IT496: Cloud Computing

MODULE 2: BUILDING THE CLOUD INFRASTRUCTURE

LECTURE 4

Based on EMC course materials

Lecture Outline:

1. Lecture objectives.
2. Cloud computing reference model.
3. The deployment options and solutions for building a cloud infrastructure.
4. Factors to consider while building a cloud infrastructure.
5. Products.

1. Lecture objectives

- **Present** the cloud computing reference model.
- **Differentiate** between Greenfield and brownfield deployment options.
- **Illustrate** technology solutions for building a cloud infrastructure.
- **Define** best-of-breed cloud infrastructure components.
- **Discuss** cloud-ready converged infrastructure.
- **Mention** the key factors to consider while building a cloud infrastructure.

Lecture Outline

1. Lecture objectives.
2. Cloud computing reference model.
3. The deployment options and solutions for building a cloud infrastructure.
4. Factors to consider while building a cloud infrastructure.
5. Products.

2. Cloud computing reference model.

1. Layers of cloud computing reference model.
2. Entities and functions of each layer.
3. Cross-layer functions of cloud computing reference model.

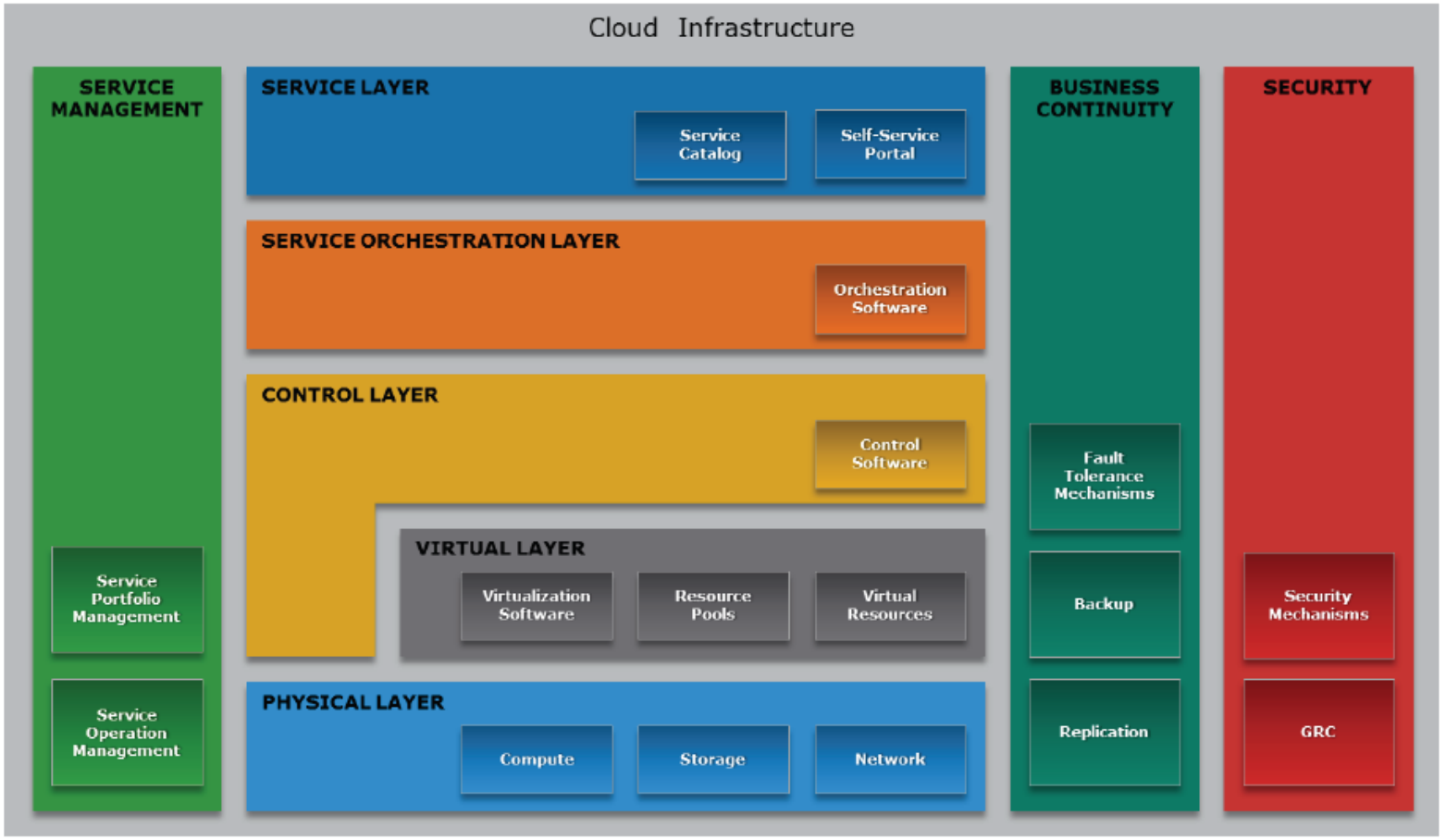
2.1 Layers of cloud computing reference model

❑Reference model

Is an **abstract framework** for understanding significant relationships among the entities of some environment.

