Certificate of Cloud Security Knowledge (CCSK) Bootcamp

Michael J Shannon

CISSP, CCSP, CCSK

AWS Security-Specialty

ITIL4 Managing Professional

Class will begin at 10:00
Central Standard Time

The Certificate of Cloud Security Knowledge (CCSK)

- According to the Cloud Security Alliance (CSA): “The Certificate of Cloud Security Knowledge (CCSK) certificate is widely recognized as the standard of expertise for cloud security and gives you a cohesive and vendor-neutral understanding of how to secure data in the cloud
- The CCSK credential is the foundation to prepare you to earn additional cloud credentials specific to certain vendors or job functions.”

The Certificate of Cloud Security Knowledge (CCSK)

- The CCSK is an open-book, online exam
- It is a 90-minute exam with 60 multiple-choice questions selected randomly from the CCSK question pool
- The exam costs $395 US and provides candidates with two test attempts, which you will have 2 years to use
- The minimum passing score is 80%.

CCSK Domains

1. Cloud Computing Concepts
2. Governance & Enterprise Risk Management
3. Legal Issues: Contracts and Electronic Discovery
4. Compliance & Audit Management
5. Information Governance
6. Management Plane & Business Continuity
7. Infrastructure Security
8. Virtualization & Containers

CCSK Domains

1. Incident Response
2. Application Security
3. Data Security & Encryption
4. Identity Entitlement and Access Management
5. Security as a Service
6. Related Technologies
7. CCM
8. ENISA

Cloud Computing Value Propositions

- **Agility** enables the speed of implementation of services, experimentation, and innovation
- **Elasticity** offers the ability to scale and de-provision on demand enhancing the ability to eliminate wasted capacity
- **Flexibility** means that the cloud provider presents a broad set of products with low to no cost to entry
- **Security and governance** is a top priority as CSPs have acquired many certifications and helps organizations get certified
  - The shared responsibility model is an agreement where the cloud provider is responsible for the infrastructure whereas the customer is responsible for everything else

Cloud Computing Value Propositions

- Trade fixed capital expenses for variable expenses
- Gain value from massive economies of scale
- Stop trying to predict capacity
- Enhance speed and agility
- Cease spending money operating and maintaining on-site data centers
- Go global in a matter of minutes or hours

Cloud Computing Characteristics

- **Broad network access** is a cloud feature that allows users to conveniently access physical and virtual resources from wherever they are using a wide variety of network-accessible devices such as cell phones, tablets, laptops, and workstations
- **Measured service** is a cloud feature where service use can be monitored, controlled, reported, and billed on metered, pay-for-use basis … an important feature that helps optimize and validate cloud services

Cloud Computing Characteristics

- **Multi-tenancy** is a function where physical or virtual resources are allocated in a way that isolates guests and their data from one another
- Typically – within the context of multi-tenancy – the group of users that form a tenant will all belong to the same cloud service
- There may be cases where the group of users involves multiple service customers e.g., public cloud and community cloud deployments

Cloud Computing Characteristics

- **On-demand self-service** allows cloud service customers to provision computing capabilities as needed, automatically, or with minimal interaction with their service provider
- The feature helps users save on cost, time, and effort since they can do what they need, when they need to, without added interactions or overhead

Cloud Computing Characteristics

- **Resource pooling** allows a cloud provider's physical or virtual resources to be aggregated to serve one or more cloud service customers
- With this feature, customers can enjoy a service that provides them resources without exposing them to the complexity of the multi-tenancy process, and they can offload some work, such as maintenance, to the provider

Cloud Computing Roles and Responsibilities

- Cloud Service **Customer (consumer) –** the entity that is paying, leasing, renting, or trying cloud services
- Cloud Service **Provider** (**CSP**) – the vendor that is providing the services from their data center, zones, regions, and edge computing locations
  - e.g., AWS, Rackspace, IBM Cloud, Microsoft Azure, and Google Cloud Platform

