The Cloud

A Primer for Project Managers

Stephen Moon
PMP, CISSP, ITIL, AWS Architect Associate

Disclaimer

The views and opinions expressed during this presentation are my own and are in no way, shape, or form those of Amazon, Amazon Web Services (AWS), or Amazon subsidiaries and associates.

Agenda

- My Background
- Defining “The Cloud”
- Types of Clouds (Deployment Models)
- Cloud Layers (Service Models)
- Total Cost of Ownership (TCO)
- Value Proposition
- Healthcare in the Cloud

My Background

Education

- Auburn University; B.S.B.A. in Management Information Systems
- University of Alabama in Huntsville (UAH); M.B.A. in Management of Technology

Evolution

- Database Architect, Engineer, and Administrator / Software Developer
- Full Stack Operations (DevOps before DevOps was cool)
- Program & Project Manager
- Enterprise Solutions Architect (DoDAF and TOGAF)

Industries

- Telecommunications (Manufacturing), Retail, e-Commerce, Finance
- Department of Defense, Department of State
- Healthcare (Federal, State/Provincial, Provider, Insurer)

Cloud Definitions

NIST

A model for enabling ubiquitous, 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.

Wikipedia

A type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand… Cloud computing relies on sharing of resources to achieve coherence [*economies of scope*] and *economies of scale*, similar to a utility (like the electricity grid) over an electricity network.

Types of Clouds (Deployment Models)

Private Cloud (*Is there such a thing?)*

- Cloud resources are provisioned for use by a single organization, business unit, etc.
- OpenStack is a common open-source platform for private cloud deployments: IaaS and PaaS (limited)
- Tend to manifest as managed services

Community Cloud

- Cloud resources are provisioned for exclusive use by a specific community of interest for organizations that have shared missions, goals, objectives, and concerns
- Examples would be government clouds (federal, defense, intelligence)

Public Cloud

- Cloud resources are provisioned for open use by the general public.
- Most common deployment model for commercial and non-profit entities

Hybrid Cloud

- Cloud resources are composed of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data integration.

Cloud Layers (Service Models)

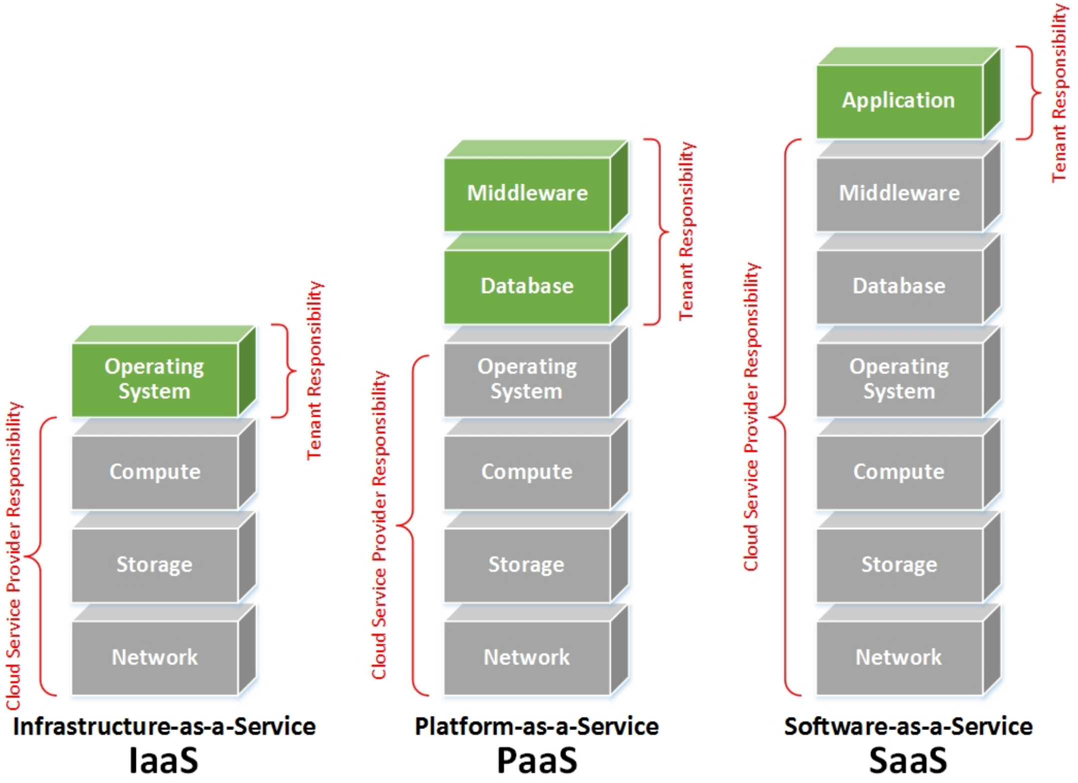
Infrastructure-as-a-Service (IaaS)