1. It is based on a small number of **unifying concepts** and may be used as a basis for education and explaining standards.
2. Facilitates efficient communication of system details **between stakeholders**.
3. Provides a point of reference for **system designers** to extract system specifications.

2.1 Layers of cloud computing reference model



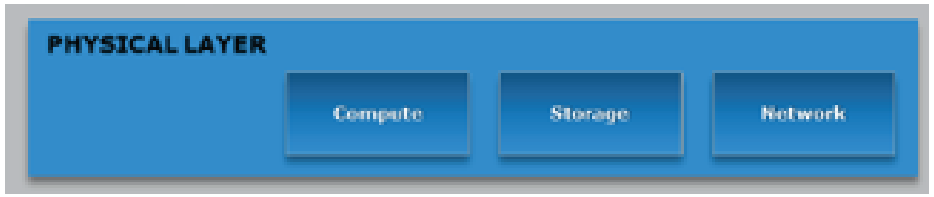
2. Cloud computing reference model.

1. Layers of cloud computing reference model.
2. Entities and functions of each layer.
3. Cross-layer functions of cloud computing reference model.

2.2.1 Physical Layer

- Foundation layer of the cloud infrastructure.

- Specifies entities that operate at this layer:
  - **Compute systems, network devices, and storage devices**.
  - Operating environment, protocol, tools, and processes.

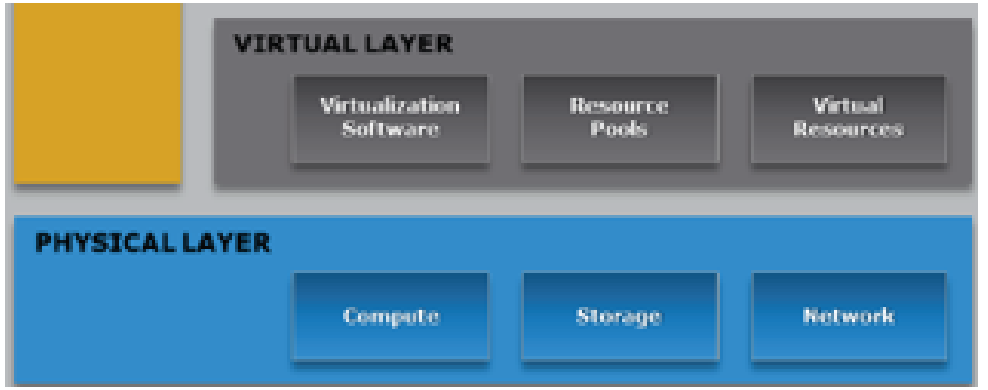


- Functions of physical layer:
  - Executes requests generated by virtualization and control layer.

2.2.2 Virtual Layer

- Deployed on the physical layer

- Specifies entities that operate at this layer:
  - **Virtualization software.**
  - **Resource pools.**
  - **Virtual resources.**

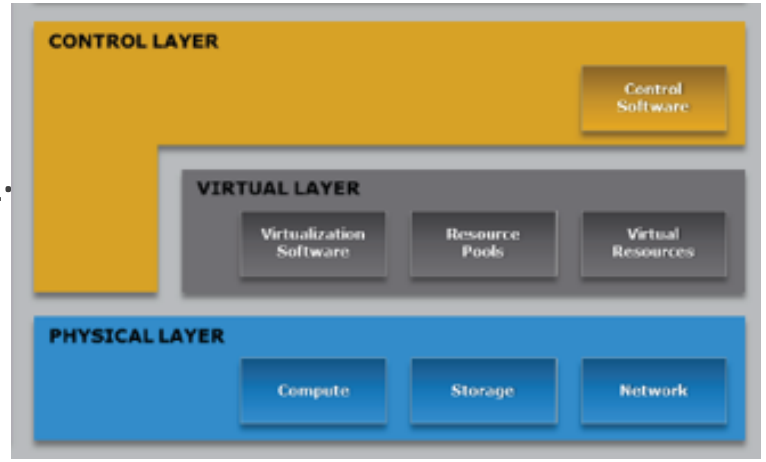


- Functions of virtual layer:
  - Abstracts **physical resources** and makes them appear as **virtual resources.**

- Enables multitenant environment, thereby improving utilization
  - Executes the requests generated by control layer.

