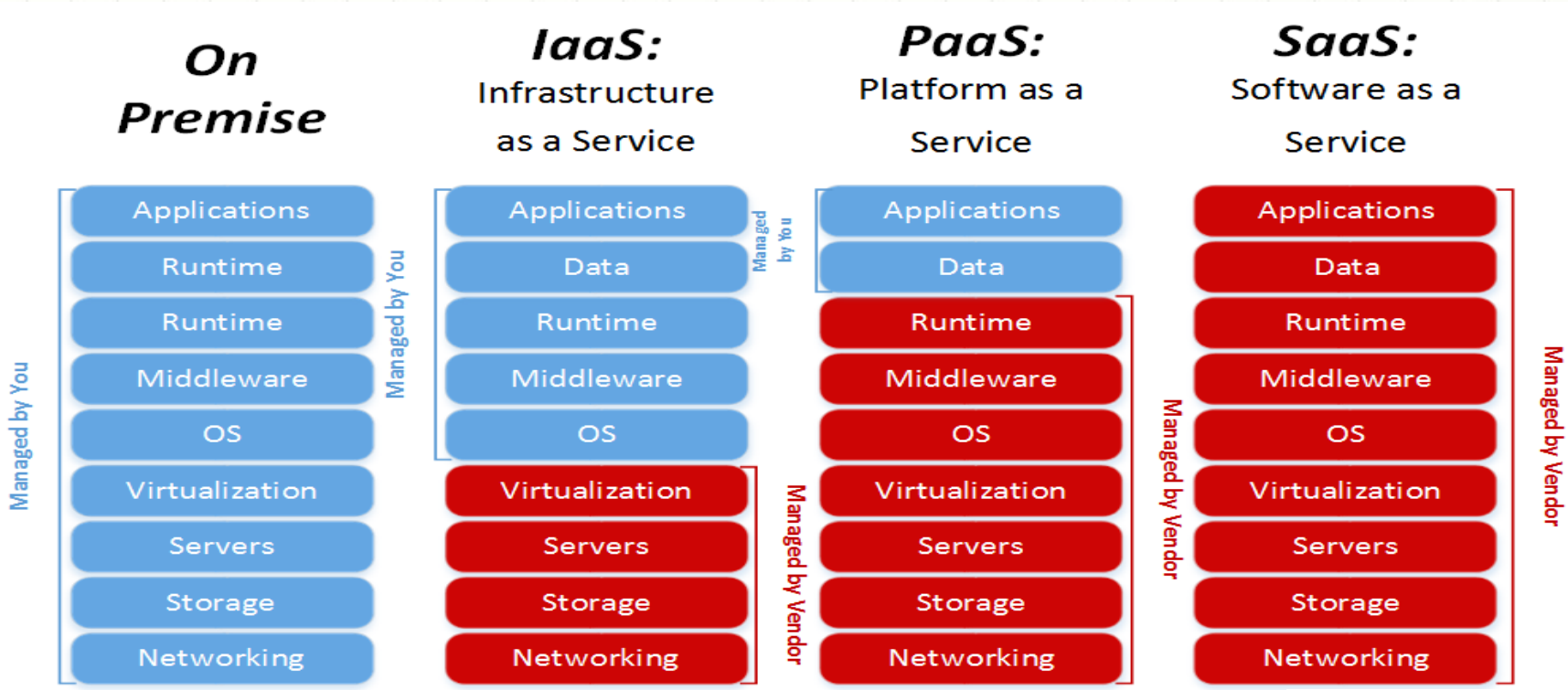
Sample Cloud Security Risks and Countermeasures

- Security risks can be assessed using a combination of selected ISO 2700x, CoBIT, ENISA, NIST and CSA Controls.

COBIT Control Objective	Controls	Cloud Risk	Sample Countermeasures
DS5.3 Identity Management	Unique ID	OWASP 2 – User Identity Federation	Individual and role-based restrictions
DS4. User account management ISO27002	Generic Accounts	ENISA R10/R28 – Malicious Insiders	Regular account access review
	Account Activity	CSA6 – Account or Service Hijacking	Logins restricted to known IP's, time of day. Monitoring. Retain logs and review them

Responsibility Within Cloud Environments

- Here is a diagram of where the responsibility typically lies with the types of cloud computing:



The Shared Responsibility Model

1. The shared responsibility model is a method for determining which roles cloud service providers and cloud service customers play in cloud security.
2. In general, the shared responsibility model outlines that providers are responsible for security of the cloud, and customers are responsible for security in the cloud. ***Cloud service providers and customers must work together to meet cloud security objectives.***
3. Think about security requirements as a spectrum. Cloud service customers add together all of the regulatory, industry, and business requirements (GDPR, PCI DSS, contracts, etc.) that apply to their organization and the sum equals all of that organization's specific security requirements.
4. These security requirements will help ensure that data is confidential, has integrity, and is available. On one end of the security requirement spectrum is cloud service providers and on the other is cloud service customers. The provider is responsible for some of these security requirements, and the customer is responsible for the rest, but some should be met by both parties. Cloud service providers and cloud service customers both have an obligation to protect data.

Shared Responsibility Model Across Service Models : CSP Perspective

When choosing which service model (IaaS, PaaS, or SaaS) your organization needs, you should consider which security responsibilities will apply to you :

- For IaaS solutions, the elements such as facilities, data centers, network interfaces, processing, and hypervisors should be managed by the cloud service provider. The cloud service customer is responsible for securing and managing the virtual network, virtual machines, operating systems, middleware, applications, interfaces, and data.
- PaaS solutions shift the cloud service provider's responsibilities and add a few elements to their duties. The customer is still responsible for securing and managing applications, interfaces, and data.
- For SaaS solutions, the responsibilities shift again. Now, the cloud service customer is responsible for the security of interfaces and data.
- Cloud service providers and cloud customers both have a responsibility to protect data. It's also important to note that execution of individual security management tasks can be outsourced, but accountability cannot. The responsibility to verify that security requirements are being met always lies with the customer.

