Cloud Audit and Assurance

An Introduction and awareness for auditor

PRESENTED BY:

Agustinus Nicholas L Tobing

CIA CRMA CFE CAMS CCRP QRGP BCCP AWS-CCP

Key Topics

- ❑ **What is Cloud?**
- ❑ **Cloud Fundamentals: Essential Characteristics, Service Models, and Deployment Models**
- ❑ **Cloud Benefits: Business Drivers**
- ❑ **Cloud Architecture Reference: CSA & TCI**
- ❑ **Cloud Control Matrix**
- ❑ **Sample of Cloud Audit**
- ❑ **Conclusions: Risks, Challenges, and Benefits**
- ❑ **Appendix**

"A pool of highly scalable, abstracted infrastructure, capable of hosting end-customer applications, that is billed by consumption."

- Forrester

"A style of computing where massively scalable IT-related capabilities are provided 'as a service' across the Internet to multiple external customers."

- Gartner

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

http://csrc.nist.gov/groups/SNS/cloud-computing/

What is Cloud?

5 Essential Characteristics

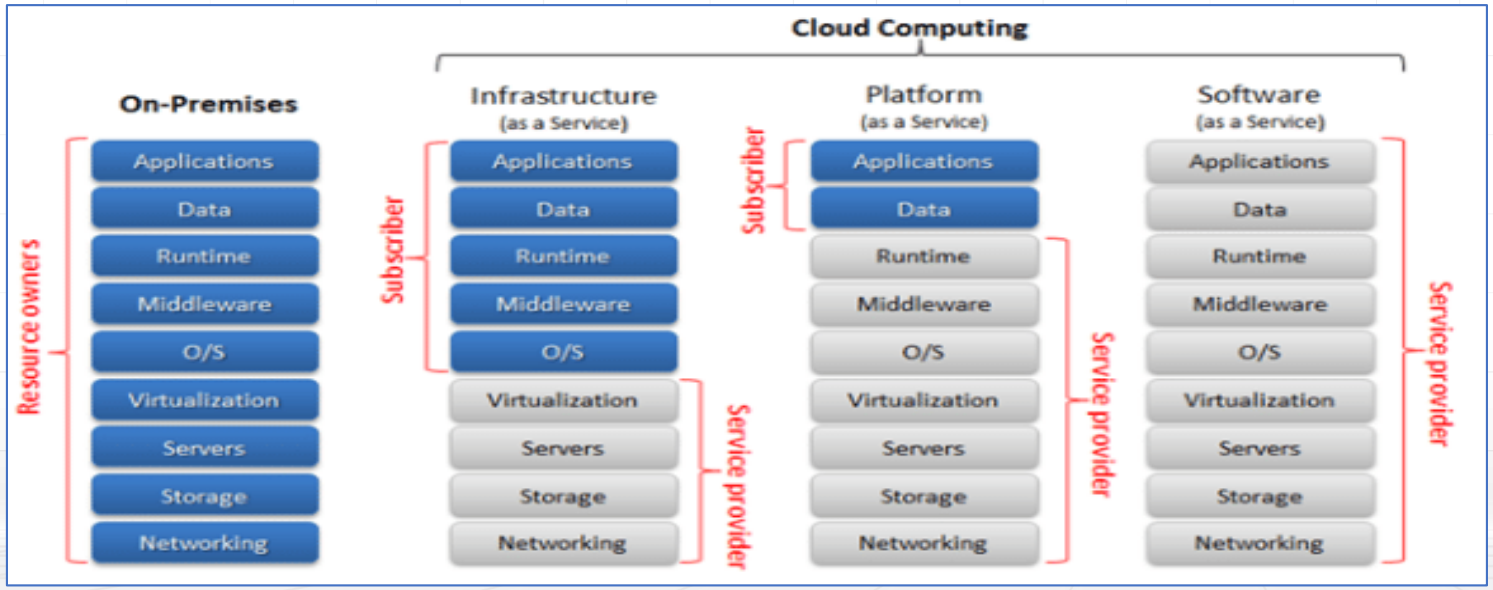
- On-demand self-service
- Resource pooling
- Rapid elasticity
- Measured service
- Broad network access