2.2.3 Control Layer

- Deployed either on virtual layer or on physical layer
  - Specifies entities that operate at this layer – control software



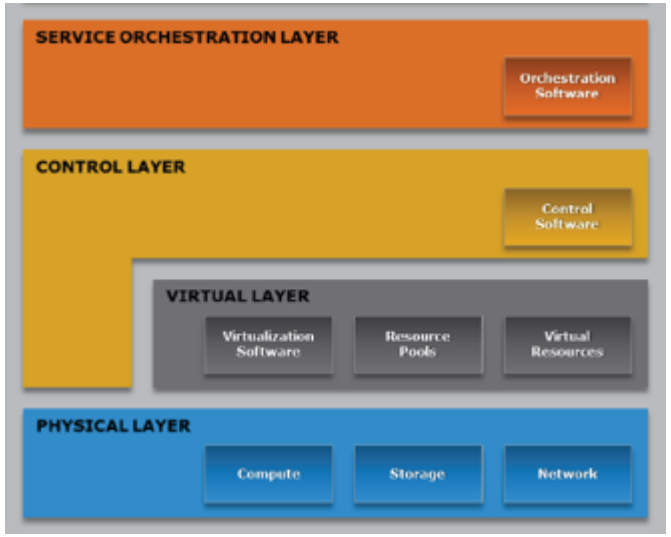
- Functions of control layer:
  - Enables **resource configuration** and **resource pool configuration**.
  - Enables **resource provisioning**.
  - Executes requests generated by service layer.
  - Exposes resources to and supports the service layer.

  - Collaborates with the virtualization software and enables
    - Resource pooling and creating virtual resources.
    - Dynamic allocation of resources.
    - Optimizing utilization of resources.

2.2.4 Service Orchestration Layer

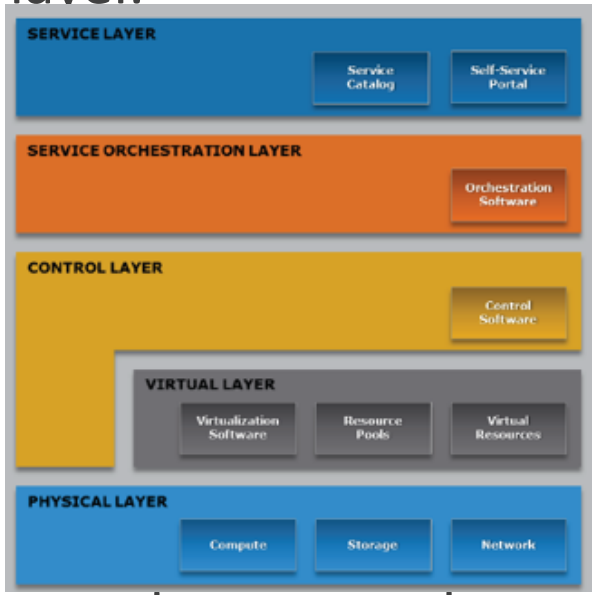
- Specifies the entities that operate at this layer:
  - Orchestration software

- Functions of orchestration layer:
  - Provides **workflows for executing automated tasks.**
  - Interacts with various entities to invoke provisioning tasks



2.2.5 Service Layer

- **Consumers** interact and consume cloud resources via this layer.



- Specifies the entities that operate at this layer:
  - **Service catalog.**
  - **Self-service portal.**
- Functions of service layer:
  - Stores information about cloud services in service catalog and presents them to the consumers.
  - Enables consumers to access and manage cloud services via a self-service portal.

2. Cloud computing reference model.

1. Layers of cloud computing reference model.
2. Entities and functions of each layer.
3. Cross-layer functions of cloud computing reference model.

2.3.1 Business Continuity Layer

- Specifies adoption of measures to mitigate the impact of downtime:

Measures	Description
Proactive	• Business impact analysis • Risk assessment • Technology solutions deployment (backup and replication)
Reactive	• Disaster recovery • Disaster restart

- Enables ensuring the availability of services in line with **SLA**.
- Supports all the layers to provide uninterrupted services.

