THE POWER OF BEING UNDERSTOOD

RSM

MOVING YOUR ORGANIZATION DATA TO THE CLOUD

May 14, 2020

RSM

Speaking With You Today

Ron Ritenour, Manager

Security, Privacy & Risk

ron.ritenour@rsmus.com

Ron has extensive experience in developing risk-based strategies, programs, policies, and standards that align with business goals to support the expansion and transformation of business requirements. Frameworks include OCR HIPAA, NIST SP 800-x, NIST CSF, CIS CSC, ISO, OWASP, PCI-DSS, SOC 1/SOC 2, and COBIT, focusing on information/IT security, people, process and technology. Ron has experience serving as a CISO and HIPAA security officer, managing an information security department and serving as the chair of an information security council.

Nick Biggers, Associate

Security, Privacy & Risk

nick.biggers@rsmus.com

Nick has experience assisting organizations across a variety of industries to identify and secure sensitive systems, data and business areas. With experience in frameworks such as NIST CSF, FFIEC CAT, CIS CSC, PCI-DSS and OCR HIPAA, Nick focuses on providing organizations solutions to their needs based on industry best practices, emerging technologies and effective risk management strategies.

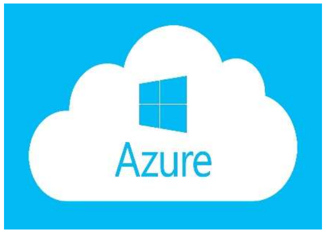
Agenda

- Intro To Cloud Computing
- Moving Your Data To The Cloud
- Cloud Risk Management
- Auditing Cloud Environments
- Questions & Answers

INTRODUCTION TO CLOUD COMPUTING

Popular Cloud Services

Cisco
webex



salesforce

The Cloud

Cloud Computing - the idea of storing and accessing data on the Internet

3 Common Cloud Services		
Software as a Service (SaaS)	**Platform as a Service (PaaS)**	**Infrastructure as a Service (IaaS)**
• Email • Calendar • Office Tools Designed to allow access to enterprise resources such as Office 365.	• Infrastructure • Software • Development Tools Designed to support a complete web application lifecycle.	• Infrastructure • Quickly scaleable • Pay for what you need Designed to provide infrastructure for the client to manage their software.

Responsibility Grid

	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
Security, Governance, Risk, and Compliance (GRC)	▨	▨	▨
Data Security	▨	▨	▨
Application Security	▨	▨	🟩
Platform Security	▨	🟩	🟦
Infrastructure Security	🟩	🟦	🟦
Physical Security	🟦	🟦	🟦

▨ Client Responsibility

🟩 Shared Responsibility

🟦 CSP Responsibility

Deployment Models

PRIVATE CLOUD

- Conforms to various regulatory standards (e.g. SOX, HIPAA, or GLBA) regarding data privacy and governance
- Buying, Building, managing organization's infrastructure

PUBLIC CLOUD

- Cloud hosting with free services
- Or pay-per-user license model
- Reduces capital expenditure and IT operational cost
- Ex: Amazon Elastic Compute Cloud(EC2), IBM Cloud, Google Public Cloud