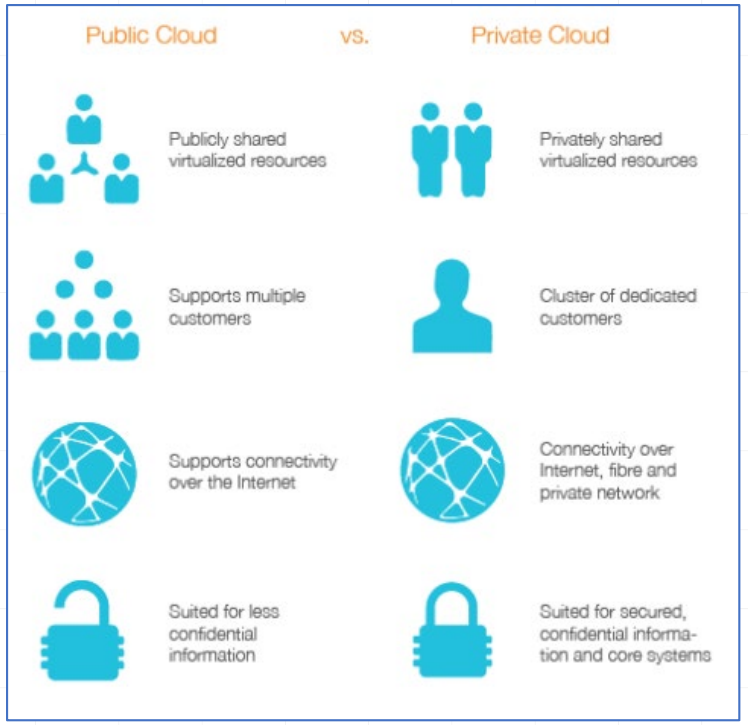
3 Service Delivery Models

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

4 Deployment Models

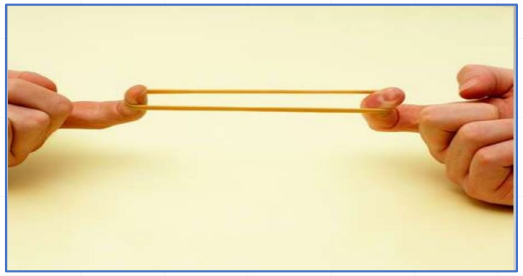
- Public Cloud
- Private Cloud
- Community Cloud
- Hybrid Cloud



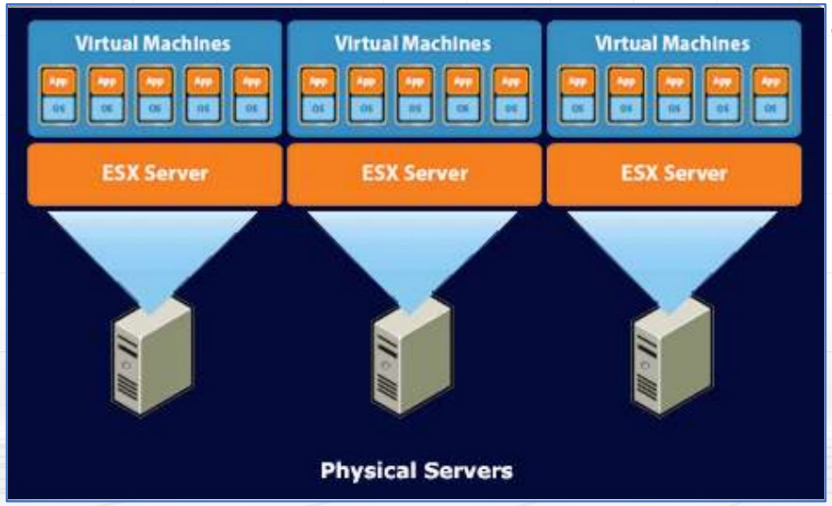


Cloud Fundamentals

Essential Characteristics



Broad Network Access	Rapid Elasticity	Measured Service	On-Demand Self-Service
Resource Pooling			



Cloud Benefits – Business Drivers

Cost Effective

- Using a cloud provider can significantly reduce the costs of buying and running a physical IT infrastructure.
- Pay-as-you-go cloud services are available, meaning you get the computing resources you need, exactly when you need them.

Scalability

- It is easy to upscale or downscale your cloud to fit your needs
- Cloud solutions are tailored to your specific situation and are scalable to any changes you may need to make.

Disaster Recovery

- Losing data would be detrimental to any business.
- Housing your data in-house poses the highest threat of a complete loss in the event of a disaster.
- Accidents such as power outages or a malfunction in your air conditioning can cause your servers to overheat and fail.