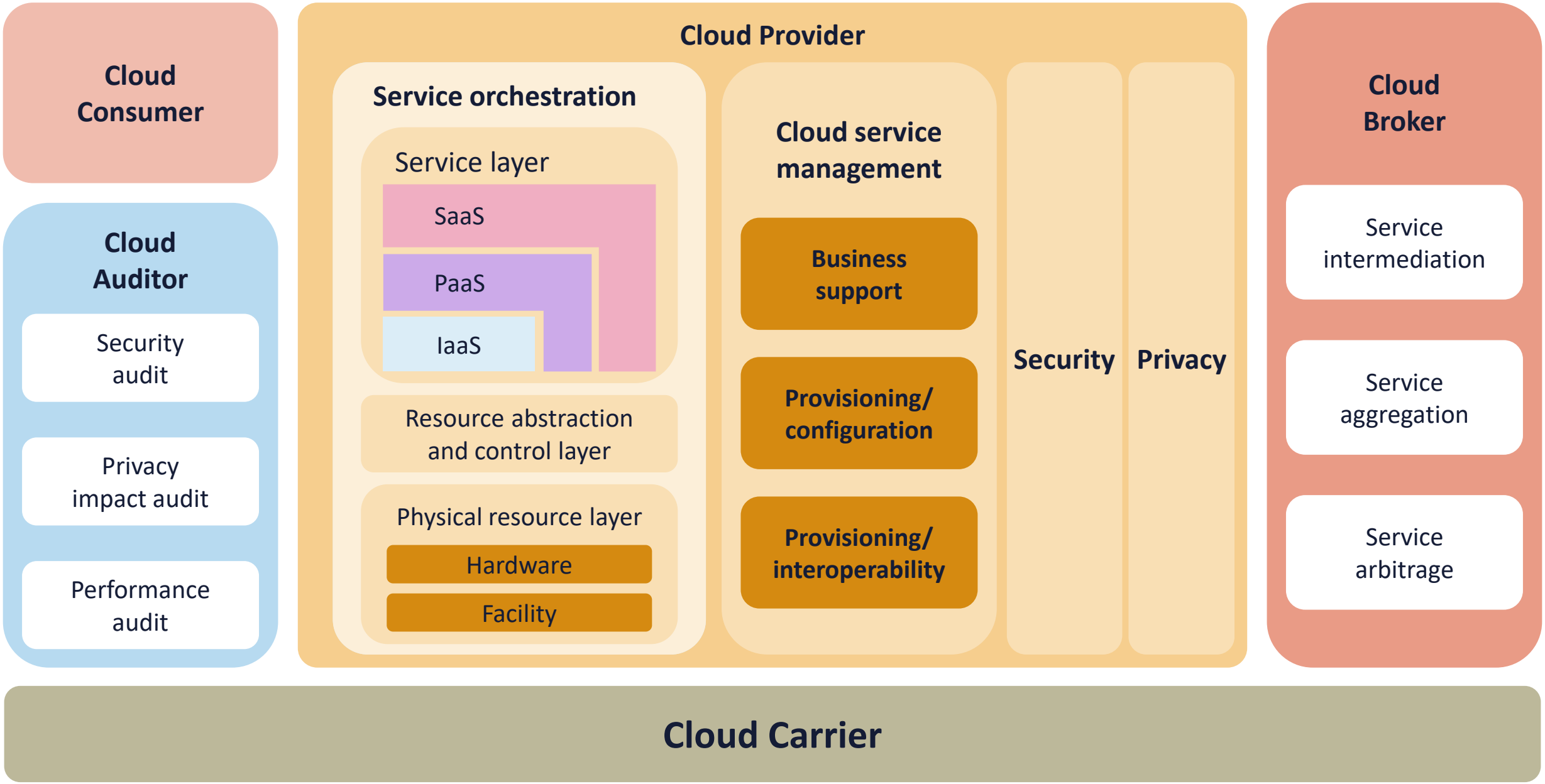
Cloud Computing Roles and Responsibilities

- Cloud Service **Partner** – an entity with various partnership agreements with the CSP such as telecoms, broadband providers, Software-as-a-Service providers, and security solution vendors e.g., AWS GuardDuty and Rapid7
- Cloud Service **Broker** – an organization that buys hosting services from a CSP and then re-sells to their own consumers e.g., Direct Connect, ExpressRoute partners of AWS and Azure, or Cloud access Security Broker

