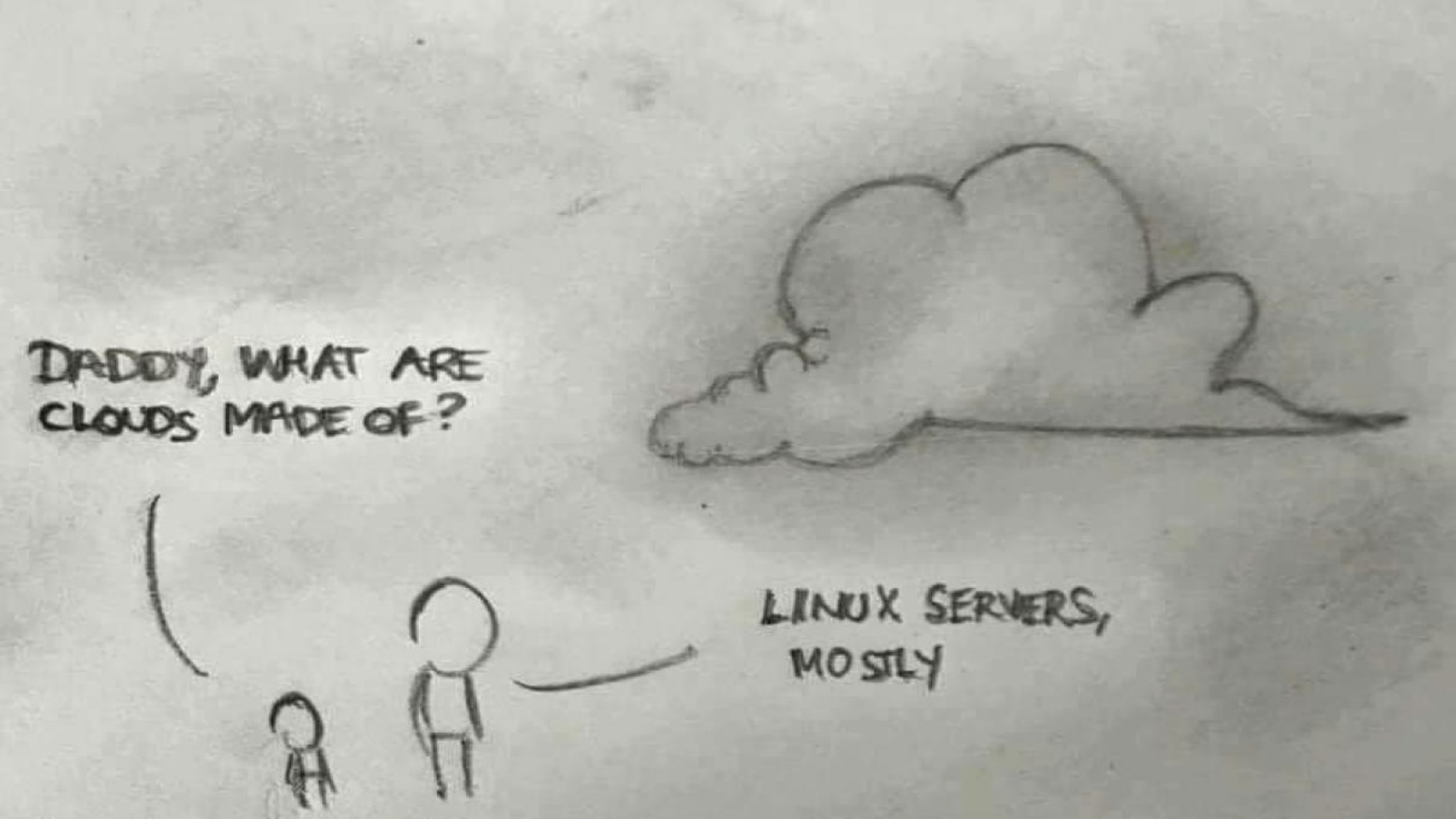
Lesson 5
Cloud Security Policy

Discussions on Cloud Security matters pertain mainly to the Public Cloud, Not Private Cloud


DADDY, WHAT ARE CLOUDS MADE OF?
LINUX SERVERS, MOSTLY

Cloud Computing in a nut shell (Characteristic)