2.3.2 Security Layer

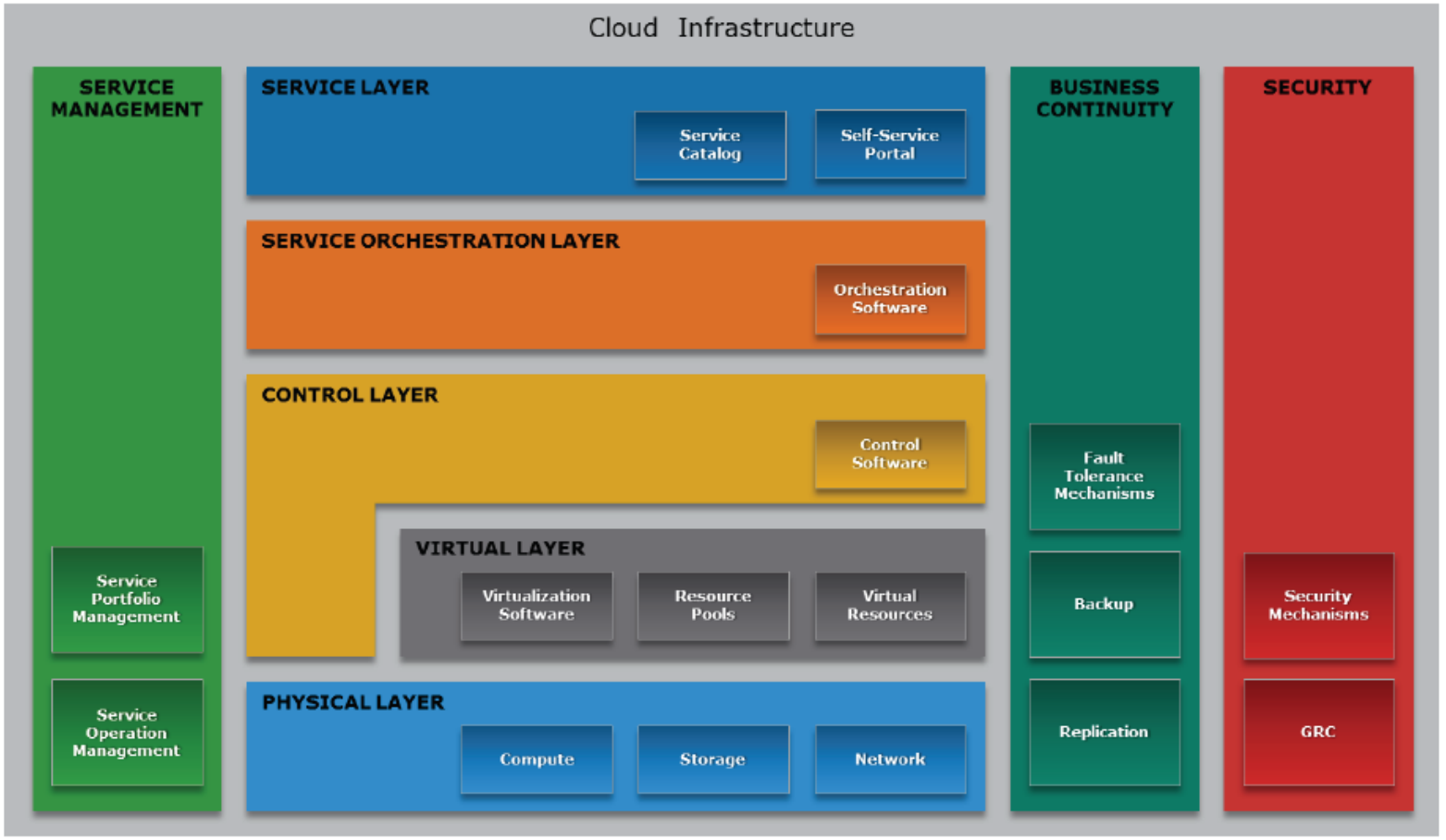
- Specifies the adoption of:
  - Administrative mechanisms
    - Security and personnel policies.
    - Standard procedures to direct safe execution of operations.
  - Technical mechanisms
    - Firewall.
    - Intrusion detection and prevention systems.
    - Antivirus.
- Deploys security mechanisms to meet GRC requirements.
- Supports all the layers to provide secure services.

2.3.2 Service Management Layer

- Specifies adoption of activities related to:

Activities	Description
Service portfolio management	• Defines service roadmap, service features, and service levels • Establishes budgeting and pricing • Deals with consumers in supporting activities • Performs market research • Collects information about competitors
Service operation management	• Enables infrastructure configuration and resource provisioning • Enables problem resolution • Enables capacity and availability management • Enables compliance conformance • Enables monitoring cloud services and their constituent elements

2.1 Layers of cloud computing reference model



Lecture Outline

1. Lecture objectives.
2. Cloud computing reference model.
3. The deployment options and solutions for building a cloud infrastructure.
4. Factors to consider while building a cloud infrastructure.
5. Products.

3. The deployment options and solutions for building a cloud infrastructure.

1. Greenfield and brownfield deployment options

2. Technology solutions for building a cloud infrastructure

3.1 Greenfield and brownfield deployment options

Greenfield Deployment Option

It is typically used when an infrastructure does not exist and an organization has to build the cloud infrastructure starting from the physical layer.

Brownfield Deployment Option

It is used when some of the infrastructure entities exist, which can be transformed to cloud infrastructure by deploying the remaining entities required for the cloud infrastructure.