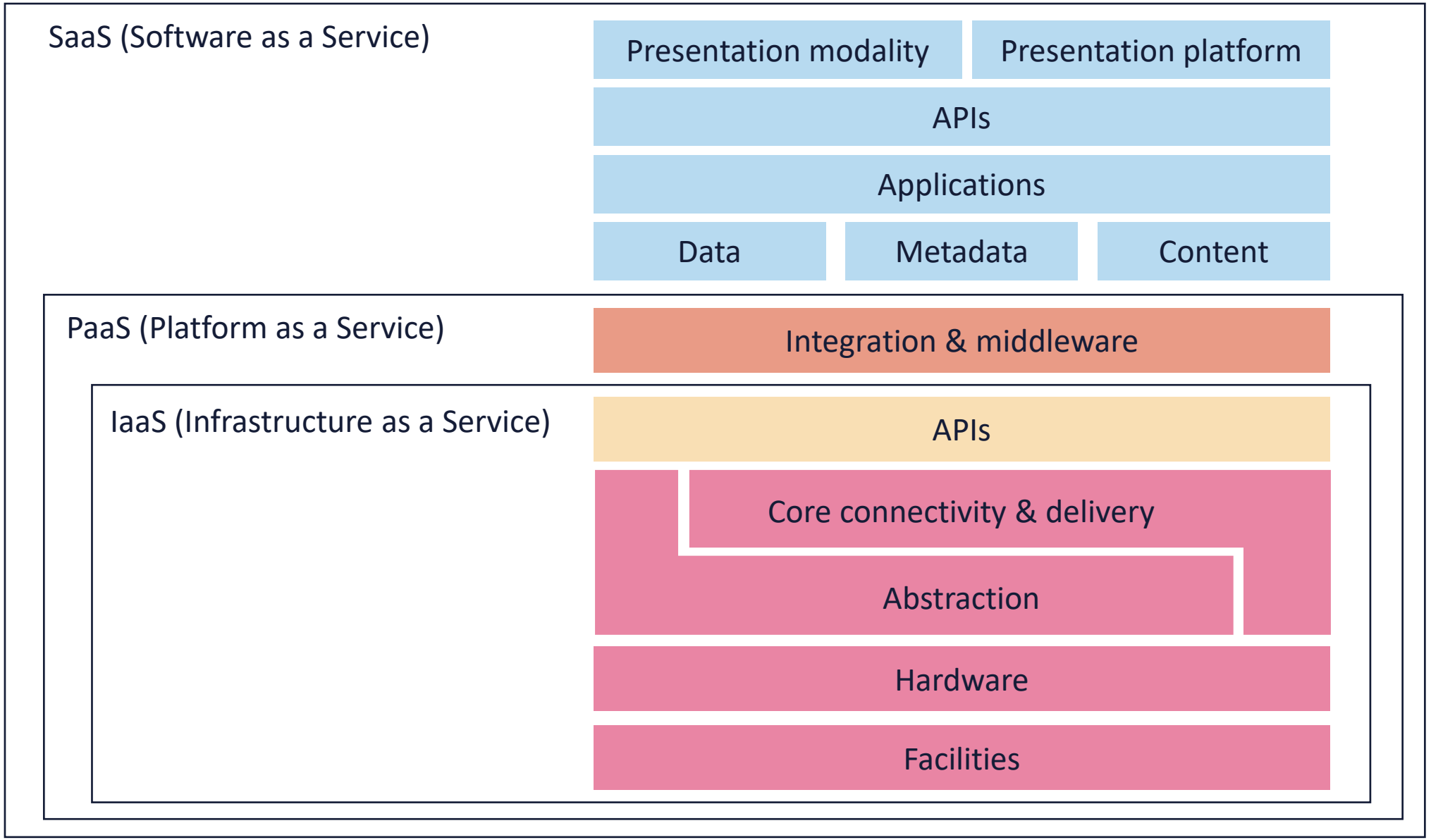
Cloud Computing Roles and Responsibilities

- Cloud **Auditor** – typically third-party regulators (CSA certified) who are ensuring compliance with frameworks such as PCI-DSS
- Cloud **Regulator** – an entity that evaluates both provider and consumer levels of data and systems safeguards, commonly focused on cybersecurity, authentication, access, identity, data privacy, business continuity, audits, and control assurance