Platform-as-a-Service (PaaS)

- *Database-as-a-Service (DBaaS)*
- *Middleware-as-a-Service (MWaaS)*
  - JVM
  - SOA / BPM
  - Data Integration (CDC and ETL)
- *Business Intelligence-as-a-Service (BIaaS)*
- *Security-as-a-Service (SECaaS)*
  - Identity and Access Management (IAM)
  - Encryption (at-rest, in-transit)

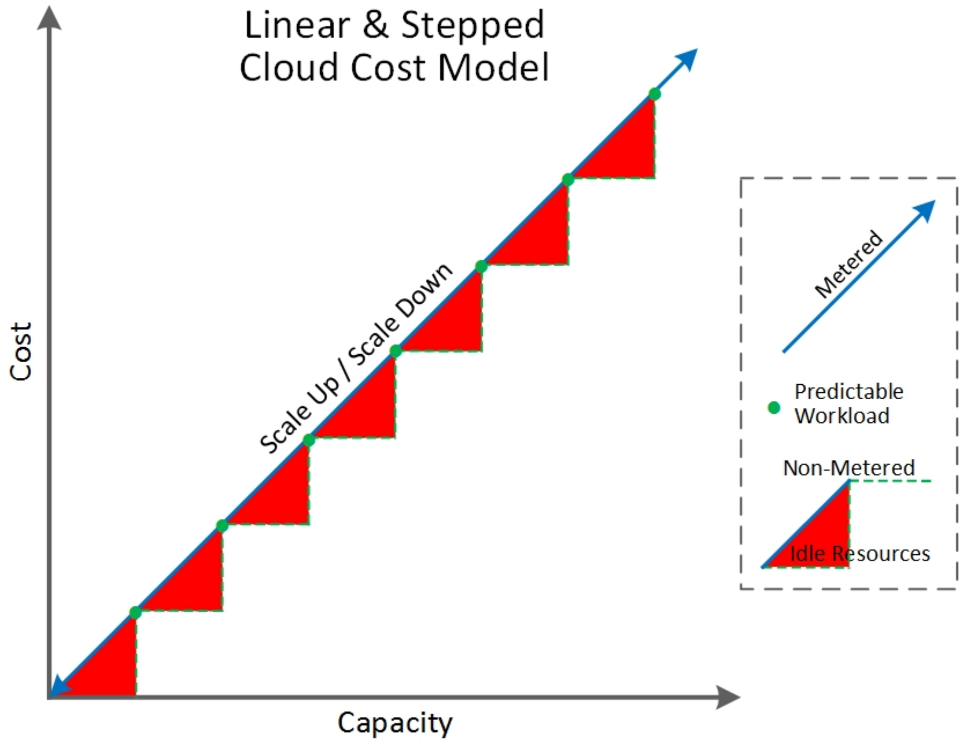
Software-as-a-Service (SaaS)

- Salesforce
- Workday

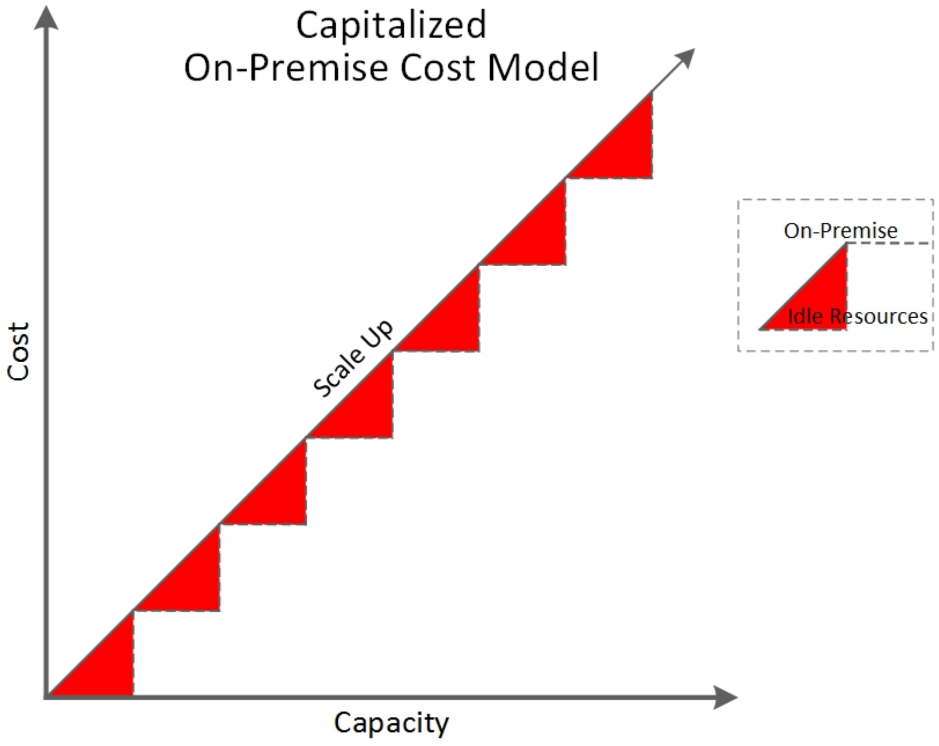


Total Cost of Ownership (TCO)