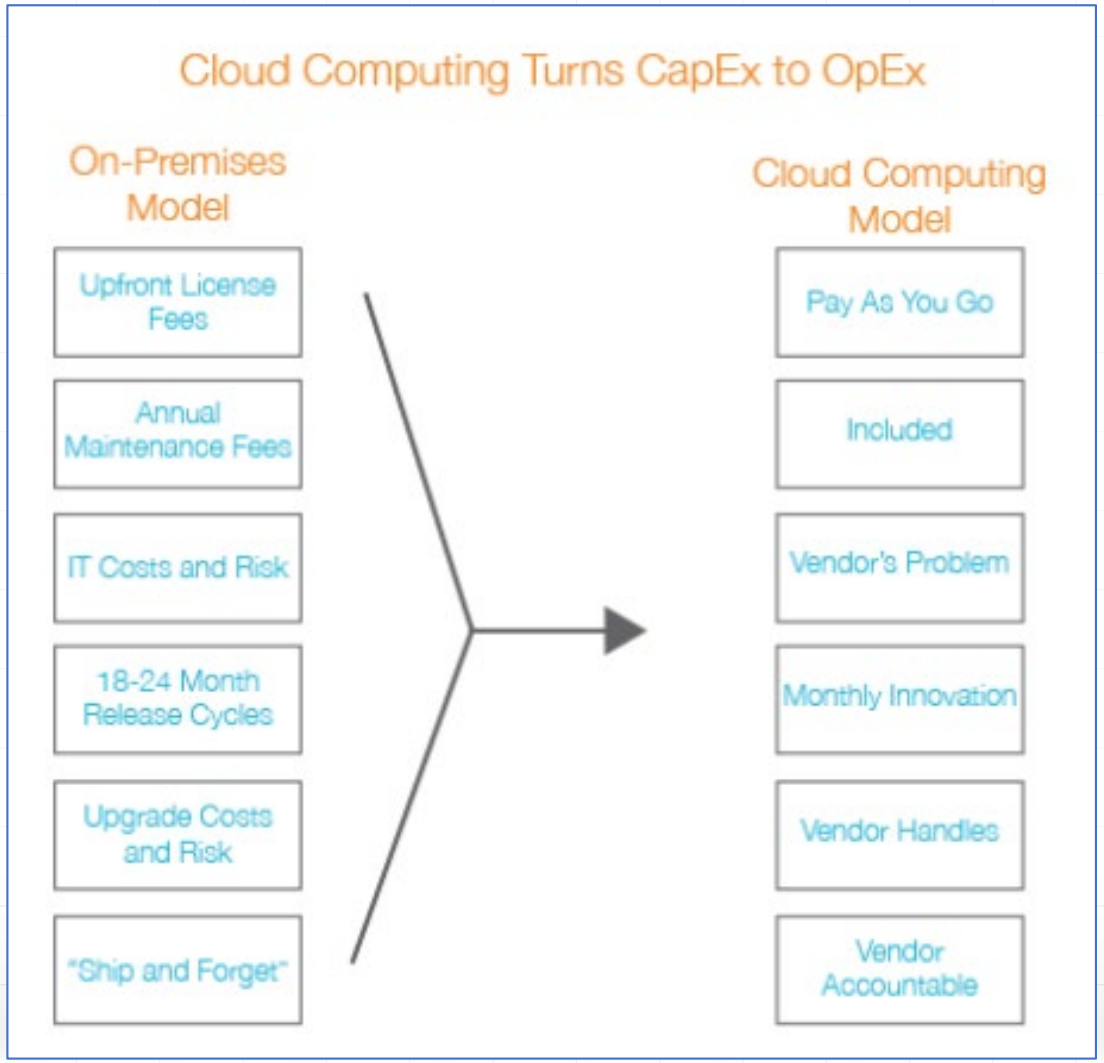
Remote Access

- Many businesses today have remote workers or branch offices.
- With the Cloud, users will have constant access to the business data and applications they need, as they have access to the virtual company work space that the cloud will create.

Management

- Traditional IT manages on-premises hardware and software, but the majority of the time your staff has more to offer than that.
- With the cloud, it's possible to transform your IT department and allow your staff to focus more energy on innovation, rather than on maintenance.
- You can implement new technology solutions in minimal time, without needing to purchase or maintain new hardware at all.
- With cloud computing, your hardware is located off-site, and management is left to an experienced cloud provider.