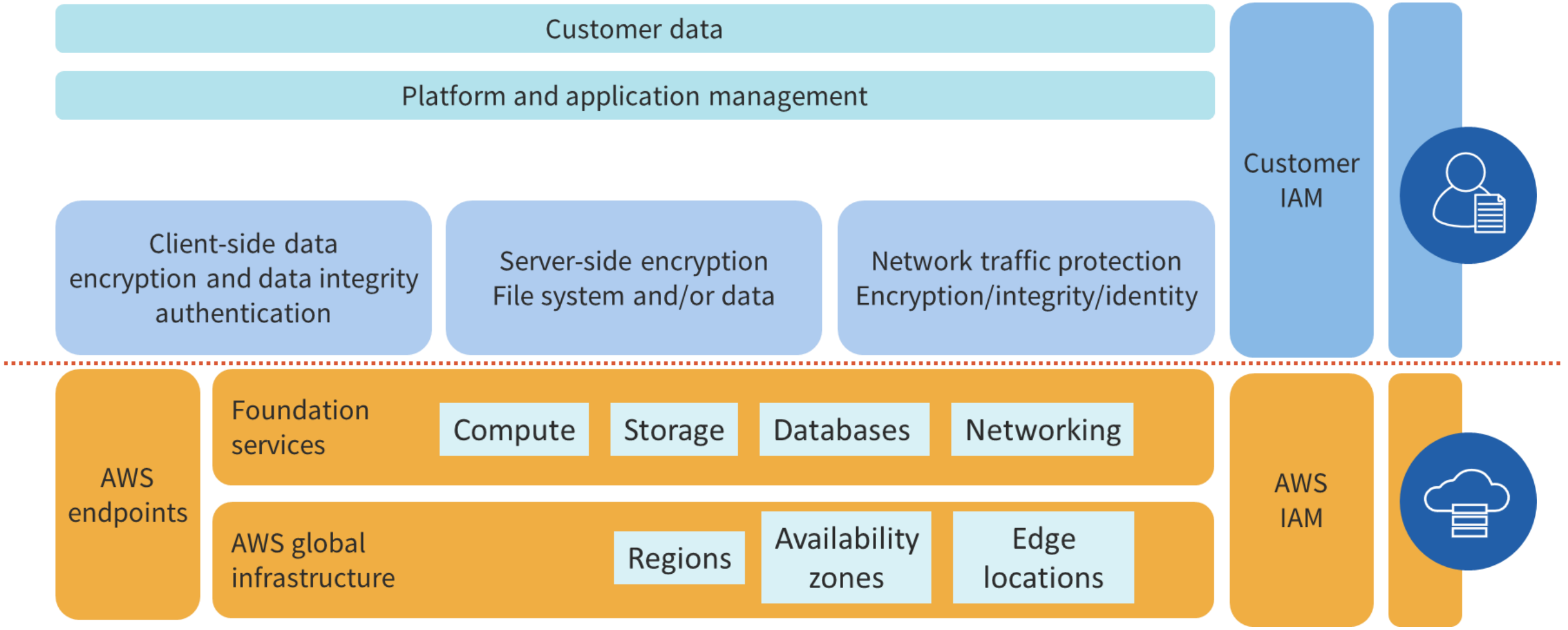
NIST 500-292 Cloud Reference Architecture



Cloud Service Types



Infrastructure-as-a-Service (IaaS) at AWS



Platform-as-a-Service (PaaS)

Development and SDK platforms for Java, PHP, Python, etc.

Container services for Docker and Kubernetes

Managed and fully managed relational and document databases

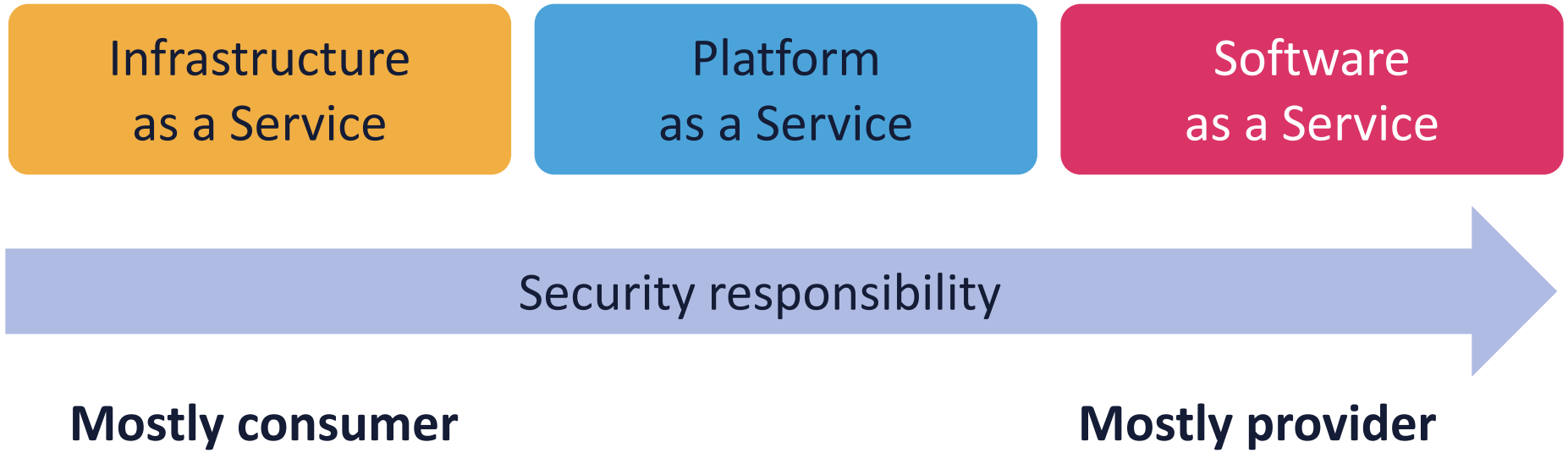
Managed security and threat modeling services