3. The deployment options and solutions for building a cloud infrastructure.

1. Greenfield and brownfield deployment options

2. Technology solutions for building a cloud infrastructure

3.2 Technology solutions for building a cloud infrastructure

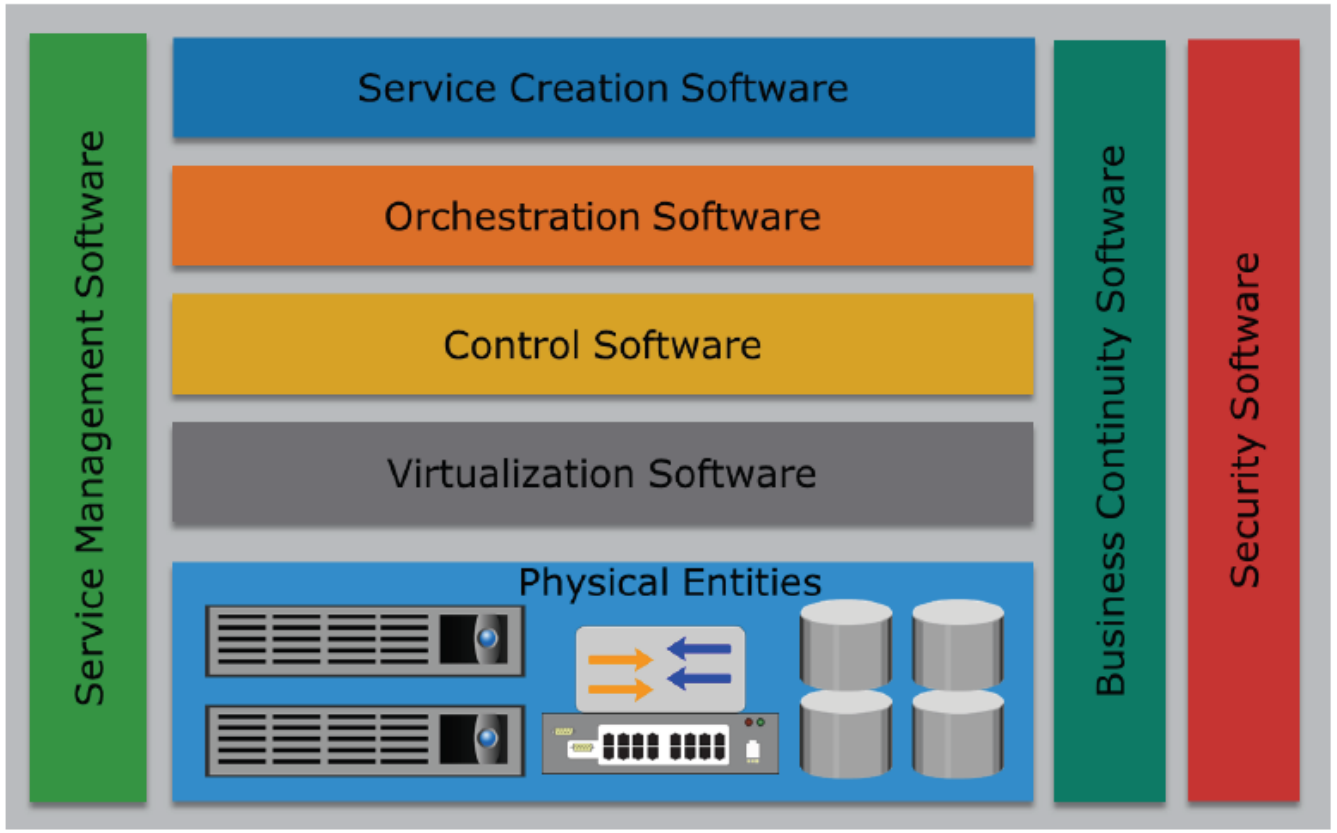
1. Integrating **best-of-breed** cloud infrastructure components.

2. **Cloud-ready converged** infrastructure.

3.2.1 Integrating best-of-breed cloud infrastructure components.

- Built by integrating **multi-vendor infrastructure** components
- Enables **repurposing** the existing infrastructure components
- Requires spending a significant amount of **IT staff time** on:
  - Evaluating individual and disparate hardware components.
  - Installing and integrating infrastructure components.
  - Testing hardware, middleware, and software.
  - Checking compatibility of all the components.
- Enables organizations to choose and switch vendors easily.

3.2.2 Cloud-ready converged infrastructure.



Lecture Outline

1. Lecture objectives.
2. Cloud computing reference model.
3. The deployment options and solutions for building a cloud infrastructure.
4. Factors to consider while building a cloud infrastructure.
5. Products.