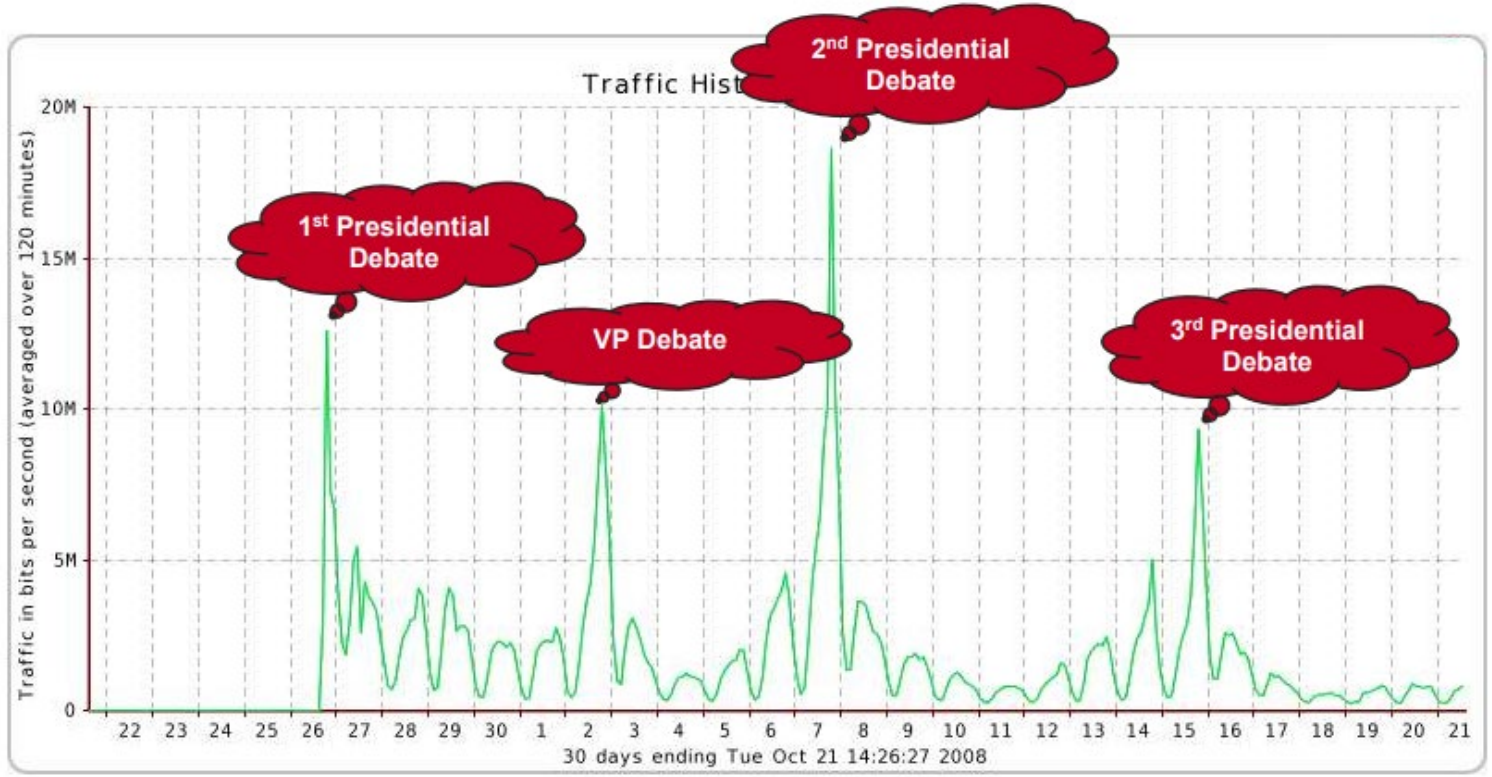
Cloud Benefits – Cost Effective



Capital expenditure refers to major upfront investments that are intended to create a future benefit. Things are considered capital expenditure most commonly if they are purchased new or purchased to improve the life of a previous capital expenditure. Once you've made a CapEx purchase, you're pretty much stuck with that product or service until it stops working.

Operational expenditure refers to expenses incurred on an ongoing basis. These are typically the expenses required for the day-to-day functioning of an organization.

Cloud Benefits - Scalability



YouDecide2008.com

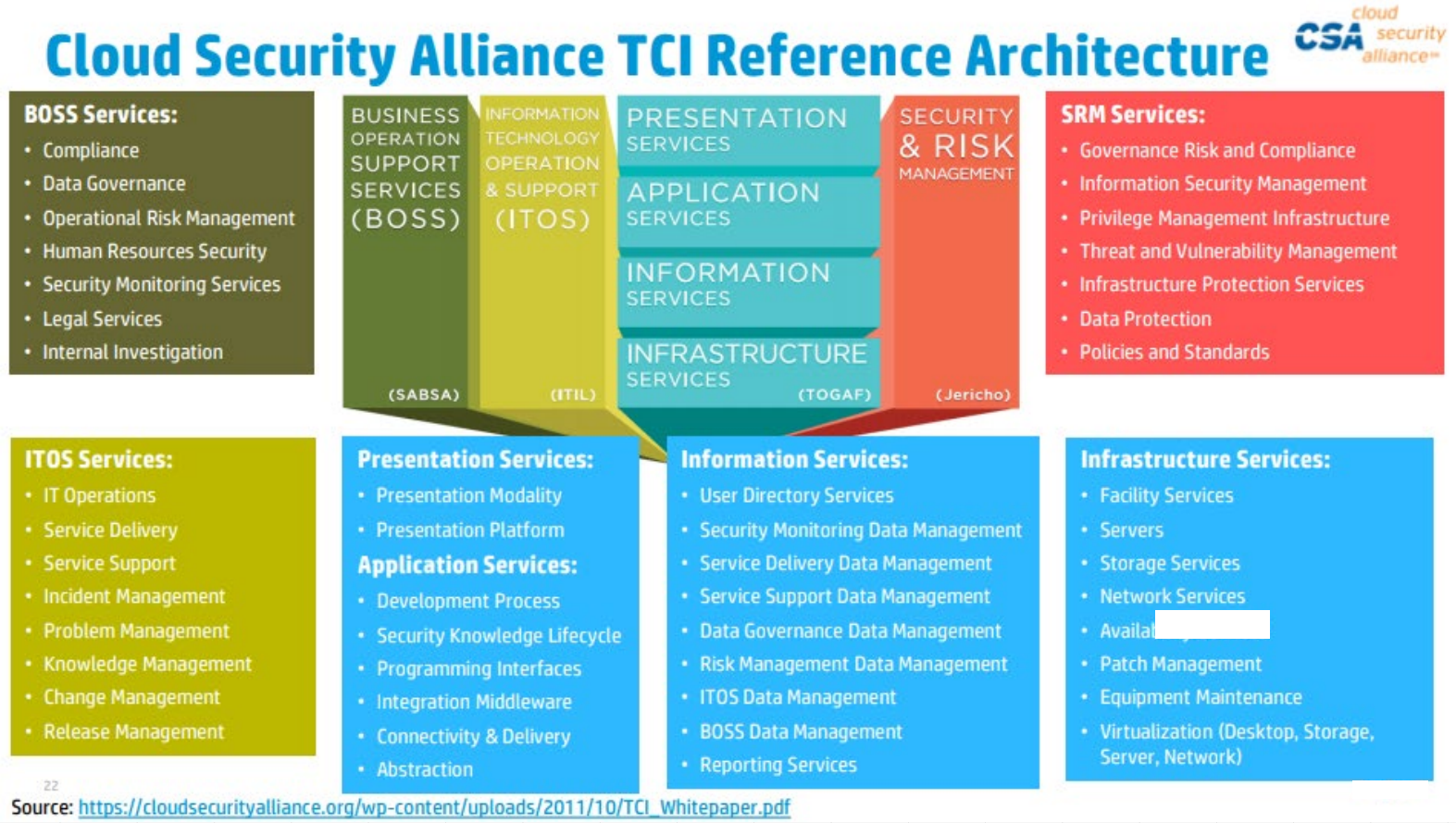
- In January 2008, information was posted about the presidential debates resulting in an increase from 25,000 visitors to more than 300,000 – in one day.

Traditional Hosting = Site Crash!

Cloud Reference Architecture: CSA & TCI

Cloud Security Alliance (CSA) is a not-for-profit organization with the mission to "promote the use of best practices for providing security assurance within cloud computing, and to provide education on the uses of cloud computing to help secure all other forms of computing."