HYBRID CLOUD

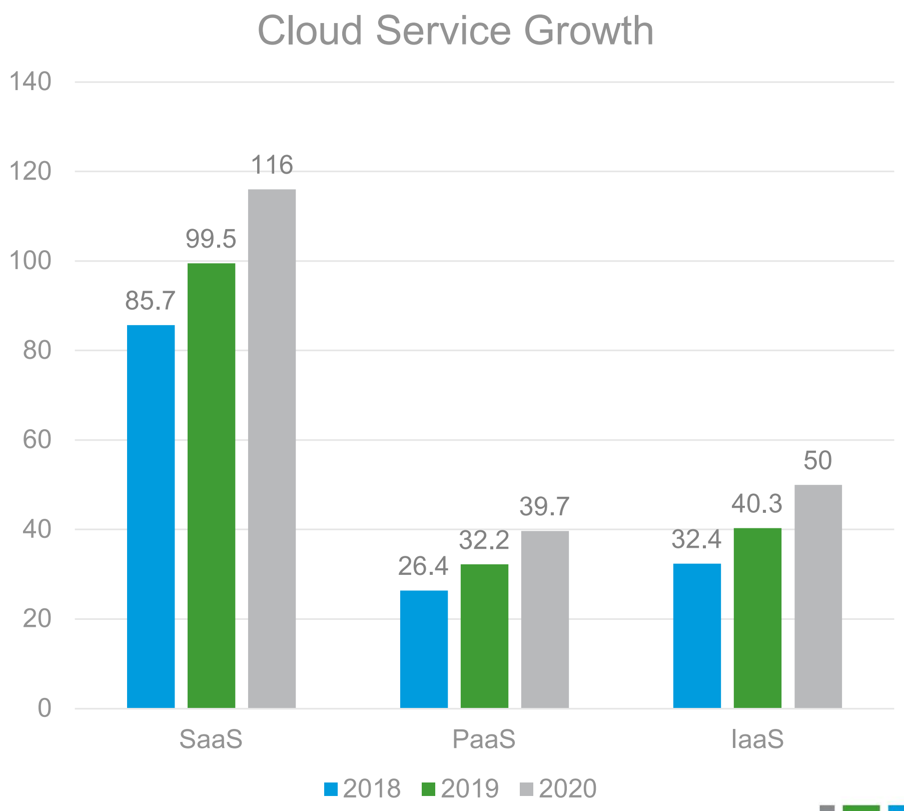
- Combination of Private and Public
- Migrates workload between public and private without disturbing users
- Saves on cost and adds security
- Ex: Salesforce.com and Microsoft Azure

COMMUNITY CLOUD

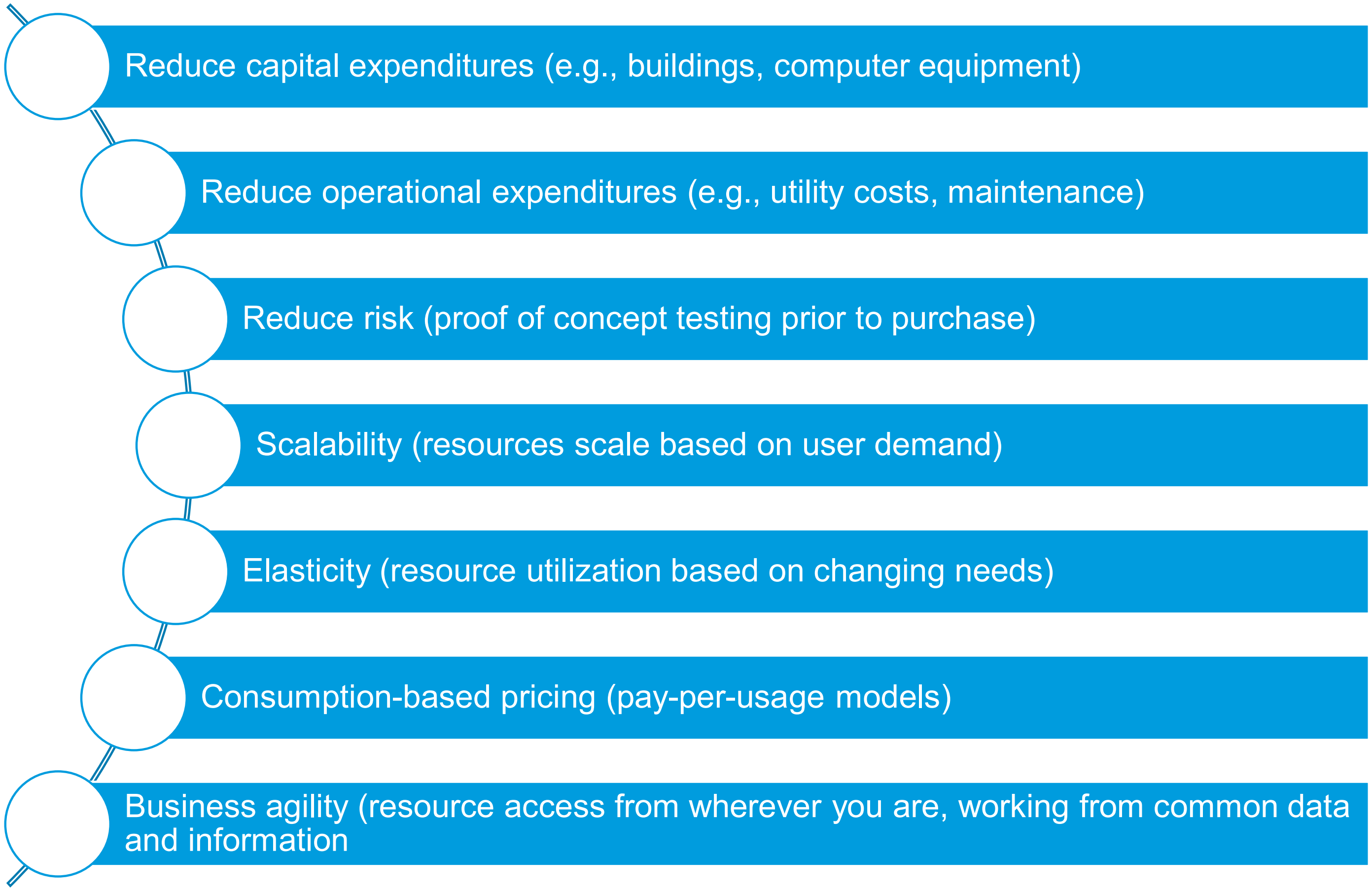
- Shared infrastructure model
- Same policy and compliance considerations
- Reduces cost
- Ex: GovCloud on AWS, FedRamp, NYSE, Euronext's Community Platform for Capital Markets.