Operationalization



Capitalization



Total Cost of Ownership (TCO)

Operationalization

- All investments are variable cost
- Metered services provide fine grained scale-up and scale-up capabilities to meet changing demand; *Best for Unpredictable Workloads*
- Non-metered services provide coarse grained scale-up and scale-up capabilities as demand changes; *Best for Predictable Workloads*

Capitalization

- Investments are fixed cost in the short to mid term (< 4-5 years)
- *Must invest for peak usage (load)*
- Scaling up requires investment in resources that will be un(der)utilized
- No ability to scale down resources during periods of reduced demand
- *Un(der)utilized Investment = Idle Resources x Scale*

Total Cost of Ownership (TCO)

Other factors to consider…

- Sustainment (Operations and Maintenance)
  - Investment can be shifted to value-added or revenue-generating activities
  - *Work Breakdown Structure (WBS) for project shifted up the stack*
- Labor
  - No more network, storage, or server "*guy*"
  - *Skill sets must shift to full-stack capabilities*

Value Proposition

Time-to-Market

- Organizational Delivery (Agile, DevOps)
- Core Competencies
- Fail Fast; Proof of Concept (PoC) / Proof-of-Principle Prototyping
- Security Inheritance (HIPAA/HITECH, PCI/DSS, FedRAMP, etc.)

Time-to-Value

- Total Cost of Ownership (TCO)
- *Cost Allocation*
- Return on Investment (ROI)

Healthcare in the Cloud

What is HIPAA?

From Wikipedia…

The Health Insurance Portability and Accountability Act of 1996 (HIPAA; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996) was enacted by the United States Congress and signed by President Bill Clinton in 1996. It has been known as the Kennedy–Kassebaum Act or Kassebaum-Kennedy Act after two of its leading sponsors. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. *Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.*

Healthcare in the Cloud

What is the HIPAA Security Rule?

Privacy Rule

- Establishes national standards for the protection of certain health information
- Regulates the use and disclosure of Protected Health Information (PHI) held by "covered entities“

Security Rule

- Established a national set of security standards for protecting certain health information that is held or transferred in electronic form
- Operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called “covered entities” must put in place to secure individuals’ “electronic protected health information”
- Specifies three types of security safeguards required for compliance: administrative, physical, and technical

Healthcare in the Cloud

What is the HIPAA Security Rule?

Administrative Safeguards

- Policies and procedures designed to show how the entity will comply with the act

Physical Safeguards

- Controlling physical access in order to protect against inappropriate access to protected data

Technical Safeguards

- Controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient.

Healthcare in the Cloud

Required vs. Addressable Implementation Specifications

Required

When a standard adopted in §164.308, §164.310, §164.312, §164.314, or §164.316 includes required implementation specifications, a covered entity or business associate must implement the implementation specifications.

Addressable

When a standard adopted in §164.308, §164.310, §164.312, §164.314, or §164.316 includes addressable implementation specifications, a covered entity or business associate must…

- Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and
- As applicable to the covered entity or business associate
    - Implement the implementation specification if reasonable and appropriate; or
    - If implementing the implementation specification is not reasonable and appropriate
        - Document why it would not be reasonable and appropriate to implement the implementation specification; and
        - Implement an equivalent alternative measure if reasonable and appropriate.

Technical Safeguards

Standard		Implementation Specification		Status	Capability
Access Control	Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).	Unique User Identification	Assign a unique name and/or number for identifying and tracking user identity.	Required	• Identity Management • Single Sign-on • Federation
		Emergency Access Procedure	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	Required	• Adaptive Access • Fine-grained Control
		Automatic Logoff	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Addressable	• Adaptive Access
		Encryption and Decryption	Implement a mechanism to encrypt and decrypt electronic protected health information.	Addressable	• Key Management • Encryption-at-Rest • Encryption-in-Transit
Audit Controls	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.				• Auditing • Reporting & Analytics
Integrity	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	Mechanism to authenticate electronic protected health information	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	Addressable	
Person or Entity Authentication	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.				• Identity Validation
Transmission Security	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	Integrity Controls	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	Addressable	• Auditing • Separation of Duties
		Encryption	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	Addressable	• Key Management • Encryption-in-Transit

! *The is no such thing as "HIPAA Certification"* !