SSO, machine learning, AI, IoT, blockchain, media services

Software-as-a-Service (SaaS)

- Customer relationship management (CRM)
- Enterprise Resource Planning
- Human resources and workplace tools
- Finance, sales, and marketing services
- Payroll services
- E-mail, collaboration, and cloud storage
- Help and service desk
- Virtual call center
- Business analytics
- SIEM and SOAR systems

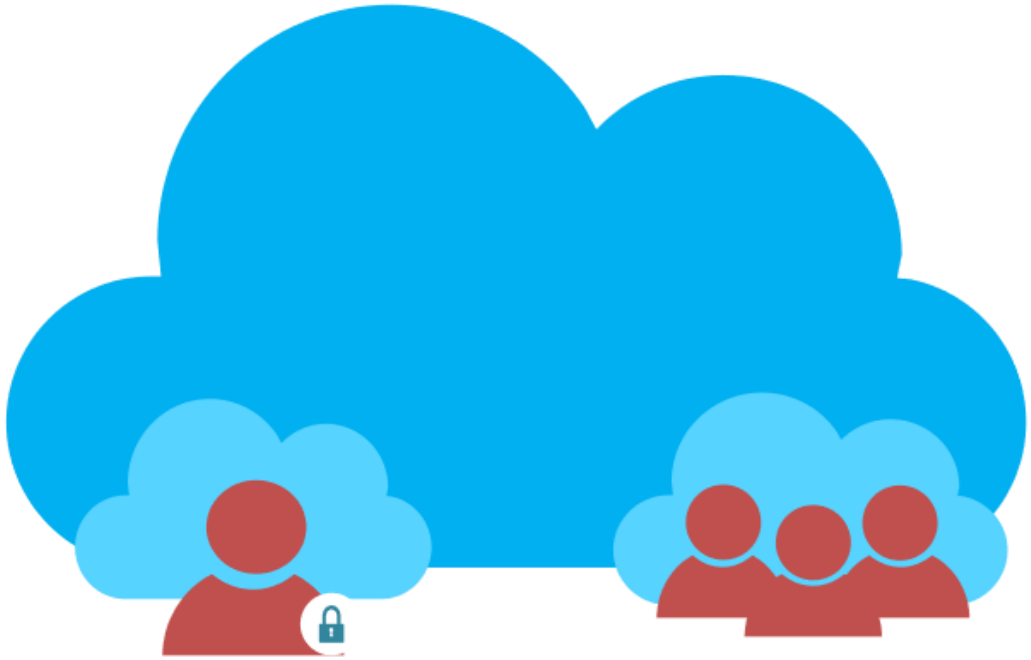
Service Type Shared Responsibility



Cloud Deployment Types

Public Cloud

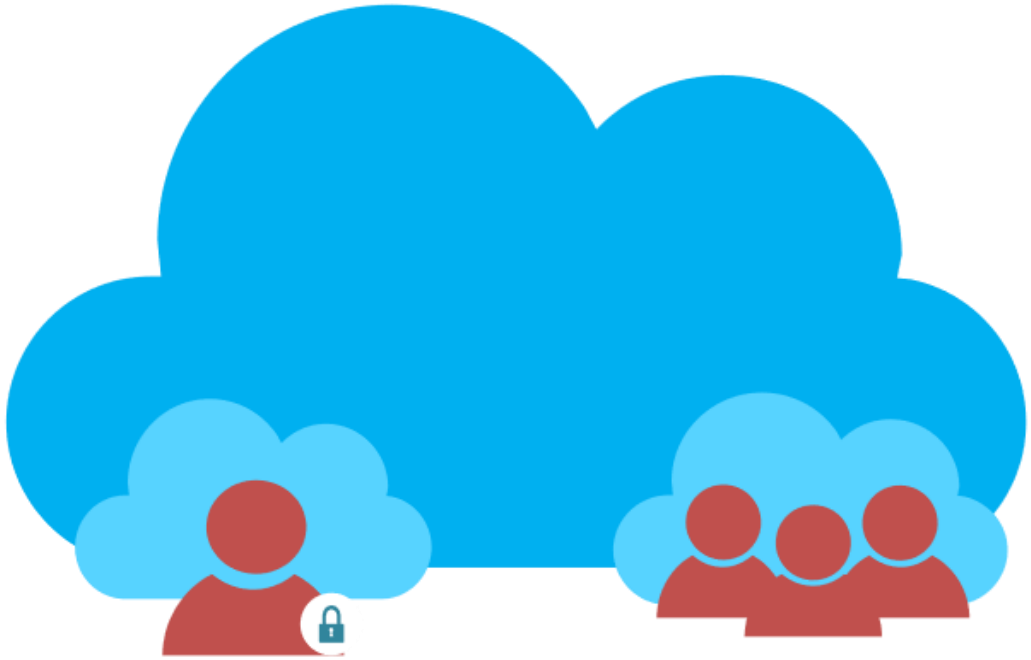
- A model where computing resources are owned and operated by a provider and shared across multiple tenants via the Internet or other public networks
- Enterprises often use public cloud for less-sensitive applications that have unpredictable spikes in usage or for storing data that does not require frequent access