- Shared / Outsourced Assets, Resources, and Services
  - Off-Premise
  - Your applications, data, etc. sit on other people's infrastructure
  - Pay-as-you-Go (e.g. Renting)
    - Operational Expenditure (OPEX) rather than Capital Expenditure (CAPEX)
  - Cost Savings
    - e.g. Don't need an army of IT staff
- Flexible, Scalable On-Demand Infrastructure Supply
  - No need to purchase own assets and infrastructure
  - Great for storage and backup of data, applications-hosting, etc.
  - Very quick provisioning for users – servers, disk space, etc.
  - Good for business continuity (BC) and disaster recovery (DR)
  - 3 Cloud Service Models
    - Infrastructure-as-a-Service (IaaS)
    - Platform-as-a-Service (PaaS)
    - Software-as-a-Service (SaaS)

It’s Just Other’s Computer

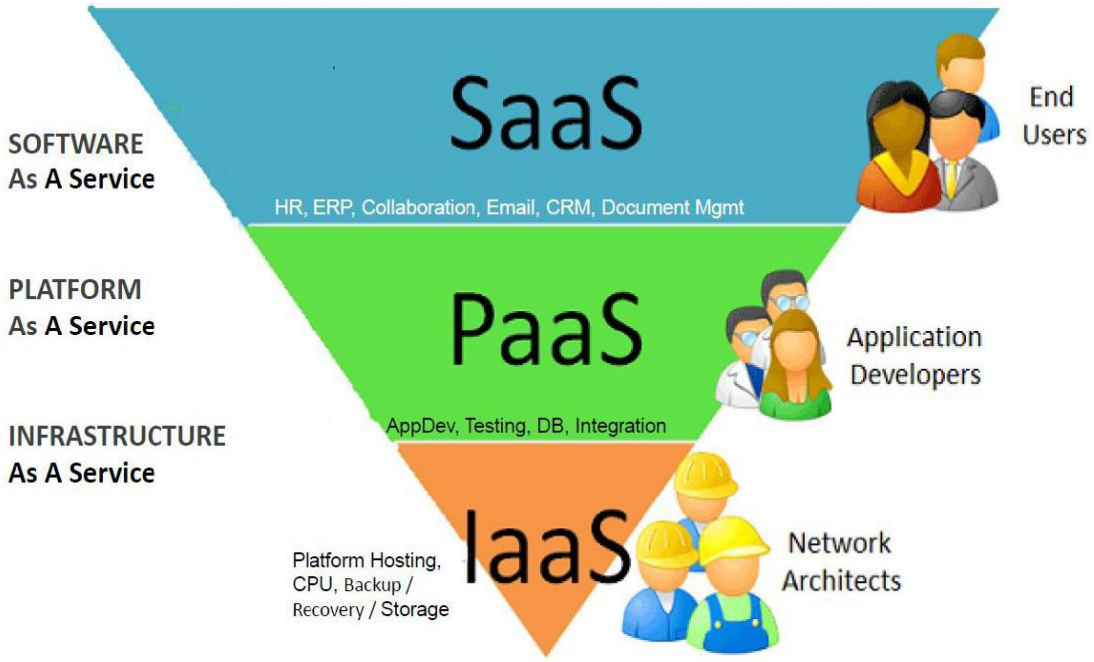
5 Essential Characteristics

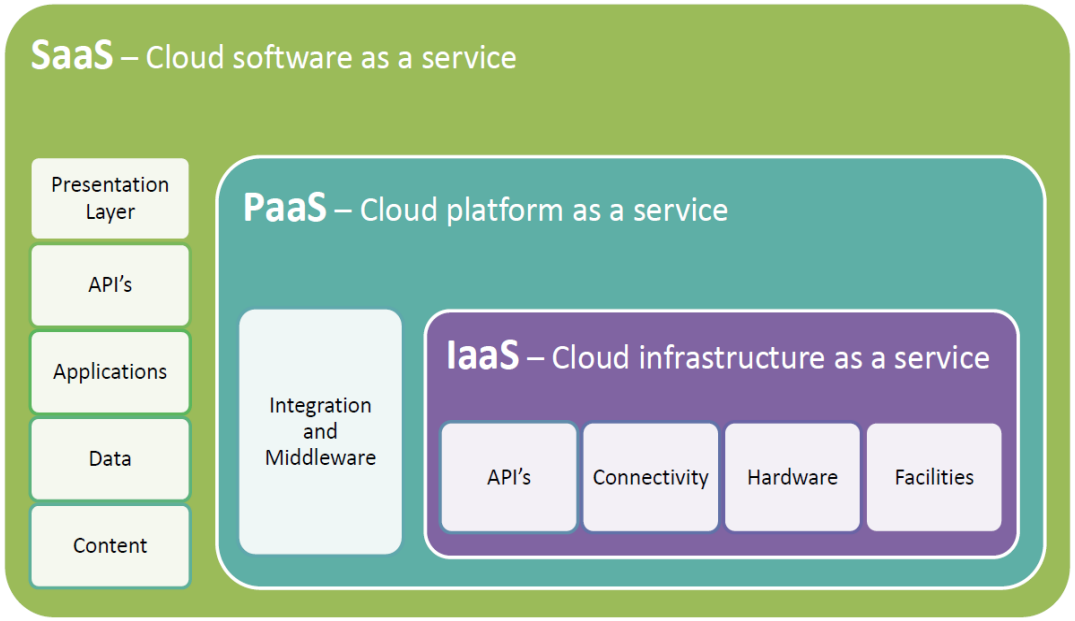
- NIST SP-800-145 Definition of Cloud Computing
  - On-Demand Self-Service
  - Broad Network Access
  - Resource Pooling
  - Rapid Elasticity
  - Measured Service