The Trusted Cloud Initiative (TCI) Reference Architecture is both a methodology and a set of tools that enable security architects, enterprise architects and risk management professionals to leverage a common set of solutions that fulfill their common needs to be able to assess where their internal IT and their cloud providers are in terms of security capabilities and to plan a roadmap to meet the security needs of their business.



Source: https://cloudsecurityalliance.org/wp-content/uploads/2011/10/TCI_Whitepaper.pdf

Cloud Control Matrix

CSA Cloud Control Matrix CCM v3.0.1; 16 Domains

cloud security alliance

1. **AIS**: Application & Interface Security (4)
2. **AAC**: Audit Assurance & Compliance (3)
3. **BCR**: Business Continuity Management & Operational Resilience (11)
4. **CCC**: Change Control & Configuration Management (5)
5. **DSI**: Data Security & Information Lifecycle Management (7)
6. **DCS**: Datacenter Security (9)
7. **EKM**: Encryption & Key Management (4)
8. **GRM**: Governance and Risk Management (11)
9. **HRS**: Human Resources (11)
10. **IAM**: Identity & Access Management (13)
11. **IVS**: Infrastructure & Virtualization Security (13)
12. **IPY**: Interoperability & Portability (5)
13. **MOS**: Mobile Security (20)
14. **SEF**: Security Incident Management, E-Discovery & Cloud Forensics (5)
15. **STA**: Supply Chain Management, Transparency and Accountability (9)
16. **TVM**: Threat and Vulnerability Management (3)

Source: https://cloudsecurityalliance.org/research/ccm/

Legend:
CSA: Cloud Security Alliance
CCM: Cloud Control Matrix
(Number of controls) for each Domain

The Cloud Controls Matrix (CCM) is a cybersecurity control framework for cloud computing aligned to the CSA best practices, that is considered the de-facto standard for cloud security and privacy. Version 4* of the CCM constitutes a significant upgrade to the previous version (v3.0.1) by delivering a significant increase of requirements as result of developing additional controls and updating existing ones. The objective of this update was to continue to lead the security industry and market as the cloud provider and user-centric control framework of choice for all.

*) In early February 2021, 1new domain (logging and monitoring) and the 64 new controls will be accompanied by mappings with ISO/IEC 27001-2013, ISO/IEC 27017-2015, ISO/IEC 27018-2019, AICPA TSC v2017, and CCM V3.0.1.

Sample #1: Identity and Access Management

CSA Cloud Control Matrix CCM v3.0.1; 133 Controls

cloud security alliance

Human Resources (HRS)

- HRS-01: Asset Returns
- HRS-02: Background Screening
- HRS-03: Employment Agreements
- HRS-04: Employment Termination
- HRS-05: Mobile Device Management
- HRS-06: Non-Disclosure Agreements
- HRS-07: Roles / Responsibilities
- HRS-08: Technology Acceptable Use
- HRS-09: Training / Awareness
- HRS-10: User Responsibility
- HRS-11: Workspace

Identity & Access Management (IAM)

- IAM-01: Audit Tools Access
- IAM-02: Credential Lifecycle / Provision Management
- IAM-03: Diagnostic / Configuration Ports Access
- IAM-04: Policies and Procedures
- IAM-05: Segregation of Duties
- IAM-06: Source Code Access Restriction
- IAM-07: Third Party Access
- IAM-08: Trusted Sources
- IAM-09: User Access Authorization
- IAM-10: User Access Reviews
- IAM-11: User Access Revocation
- IAM-12: User ID Credentials
- IAM-13: Utility Programs Access

26

Source: https://cloudsecurityalliance.org/research/ccm/

Sample #1: Identity and Access Management

The difference in auditing cloud versus on-premises access management is that access management is a shared responsibility in the cloud

The CSP is responsible for controlling the identity and access "***of***" the cloud

The CSC is responsible for controlling the identity and access "***in***" the cloud

- Control access to critical information and systems based on **need-to-know** classification
- Create and manage users and groups and **use permissions** for access control
- **Enable users to securely control** access to CSP services and resources

A main risk is that **a user can log in from anywhere** and theoretically **delete a resource group or data center**.

Root access in the cloud is the ability to create or change any resource and any change you want in the environment.

To mitigate this risk, follow root access best

Focus:

*Access management is **the process of identifying, tracking, controlling, and managing** authorized or specified users' access to a system, application or any IT instance. The most important principle for the CSC to apply and for you to look for here is **Least Privilege**.*

*Least privilege refers to granting **only the permissions required to perform a specific task**.*

***Logical access controls** determine **not only who, or what**, can have access to a specific system resource, but also **the type of actions that can be performed on the resource** (read, write, etc.). As part of controlling access to resources, users and processes **must present credentials** to confirm that they are authorized to perform specific functions or have access to specific resources. The credentials required vary depending on the type of service and the access method, and include **passwords, cryptographic keys, and certificates**.*