Cloud Deployment Types

- Public cloud makes computing resources available to anyone for purchase and multiple users usually share the use of a public cloud
- Many businesses use a public cloud to scale existing IT resources on demand without having to commit to growing their physical IT infrastructure

Public Cloud



Cloud Deployment Types

- A model that is dedicated to a single customer (or organization) with no other sharing of cloud resources – not a multi-tenant environment
- The private cloud can be a dedicated part of the Cloud Service Provider in a sandbox environment for an additional cost
- The private cloud can be an on-premises solution using virtualization and other cloud service characteristics

Private Cloud

Cloud Deployment Types

- Linking infrastructure and applications between similar entities in a certain sector (public or private use)
- Often used to share information and research among parties with various types of cooperative relationships
- Common examples are:
  - Government agencies and departments
  - Healthcare provider networks
  - Gaming communities
  - Insurance holding companies
  - Financial services companies

Community Cloud

Cloud Deployment Types

- Technically a combination of private, public, and/or community cloud deployments
- Can also be a method for connecting infrastructure and applications between cloud-based resources and other resources that are not placed in the cloud
- The most common type of hybrid deployment is between the provider's Public cloud and a standing on-premises enterprise Private cloud

Hybrid Cloud

Cloud Deployment Types

Hybrid Cloud

- Can be used to migrate, expand, or grow an organization's infrastructure into a cloud solution while linking internal systems to cloud resources
- Often used by organizations to "burst up" to the cloud during peak demand times or special situations
- May also refer to “edge” or “fog” computing where the consumer has a direct high-speed connection to the provider cloud through a partner (AWS Direct Connect, Google Interconnect, Azure ExpressRoute)

Cloud Deployment Types

- Multi-cloud is a cloud computing model where an enterprise leverages a combination of clouds (two or more public clouds, two or more private clouds, or a combination of public, private and edge clouds)
- Enables the distribution of applications and services to accelerate app transformation and the delivery of new apps