Cloud Service Growth Trends

- Cloud services expected to grow 17% in 2020
- Up to 60% of organizations will utilize cloud services by 2022



Drivers for Cloud Computing Migration



- Reduce capital expenditures (e.g., buildings, computer equipment)
- Reduce operational expenditures (e.g., utility costs, maintenance)
- Reduce risk (proof of concept testing prior to purchase)
- Scalability (resources scale based on user demand)
- Elasticity (resource utilization based on changing needs)
- Consumption-based pricing (pay-per-usage models)
- Business agility (resource access from wherever you are, working from common data and information

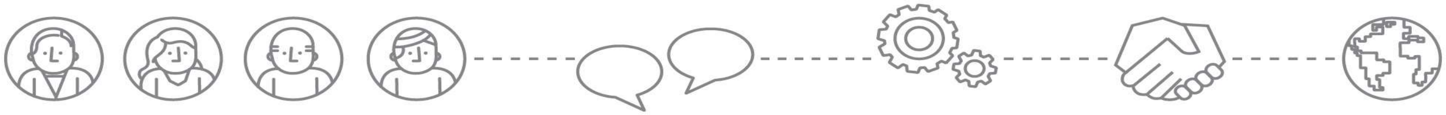
On-Premise Considerations

Pros

- Tailorable and adaptable
- Compatible
- Can be cheaper in the long run
- Full control of organization data

Cons

- Upfront Hardware Costs
  - Hard drive
  - RAM
  - CPU
  - Peripherals
- Location
- Maintenance
- Support



Cloud Considerations

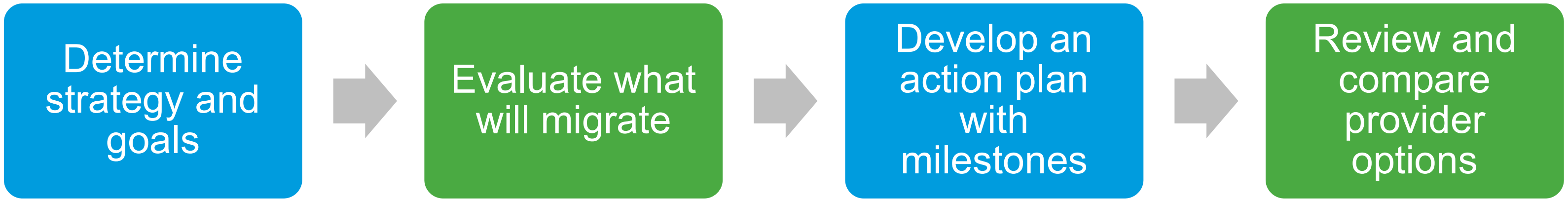
Pros

- Predictable set pricing
- Data security standards
- Rapidly scalable
- Resilient
- Rapid deployment

Cons

- Costs can add up over time
- 3rd party access to data
- Management is up to the provider
- Steep learning curve for cloud technology

Migration Checklist



Determine strategy and goals

Evaluate what will migrate

Develop an action plan with milestones

Review and compare provider options

Collaboration across these steps will ensure a successful migration!

