MANAGING SECURITY IN THE CLOUD

Tolu Onireti, CISSP, CCSP, PMP, CompTIA Sec+

Cybersecurity Consultant

21st Feb, 2019

AGENDA

- Cloud computing trends
- Reality of cloud computing
- Threats to cloud computing
- Considerations for securing the cloud

WHO IS RESPONSIBLE FOR SECURITY IN THE CLOUD?

A. Cloud Service Provider

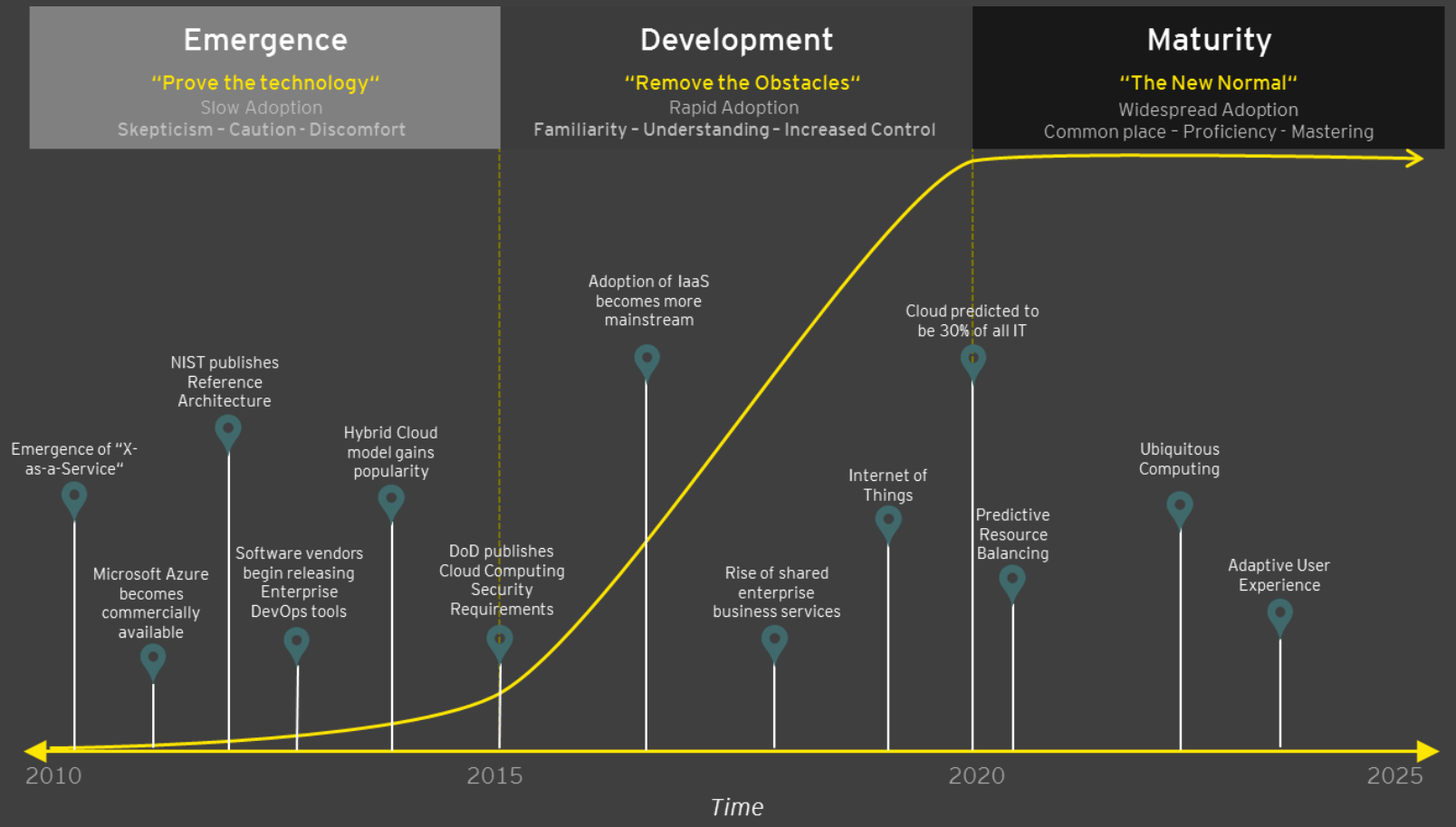
B. Cloud Service Customer

C. Both A and B

CLOUD COMPUTING TRENDS

By 2020, cloud adoption will dominate IT and become the new normal

- Emerged and gained rapid foothold in last 5 to 6 years
- Initial key challenges:
  - Uncertainty about data location
  - Uncertainty about access to the data
  - Security of cloud service providers' infrastructure
  - Regulation of cloud computing
- Increase in adoption due to publication of cloud security standards and reference architectures by NIST, ISO and the DoD (among others)