Drives for Cloud Adoption

- Cost Management (OPEX v. CAPEX)
  - Pay-as-you-Use
- Risk Reduction e.g. Testing before Commitment
- Scalability
- Elasticity
  - Consumption-based Pricing
- Business Agility & Mobility
- Focus on Core Business
- Business Continuity
- Collaboration & Innovation Platform
- “Green” IT
- “Simplicity, Expandability & Elasticity”
  - NIST SP-800-145 & ISO/IEC 17788:2014

3 Cloud Service Models





Class Activity: Match the Description

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

- ❑Self-service models for accessing, monitoring, and managing remote data centre infrastructure
- ❑Many applications can be run indirectly from a web browser without any downloads or installations although some require small plugins
- ❑Provides developers with a framework they can build upon to develop or customise applications
- ❑With this technology, enterprise operations, or a 3rd-party provider, can manage operation systems, virtualisation, servers, storage and networking
- ❑Uses the web to deliver applications that are managed by a 3rd-party vendor and whose interface is accessed on the client's side

Key Issues

- Hard to Approach Governance, Risk & Compliance (GRC)
- Examples:
  - Risk of data “spillage” (leakage) due to multi-tenancy and co-mingling nature of the cloud
  - Risk of “mis-provisioning” or “mis-configuration”
  - Difference in security standards, policies and processes
    - e.g. Contingency backup and mirror resources of cloud provider may not meet your policies nor requirements.
  - If supplier cut corners, has internal issues, or got attacked, your data, applications and services will be affected
    - i.e. Their risks are now your risks.
  - Traditional enterprise security solutions may not be effective or adequate to protect cloud-hosted data, applications and/or services

Data Security Issues

Issues

- Data Loss
  - i.e. Availability
- Data Leakage
  - i.e. Confidentiality
- Data Rights Management (DRM)
  - i.e. intellectual property
- Compliance
  - i.e. Data Sovereignty issues

Some Proposed Solutions

- Data Management / Handling Polices
- Data Encryption
- Data Sanitisation

Some Policy Considerations

- Ensure Provider's Security Policies and Practices and Service Level meet your Requirement
- Legal, Regulatory and Insurance Considerations
- Data Protection
  - e.g. Data Sovereignty and Ownership, etc.
- Service Availability, Performance and Quality
- Backup & Storage
- Cyber Resiliency Provisions
  - i.e. BC, DR and Incident Management (IM)
- Communications Protocol between User and Provider especially in Time of Conflict
- Vendor Lock-In
- Service Exit Clauses
  - e.g. Immediate and definite de-provisioning of users, applications and data resources and storage upon the end of use

Top Threats in 2016 Cloud Security Alliance's Treacherous 12

1. Data Breaches
2. Weak Identity, Credential and Access Management
3. Insecure Application Programming Interfaces (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 and Cloud Services
11. Denial of Service
12. Shared Technology Issues

Policy/Management Considerations

- How would we be harmed if …
  - The asset (data and services) became public and distributed?
  - An employee of our cloud provider accessed the asset?
  - The process or function were manipulated by an outsider?
  - The process of function failed to provide expected results?
  - The information/data were unexpectedly changed?
  - The asset were unavailable for a period of time?

