MODULE 4 -Security Management in Cloud

Submitted By: Anshika Malsaria

Assistant Professor

JECRC Foundation

Books

Text Books:

1. David S Linthicum, "Cloud Computing and SOA Convergence in your Enterprise A Step by Step Guide", Addison Wesley Information Technology Series.

2.Anthony T Velte, Toby J.Velte, Robert Elsenpeter, "Cloud computing A Practical Approach ", Tata McGraw Hill Publication

3.Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy –

Reference Books:

1. An Enterprise Perspective on Risks and Compliance" , O'Reilly Publications, First Edition
2. Michael Miller, "Cloud Computing – Web-Based Applications that Change the Way You Work and Collaborate Online", Pearson Education, New Delhi, 2009.
3. Cloud Computing Specialist Certification Kit – Virtualization Study Guide

Syllabus

BCO 064B	CLOUD COMPUTING	3-0-0 [3]

OBJECTIVE: At the end of the course, the student should be able to:

1. To understand the architecture of Cloud.
2. To develop an understanding of various aspects of cloud computing.
3. To familiarize the students with fault Tolerance and security measures in cloud.

UNIT 1	**Understanding cloud computing:** Introduction to Cloud Computing - Benefits and Drawbacks - Types of Cloud Service Development - Deployment models
UNIT 2	**Cloud Architecture Technology and Architectural Requirements:** The Business Case for Clouds - Hardware and Infrastructure – Accessing the cloud – Cloud Storage – Standards- Software as a Service – Discovering Cloud Services Development tools. Three Layered Architectural Requirement - Provider Requirements - Service Centric Issues - Interoperability – QoS.
UNIT 3	Fault Tolerance - Data Management Storage and Processing - Virtualization Management - Scalability - Load Balancing - Cloud Deployment for Enterprises - User Requirement - Comparative Analysis of Requirement.
UNIT 4	**Security Management in Cloud:** Security Management Standards - Security Management in the Cloud Availability Management - SaaS Availability Management - PaaS Availability Management - IaaS Availability Management - Access Control - Security Vulnerability, Patch, and Configuration Management – Privacy in Cloud- The Key Privacy Concerns in the Cloud - Security in Cloud Computing.
UNIT 5	**Virtualization:** Objectives - Benefits - Virtualization Technologies - Data Storage Virtualization – Storage Virtualization – Improving Availability using Virtualization - Improving Performance using Virtualization- Improving Capacity using Virtualization.

SECURITY MANAGEMENT

STANDARDS

Introduction

- Cloud Computing Industry is growing
- Businesses are increasing Cloud adoption
- How can IT leaders ensure security in the cloud?

JECRC UNIVERSITY
BUILD YOUR WORLD
JECRC Foundation

Cloud Basics

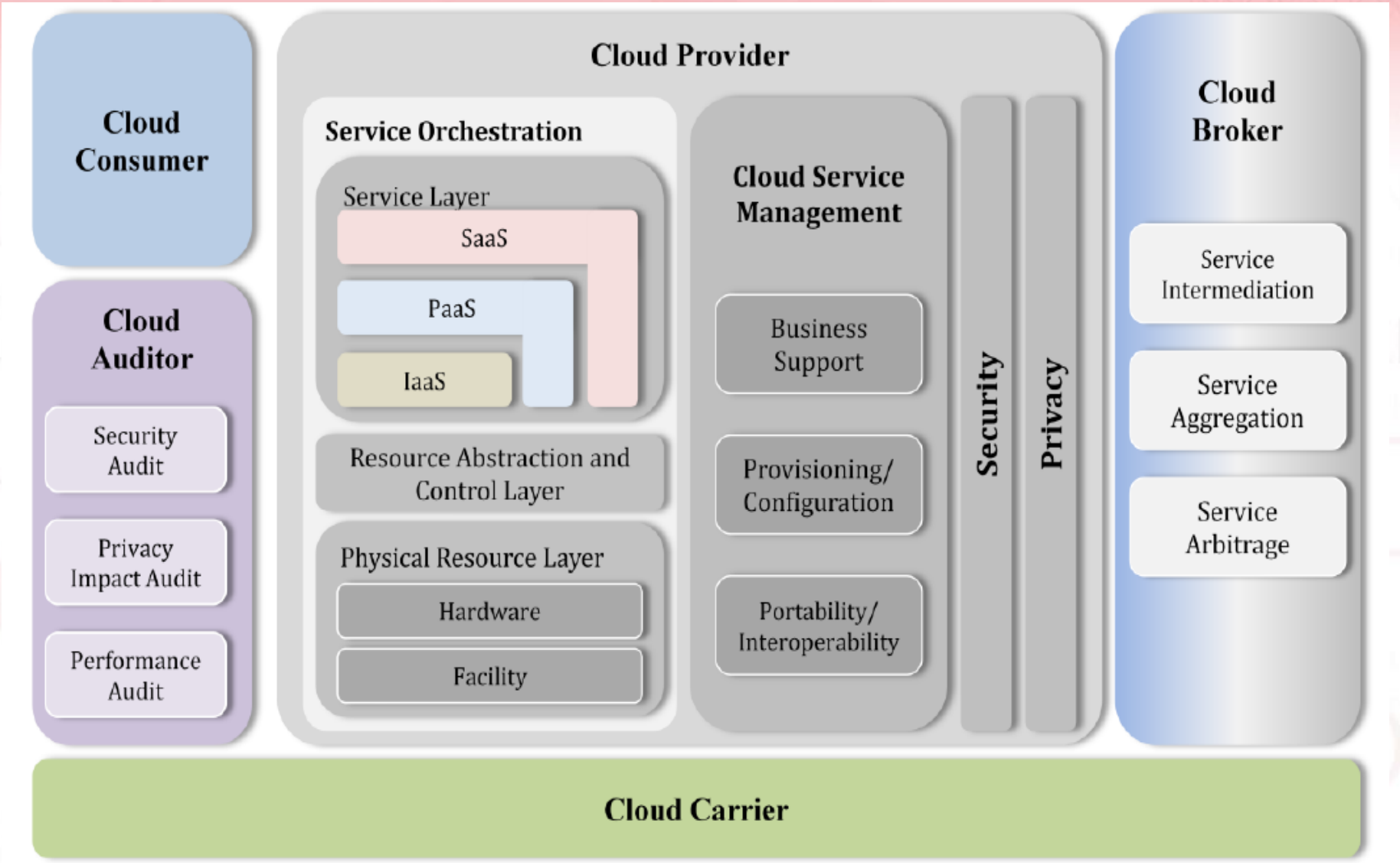
JECRC UNIVERSITY
BUILD YOUR WORLD

- Cloud Characteristics
- Service Models
  - SaaS
  - IaaS
  - PaaS
- Deployment Models
  - Public
  - Private
  - Community
  - Hybrid