EFFECTIVE RISK MANAGEMENT IN A CLOUD ENVIRONMENT

RSM

Risk Management Considerations

Common legal requirements (U.S. Federal laws, U.S. State laws, standards)

International and regional regulations

Contractual obligations – SLAs, HIPAA, GDPR, GLBA

Restrictions of cross-boarder transfers

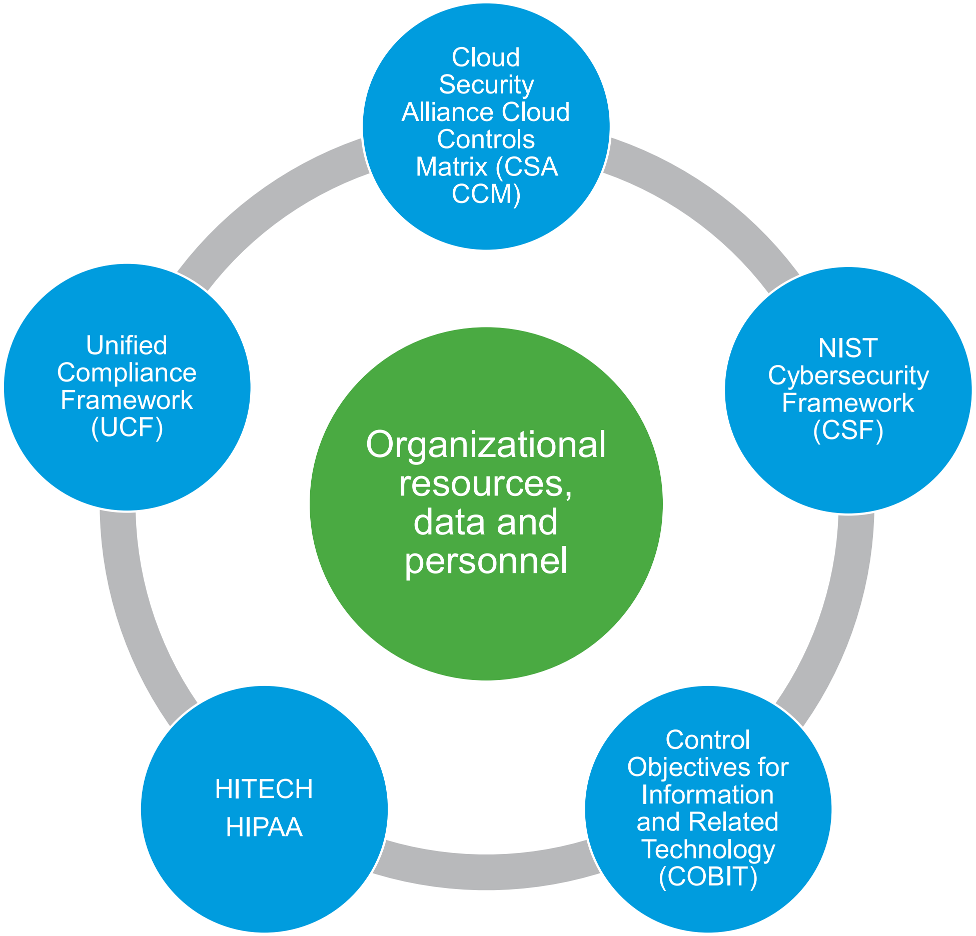
Contractual and regulated PII

Risk profile and risk appetite versus business requirements

Understanding risk exposure

Vendor management

Frameworks for Securing Your Cloud Environments


Cloud Security Alliance Cloud Controls Matrix (CSA CCM)
NIST Cybersecurity Framework (CSF)
Control Objectives for Information and Related Technology (COBIT)
HITECH
HIPAA
Unified Compliance Framework (UCF)
Organizational resources, data and personnel

Responsibility Grid

	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
Security, Governance, Risk, and Compliance (GRC)	◼	◼	◼
Data Security	◼	◼	◼
Application Security	◼	◼	🟩
Platform Security	◼	🟩	🟦
Infrastructure Security	🟩	🟦	🟦
Physical Security	🟦	🟦	🟦