Ultimate Issue & Key Solutions

- Ultimate Issue – Cloud Computing is an Outsource Model
  - Hence, the key issues of: Loss of Visibility, Loss of Control, and Hard to approach GRC
- Key Solutions
  - Measurement and ascertainment against Frameworks e.g. Standards and Certifications
  - Contractual Agreements, **typically in the form of Service Level Agreements (SLAs)**
    - "SLA is an agreement between the service providers and the service user as to the nature,availability, quality, scope of the service to be provided."
    - In an outsourced and off-premise service model like cloud computing, due to the lack of visibility, it is difficult for the consumer to ensure adequate control and compliance. Hence, in order to ensure satisfaction of meeting governance and security policy needs, it through legal agreement means.

Frameworks & Standards (Some examples)

- Organisational
  - Cloud/Outsource-Specific
    - Cloud Security Alliance – Security, Trust & Assurance Registry (STAR)
    - ISO/IEC 27017 Information Security Controls for Cloud Services
    - ISO/IEC 27018 Personal Identifiable Information (PII) in Public Clouds Acting as PII Processors
    - NIST SP-800-144 Guidelines on Security & Privacy in Public Cloud Computing
    - Singapore's Multi-Tier Cloud Security (MTCS) Standard i.e. the SS584
    - Singapore's Cloud Outage Incident Response (COIR) Guidelines
    - MAS' TRM Guidelines for Service Providers
  - General
    - ISO/IEC 27001 Information Security Management Systems
    - NIST SP-800-53 Security & Privacy Controls for Information Systems & Organisations
    - PDPC's Guidelines to Securing Personal Data in Electronic Medium
    - EU's General Data Protection Regulation (GDPR)
- Individual
  - Cloud Security Alliance – Certificate of Cloud Security Knowledge (CCSK)
  - (ISC)2 – Certified Cloud Security Professional (CCSP)

Information Security Controls for Cloud Services ISO/IEC 27017:2015

Sections

1. Cloud-based specific concepts
2. Information security policies
3. Organisation of information security
4. Human resource security
5. Asset management
6. Access control
7. Cryptography
8. Physical and environment security
9. Operations security
10. Communications security
11. System acquisition, development and maintenance
12. Supplier relationship
13. Information security incident management
14. Information security aspects of business continuity management (BCM)

Annex A – Cloud Service Extended Control Sets

- (Access Control) 6.3
  - Relationship between cloud service customer and cloud service provider
- (Physical and environment security) 8.1
  - Responsibility for assets
- (Operations security) 9.5
  - Access control of cloud service customer data in shared virtual environment
- (Supplier relationship) 12.1
  - Operational procedures and responsibilities
- (Supplier relationship) 12.4
  - Logging and monitoring
- (Information security incident management) 13.1
  - Network security

Service Level Agreement (Some Key Issues)

- Availability Standards
  - Specify parameters and minimum levels required from each element of the service, as well as remedies for failure to meet those requirements
- Data Ownership & Protection Policies
  - Affirm your institution's ownership of its data stored on the service provider's system, and specifies your rights to get it back
- Security Standards & Compliance
  - Details the system infrastructure and security standards to be maintained by the service provider, along with your rights to audit their compliance
- Incident Response, Conflict Resolution & Exit Strategy
  - Specifies your rights and cost to continue and discontinue using this service, and ensure definitive and timely removal of your data in the service

Service Level Agreement (Some Key Points)

1. Availability
   - e.g. 99.99% during work days, 99.9% for nights/weekends
2. Performance
   - e.g. Maximum Response Time
3. Security/Protection/Privacy of the Data
   - e.g. Encrypt all stored and transmitted data
4. Location of the Data
   - e.g. Consistent with Local Legislation
5. Access to the Data
   - e.g. Data Retrievable from Provider in Readable Format
6. Portability of the Data
   - e.g. Ability to Move Data to a Different Provider
7. Process to Identify Problems & Resolution Expectations
   - e.g. Call Centre
8. Disaster Recovery Expectations
   - e.g. Worst Case Recovery Commitment
9. Change Management Process
   - e.g. Updates or New Services
10. Exit Strategy
    - e.g. Provider to ensure Smooth Transition

Best Practices to Develop SLAs for Cloud Computing (IBM)

1. Identify the Cloud Actors
2. Evaluate Business-Level Policies
3. Understand SaaS, PaaS, IaaS
4. Metrics
   - Identify what metrics should be used to achieve performance objectives.
5. Security
   - Asset Sensitivity
   - Legal/Regulatory Requirements
   - Cloud Providers' Security Capabilities
6. Identify Service Management Requirements
7. Prepare for and Manage Service Failure