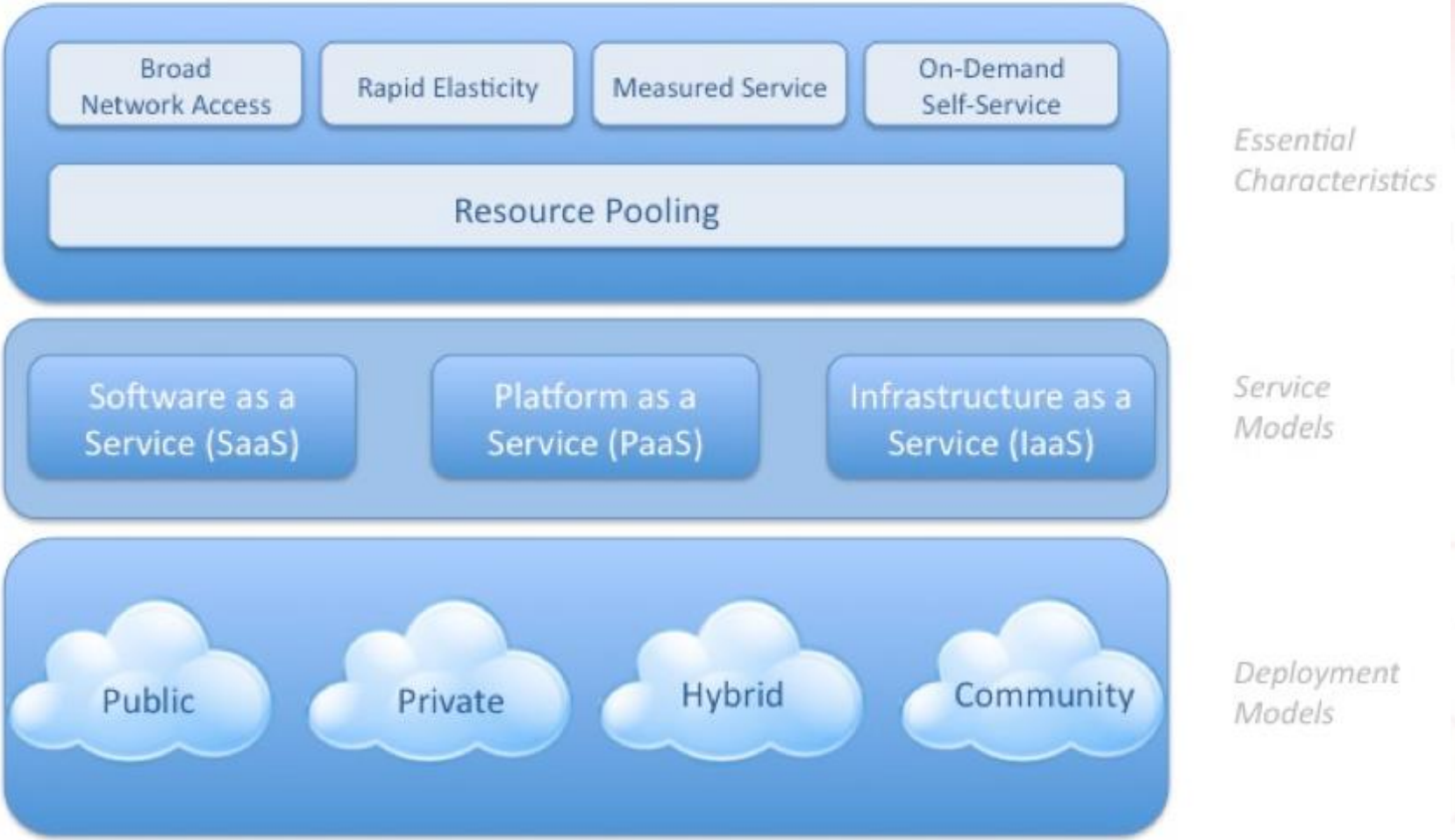
JECRC Foundation

NIST(National Institute of Standards and Technology) reference architecture

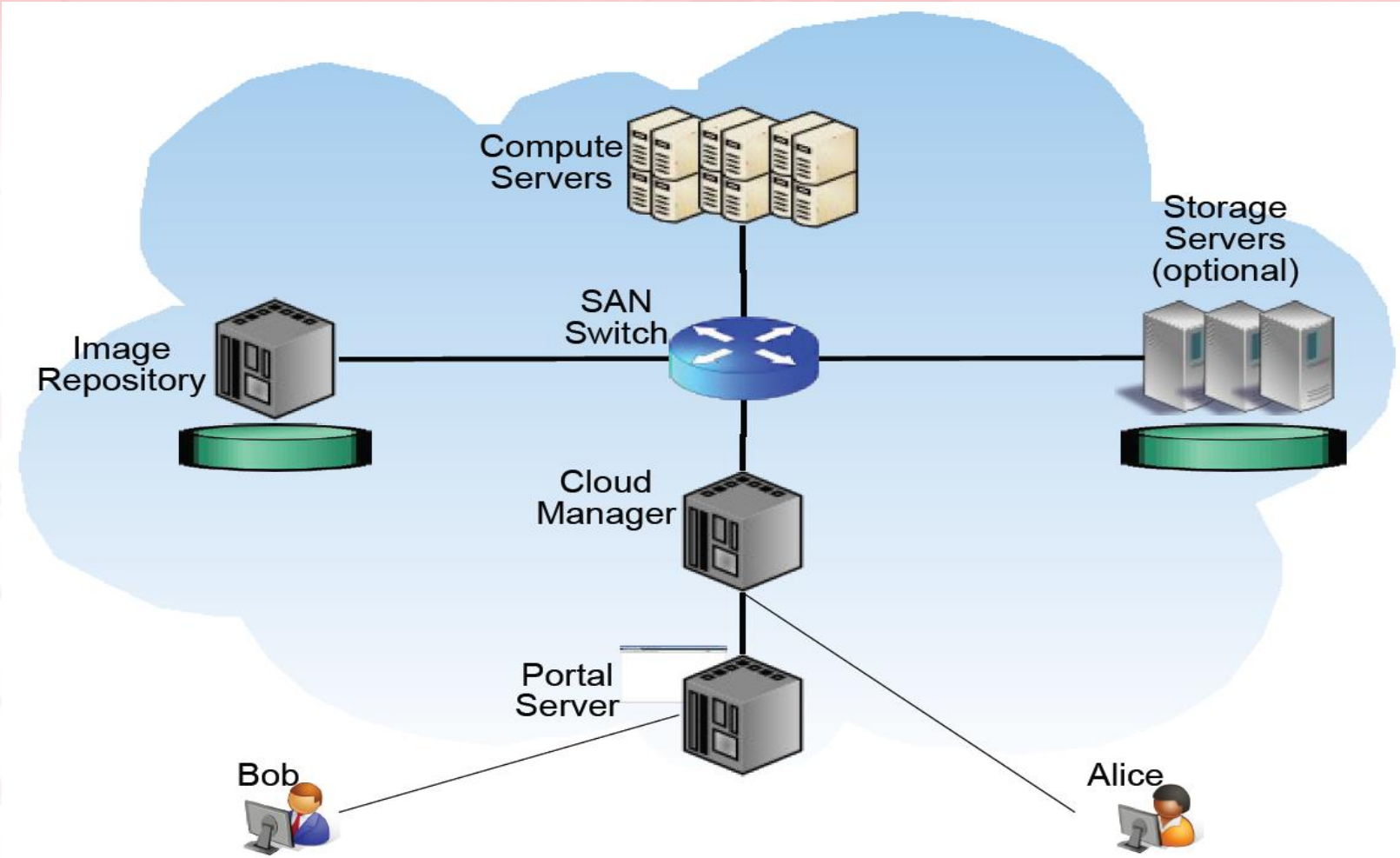
JECRC UNIVERSITY
BUILD YOUR WORLD



Cloud Characteristics



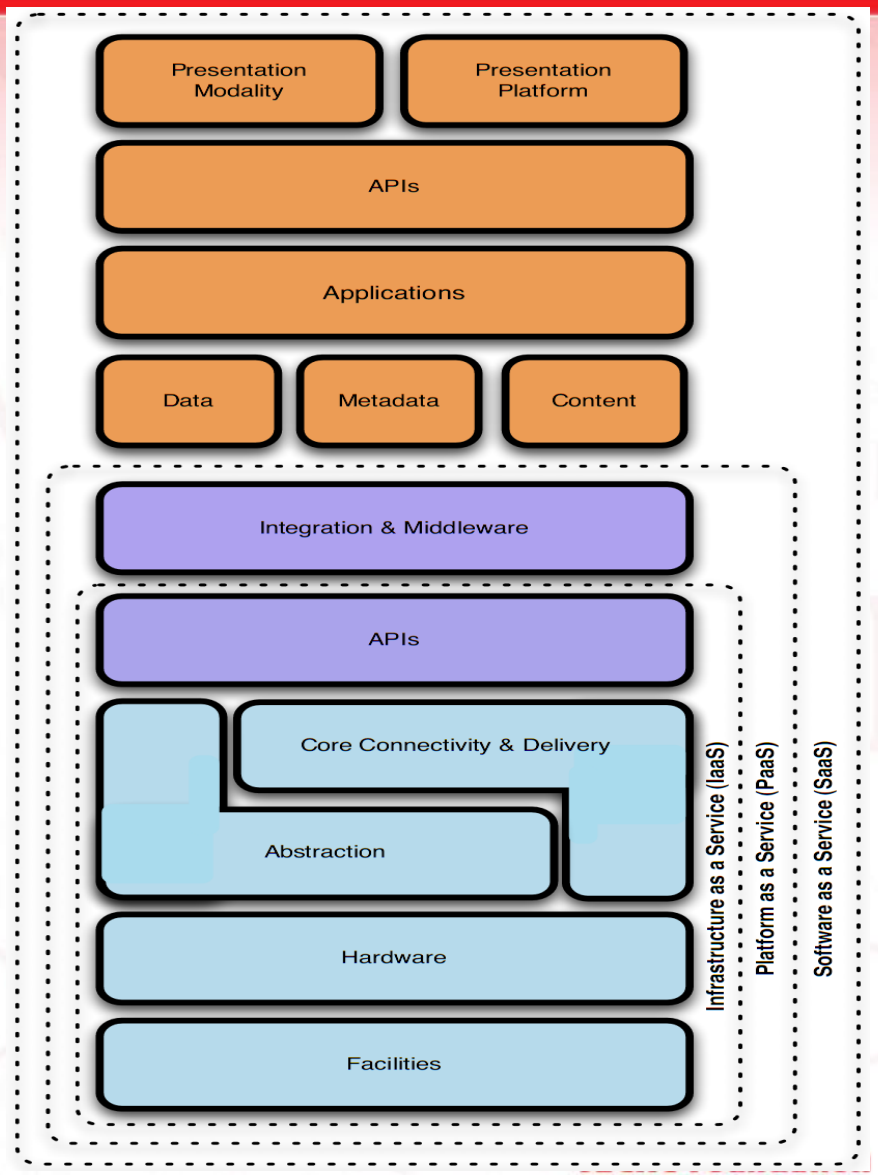
JECRC UNIVERSITY
BUILD YOUR WORLD
JECRC Foundation


Compute Servers
Storage Servers (optional)
SAN Switch
Image Repository
Cloud Manager
Portal Server
Bob
Alice

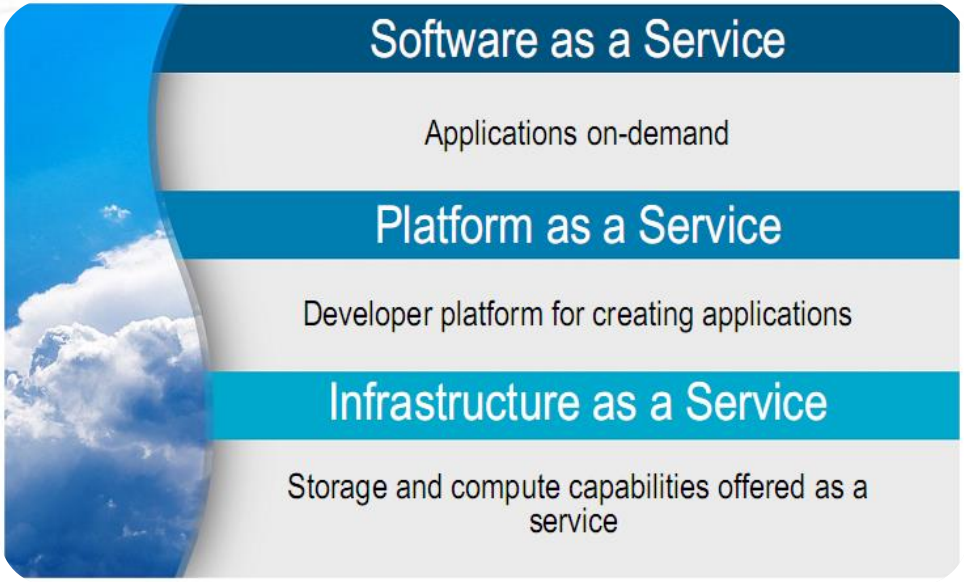
Actor	Definition
Cloud Consumer	A person or organization that maintains a business relationship with, and uses service from, *Cloud Providers*.
Cloud Provider	A person, organization, or entity responsible for making a service available to interested parties.
Cloud Auditor	A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.
Cloud Broker	An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between *Cloud Providers* and *Cloud Consumers*.
Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from *Cloud Providers* to *Cloud Consumers*.