4. Factors to consider while building a cloud infrastructure.

- Governance
- Organization
- Finance
- Tools
- Service-level agreement and service contract

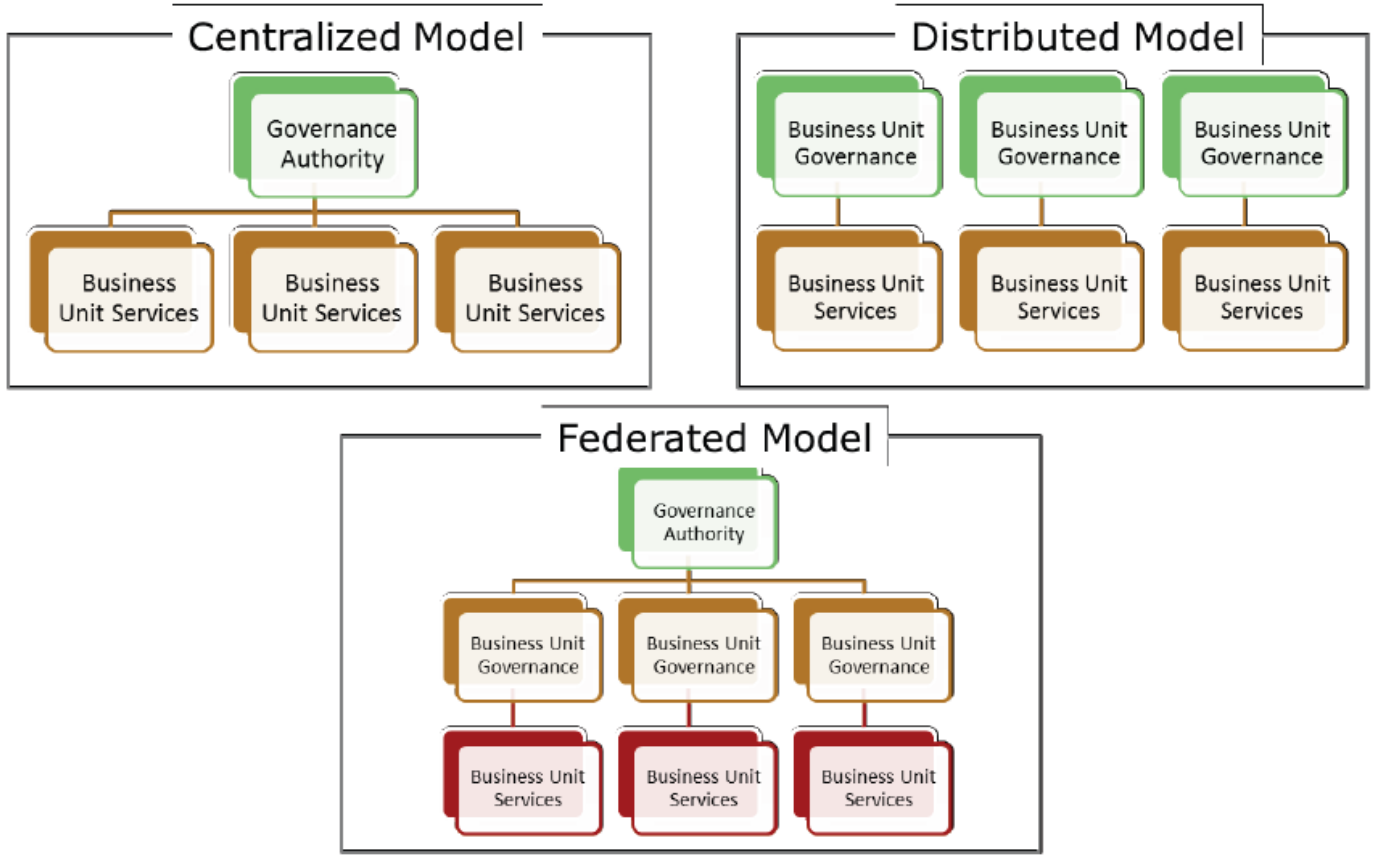
- Avoiding vendor lock-in
- Software licensing concerns
- Service model considerations
- Migration
- Testing

4.1 Governance

- Governance is the active distribution of **decision-making rights** and accountability among different stakeholders in an organization.

- **IT governance** enables the service provider to:
  - Ensure IT resources are implemented and used according to policies and procedures.
  - Ensure the resources are properly controlled and maintained.
  - Ensure the resources are providing value to the organization.

4.1 Governance



4.2 Organization

New Roles in Cloud

Service Manager

- Key interface between clients and IT staff
- Understands consumers' needs and industry trends
- Ensures IT delivers cost-competitive services
- Manages consumers' expectations of product offerings

Account Manager

- Supports service managers in service planning, development, and deployment

Cloud Architect

- Creates detailed designs for the cloud infrastructure

Service Operations Manager

- Streamlines service delivery and execution
- Coordinates with architecture team to define technology roadmaps and ensure SLOs are met

4.3 Finance

- Determines the price (or chargeback) that a service consumer is expected to pay to meet the provider's **business goals**.

- Business Goals
  - Recovery of cost.
  - Profit.
  - ROI goal.
  - Reinvestment goal.