IBM

developerWorks

Best practices to develop SLAs for cloud computing

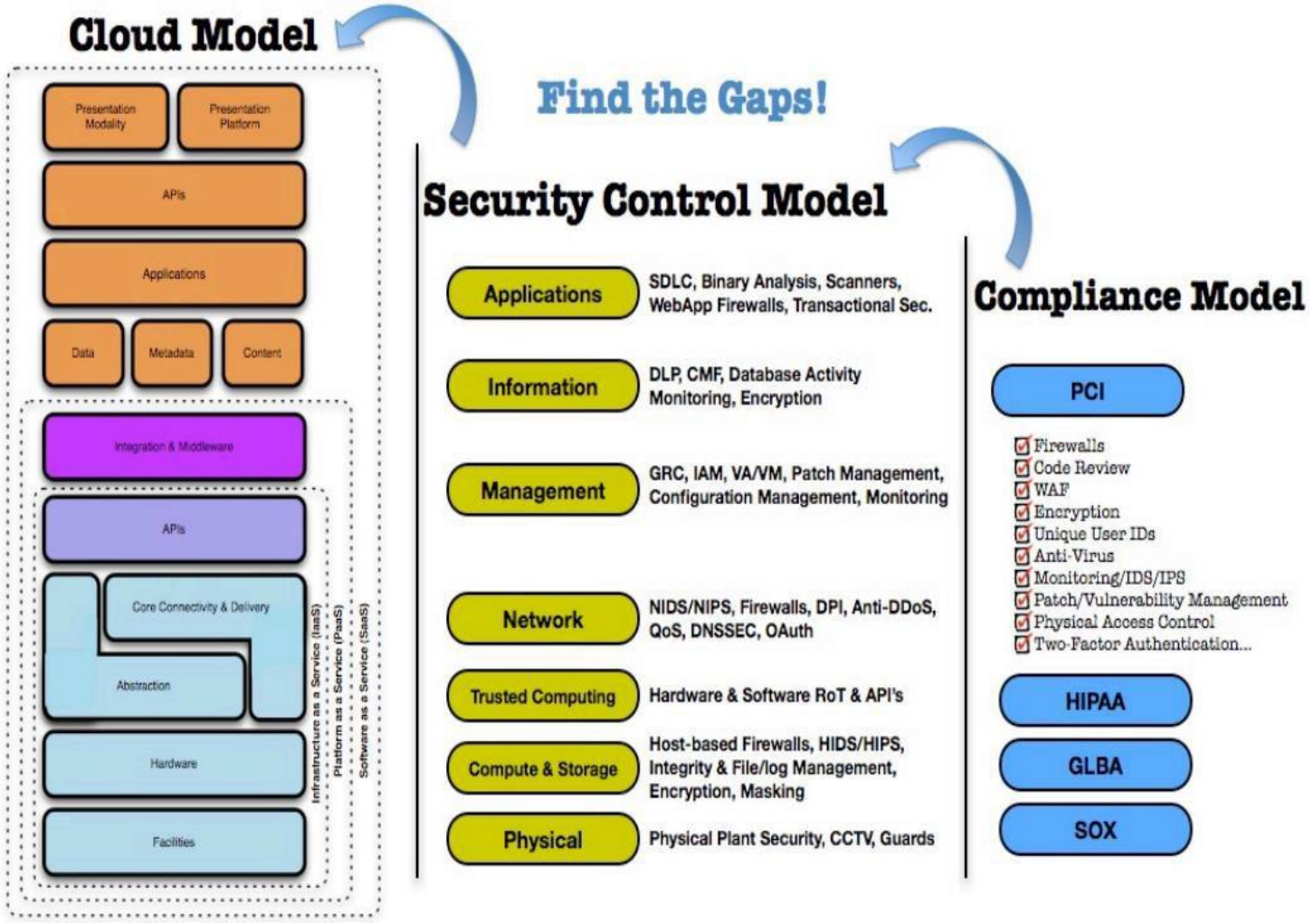
Develop a standard way to create service level agreements that multiple partners can use