From HHS…

…*there is no standard or implementation specification that requires a covered entity to "certify" compliance.* The evaluation standard § 164.308(a)(8) requires covered entities to perform a periodic technical and non-technical evaluation that establishes the extent to which an entity's security policies and procedures meet the security requirements. The evaluation can be performed internally by the covered entity or by an external organization that provides evaluations or "certification" services. A covered entity may make the business decision to have an external organization perform these types of services. It is important to note that *HHS does not endorse or otherwise recognize private organizations' "certifications" regarding the Security Rule*, and such certifications do not absolve covered entities of their legal obligations under the Security Rule. Moreover, performance of a "certification" by an external organization does not preclude HHS from subsequently finding a security violation.

HIPAA Compliance in the Cloud

Covered Entity – *Cloud Tenant*

Covered entity is any organization or corporation that directly handles Personal Health Information (PHI) or Personal Health Records (PHR). The most common examples of covered entities include hospitals, doctors' offices and health insurance providers.

Business Associate (BA) – *Cloud Service Provider (CSP)*

Any organization or person working in association with or providing services to a covered entity who handles or discloses Personal Health Information (PHI) or Personal Health Records (PHR).

Business Associate Agreement (BAA)

A contract between a HIPAA covered entity and a HIPAA business associate (BA). The contract protects Personal Health Information (PHI) in accordance with HIPAA guidelines.

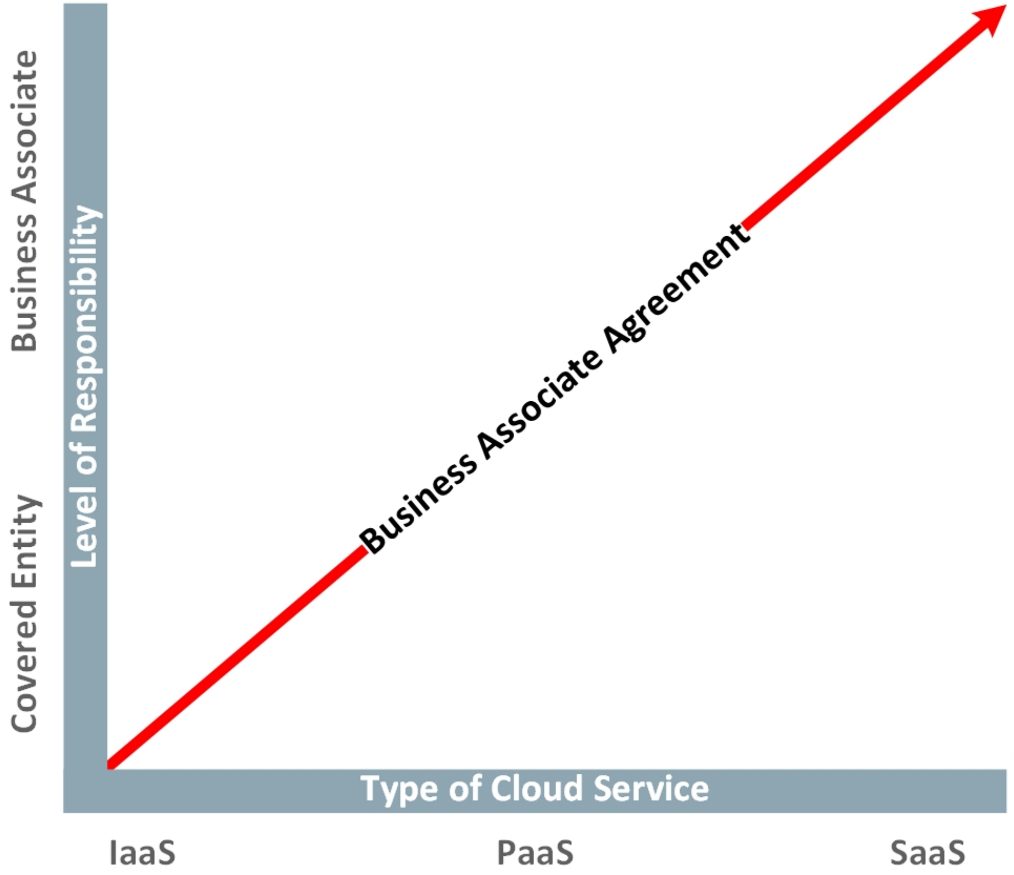
HIPAA Compliance in the Cloud

The Covered Entity *inherits* the security posture of the cloud service(s) provided by the Business Associate.

It is up to the Covered Entity and the Business Associate…

- to determined what level of cloud service(s) will be leveraged and
- to establish the level of responsibility for HIPAA compliance

…in the Business Associate Agreement



Wrapping Up

Questions?

Links

- NIST Special Publications
- Public Cloud Services Comparison

Contact Information

- Stephen.C.Moon@gmail.com
- www.linkedin.com/in/stephencmoon