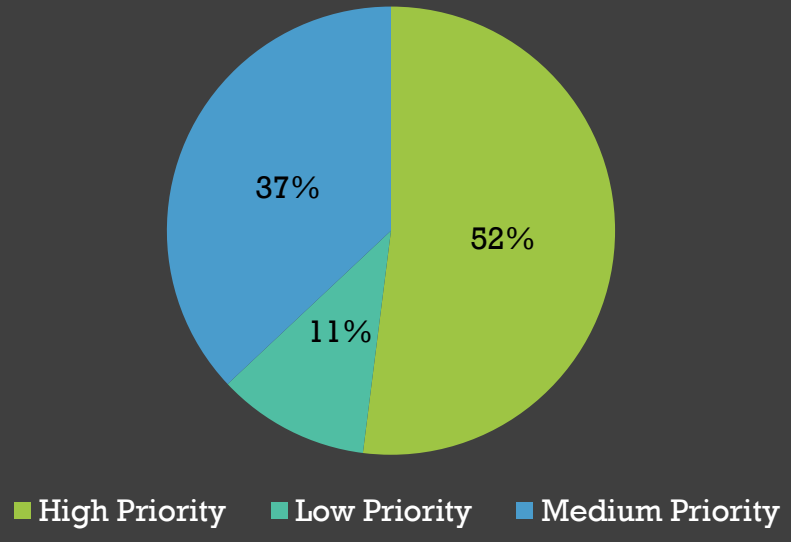


CLOUD COMPUTING TRENDS

Market research indicates that companies are increasingly adopting a "cloud first" or "hybrid" strategy to keep pace with the evolving digital ecosystem.

- 50% of companies will be adopting services, applications and platforms enabled by cloud in 2018 (Forrester)
- 6x rate of growth for cloud computing spending in comparison to traditional IT spending through 2020 (IDC Research)
- $459m forecasted cloud security spend across the world in 2019, an increase of 50% from 2018 (Gartner)
- 95% of cloud security failures through 2022 are estimated to be the customer's fault (Gartner)
- $7.3m average total cost of a data breach for a US-based company in 2018 (Ponemon Institute)
- 83% of companies store sensitive and confidential data in the public cloud in 2018 (McAfee)

Priorities for cybersecurity investment in 2018*



*Source: EY Global Information Security Survey 2018-19 https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf

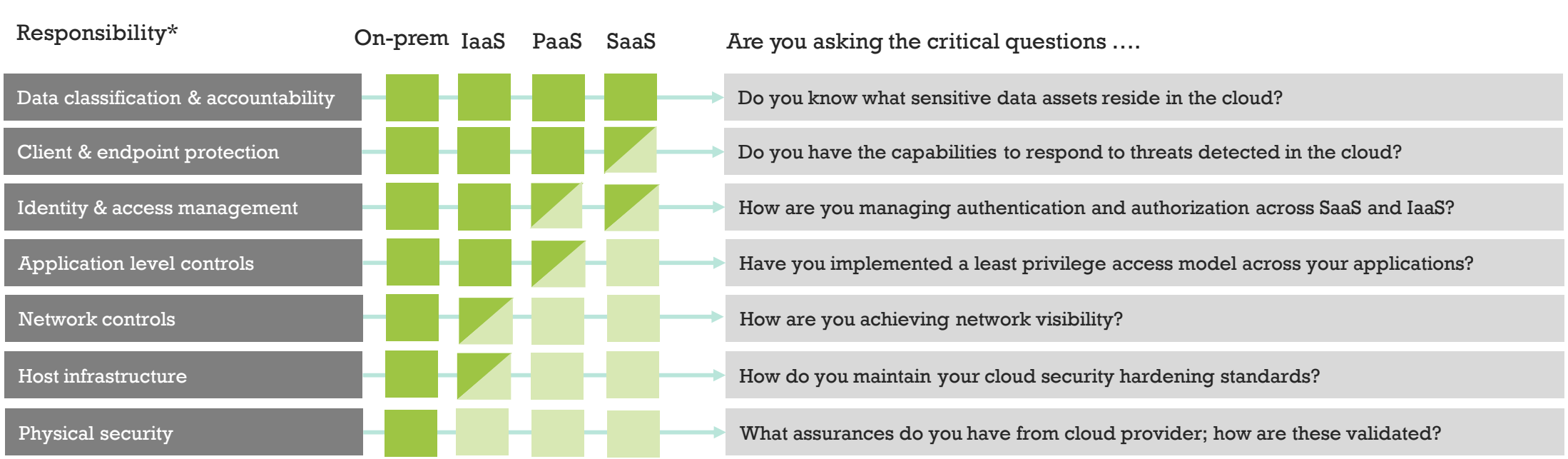
CLOUD COMPUTING TRENDS

Adoption of cloud first strategy enables companies to achieve their business objectives.
IT, HR, Sales marketing and other business functions are adopting cloud.
How is security enabling the business?