CSP: Cloud Service Provider
CSC: Cloud Service Customer

Identity and Access Management – Audit Program

☐	**1. Ensure there are internal policies and procedures for managing access to CSP services and compute instances.** a. Obtain a list of users with cloud access, validate their privileges are in line with their role. b. Obtain the cloud password/certificate/tokens policies, validate through a sample of users that they are compliant (check if there is a way to continuously monitor this) or ideally, federated to existing systems. c. Validate that access to the cloud is approved by appropriate personnel. d. Verify that periodic review of cloud users is preformed accurately and completely (e.g. is access updated when employees move between roles or outside of the CSC). e. Ensure documentation of use and configuration of CSP access controls.
☐	2. Ensure there is an approval process, logging process, or controls to prevent unauthorized remote access. a. Validate logs are complete and accurate. What is in place to demonstrate the logs are complete and accurate? If they do not have proof, you can validate by same testing to see if logs produce expected results. b. Review process for preventing unauthorized access. c. Review connectivity between firm network and CSP.
☐	3. Ensure restriction of users to those CSP services strictly for their business function. Review the type of access control in place as it relates to CSP services. a. CSP access control at a CSP level – using access management with Tagging to control management of compute instances (start/stop/terminate) within networks. b. CSC Access Control – using an access management (LDAP solution) to manage access to resources which exist in networks at the Operating System /Application layers. c. Ensure segregation of duties is documented and followed. d. Network Access control – using CSP virtual firewalls Network Access Control Lists (NACLs), Routing Tables, VPN Connections, private cloud peering to control network access to resources within CSC owned private cloud. e. Access to edit/view/delete data – although not administering security, sensitive information still needs privileged access.
☐	**4. How does the CSC federate identity to the cloud? Is active directory the single source of code? Do they have multi- factor authentication on the root account? Who has the ability to create/delete accounts?**
☐	5. Review the access management system (which may be used to allow authenticated access to the applications hosted on top of cloud services) and validate whether it is federated with the cloud systems.

Sample #2: Data Security & Information Lifecycle Management

CSA Cloud Control Matrix CCM v3.0.1; 133 Controls

cloud security alliance

Application & Interface Security (AIS)

- AIS-01: Application Security
- AIS-02: Customer Access Requirements
- AIS-03: Data Integrity
- AIS-04: Data Security / Integrity

Audit Assurance & Compliance (AAC)

- AAC-01: Audit Planning
- AAC-02: Independent Audits
- AAC-03: Information System Regulatory Mapping

Business Continuity Management & Operational Resilience (BCR)

- BCR-01: Business Continuity Planning
- BCR-02: Business Continuity Testing
- BCR-03: Datacenter Utilities / Environmental Conditions
- BCR-04: Documentation
- BCR-05: Environmental Risks
- BCR-06: Equipment Location
- BCR-07: Equipment Maintenance
- BCR-08: Equipment Power Failures
- BCR-09: Impact Analysis
- BCR-10: Policy
- BCR-11: Retention Policy

Change Control & Configuration Management (CCC)

- CCC-01: New Development / Acquisition
- CCC-02: Outsourced Development
- CCC-03: Quality Testing
- CCC-04: Unauthorized Software Installations
- CCC-05: Production Changes

Data Security & Information Lifecycle Management (DSI)

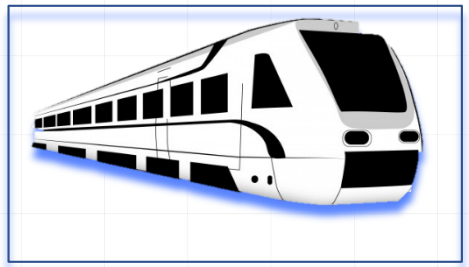
- DSI-01: Classification
- DSI-02: Data Inventory / Flows
- DSI-03: eCommerce Transactions
- DSI-04: Handling / Labeling / Security Policy
- DSI-05: Non-Production Data
- DSI-06: Ownership / Stewardship
- DSI-07: Secure Disposal

Source: https://cloudsecurityalliance.org/research/ccm/

Sample #2: Data Security & Information Lifecycle Management

Design of an information system to classify data and ensure its confidentiality and integrity during handling

SENSITIVE
CONFIDENTIAL
PUBLIC



Data Classification

Data at rest

Data in transit

Key Management

	1. Understand what data the CSC has in the cloud and where the data resides, and validate the methods used to protect the data at rest and in transit (also referred to as "data in-flight" or "in motion"). a. Ask if the CSC has asked their CSP for evidence that their data doesn't go where it's not supposed to. Is it part of the contractual obligation? b. Determine what's in scope regarding regions and legislation. What CSP regions are being used? What regional/global legislation should be considered?
	2. Understand and verify the CSC approach to data protection: a. Data policies, data communication, and procedures in the cloud? How are they enforcing it? b. Data sanitization process, Data transmission footprint and sovereignty rules c. System and information integrity policy and procedure d. Flaw remediation, Malicious code protection, Information System monitoring e. Security alerts, advisories, and directives, Security function verification f. Software, firmware, and information integrity, Information input validation g. Memory protection, Review regional considerations h. Multi-region backups, fault tolerant zones, failover zones

Data Security & Lifecycle Information – Audit Program

Focus:

The difference between on-premises and in cloud auditing with regard to data security is that

*1. Encryption and key management can be a **shared responsibility for both**.*

*2. For data in transit – in the cloud, the data transmission process changes **based on the cloud mode** (where the data originates, passes through, and ends up). It is highly configurable, and routing can be specified within the CSP regions.*

*3. It is also important for CSCs to know **when it's their versus the CSP responsibility to encrypt**, and if the CSP provided encryption is to their standards.*