Multi-Cloud

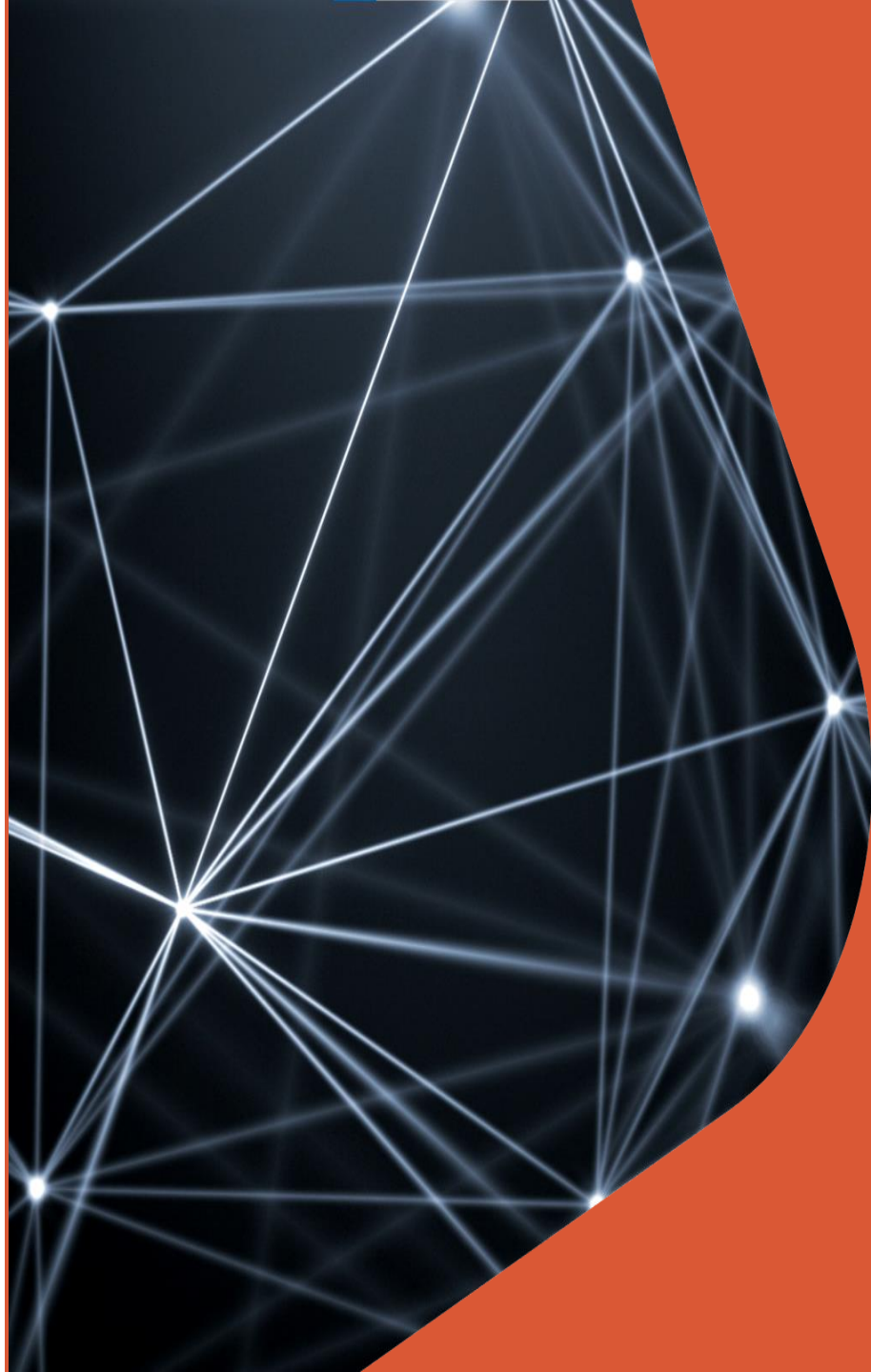
Cloud Deployment Types

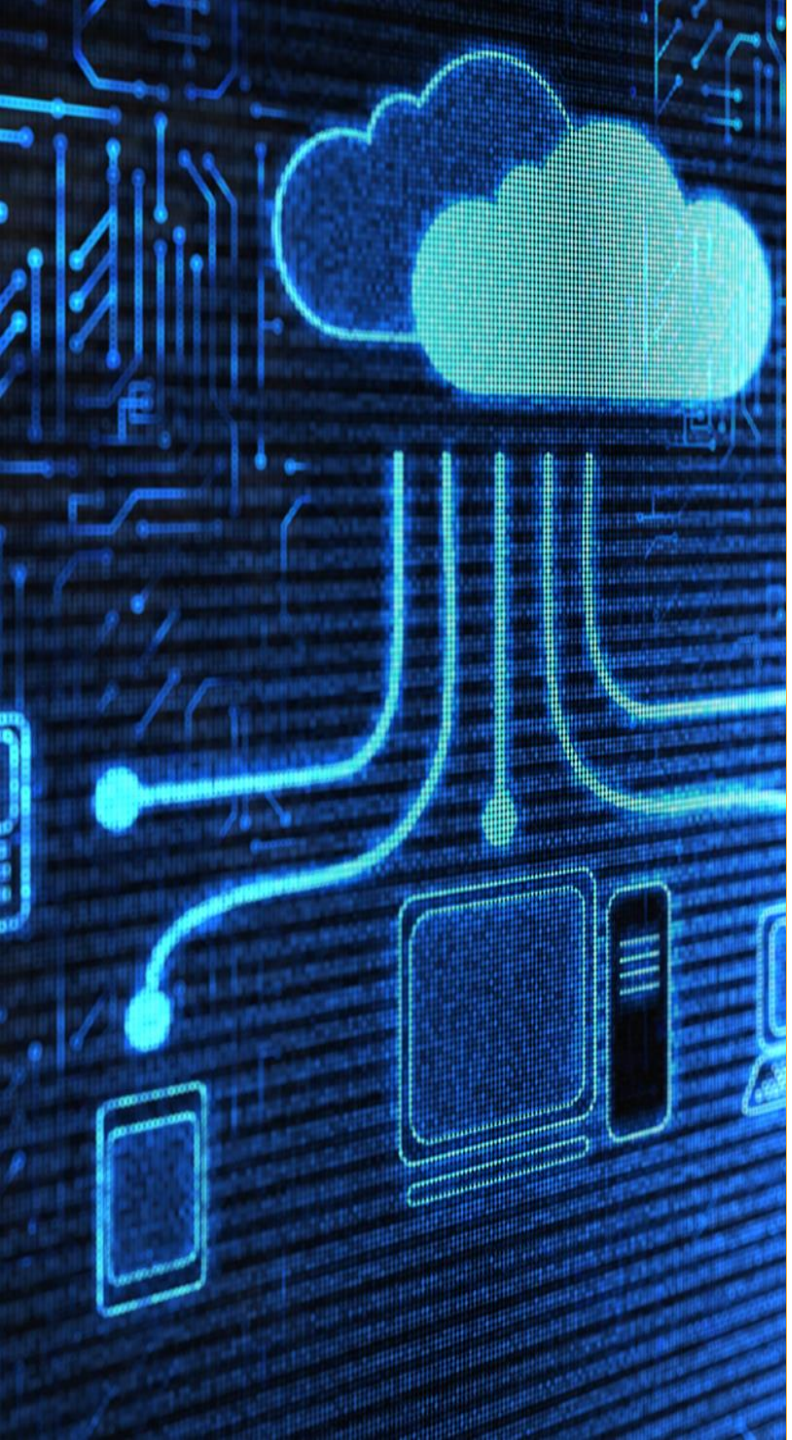
- Allows for allocation of applications and services to the edge in industries such as logistics, retail and manufacturing, the next generation of gains in automation, efficiency
- Improves the customer experiences that require applications to be distributed to the edge, closer to physical devices and users
- Supports the rise of the distributed workforce that secure and manage users and their devices