◼ Client Responsibility

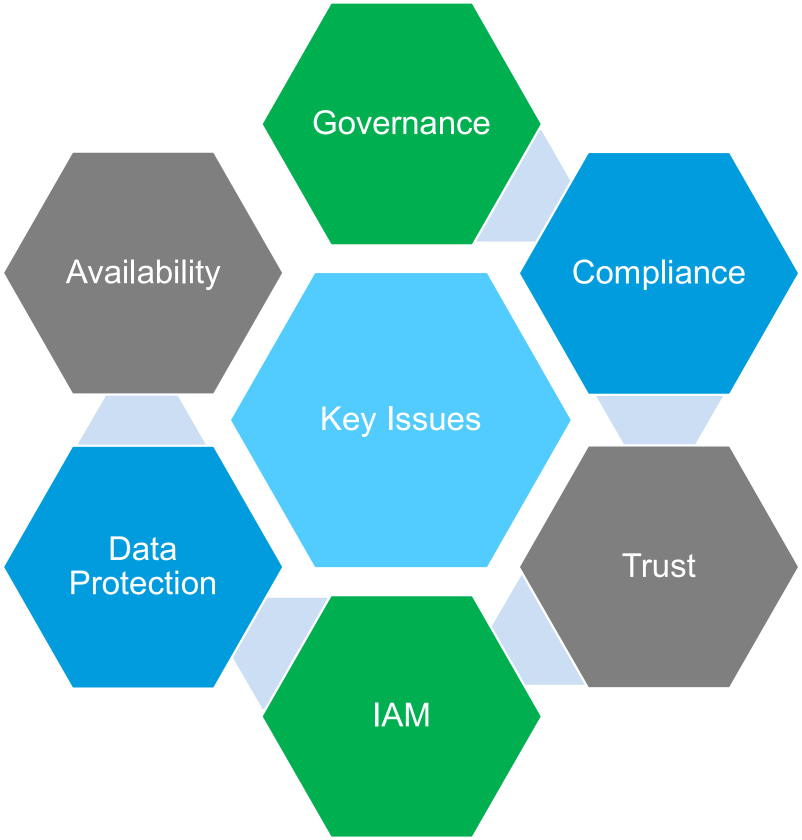
🟩 Shared Responsibility

🟦 CSP Responsibility

Security and Privacy Risk Issues

Data Protection
Value Concentration
Data Isolation
Data Sanitization

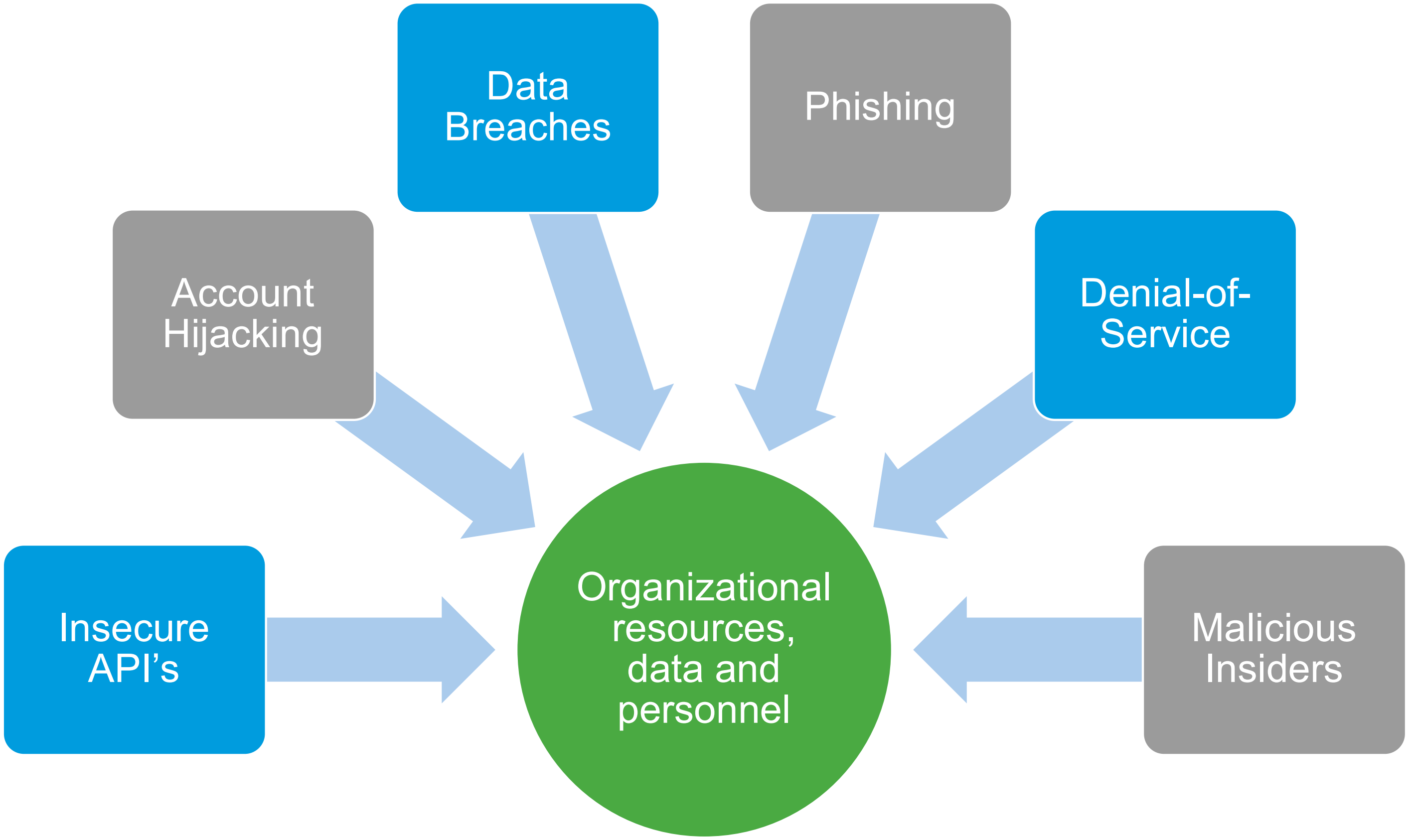
Access
Authentication
Access Control



Compliance
Laws & Regulations
Data Location

Trust
Insider Access
Data Ownership
Composite Services
Visibility
Ancillary Data
Risk Management

Top Risks, Threats and Vulnerabilities



Data Breaches

Phishing

Account Hijacking

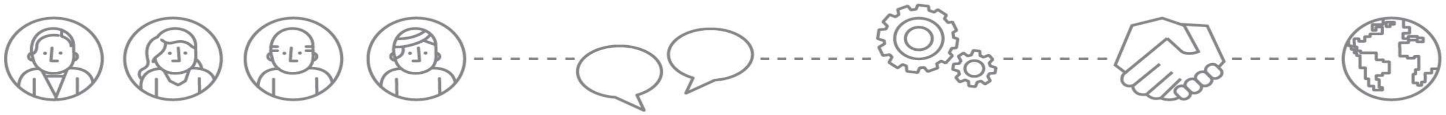
Denial-of-Service

Insecure API's

Organizational resources, data and personnel

Malicious Insiders

Effective Countermeasures



Data Breaches	Data Loss	Account Hijacking	Insecure API’s	Denial-of-Service	Malicious Insiders
Encryption	Redundancy	MFA	Patch Management	IDS/IPS	Logging & Monitoring
BYOD	Asset Lifecycles	IAM Program	Penetration Testing	Netflow Monitoring	Encryption
Strong Passwords	Stress Testing	Logging & Monitoring	Security Standards	Access Control Lists	Access Management
MFA			Vendor Management		

Auditing Cloud Environments

Challenges of the cloud and virtualization

- Understanding the virtualization management architecture
- Verify systems are up to date and hardened according to security industry-practices
- Verify configuration of hypervisor according to organizational policy

Cloud auditing goals

- Understand, measure, and communicate the effectiveness of CSP controls and security to organizational stakeholders and executives
- Identify and control weaknesses or deficiencies, while maintaining communication
- Obtain levels of assurance and verification as to the CSP’s ability to meet SLA and contractual obligations