☐	3. Understand if CSC is leveraging the existing mechanisms for encryption or building on-top-of the CSPs. a. Ensure there are appropriate encryption controls in place to protect confidential information (or highly sensitive) in transit and at rest while using CSP services. b. How is data shared in the cloud? Cloud access security broker (CASB)?
☐	4. Assess if the CSP services are compliant to the framework being assessed. If they are not, is it documented in the CSC's risk management documentation? Does the CSC have additional controls in place covering the service thereby mitigating the risk?
☐	5. Review methods for connection to CSP console.
☐	6. Review management API, storage, and databases for enforcement of encryption.
☐	7. Review internal policies and procedures for key management, including CSP services and compute instances.
☐	8. Review the controls the CSC has in place to manage shadow IT (hardware, software, applications being used without the knowledge of virtual firewalls).
☐	**9. Review the procedure for conducting a specialized wipe prior to deleting the volume for compliance with established requirements. This is to ensure the deletion of CSC data.**

Conclusion: Risk, Challenges, and Benefits

Potential risks & trade-offs:

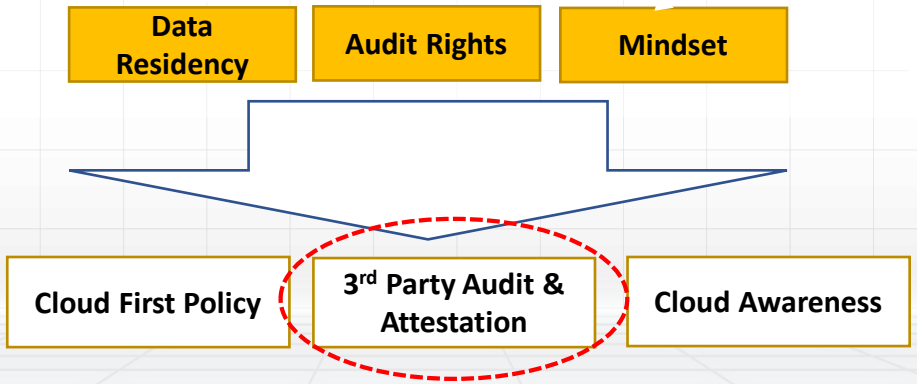
- Security, Privacy, and Data Confidentiality
- Loss of Control & Governance
- Vendor Lock-in
- Management Interface Compromise
- Incomplete or Insecure Data Deletion, Data Protection
- Malicious Insider & Investigative Support
- Segmentation or, Isolation Failure
- Availability, Reliability, Speed, Cost
- Learning Curve
- Quality of support
- Change in organization culture
- Interoperability Standards; Portability for Legacy IT in Clouds
- Shift in Liability
- Regulatory Compliance
- Transparent Infrastructure Scalability
- Application Deployment Mechanisms
- Economic Modeling of new Market

Challenges & success factors...

- Legacy migration
- Integration & Interoperability
- Data & Applications Architecture
- Technology compatibility Issues
- Security & Privacy risks
- Legal & Regulatory Compliance
- Management of Change

Expected Benefits:

- Economies of Scale
- Multi-Tenancy
- Capacity Utilization
- "Zero" capex model
- Long term Total Cost of Ownership for IT Services
- Lower barriers to entry for new business models which were constrained by the IT resources in the past
- Allows Businesses to focus more on their core competencies
- Speed and Flexibility of business Changes
  - On Demand self service
  - Automation
  - Standardization
  - Elasticity
  - Pay per Use Model
  - Reduced time to market
- Efficiency in global communication and collaboration



3rd Party Audit & Attestation: Do not Audit the Auditor

Focus areas	Standards	Certifications
Step 1: Ensure effective governance, risks & compliance	• ISO 38500 – IT Governance1 • COBIT • ITIL (ISO 27002) • ISO 20000-7 & ISO 20000-11 (jn devl) • SSAE 16 • PCI-DSS	• ISO 27002 (ISO 27017) • SSAE 16 • HIPAA • PCI-DSS • FedRAMP • FISMA
Step 2: Audit operational and business processes	• DMTF Cloud Auditing Data Federation (CADF)	• ISO 27002 (ISO 27017) • SSAE 16
Step 3: Manage people, roles and identities	• ISO 27002 • IAM Kerberos, LDAP, SAML 2.0, Oauth 2.0, WS-Federation, OpenID Connect • SCIM • Active Directory Federated Services (ADFS2) • XACML • PKCS, X.509, OpenPGP	• ISO 27002 (ISO 27017)
Step 4: Ensure proper protection of data & information	• ISO 27002 / 27017 (in devl) • Data in motion: HTTPS, SFTP, VPC using IPSec or SSL • US FIPS 140-2 • OASIS KMIP	• ISO 27002 (ISO 27017)

Focus areas	Standards	Certifications
Step 5: Enforce privacy policies	• Personally Identifiable Information (PII) • U.S – EU Safe Harbor framework • ISO 27018 (in devl)	• TRUSTe Safe Harbor certification seal program • ISO 27018 (in devl)
Step 6: Assess the security provisions for cloud apps	• NIST Guidelines on Firewalls and Firewall Policy • Open Web Application Security Project (OWASP) • OVF 2.0 & OASIS TOSCA	• ISO 27002 (ISO 27017)
Step 7: Ensure cloud networks and connections are secure	• ISO 27001 & 27002 • ISO/IEC 27033-1/2/3 • FISMA (FIPS 199 & 200) • OpenFlow, TM Forum Frameworx, NIST SP 800-53	• ISO 27002 (ISO 27017)
Step 8: Evaluate security controls on physical infrastructure & facilities	• ISO 27002 • ISO 27017 & 18 (in devl)	• ISO 27002 (ISO 27017)
Step 9: Manage security terms in the cloud SLA	• CSCC Practical Guide to SLA • ISO 27004, NIST SP 800-55 • CIS Consensus Security Metrics • ENISA	• ISO 27002 (ISO 27017) • SSAE 16 (financial)
Step 10: Understand the security requirements of exit process	• None, ISO SC38 WG3 (future)	• None