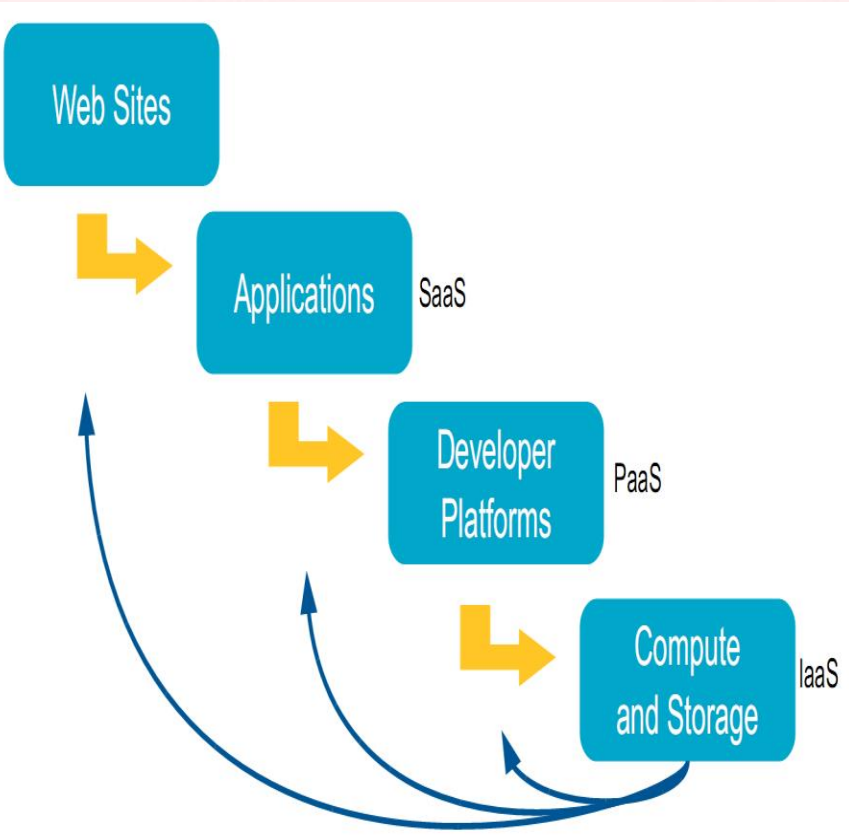
Cloud Service Models

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



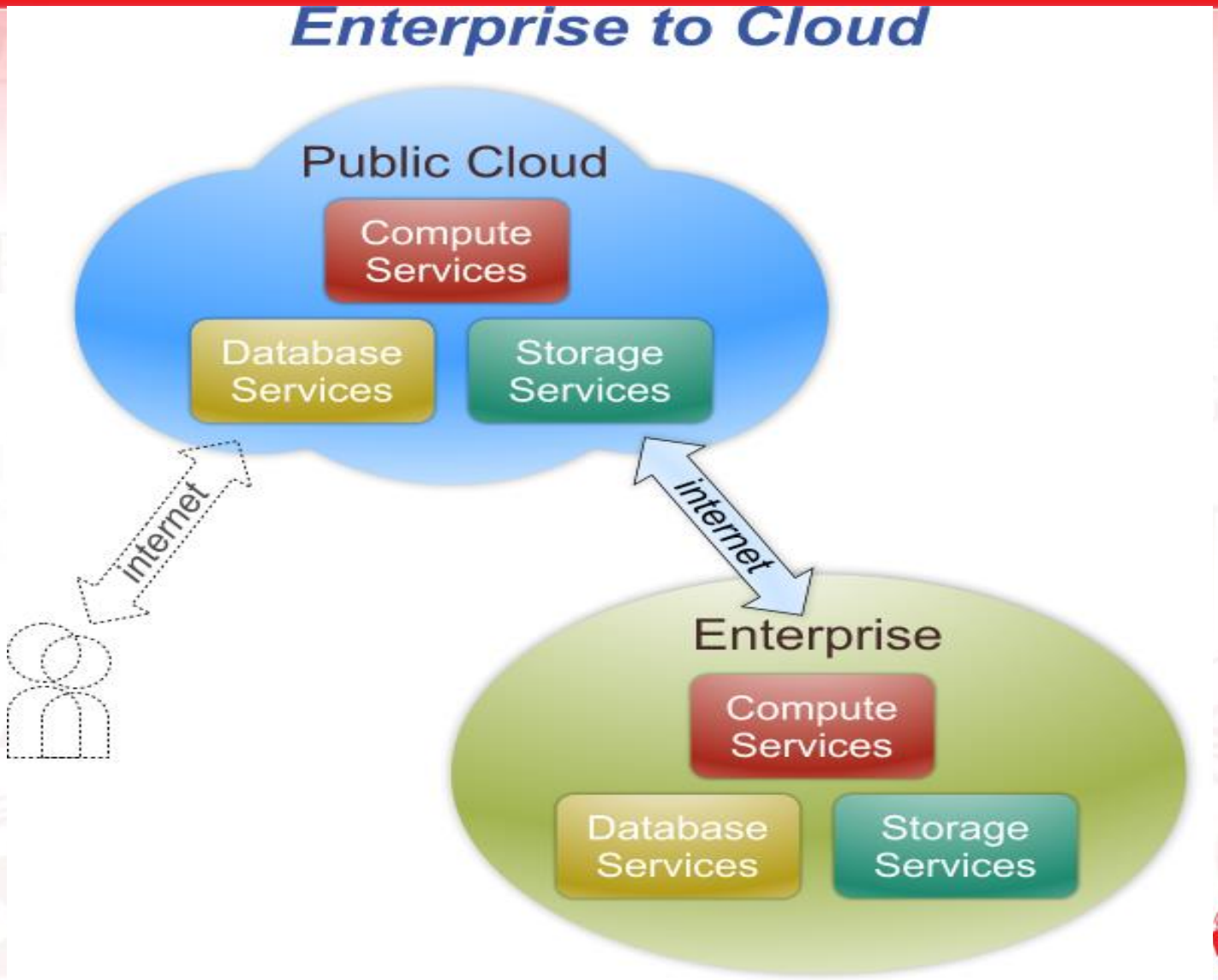
Natural Evolution of the Web





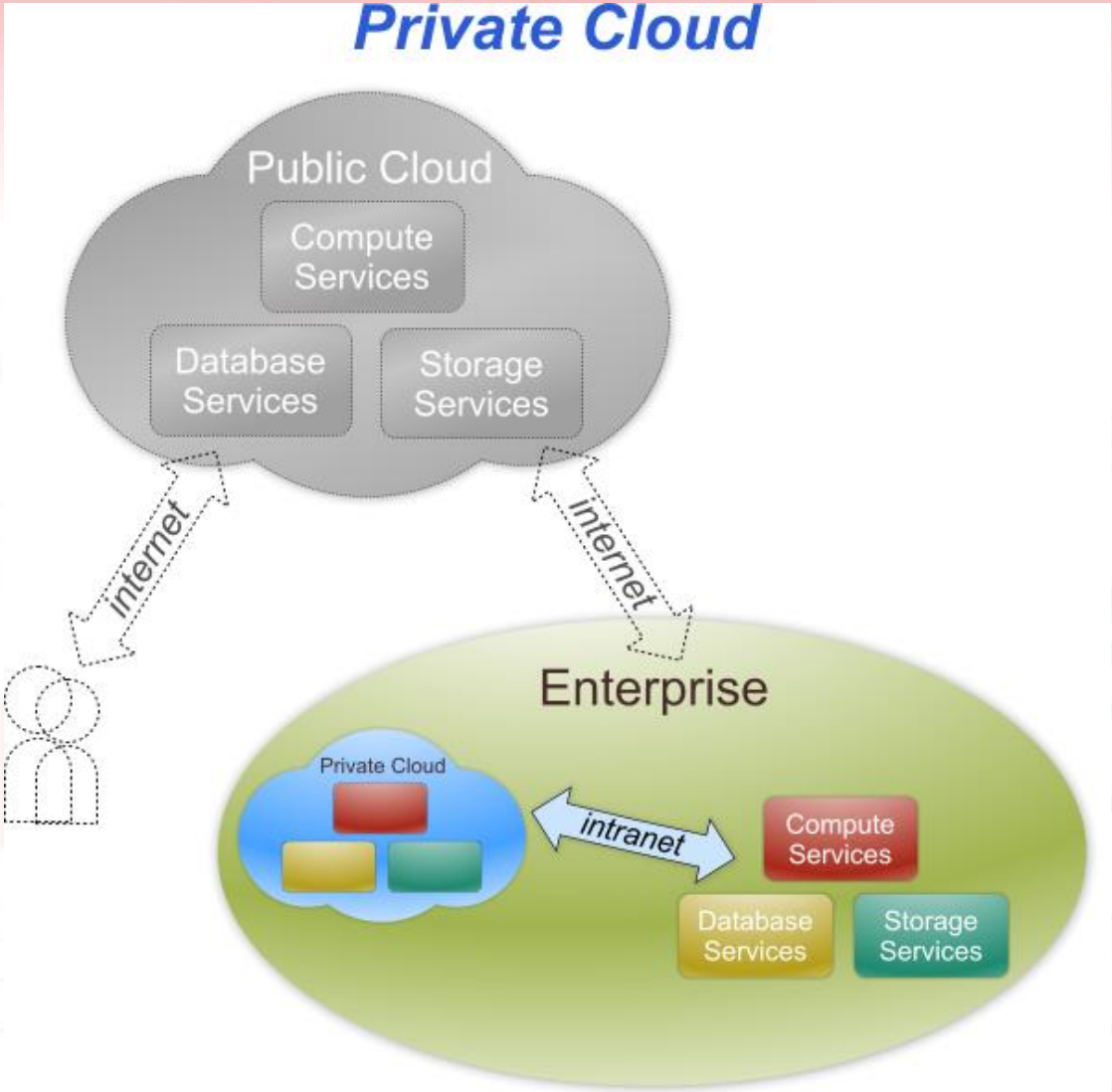
JECRC UNIVERSITY
BUILD YOUR WORLD
JECRC Foundation