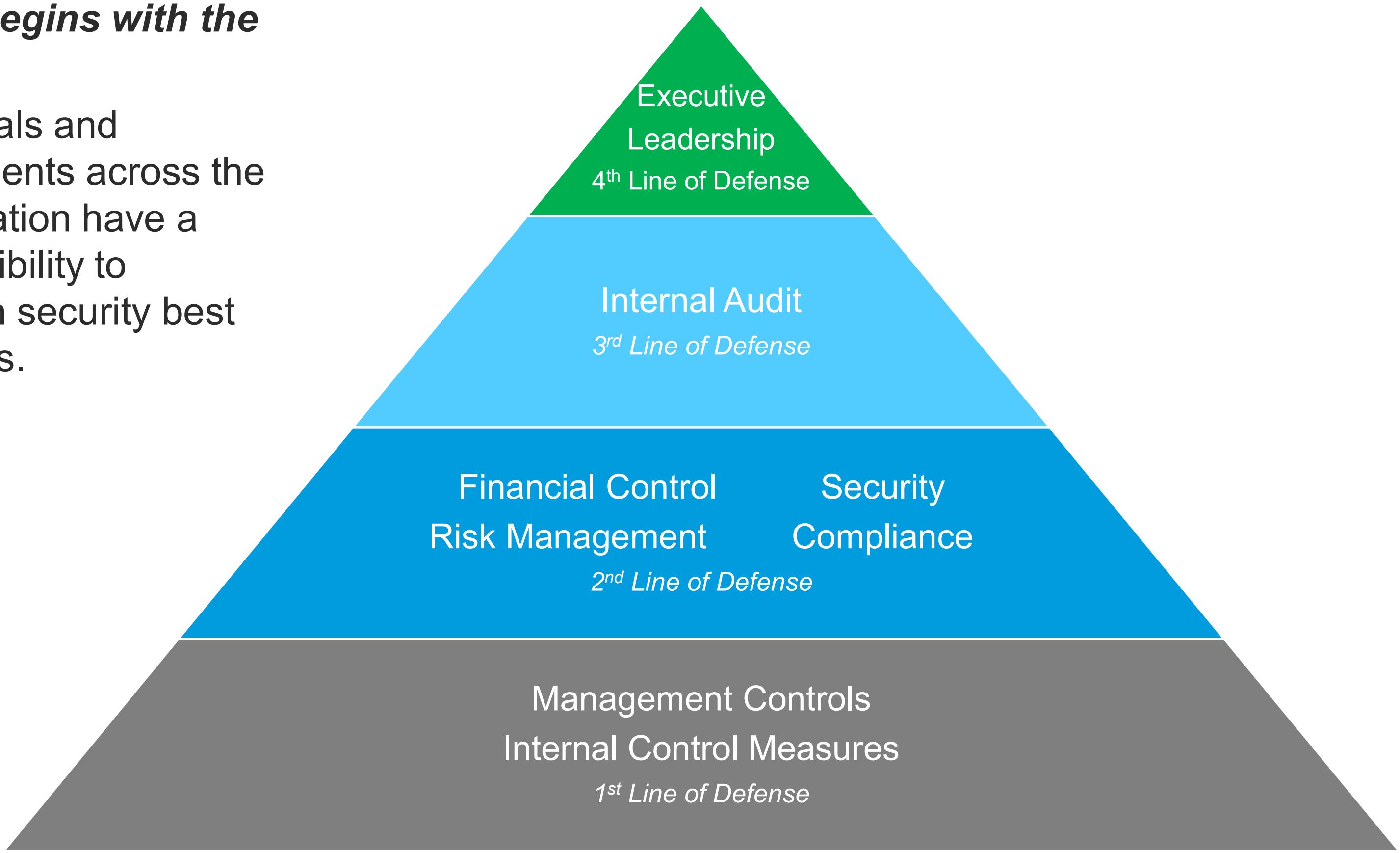
Audit and Compliance Checklist

Area	Details
Governance	Organizational strategy, vendor management, roles and responsibilities
Data Management	Data labelling and protections, privacy requirements, data transfer
Cyber Threat	Patch and vulnerability management, security monitoring, secure development
Infrastructure	Asset monitoring, system security, change management
Logging and Auditing	Log collection, storage and retention, forensics and event investigation
Availability	SLAs, resiliency requirements, backup management and testing, response plans
Identity and Access Management	Access control, multifactor authentication, privileged access
Encryption	Encryption at rest and in transit, encryption key management, backup encryption
Privacy	Credential management and protections, data use and retention
Regulations	Compliance requirements, SOC reporting, documentation

Security Throughout the Organization

Security begins with the individual

- Individuals and departments across the organization have a responsibility to maintain security best practices.



QUESTIONS AND ANSWERS