Q & A

PRESENTED BY:

Agustinus Nicholas L Tobing

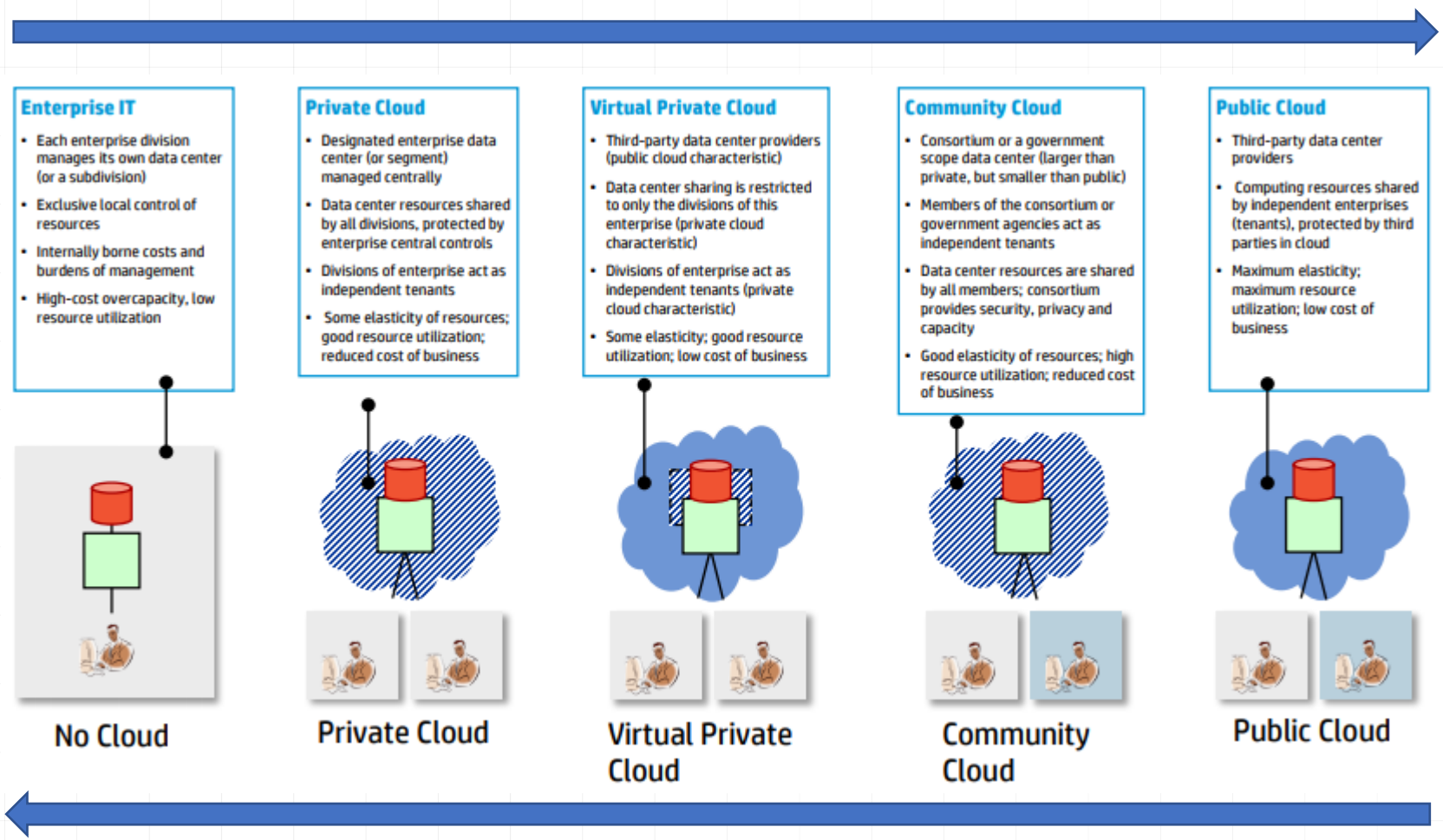
SPEAKER TITLE HERE

Appendix

- **Cloud – Essential Characteristics**
- **Public vs Private: A Trade Off**

Cloud -Essential Characteristics

Characteristics	Description
On-Demand Self Service	Authorized agencies must be able to provide and release capabilities, as needed, automatically, without requiring human interaction with each services provider.
Broad Network Access	Once provisioned, the software, platform, or infrastructure maintained by the cloud provider should be available over a network using thin or thick clients.
Resource Pooling	The resources provisioned from the cloud provider should be pooled to serve multiple agencies or programs using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to the agency's self-service demand.
Rapid Elasticity	Elasticity is defined as the ability to scale resources both up and down as needed. Cloud Computing capabilities should be rapidly and elastically provisioned and released.
Measured Service	Cloud resource usage should be monitored, controlled, and reported providing transparency for both the provider and consumer of the service.



Public vs Private: A Trade Off

THANK YOU

PRESENTED BY:

SPEAKER NAME HERE

CIA CRMA CFE CAMS CCRP QRGP BCCP AWS-CCP