Shared Responsibility Model Across Service Models : Customer Perspective

If you're a cloud customer, consider these best practices:

- Define your cloud security requirements before selecting a cloud service provider. If you know what you're looking for in a cloud service provider, you can better prioritize your needs.
- Harmonize your corporate governance program between traditional and cloud-based IT delivery. Migrating systems and applications into the cloud is going to require a difference in policy.
- Establish contractual clarity on the roles and responsibilities of each party, especially when you get into the public cloud. Who's responsible for cloud security? How far does the cloud service provider go?
- Develop a responsibility matrix that defines the security roles and responsibilities for you and for each vendor, including cloud service providers.

Best Practices for Managing the Shared Responsibility Model

If you're a cloud service provider, these best practices will help you better manage the shared responsibility model:

- Consider risks from your customers' perspectives, then implement controls that will demonstrate you're doing everything you can to mitigate those risks.
- Document the internal controls you use to manage risks.
- Provide ample documentation on how your customers can use the security features that you provide in your solution. AWS/Azure/Google do a great job of this through their educational programs.
- Create a responsibility matrix that defines how your solution will help your customers meet their various compliance requirements.
- Turn to the CSA's CAIQ and CCM as starting points for establishing the shared responsibility model.

Addendum: Key Cloud Oversight Principles

Key Cloud Oversight Principles

1. Executives must have oversight over the cloud—The business needs to recognise the value of the cloud-based technology and data. There must be constant vigilance and continuous monitoring of risk to these information assets, including ensuring compliance with appropriate laws, regulations, policies and frameworks.
2. Management must own the risks in the cloud—The management of the relevant business unit must own the risk associated with its use of cloud services, and must establish, direct, monitor and evaluate commensurate risk management on an on-going basis.
3. All necessary staff must have knowledge of the cloud—All users of the cloud should have knowledge of the cloud and its risk (commensurate with their role in the organisation), understand their responsibilities and be accountable for their use of the cloud.

Key Cloud Oversight Principles

4. Management must know who is using the cloud—Appropriate security controls must be in place for all uses of the cloud, including human resources practices (e.g., recruitment, transfers, terminations).
5. Management must authorise what is put in the cloud—All cloud-based technology and data must be formally classified for confidentiality, integrity and availability (CIA) and must be assessed for risk in business terms, and best practice business and technical controls must be incorporated and tested to mitigate the risk throughout the asset life cycle.
6. Mature IT processes must be followed in the cloud— All cloud-based systems development and technical infrastructure processes must align with policy, meet agreed business requirements, be well documented and communicated to all stakeholders, and be appropriately resourced.

Key Cloud Oversight Principles

7. Management must buy or build management and security in the cloud—Information risk and security, as well as its monitoring and management, must be a consideration in all cloud investment decisions.
8. Management must ensure cloud use is compliant—All providers and users of the cloud must comply with regulatory, legal, contractual and policy obligations; uphold the values of integrity and client commitment; and ensure that all use is appropriate and authorised.
9. Management must monitor risk in the cloud—All cloud-based technology developed or acquired must enable transparent and timely reporting of information risk and be supported by well-documented and communicated monitoring and escalation processes.
10. Best practices must be followed in the cloud

Roles and Responsibilities

	Business Unit Owner	Business Delegate (Operational Risk Manager)	Risk and Security Consulting and IT Risk Manager	Provider
Objective setting	Determine risk appetite for business.	Accept risk on behalf of owner or escalate.	Evaluate risks on behalf of business.	Deliver IT services including security.
Event identification	Approve incident management process.	Monitor and escalate incidents within business.	Evaluate threats and manage incidents.	Identify and manage threats and incidents.
Risk assessment	Approve risk and control profile.	Compile and monitor risk and control profile.	Classify and assess asset risk and controls.	Identify and assess risk and controls.
Risk response	Oversee significant remediation work.	Oversee remediation work.	Evaluate and report on remediation.	Execute remediation activities.
Control activities	Approve controls within the business and provider.	Operate business controls.	Define and evaluate controls.	Design, integrate and operate controls.
Compliance	Provide legal oversight of control assessment and testing.	Oversee control assessment and testing.	Conduct independent reviews and testing.	Maintain evidence of control effectiveness.
Reporting		Report on status of compliance, threats and controls.	Report on status of compliance, threats and controls.	Report on status of compliance, threats and controls.

Some Cloud Security Sources

More Links to Great Resources

1. AWS Shared Responsibility Model:
https://aws.amazon.com/compliance/shared-responsibility-model/
2. Azure Shared Responsibility Model:
https://gallery.technet.microsoft.com/Shared-Responsibilities-81d0ff91
3. Google Cloud Shared Responsibility Model:
https://cloud.google.com/files/PCI_DSS_Shared_Responsibility_GCP_v32.pdf
4. OWASP Cloud Security Project:
https://www.owasp.org/index.php/OWASP_Cloud_Security_Project
5. Cloud Security Alliance:
https://cloudsecurityalliance.org/working-groups/cloud-controls-matrix/#_overview
6. NIST Cloud Computing Reference Architecture:
7. https://bigdatawg.nist.gov/_uploadfiles/M0007_v1_3376532289.pdf
8. ENISA:
9. https://www.enisa.europa.eu/
10. ISO Standards: 27017 - https://www.iso.org/standard/43757.html
27001 - https://www.iso.org/isoiec-27001-information-security.html

ALLIANCE Media Group

QUESTIONS?