Four Deployment Models



BY-SA

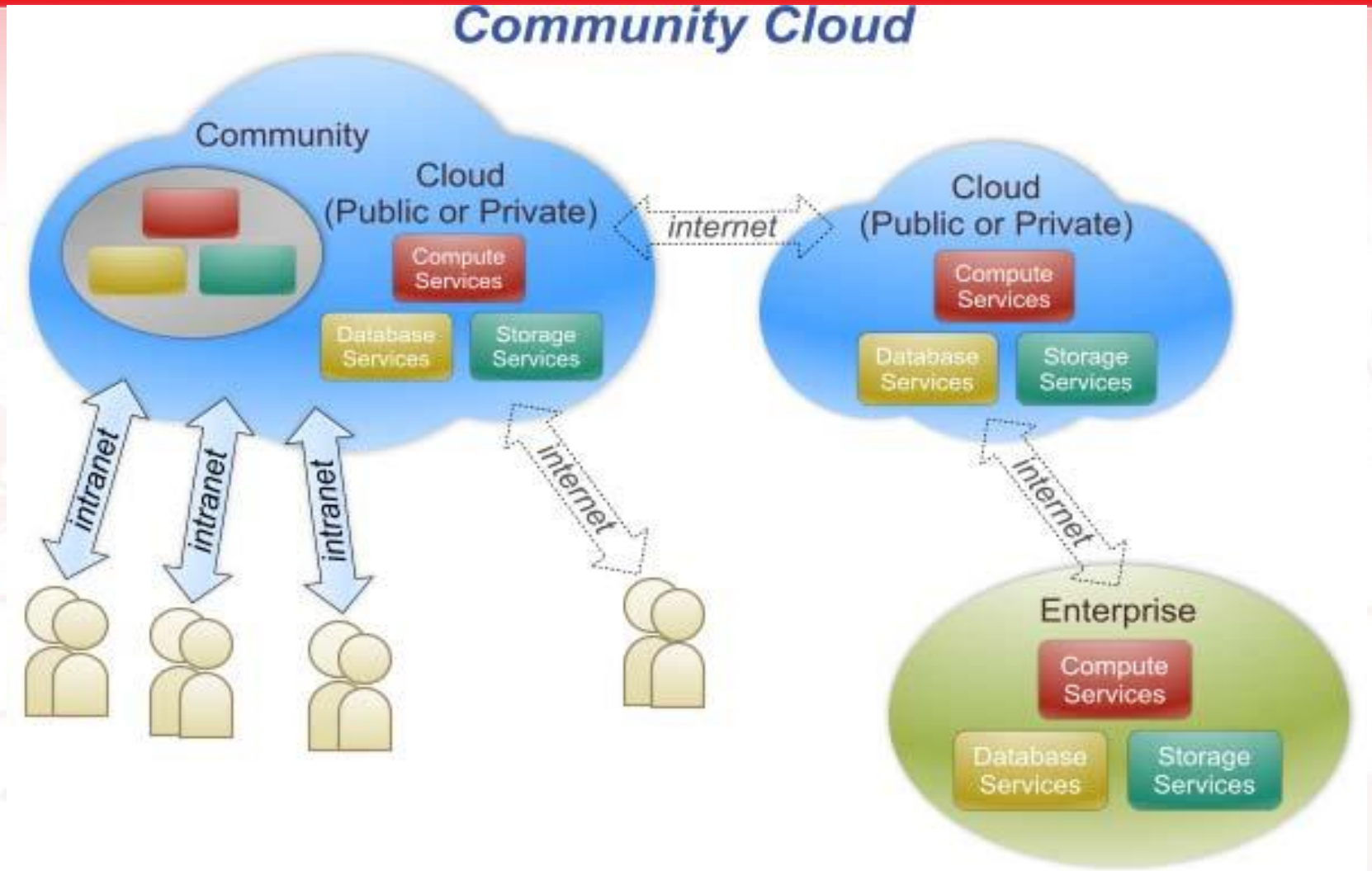
Four Deployment Models



BY-SA

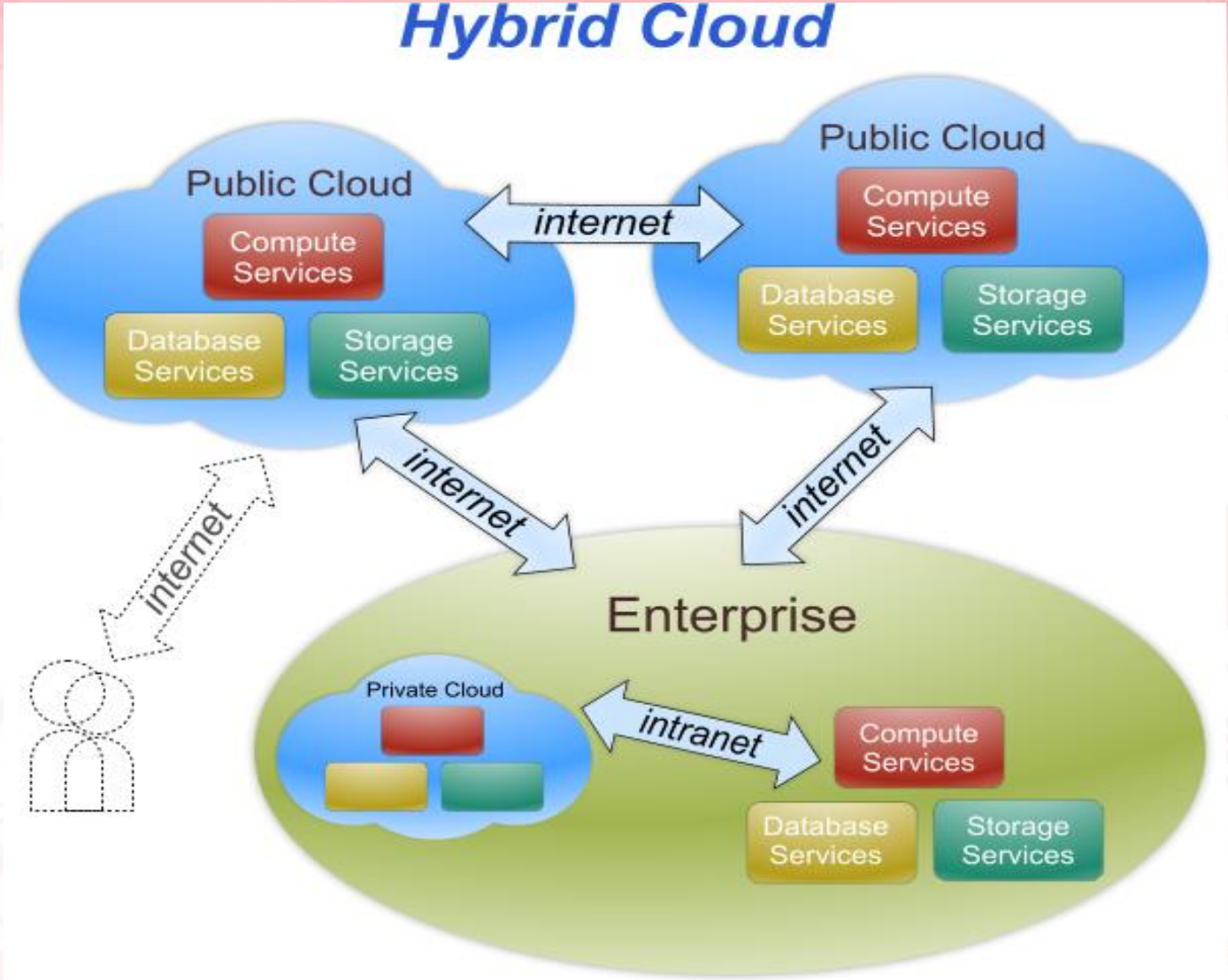
JECRC UNIVERSITY
BUILD YOUR WORLD
JECRC Foundation

Four Deployment Models



BY-SA

Four Deployment Models



BY-SA

Standard:Why?

- Standards promote interoperability, reducing vendor lock-in
- Standards facilitate hybrid cloud computing by making it easier to integrate on-premises security technologies with those of cloud service providers (CSPs)
- Standards provide assurance that best practices are being followed both internally within an enterprise and by CSPs
- Standards support provides an effective means by which cloud service customers can compare and contrast CSPs
- Standards support enables an easier path to regulatory compliance

Cloud security standards - maturing

- Different *types* of standards need to be considered
- Formal standards specific to cloud security already published

General IT security standards applicable to cloud computing

- Insist that cloud service providers support these

Cloud service customers: insist on security certifications from providers

- Cloud specific security certifications available today (emerging)
- Existing general security certifications are applicable

Advisory Standards
▪ Interpreted and applied to all types and sizes of organizations ▪ Flexibility: latitude to adopt information security controls that make sense to users ▪ Unsuitable for compliance testing
Examples
ISO 27002, ISO 38500, COBIT

Security Frameworks
▪ Define specific policies, controls, checklists, procedures ▪ Define processes for examining support - auditors use to assess & measure CSP conformance ▪ Suitable for compliance testing
Examples
ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018

Standards Specifications
▪ Define APIs and protocols ▪ Extensibility - optional functions that go beyond those defined in standard ▪ Formal certifications not provided - compliance and interoperability test suites may be available
Examples
OAuth 2.0, SAML 2.0, SSL/TLS, X.509

10 Steps to Evaluate Cloud Security

1. Ensure effective governance, risk & compliance
2. Audit operational & business processes
3. Manage people, roles & identities
4. Ensure proper protection of data & information
5. Enforce privacy policies
6. Assess the security provisions for cloud applications
7. Ensure cloud networks & connections are secure
8. Evaluate security controls on physical infrastructure & facilities
9. Manage security terms in the cloud service agreement
10. Understand the security requirements of the exit process

Step 1: Ensure effective governance, risk and compliance

GRC Requirements

- Cloud computing presents different risks than traditional IT solutions
- Customers must understand their risk tolerance and must focus on mitigating the risks that are most crucial to the organization
- Customers must fully understand specific laws or regulations that apply to the services (data retention, privacy requirements, etc.)
- Customers should be notified if any breach occurs regardless if the customer is directly impacted
- Primary means to ensure application and data security is through Cloud Service Agreement
- **General IT governance standards apply to cloud**
- **Country & industry specific governance standards also apply**

General IT Governance Standards

Country / Industry Standards

Step 2: Audit operational & business processes

Audit Requirements

- Security audit of cloud service providers is essential
- Security audits should be carried out by appropriately skilled staff
- Security audits should leverage an established standard for security controls
- Typically done as part of a formal certification process
- **Insist on ISO/IEC 27001 and ISO/IEC 27017 or equivalent certification**
- **For cloud services with impact on financial activities seek SSAE 16 certification**

- ISO-27001 holds identification for Information Security Management System (ISMS).
- This is useful when the project is in its starting phase or if you can't commit to full implementation of the project.
- ISO-27002 it exhibits that the organization follows information security seriously and is eligible to do best practices to secure data.