- Business drivers for cloud adoption:
  - High availability infrastructure configures with limited forecasting
  - Rapid procurement and provisioning of IT resources to improve speed to market
  - Limited resources committed for innovation and proof-of-concept life cycles
  - Reduction of long-term technical debt occurred by purchasing infrastructure
  - Minimal dependency on demand planning with scalable infrastructure
  - Focus on business core competencies by outsourcing non-proprietary IT services

REALITY OF CLOUD COMPUTING

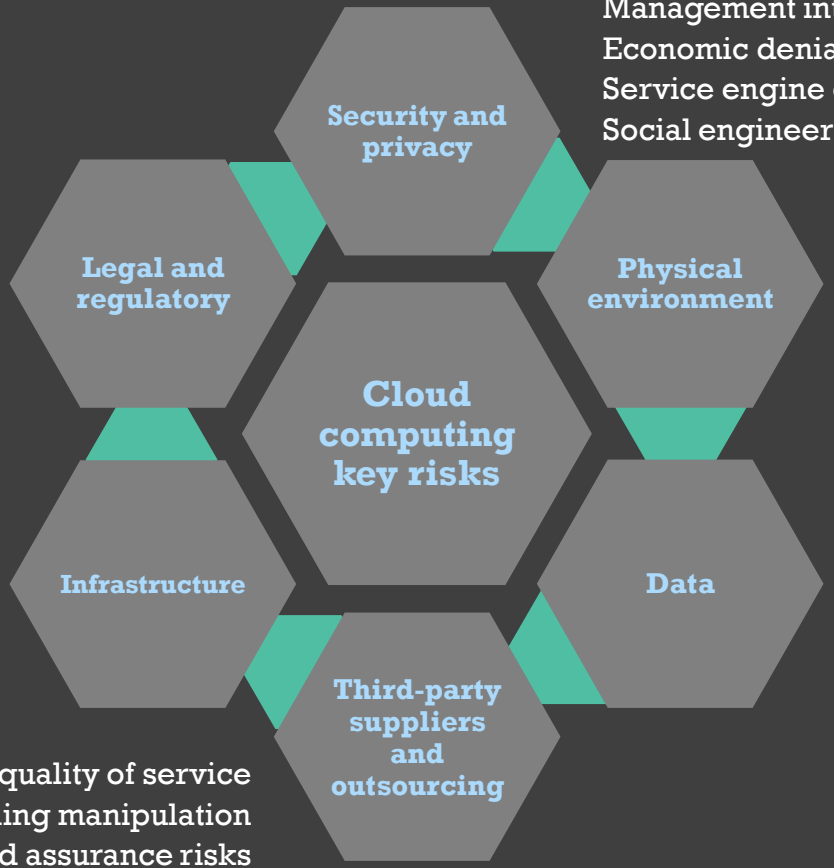
While tenant is transferring technical controls of the computing environment to the service provider, tenant retains liability and legal responsibility for data protection.



*Source: Thomas Shinder, "What does Shared Responsibility in the Cloud Mean," Microsoft, April 18, 2016. https://blogs.msdn.microsoft.com/azuresecurity/2016/04/18/what-does-shared-responsibility-in-the-cloud-mean/

REALITY OF CLOUD COMPUTING

The lack of cloud governance and adequate controls for cloud services could increase an organization's risk.



Privileged user access abuse
Management interface compromise
Economic denial of service
Service engine compromise
Social engineering attacks

Backups lost or stolen
Unauthorised access to premises
Theft of computer equipment
Natural disasters

Data leakage
Insecure or inefficient deletion of data
Distributed denial of service
Loss of encryption keys
Data recovery

Poor quality of service
Metering or billing manipulation
Liability and assurance risks
Lack of certified resources

Network management
Modifying network traffic
Cloud hopping (between tenants)

Subpoena and e-discovery
Risk from changes of jurisdiction
Data protection risks
Licensing risks
Compliance challenges

Source: ENISA – Cloud computing benefits, risk and recommendation for information security
https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security

THE TREACHEROUS 12 - TOP THREATS TO CLOUD COMPUTING

The list of the *treacherous 12 top threats to cloud computing is the result of a survey conducted by the Cloud Security Alliance (CSA) of industry experts. The list starts with the issue of greatest concern to the experts.