Judith M. Myerson
Systems Engineer and Architect

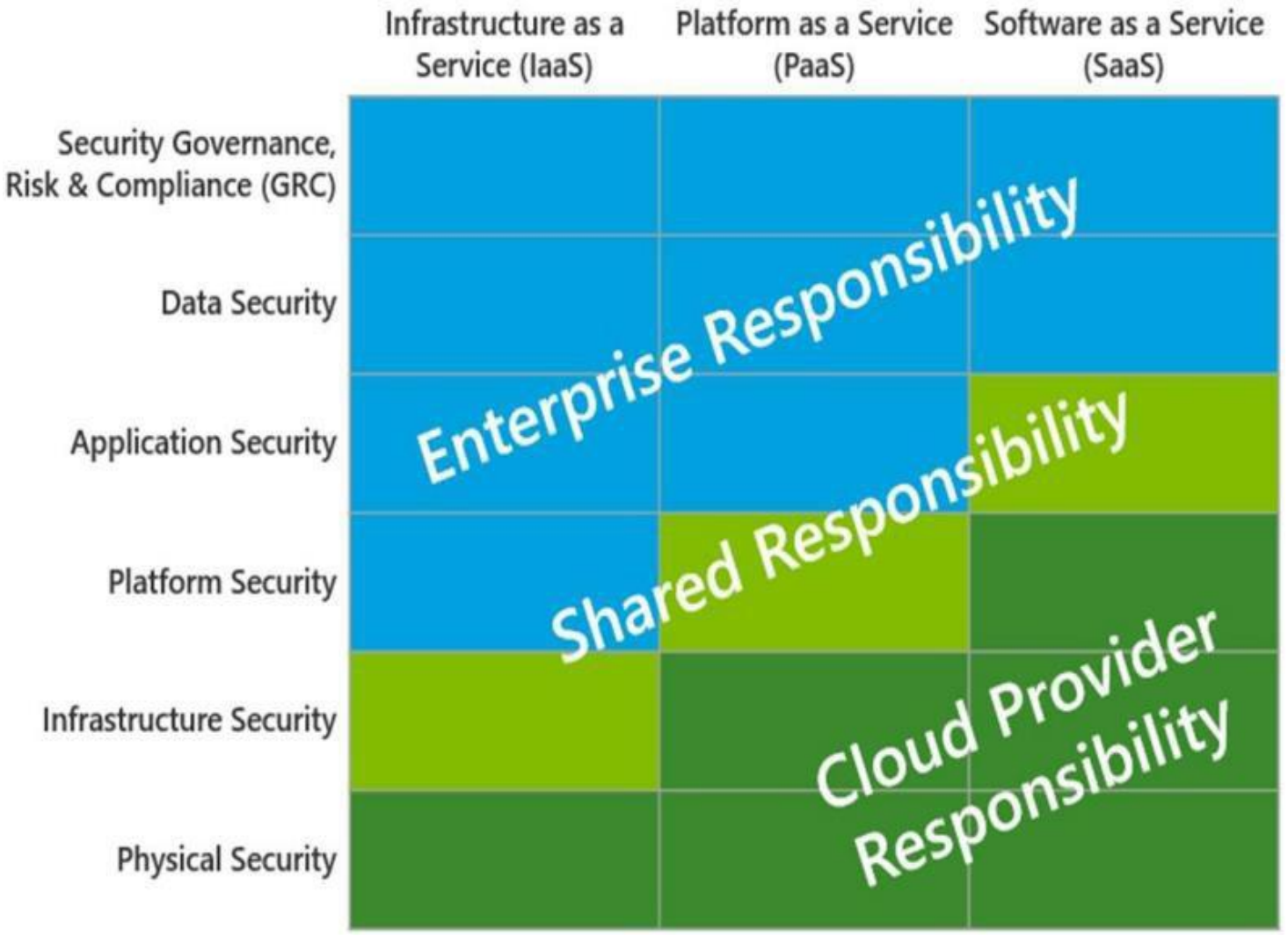
January 07, 2013

You can't rush the process of developing service level agreements (SLAs) between cloud consumers and providers. What service guarantees do consumers expect? What terms and conditions can cloud computing providers and consumers agree on? What terminologies will they use? Plus, the cloud provider must evaluate its relationships and SLAs with vendors, enterprise data centers, network providers, and content providers. There's much to consider. In this article, the author discusses some best practices and how SLAs can be standardized.

Mapping the Cloud Model –> Security Control –> Compliance Gaps



Responsibility (Enterprise v. Shared v. Cloud Provider)



You Cannot Outsource (Risk & Accountability)

- **Responsibility v. Accountability**
  - Accountability – Accountable is to be liable and answerable to, or being called to account as of one's actions, or of the discharge of a duty or trust.
- Recall: Risk Management / Risk Treatment Options
  - Risk Avoidance
  - Risk Reduction
  - Risk Transference
  - Risk Acceptance