JECRC Foundation

Step 3: Manage people, roles & identities

Considerations

- Cloud service provider should support:
  - Federated identity management
  - Delegated user administration
  - Single sign-on
  - Strong, multi-factor, mutual and/or even biometric authentication
  - Role, entitlement and policy management
  - Identity & Access audit
- Any access to the provider's management platform should be monitored and logged
- **Several standards available for federated IDs, single sign-on and access control**

SCIM

OASIS

WS-Federation

Step 4: Ensure proper protection of data & information

Considerations

- Security considerations apply to data at rest as well as data in motion
- Controls for securing data in the cloud:
  - Create a data asset catalog
  - Consider all forms of data
  - Consider privacy requirements
  - Apply confidentiality, integrity and availability principles
  - Apply identify and access management
- **Seek security standards for control framework, data in motion and data encryption**

Control Standards

Data In Motion Standards

Data Encryption Standards

Step 5: Enforce policies for Protection of Personal Data

Considerations

- "Privacy": acquisition, storage, use of personally identifiable information (PII)
  - Gaining importance
  - Law and regulations usually apply
- Privacy requirements include:
  - Limitations on use of and access to PII
  - Tagging PII data correctly
  - Securing storage of PII
  - Limiting access to authorized users
- Specific types of PII require special treatment
  - **Health data: HIPAA**
  - **Credit card data: PCI-DSS**
- Privacy issues should be addressed in CSA
  - **ISO/IEC 19086 Cloud SLAs**
- **Required controls specified in ISO/IEC 27018**

ISO
ISO/IEC 27018

EU-US Privacy Shield

GDPR
EU General Data Protection Regulation

HIPAA
Health Insurance Portability & Accountability Act

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

PCI DSS COMPLIANT

Step 6: Assess the security provisions for cloud applications

Considerations

- Application security in cloud environment over complete lifecycle
  - **Secure development, secure deployment (OWASP, ISO 27034)**
  - **Security testing (NIST 800-115)**
- Deployment model impacts application security
  - Infrastructure as a Service
    - Customer responsible for majority of security components
  - Platform as a Service
    - Provider responsible to provide secure operating system, middleware, network
    - Customer responsible for application security
  - Software as a Service
    - Provider provides application security
    - Customer must understand data encryption standards, audit capabilities, SLAs

ISO 27034
Application Security

OWASP
Open Web Application Security Project

NIST
SP 800-115

Step 7: Ensure cloud networks & connections are secure

Considerations

- Customer should gain assurance on provider's internal and external network security
- Areas of concern
  - Confidentiality Integrity Availability
- External network requirements
  - Traffic screening
  - Intrusion detection / prevention
  - Logging and notification
- Internal network requirements
  - Protect clients from each other
  - Protect the provider's network
  - Monitor for intrusion attempts
- **ISO 27033 addresses network security**
- **NIST 800-53 R4 has useful controls**
- **FedRAMP specifies specific controls**

ISO 27033
Network Security

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Step 8: Evaluate security controls on physical infrastructure & facilities

Considerations

- Customer should gain assurance on provider's physical security
  - Physical infrastructure & facilities should be in a secure area
  - Protection against external & environmental threats
  - Control of personnel in working areas
  - Equipment security controls
  - Controls on supporting utilities
  - Control security of cabling
  - Proper equipment maintenance
  - Removal & disposal of assets
  - Human resource security
  - DR & BC plans in place
- **Look for certification to ISO/IEC 27002 standard**
- **ANSI TIA-942 covers physical security**

ISO 27002

Security Techniques: Code of Practice for Information Security Controls

TIA-942

Step 9: Manage security terms in the cloud service agreement (CSA)

Considerations

- Understand who is responsible for what (provider or customer)
- CSA should specify that (and how) customer is notified of security incidents
- CSA must also cover recovery measures and customer compensation
- Security clauses in the CSA apply to cloud provider as well as its subcontractors
- SLAs must include metrics for performance and effectiveness of information security management (see **ISO/IEC 27004 and 19086, NIST 800-55 and CIS Consensus Metrics**)
- Data protection should follow **ISO/IEC 27018**
- Require compliance reports to covering security controls, services and mechanisms
- **ISO/IEC 27017 specializes ISO/IEC 27002 to the cloud**

ISO/IEC 19086
ISO/IEC 27004
ISO/IEC 27017
ISO/IEC 27018

SP 800-55

CIS Consensus Metrics 1.1.0

Common Weakness Enumeration

STAR Registry

TR178

Step 10: Understand the security requirements of the exit process

Considerations

- Once termination process is complete, "the right to be forgotten" should be achieved
- No customer data should reside with provider after the exit process
- Require provider to cleanse log and audit data
    - Some jurisdictions may require retention of records of this type for specified periods by law
- Exit process must allow customer a smooth transition without loss or breach of data
- **The emerging ISO/IEC 19086 standard contains language on the exit process**

ISO/IEC 19086
Cloud Computing – Service Level Agreement Framework

Cloud Security Certifications

Certification

- Means by which provider demonstrates conformance to standard / specification
  - Typically for specific services
- Certificate typically issued via third-party auditor
  - Belongs to certification organization
  - Certification issued on regular basis
- Certification organization in turn accredited by national body
  - Establish skill & procedure requirements for audits

Relevant certifications

- ISO/IEC 27001 & ISO/IEC 27018 (information security)
- ISO/IEC 27018 (privacy)
- TRUSTe Safe Harbor (privacy)


BUREAU VERITAS
Certification

Certification
Awarded to

IBM Global Technology Services - Global Managed Cloud Services

This is a multi-site certificate, site details are listed in the appendix to this certificate

Bureau Veritas Certification certify that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below

Standards

ISO/IEC 27001:2005

Scope of certification

The planning, design, implementation and operation of IBM SmartCloud Services, including SmartCloud Enterprise (SCE) and SmartCloud Enterprise Plus (SCE+), using local and global capabilities.

Statement of Applicability RE-0317 rev 5, dated 08 May 2013

Certification cycle start date: 1 JUNE 2012

Subject to the continued satisfactory operation of the organisation's Management System, this certificate expires on: 31 MAY 2015

Original certification date: 1 JUNE 2012

Certificate No. IND12.2523U
File No. 6028947

Version 2, Revision date: 24 June 2013

Jacques Mallion
Managing Director

Page 1 of 2

AVAILABILITY MANAGEMENT

"In practice, availability management is the art of meeting a company's needs in a cost-effective way. This involves managing users' expectations almost as much as the technology."

The Information Technology Infrastructure Library(ITIL) Availability Management

JECRC UNIVERSITY
BUILD YOUR WORLD

- Cloud providers should utilize numerous technologies such as autoscaling and bursting, redundancy, failover, disaster recovery, data replication, and multiple datacenters to ensure system availability.
- Inclusion of availability statistics should be included in the cloud management portal for customer visibility.
- The expectation is that a cloud provider should never intentionally or accidentally have all systems offline and unavailable to its customers.

JECRC Foundation

what comprises availability management from the ISO/IEC 20000 standard:

JECRC UNIVERSITY
BUILD YOUR WORLD

- Assessing and documenting risks to service availability at regular intervals
- Determining and documenting service availability requirements and targets, by considering relevant business requirements, service requirements, SLAs, and risks
- Monitoring and recording service availability results and comparing to targets
- Investigating and addressing instances of unplanned non-availability

JECRC Foundation

Monitoring and measurement of availability

JECRC UNIVERSITY
BUILD YOUR WORLD

The success of availability management at a service level will be measured by two main metrics:

- **Mean time to restore service (MTRS):** How quickly your company addresses non-availability, e.g. 4 hours

- **Mean time between failures (MTBF):** The frequency of non-availability, e.g. twice a year

JECRC Foundation

The Availability Manager role

JECRC UNIVERSITY
BUILD YOUR WORLD

- Architecture design
- Problem management
- Information security strategy development
- Information security management
- The data administrator role
- The DevOps expert role

IaaS Availability Management:

IaaS Providers Availability Considerations include computing and building Storage Infrastructure. Other services such as account management, a message queue service, an identity and authentication service, a database service, a billing service, and monitoring services. Customer Responsibility for the IaaS are to provision and manage the life cycle of virtual servers.

JECRC Foundation

Availability Management Activities:

JECRC UNIVERSITY
BUILD YOUR WORLD

Availability Management process includes two types of activities:

- Reactive
- Proactive.