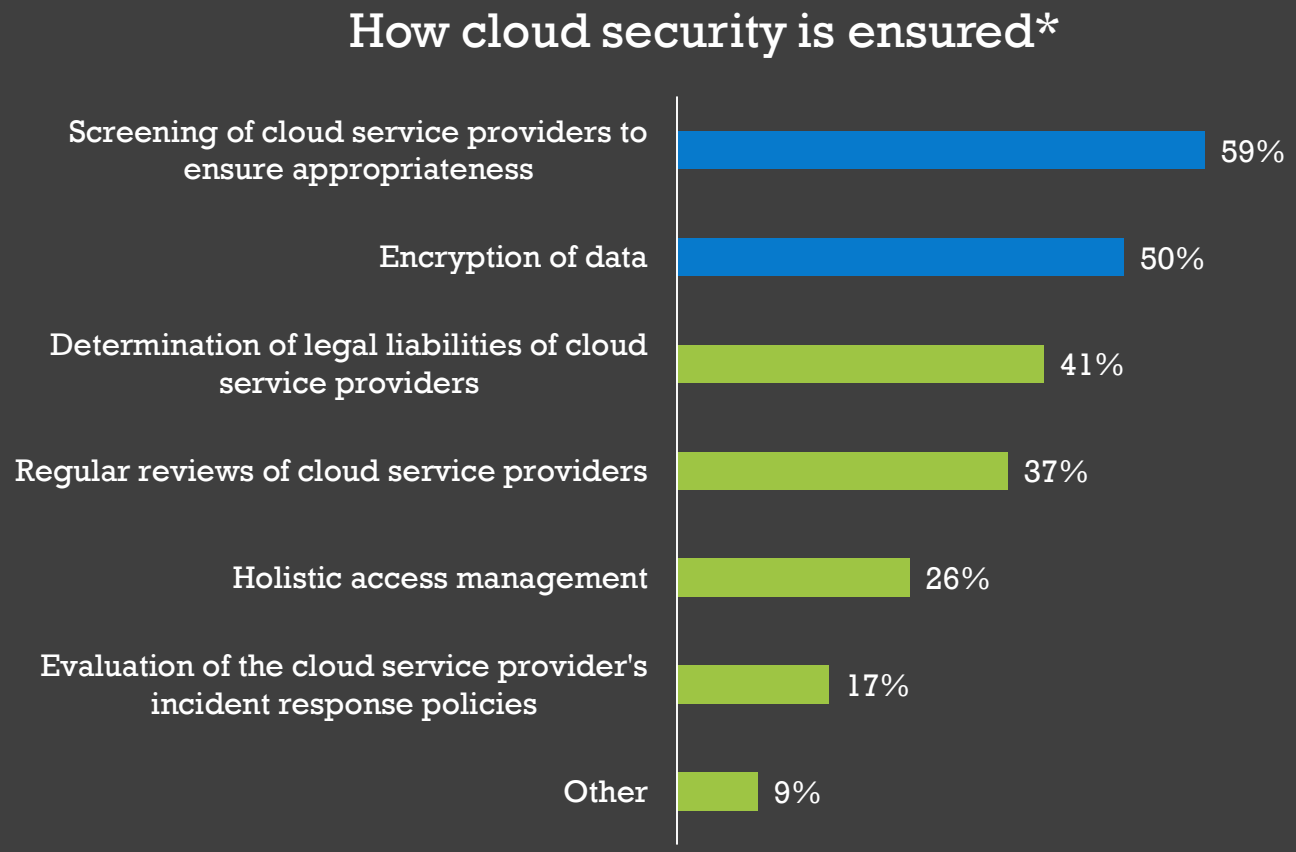
1	Data Breaches
2	Weak Identity, Credential and Access Management
3	Insecure APIs
4	System and Application Vulnerabilities
5	Account Hijacking
6	Malicious Insiders
7	Advanced Persistent Threats (APTs)
8	Data Loss
9	Insufficient Due Diligence
10	Abuse and Nefarious Use of Cloud Services
11	Denial of Service
12	Shared Technology Vulnerabilities

Cloud computing services are popular targets because they can be used as a door way into a customer's network.

*Source: CLOUD SECURITY ALLIANCE The Treacherous 12 - Top Threats to Cloud Computing + Industry Insig

WHAT ARE ORGANIZATIONS DOING ON CLOUD SECURITY?