4.3 Finance

Chargeback Models

Model	Description
Pay-as-you-go	• Metering and pricing is based on consumption of resources • Consumers do not pay for unused resources
Subscription by time	• Cost of providing a service for a subscription period is divided among a predefined number of consumers
Subscription by peak usage	• Consumers are billed according to their peak usage of IT resources for a subscription period
Fixed cost or pre-pay	• Consumers commit needed resources upfront for committed period • Consumers pay fixed charge periodically through a billing cycle regardless of the utilization of resources
User-based	• Billing is based on the number of users logged in

4.4 Tools

- Tools play an important role in building a cloud infrastructure:
  - Virtualization and orchestration software.
  - Security and business continuity software.
  - Self-service portal software.
- Other tools that should be considered specially when deploying hybrid cloud, community cloud, or brokerage service:
  - Cloud integration tools.
  - Application Programing Interface (API).
  - Specialized connection.
  - Transformation and business logic programs.

4.5 Service-level Agreement and Legal Contract

- **Service-level Agreement**
  - A **contract** negotiated between a **provider and a consumer** that specifies various parameters and metrics such as cost, service availability, maintenance schedules, performance levels, service desk response time, and consumer's and provider's responsibilities.

  - **Key points** that must be included in a legal contract are:
    - Business level policies such as data privacy, data ownership, security.
    - Availability and performance metrics.
    - Exit plan, and penalties for not meeting SLA.
    - How unexpected incidents and prolonged service outage will be handled.

4. Factors to consider while building a cloud infrastructure.

- ~~Governance~~
- ~~Organization~~
- ~~Finance~~
- ~~Tools~~
- ~~Service-level agreement and service contract~~

- Avoiding vendor lock-in
- Software licensing concerns
- Service model considerations
- Migration
- Testing

4.6 Avoid Vendor Lock-in

- A situation where a **consumer is unable to move** readily from the current provider to another.

- Causes for vendor lock-in includes:
  - High migration cost.
  - Application requires significant re-engineering for migration.
  - Lack of open standards.
  - Restrictions or burdensome penalties imposed by the current provider.

- Vendor lock-in can be prevented by:
  - Using open standard tools, APIs, and file formats.
  - Including appropriate exit clause in the agreement.

4.7 Software Licensing Concerns

- Typically, relevant to **IaaS and PaaS models**.
- Consumers can use their existing license if it is cloud enabled.
- If consumer's existing license is **not cloud enabled** then:
  - Paying additional fees may get their license cloud enabled.
  - May use software provided by the service provider.
- Providers must work to understand the software license rights and its usage:
  - Prevents any non-compliance and violation of license agreements.

4.8 Service Model Considerations

- **Software as a Service:**
  - Ensures the software offered are thoroughly **tested**.
  - Ensures the new features and functionalities are developed to the software to **meet consumer's needs**.
  - Ensures applications are **scalable and can handle** increasingly larger consumer workloads.
  - Ensures the consumers are provided a **secure environment**.

- **Platform as a Service:**
  - Provides **application development platform** to the consumers.
  - Ensures the consumers are provided a **secure environment.**
  - Provides the consumer the **required computing resources** to operate the application.

4.8 Service Model Considerations

- **Infrastructure as a Service:**
  - Provides the consumer the required **infrastructure resources** to deploy their OS, application, and data.
  - Ensures that the consumers are provided a **secure environment**.