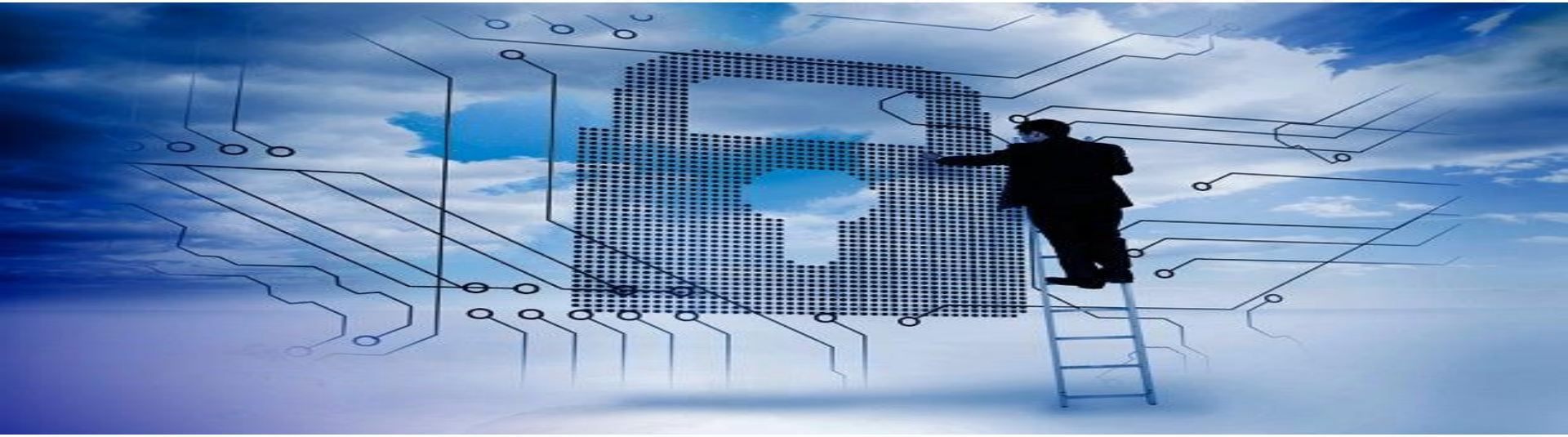
Reactive Activities: Reactive Availability Management includes activities such as monitoring, measuring, analysis and management of all events, incidents, and problems causing service unavailability. These activities are generally performed by operational roles.

Proactive Activities: Proactive Availability Management includes proactive planning, design, and monitoring of services to improve the availability. These activities are typically performed by design and planning roles.

JECRC Foundation

Securing the Cloud

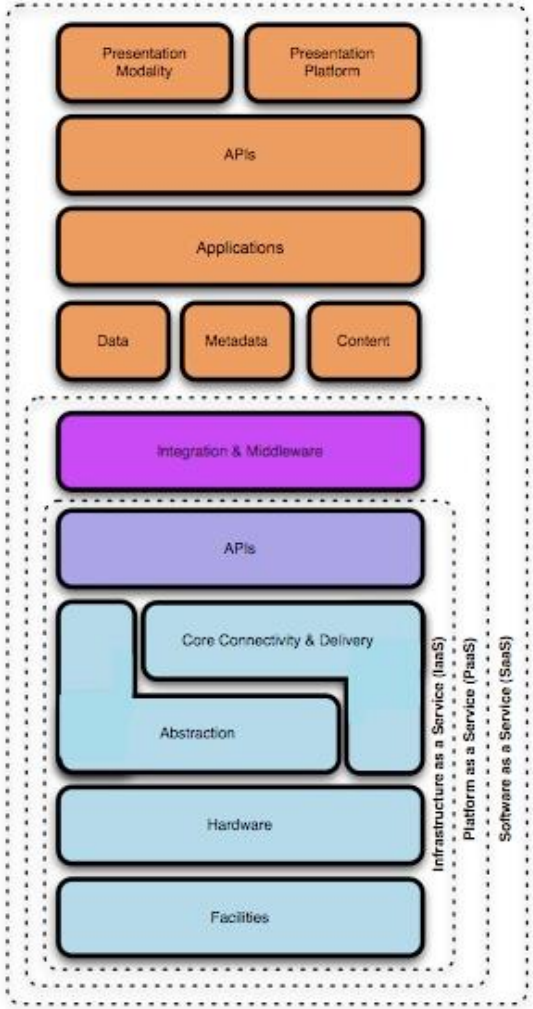
- Security Interaction Model
- Top Security Threats/Model
- Cloud Provider Security Practices – Google Case Study



Security Interaction Model

JECRC UNIVERSITY
BUILD YOUR WORLD

Cloud Model



Find the Gaps!

Security Control Model

Applications	SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
Information	DLP, CMF, Database Activity Monitoring, Encryption
Management	GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
Network	NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
Trusted Computing	Hardware & Software RoT & API's
Compute & Storage	Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking
Physical	Physical Plant Security, CCTV, Guards

Compliance Model

PCI

- ☑ Firewalls
- ☑ Code Review
- ☑ WAF
- ☑ Encryption
- ☑ Unique User IDs
- ☑ Anti-Virus
- ☑ Monitoring/IDS/IPS
- ☑ Patch/Vulnerability Management
- ☑ Physical Access Control
- ☑ Two-Factor Authentication...

HIPAA

GLBA

SOX

Threat Model

• A threat model helps in analyzing a security problem, design mitigation strategies, and evaluate solutions

•Steps:

Identify attackers, assets, threats and other components

Rank the threats

Choose mitigation strategies

Build solutions based on the strategies

Threat Model

Basic components

- Attacker modeling
  - Choose what attacker to consider
    - insider vs. outsider?
    - single vs. collaborator?
  - Attacker motivation and capabilities
- Attacker goals
- Vulnerabilities / threats

What is the issue?

The core issue here is the levels of trust

- Many cloud computing providers trust their customers
- Each customer is physically commingling its data with data from anybody else using the cloud while logically and virtually you have your own space
- The way that the cloud provider implements security is typically focused on they fact that those outside of their cloud are evil, and those inside are good.

- But what if those inside are also evil?

Attacker Capability: Malicious Insiders

- At client
  - Learn passwords/authentication information
  - Gain control of the VMs
- At cloud provider
  - Log client communication
  - Can read unencrypted data
  - Can possibly peek into VMs, or make copies of VMs
  - Can monitor network communication, application patterns

Why?

- Gain information about client data
- Gain information on client behavior
- Sell the information or use itself

Attacker Capability: Outside attacker

- What?
  - Listen to network traffic (passive)
  - Insert malicious traffic (active)
  - Probe cloud structure (active)
  - Launch DoS
- Goal?
  - Intrusion
  - Network analysis
  - Man in the middle
  - Cartography-A scheme for pinpointing the physical locations of Web servers hosted on a third-party cloud computing service.

Challenges for the attacker

- How to find out where the target is located?
- How to be co-located with the target in the same (physical) machine?
- How to gather information about the target?

Vulnerabilities in Cloud Computing

JECRC UNIVERSITY
BUILD YOUR WORLD

ID	Vulnerabilities	Description	Layer
V01	Insecure interfaces and APIs	Cloud providers offer services that can be accessed through APIs (SOAP, REST, or HTTP with XML/JSON) [65]. The security of the cloud depends upon the security of these interfaces [40]. Some problems are: a) Weak credential b) Insufficient authorization checks c) Insufficient input-data validation Also, cloud APIs are still immature which means that are frequently updated. A fixed bug can introduce another security hole in the application [76].	SPI
V02	Unlimited allocation of resources	Inaccurate modeling of resource usage can lead to overbooking or over-provisioning [41].	SPI
V03	Data-related vulnerabilities	a) Data can be colocated with the data of unknown owners (competitors, or intruders) with a weak separation [59] b) Data may be located in different jurisdictions which have different laws [43][76][77] c) Incomplete data deletion – data cannot be completely removed [43][44][49][78] d) Data backup done by untrusted third-party providers [78][79] e) Information about the location of the data usually is unavailable or not disclosed to users [49] f) Data is often stored, processed, and transferred in clear plain text	SPI

ID	Vulnerabilities	Description	Layer
V04	Vulnerabilities in Virtual Machines	a) Possible covert channels in the colocation of VMs [70][80][81] b) Unrestricted allocation and deallocation of resources with VMs [79] c) Uncontrolled Migration - VMs can be migrated from one server to another server due to fault tolerance, load balance, or hardware maintenance [65][67] d) Uncontrolled snapshots – VMs can be copied in order to provide flexibility [53], which may lead to data leakage e) Uncontrolled rollback could lead to reset vulnerabilities - VMs can be backed up to a previous state for restoration [67], but patches applied after the previous state disappear f) VMs have IP addresses that are visible to anyone within the cloud - attackers can map where the target VM is located within the cloud (Cloud cartography [80])	I
V05	Vulnerabilities in Virtual Machine Images	a) Uncontrolled placement of VM images in public repositories [48] b) VM images are not able to be patched since they are dormant artifacts [67]	I
V06	Vulnerabilities in Hypervisors	a) Complex hypervisor code [82] b) Flexible configuration of VMs or hypervisors to meet organization needs can be exploited	I
V07	Vulnerabilities in Virtual Networks	Sharing of virtual bridges by several virtual machines [73]	I

Threats in Cloud Computing

JECRC UNIVERSITY
BUILD YOUR WORLD

ID	Threats	Description	Layer
T01	Account or service hijacking	An account theft can be performed by different ways such as social engineering and weak credentials. If an attacker gains access to a user's credential, he can perform malicious activities such as access sensitive data, manipulate data, and redirect any transaction [40].	SPI
T02	Data scavenging	Since data cannot be completely removed from unless the device is destroyed, attackers may be able to recover this data [41][49][39].	SPI
T03	Data leakage	Data leakage happens when the data gets into the wrong hands while it is being transferred, stored, audited or processed [40][41][44][80].	SPI
T04	Denial of Service	It is possible that a malicious user will take all the possible resources. Thus, the system cannot satisfy any request from other legitimate users due to resources being unavailable.	SPI
T05	Customer-data manipulation	Users attack web applications by manipulating data sent from their application component to the server's application [44][55]. For example, SQL injection, command injection, insecure direct object references, and cross-site scripting.	S