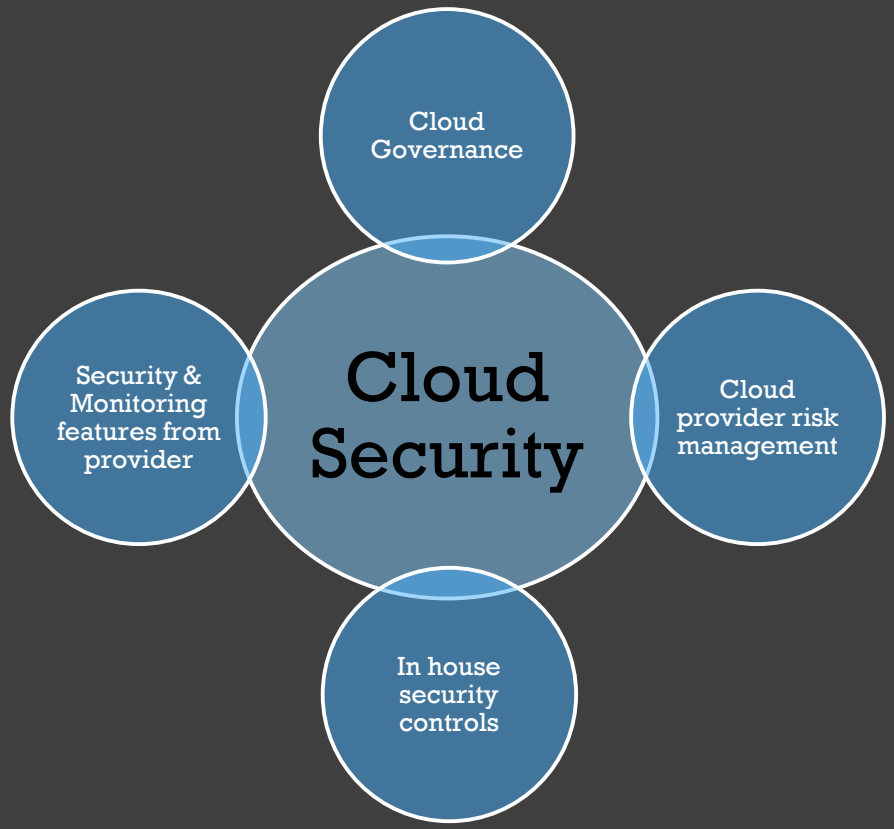
Organizations are conducting cloud provider (vendor) risk assessments, encrypting critical data and implementing a holistic access management program.



Source: Capgemini Consulting – Information Security Benchmarking 2017
https://www.capgemini.com/consulting-de/wp-content/uploads/sites/32/2017/11/information-security-benchmark-2017.pdf

CONSIDERATIONS FOR SECURING CLOUD COMPUTING

Cloud governance provides standardized policies to guide the people, process and technology associated with cloud infrastructure, security and operations.*



Published guidance

- Cloud Security Alliance (CSA)
  - Trusted Cloud Initiative reference architecture (TCI-RA v1.1, 2011)
  - Cloud Controls Matric (CCM v3.0.1, 2017)
- National Institute of Standards and Technology (NIST)
  - NIST Cloud Computing Security Reference Architecture (NIST SP 500-299, 2013)
- International Organization for Standardization (ISO)
  - Code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC 27017:2015 / ITU-T X.1631)
  - Information technology – Cloud Computing – Reference architecture (ISO/IEC 17789, 2014)

*Source: Adapt Your Governance Framework For Cloud, Forrester Research, Inc., November 14, 2017

CONSIDERATIONS FOR CLOUD COMPUTING AUDIT

Operating in the cloud increases the risk exposure of an organization.
Identifying the exploitable vulnerabilities and remediating them using controls could reduce the risk.

- Act as a catalyst to enable inclusion of risk associated with operating in the cloud as part of Enterprise risk
- Conduct internal audits of the various components of the organisation's cloud activities and implementation
- Communicate the hidden costs of rushing to the Cloud and unchecked procurement of cloud Services
- Assessment of the control environment to management and audit committee

WHO IS RESPONSIBLE FOR SECURITY IN THE CLOUD?

A. Cloud Service Provider

B. Cloud Service Customer

C. Both A and B

WHO IS RESPONSIBLE FOR SECURITY IN THE CLOUD?

A. Cloud Service Provider

B. Cloud Service Customer

C. Both A and B

IN CONCLUSION

- Cloud is the way to go to achieve some business objectives and vision
- Collaboration of all the key players within an organizations enables development of a realistic cloud governance
- Trust and assurance of cloud service provider

- Leverage security and monitoring features provided by cloud service provider
- Extend in house security controls to the cloud for critical or sensitive assets