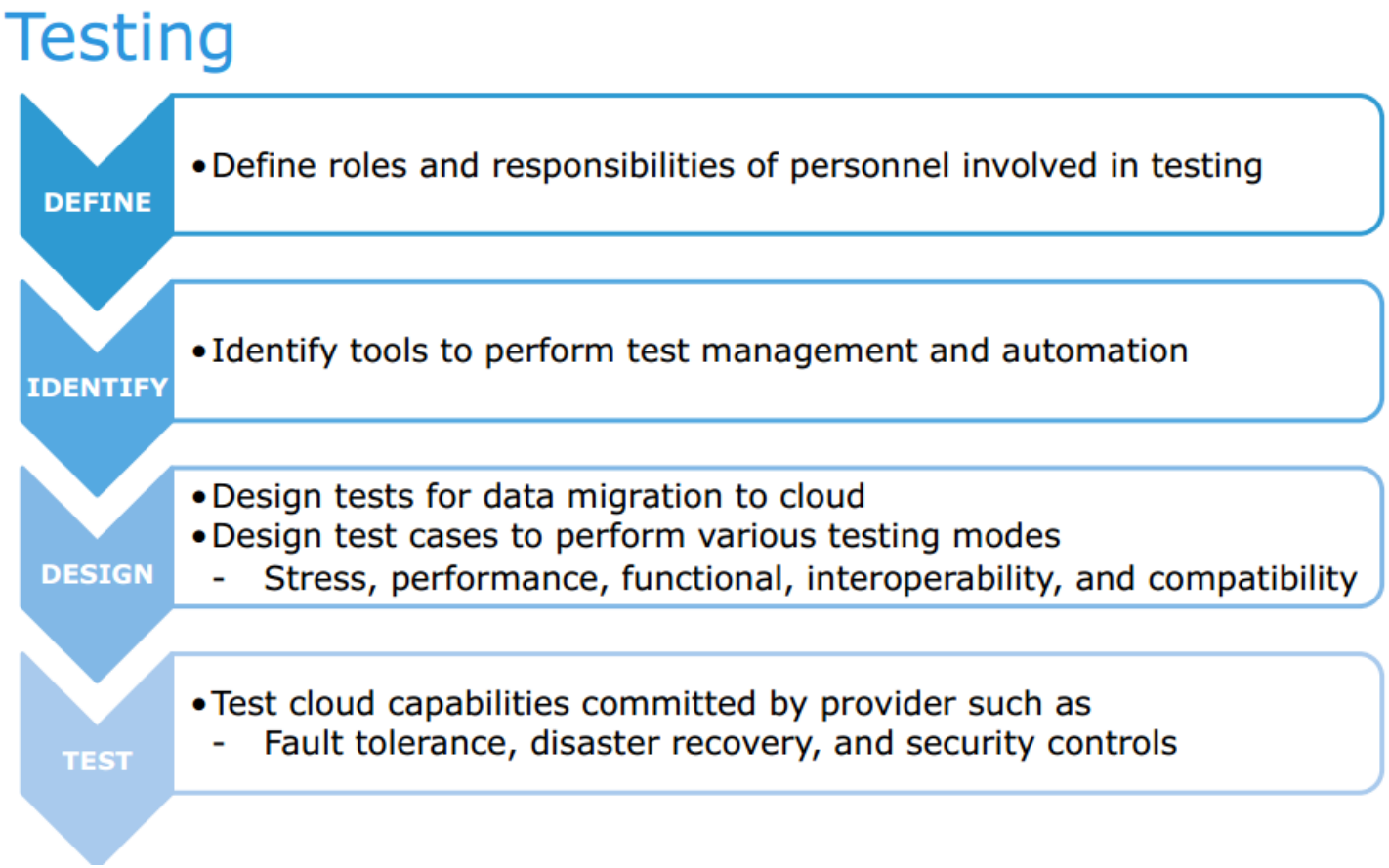
4.9 Migration

- Consumer may plan to migrate **application or only data**
- Two application migration strategies are:

Migration Strategy	Description
Forklift	• Entire application is migrated at once instead of in parts • Good for tightly coupled or self contained applications
Hybrid migration strategy	• Applications and its components are moved in parts • Lower-risk approach to migrate applications to the cloud • Good for application that have loosely coupled components

- For migrating data to cloud:
  - Consider copying data to cloud using replication technology.
  - Consider factors such as **network bandwidth, data security and integrity**.

4.10 Testing


Testing
DEFINE
• Define roles and responsibilities of personnel involved in testing
IDENTIFY
• Identify tools to perform test management and automation
DESIGN
• Design tests for data migration to cloud
• Design test cases to perform various testing modes
- Stress, performance, functional, interoperability, and compatibility
TEST
• Test cloud capabilities committed by provider such as
- Fault tolerance, disaster recovery, and security controls

4. Factors to consider while building a cloud infrastructure.

- Governance
- Organization
- Finance
- Tools
- Service-level agreement and service contract

- Avoiding vendor lock-in
- Software licensing concerns
- Service model considerations
- Migration
- Testing

Lecture Outline

1. Lecture objectives.
2. Cloud computing reference model.
3. The deployment options and solutions for building a cloud infrastructure.
4. Factors to consider while building a cloud infrastructure.
5. Products.

5. Products

ESXi

- Bare-metal hypervisor
- Abstracts processor, memory, storage, and network resources into multiple VMs
- Comprises underlying VMkernel OS that supports running multiple VMs
  - VMkernel controls and manages compute resources

5. Products

Vblock	VSPEX
• Integrated IT infrastructure solution for cloud deployment • Combines compute, storage, network, virtualization, security, and management software in a package • Validated solution and ready for deployment	• IT infrastructure solution for cloud deployment • Includes compute, storage, network, virtualization, and backup products • Offers choice of hypervisor, compute system, and network technology

Lecture Objectives:

- The cloud computing reference model was presented. ✓
- Greenfield and brownfield deployment options. ✓
- Technology solutions for building a cloud infrastructure were illustrated. ✓
- Best-of-breed cloud infrastructure components. ✓
- Cloud-ready converged infrastructure. ✓
- The key factors to consider while building a cloud infrastructure. ✓

Thanks