JECRC Foundation

Threats in Cloud Computing

JECRC UNIVERSITY
BUILD YOUR WORLD

T06	VM escape	It is designed to exploit the hypervisor in order to take control of the underlying infrastructure [48][83].	I
T07	VM hopping	It happens when a VM is able to gain access to another VM (i.e by exploting some hypervisor vulnerability) [41][66]	I
T08	Malicious VM creation	An attacker who creates a valid account can create a VM image containing malicious code such as a Trojan horse and store it in the provider repository [44].	I
T09	Insecure VM migration	Live migration of virtual machines exposes the contents of the VM state files to the network. An attacker can do the following actions: a) Access data illegally during migration [65] b) Transfer a VM to an untrusted host [67] c) Create and migrate several VM causing disruptions or DoS	I
T10	Sniffing/Spoofing virtual networks	A malicious VM can listen to the virtual network or even use ARP spoofing to redirect packets from/to other VMs [68][73].	I

JECRC Foundation

Relationships between Threats, Vulnerabilities, and Countermeasures

JECRC UNIVERSITY
BUILD YOUR WORLD

Threat	Vulnerabilities	Incidents	Countermeasures
T01	V01	An attacker can use the victim's account to get access to the target's resources.	Identity and Access Management Guidance [86] Dynamic credential [87]
T02	V03a, V03c	Data from hard drives that are shared by several customers cannot be completely removed.	Specify destruction strategies on Service-level Agreements (SLAs)
T03	V03a, V03c, V03d, V03f, V04a-f, V05a, V07	Authors in [80] illustrated the steps necessary to gain confidential information from other VMs co-located in the same server as the attacker. Side channel [88]	FRS techniques [89] Digital Signatures [90] Encryption [88] Homomorphic encryption [91]
T04	V01, V02	An attacker can request more computational resources, so other legal users are not able to get additional capacity.	Cloud providers can force policies to offer limited computational resources
T05	V01	Some examples are described in [55] such as SQL, command injection, and cross-site scripting	Web application scanners [92]
T06	V06a, V06b	A zero-day exploit in the HyperVM virtualization application that destroyed about 100,000 websites [93]	HyperSafe [82] TCCP (Trusted Cloud Computing Platform) [84] TVDc (Trusted Virtual Datacenter) [94][95]
T07	V04b, V06b	[96] presents a study that demonstrates security flaws in most virtual machines monitors	
T08	V05a, V05b	An attacker can create a VM image containing malware and publish it in a public repository.	Mirage [71]
T09	V04d	[97] has empirically showed attacks against the migration functionality of the latest version of the Xen and VMware virtualization products.	PALM [85] TCCP [84] VNSS [74]
T10	V07	Sniffing and spoofing virtual networks [73]	Virtual network framework based on Xen network modes:

Threats vs. Defenses

JECRC UNIVERSITY
BUILD YOUR WORLD

ID	Threats	Defense
T11	The cloud consumer is malicious and inserts malicious code into the VMI	Authenticator - Authorizer
T21	An external attacker listens to the network to obtain information about the VMI	Secure Channel
T22	VMI may be modified while in transit	Secure Channel
T23	Disavows sending a VMI	Security Logger/Auditor
T31	The IaaS administrator is malicious and collects information within the VMI	Authenticator - Authorizer
T32	The IaaS disavows receiving a VMI	Security Logger/Auditor
T33	Insert malicious code in the image	Authenticator - Authorizer
T41	The IaaS administrator stores a malicious VMI	Authorizer – Authorizer Filter

JECRC Foundation

Google Security Practices-Case Study

- Organizational and Operational Security
- Data Security
- Threat Evasion
- Safe Access
- Privacy

Google Organizational and Operational Security

- Holistic approach to security
- Security team
- Develop with security in mind
- Regularly performs security audits and threat assessments
- Employees screened, trained
- Works with security community and advisors

JECRC UNIVERSITY
BUILD YOUR WORLD
JECRC Foundation

Google Data Security

- Google Code of Conduct – “Don’t be evil.”
- Physical security
- Logical Security
- Accessibility
- Redundancy

JECRC UNIVERSITY
BUILD YOUR WORLD
JECRC Foundation

Google Threat Evasion

- Spam and virus protection built into products
- Protects against application & network attacks

JECRC UNIVERSITY
BUILD YOUR WORLD
JECRC Foundation

Google Safe Access

- Avoids local storage
- Access controls
- Encrypted connections
- Integrated security

JECRC UNIVERSITY
BUILD YOUR WORLD
JECRC Foundation

Google Privacy

- Privacy policy
- Does not access confidential user data
- Does not alter data
- Maintain own IP rights
- Indemnification, liability
- End of use

JECRC UNIVERSITY
BUILD YOUR WORLD
JECRC Foundation

Configuration management

JECRC UNIVERSITY
BUILD YOUR WORLD

- Cloud configuration is the action of configuring hardware and software settings for cloud-based elements to verify they will work together and communicate efficiently between them. Cloud configurations are based on one of the three major cloud provision elements: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

JECRC Foundation

Configuration management tools

JECRC UNIVERSITY
BUILD YOUR WORLD

- Software Configuration Management (SCM) is the management of a software project as it becomes a software product or system. This process encompasses the technical aspects, communication between business units, the overall organization of the project, and any changes to the project plan.

JECRC Foundation

Best configuration management tools

JECRC UNIVERSITY
BUILD YOUR WORLD

- **Ansible**: Software for automating provisioning, CM, and deployment of the application
- **Chef**: Platform for automating infrastructure into code; handles the configuration, deployment, and management of the infrastructure
- **Puppet**: Open source CM tool to handle your organization's IT inventory in your data center or cloud.
- **SaltStack**: Uses event-driven automation of compute, storage, and network complexities via time-saving configuration and control

JECRC Foundation

Infrastructure Security

1. Network Level

2. Host Level

3. Application Level

1. The Network Level

- Ensuring confidentiality and integrity of your organization's data-in-transit to and from your public cloud provider
- Ensuring proper access control (authentication, authorization, and auditing) to whatever resources you are using at your public cloud provider
- Ensuring availability of the Internet-facing resources in a public cloud that are being used by your organization, or have been assigned to your organization by your public cloud providers
- Replacing the established model of network zones and tiers with domains

The Network Level - Mitigation

- Note that network-level risks exist regardless of what aspects of “cloud computing” services are being used
- The primary determination of risk level is therefore not which *aaS is being used,
- But rather whether your organization intends to use or is using a public, private, or hybrid cloud.

2. The Host Level

- SaaS/PaaS

  Both the PaaS and SaaS platforms abstract and hide the host OS from end users

  Host security responsibilities are transferred to the CSP (Cloud Service Provider)

  - You do not have to worry about protecting hosts

  However, as a customer, you still own the risk of managing information hosted in the cloud services.

3. The Application Level

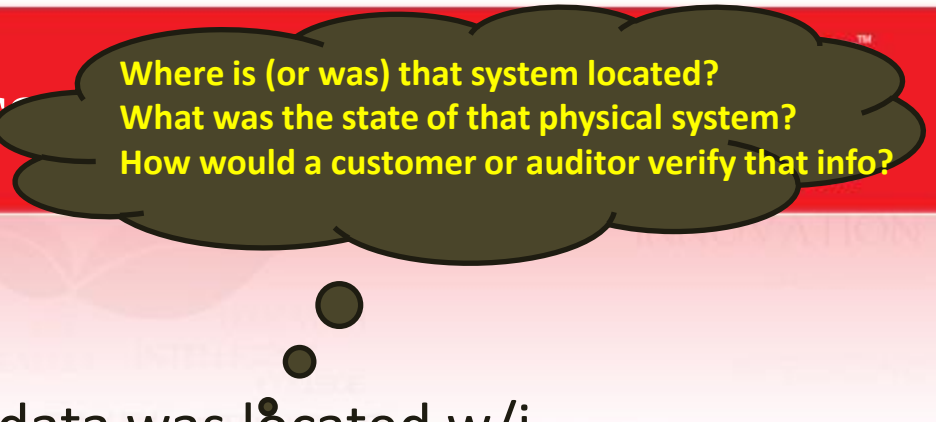
- DoS
- EDoS(Economic Denial of Sustainability)

  An attack against the billing model that underlies the cost of providing a service with the goal of bankrupting the service itself.
- End user security
- Who is responsible for Web application security in the cloud?
- SaaS/PaaS/IaaS application security
- Customer-deployed application security

Data Security and Storage

- Several aspects of data security, including:
  - Data-in-transit
    - Confidentiality + integrity using secured protocol
    - Confidentiality with non-secured protocol and encryption
  - Data-at-rest
    - Generally, not encrypted , since data is commingled with other users' data
    - Encryption if it is not associated with applications?
      - But how about indexing and searching?
      - Then homomorphic encryption vs. predicate encryption?
  - Processing of data, including multitenancy
    - For any application to process data, not encrypted

Data Security and Storage (c



- Data lineage
  - Knowing when and where the data was located w/i cloud is important for audit/compliance purposes
  - e.g., Amazon AWS
    - Store <d1, t1, ex1.s3.amazonaws.com>
    - Process <d2, t2, ec2.compute2.amazonaws.com>
    - Restore <d3, t3, ex2.s3.amazonaws.com>
- Data provenance
  - Computational accuracy (as well as data integrity)
  - E.g., financial calculation: sum ((((2*3)*4)/6) -2) = $2.00 ?
    - Correct : assuming US dollar
    - How about dollars of different countries?
    - Correct exchange rate?

JECRC Foundation

Data Security and Storage

- Data remanence

Inadvertent disclosure of sensitive information is possible

- Data security mitigation

Do not place any sensitive data in a public cloud

Encrypted data is placed into the cloud?

- Provider data and its security: storage

To the extent that quantities of data from many companies are centralized, this collection can become an attractive target for criminals

Why IAM?

- Organization's trust boundary will become dynamic and will move beyond the control and will extend into the service provider domain.
- Managing access for diverse user populations (employees, contractors, partners, etc.)
- Increased demand for authentication
  personal, financial, medical data will now be hosted in the cloud
  S/W applications hosted in the cloud requires access control
- Need for higher-assurance authentication
  authentication in the cloud may mean authentication outside F/W
  Limits of password authentication
- Need for authentication from mobile devices

Early this morning, at 3:30am PST, we started seeing elevated levels of authenticated requests from multiple users in one of our locations. While we carefully monitor our overall request volumes and these remained within normal ranges, we had not been monitoring the proportion of authenticated requests. Importantly, these cryptographic requests consume more resources per call than other request types.

Shortly before 4:00am PST, we began to see several other users significantly increase their volume of authenticated calls. The last of these pushed the authentication service over its maximum capacity before we could complete putting new capacity in place. In addition to processing authenticated requests, the authentication service also performs account validation on every request Amazon S3 handles. This caused Amazon S3 to be unable to process any requests in that location, beginning at 4:31am PST. By 6:48am PST, we had moved enough capacity online to resolve the issue.

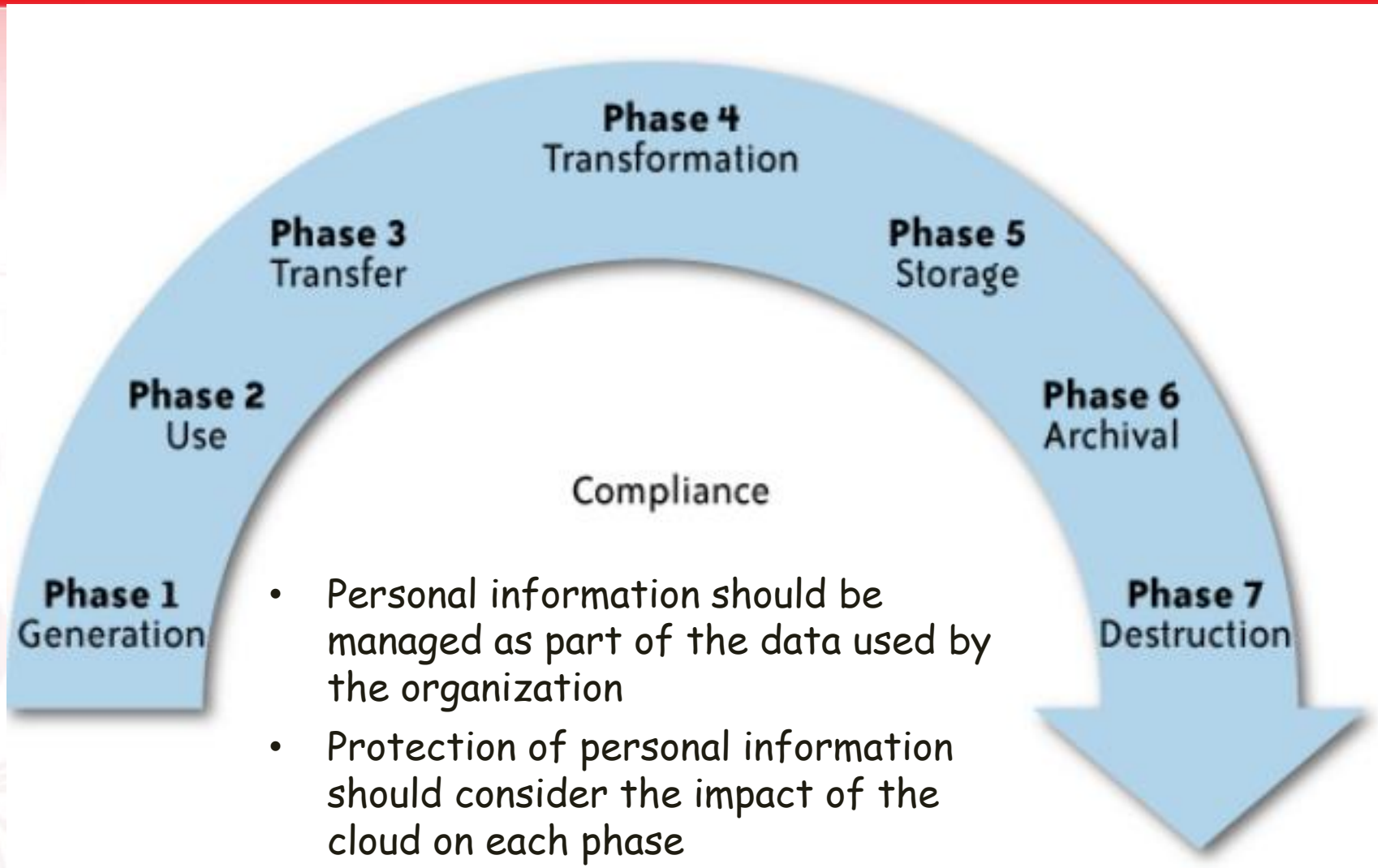
As we said earlier today, though we're proud of our uptime track record over the past two years with this service, any amount of downtime is unacceptable. As part of the post mortem for this event, we have identified a set of short-term actions as well as longer term improvements. We are taking immediate action on the following: (a) improving our monitoring of the proportion of authenticated requests; (b) further increasing our authentication service capacity; and (c) adding additional defensive measures around the authenticated calls. Additionally, we've begun work on a service health dashboard, and expect to release that shortly.

Privacy

What is Privacy?

- The concept of privacy varies widely among (and sometimes within) countries, cultures, and jurisdictions.
- It is shaped by public expectations and legal interpretations; as such, a concise definition is elusive if not impossible.
- Privacy rights or obligations are related to the collection, use, disclosure, storage, and destruction of personal data (or Personally Identifiable Information—PII).
- At the end of the day, privacy is about the accountability of organizations to data subjects, as well as the transparency to an organization's practice around personal information.

What is the data life cycle?



- Personal information should be managed as part of the data used by the organization
- Protection of personal information should consider the impact of the cloud on each phase

What Are the Key Privacy Concerns?

- Typically mix security and privacy
- Some considerations to be aware of:

1.Storage

2. Retention

3. Destruction

4. Auditing, monitoring and risk management

5. Privacy breaches

6. Who is responsible for protecting privacy?

1. Storage

- Is it commingled with information from other organizations that use the same CSP?
- The aggregation of data raises new privacy issues

  Some governments may decide to search through data without necessarily notifying the data owner, depending on where the data resides
- Whether the cloud provider itself has any right to see and access customer data?
- Some services today track user behaviour for a range of purposes, from sending targeted advertising to improving services

2. Retention

- How long is personal information (that is transferred to the cloud) retained?
- Which retention policy governs the data?
- Does the organization own the data, or the CSP?
- Who enforces the retention policy in the cloud, and how are exceptions to this policy (such as litigation holds) managed?

3. Destruction

- How does the cloud provider destroy PII at the end of the retention period?
- How do organizations ensure that their PII is destroyed by the CSP at the right point and is not available to other cloud users?
- Cloud storage providers usually replicate the data across multiple systems and sites—increased availability is one of the benefits they provide.

  How do you know that the CSP didn't retain additional copies?

  Did the CSP really destroy the data, or just make it inaccessible to the organization?

  Is the CSP keeping the information longer than necessary so that it can mine the data for its own use?

4. Auditing, monitoring and risk management

- How can organizations monitor their CSP and provide assurance to relevant stakeholders that privacy requirements are met when their PII is in the cloud?
- Are they regularly audited?
- What happens in the event of an incident?
- If business-critical processes are migrated to a cloud computing model, internal security processes need to evolve to allow multiple cloud providers to participate in those processes, as needed.

  These include processes such as security monitoring, auditing, forensics, incident response, and business continuity

5. Privacy breaches

- How do you know that a breach has occurred?
- How do you ensure that the CSP notifies you when a breach occurs?
- Who is responsible for managing the breach notification process (and costs associated with the process)?
- If contracts include liability for breaches resulting from negligence of the CSP?

  How is the contract enforced?

  How is it determined who is at fault?

6. Who is responsible for protecting privacy?

JECRC UNIVERSITY
BUILD YOUR WORLD

- Data breaches have a cascading effect
- Full reliance on a third party to protect personal data?
- In-depth understanding of responsible data stewardship
- Organizations can transfer liability, but not accountability
- Risk assessment and mitigation throughout the data life cycle is critical.

e.g., Suppose a hacker breaks into Cloud Provider A and steals data from Company X.
Assume that the compromised server also contained data from Companies Y and Z.

- **Who investigates this crime?**
- **Is it the Cloud Provider, even though Company X may fear that the provider will try to absolve itself from responsibility?**
- **Is it Company X and, if so, does it have the right to see other data on that server, including logs that may show access to the data of Companies Y and Z?**

- Many new risks and unknowns

The overall complexity of privacy protection in the cloud represents a bigger challenge.

JECRC Foundation

Possible Solutions

- Minimize Lack of Trust

  Policy Language

  Certification

- Minimize Loss of Control

  Monitoring

  Utilizing different clouds

  Access control management

  Identity Management (IDM)

- Minimize Multi-tenancy

Security Issues in the Cloud

JECRC UNIVERSITY
BUILD YOUR WORLD

- In theory, minimizing any of the issues would help:

Third Party Cloud Computing

Loss of Control

- Take back control
  - Data and apps may still need to be on the cloud
  - But can they be managed in some way by the consumer?

Lack of trust

- Increase trust (mechanisms)
  - Technology
  - Policy, regulation
  - Contracts (incentives): topic of a future talk

Multi-tenancy

- Private cloud
  - Takes away the reasons to use a cloud in the first place
- VPC: its still not a separate system
- Strong separation

JECRC Foundation

Third Party Cloud Computing

JECRC UNIVERSITY
BUILD YOUR WORLD

Like Amazon's EC2, Microsoft's Azure

- Allow users to instantiate Virtual Machines
- Allow users to purchase required quantity when required
- Allow service providers to maximize the utilization of sunk capital costs
- Confidentiality is very important

JECRC Foundation

Known issues: Already exist

JECRC UNIVERSITY
BUILD YOUR WORLD

- Confidentiality issues
- Malicious behavior by cloud provider
- Known risks exist in any industry practicing outsourcing
- Provider and its infrastructure needs to be trusted

JECRC Foundation