Multi-Cloud

Cloud Logical Models

- **Infrastructure** Layer – Security of the infrastructure which includes the data center network, storage, and servers
- **Metastructure** Layer – Securing the virtual environment which represents the logical layer using tools and configuration of the management plane often using software-defined networking (OpenFlow and Cisco ACI)
- **Infostructure** Layer – Where the data and information reside
- **Applistructure** Layer – server-based and serverless cloud-native applications and services





Governanc

e

- The need for governance exists anytime a group of people comes together to accomplish an end
- Typically focuses on three attributes or characteristics:
  - authority
  - decision-making, and
  - accountability
- Is focused on the structure and processes for sound decision-making, accountability, management, and conduct at the top of an organization
- It directs how an organization's objectives are determined and achieved, how risk is controlled and addressed, and how the delivery of value is improved

Corporate Governance

Cloud Security Governance

- Broadly defined as the rules that protect the assets and continuity of an organization when using a cloud deployment model (public, private, community, and/or hybrid)
- Includes cloud computing mission statements, charters, declarations of value propositions, policies, standards, and procedures

Cloud Security Governance

- Guides the course and control of organizational security operations, initiatives, and activities when using various cloud service types and shared responsibilities
- The security practitioner's strategy will be derived from effective security governance

Cloud Governance Tools

Contracts

- A mutually binding legal relationship obligating the seller to furnish the supplies or services (including construction) and the buyer to pay for them
- It includes all types of commitments that obligate the Government to an expenditure of appropriated funds and that, except as otherwise authorized, are in writing

Cloud Governance Tools

Cloud Provider Assessments

- Customers must perform their due diligence exercise before selecting a provider/vendor
- Assessments should take advantage of all available information and collection tools
- It is almost impossible that a customer will be able to go to a cloud provider datacenter and conduct an audit or assessment
- **The Cloud Controls Matrix (CCM+CAIQ) and CSA Star registry are the primary methods for provider assessment for this exam – these will be explored in greater detail later in the course**

Cloud Governance Tools

Compliance Reporting

- **ISO/IEC 27017** – based on 27002 control set but customized for cloud services
- **NIST 800-53** – more than 600 controls as part of the larger NIST Risk Management Framework
- **FedRAMP** – modifies 800-53 for providers who want to have Authority to Operate (ATO) with US government
- **PCI** – Bank cards and credit card data risk compliance
  - Just because a provider is PCI compliant does not mean your applications are compliant
- **COBIT** – ISACA IT enterprise management and governance (instead of ITIL 4)
- **HIPAA** – security and privacy of PHI

COMPARING SECURITY AUDITING STANDARDS

Standards applicable to cloud security auditing.			
Standard	**Type**	**Strength**	**Sponsoring organization**
Service Organization Control (SOC) 2	Audit for outsourced services	Technology neutral	American Institute of CPAs
ISO 27001 and 27002	Traditional security audit	Technology neutral	ISO
NIST 800-53 rev, 4	Federal government audit	Technology neutral	National Institute of Standards and Technology
Cloud Security Alliance (CSA)	Cloud-specified audit	Dedicated to cloud security auditing	CSA
Payment Card Industry (PCI) Data Security Standard (DSS)	PCI Qualified Security Assessor cloud supplement	Cloud specific and Provides guidance	PCI DSS

CSA Enterprise Reference Architecture

Business Operation Support Services (BOSS)

(SABSA)

Information Technology Operation & Support (ITOS)

(SABSA and ITIL4)

Presentation Services

Application Services

Information Services

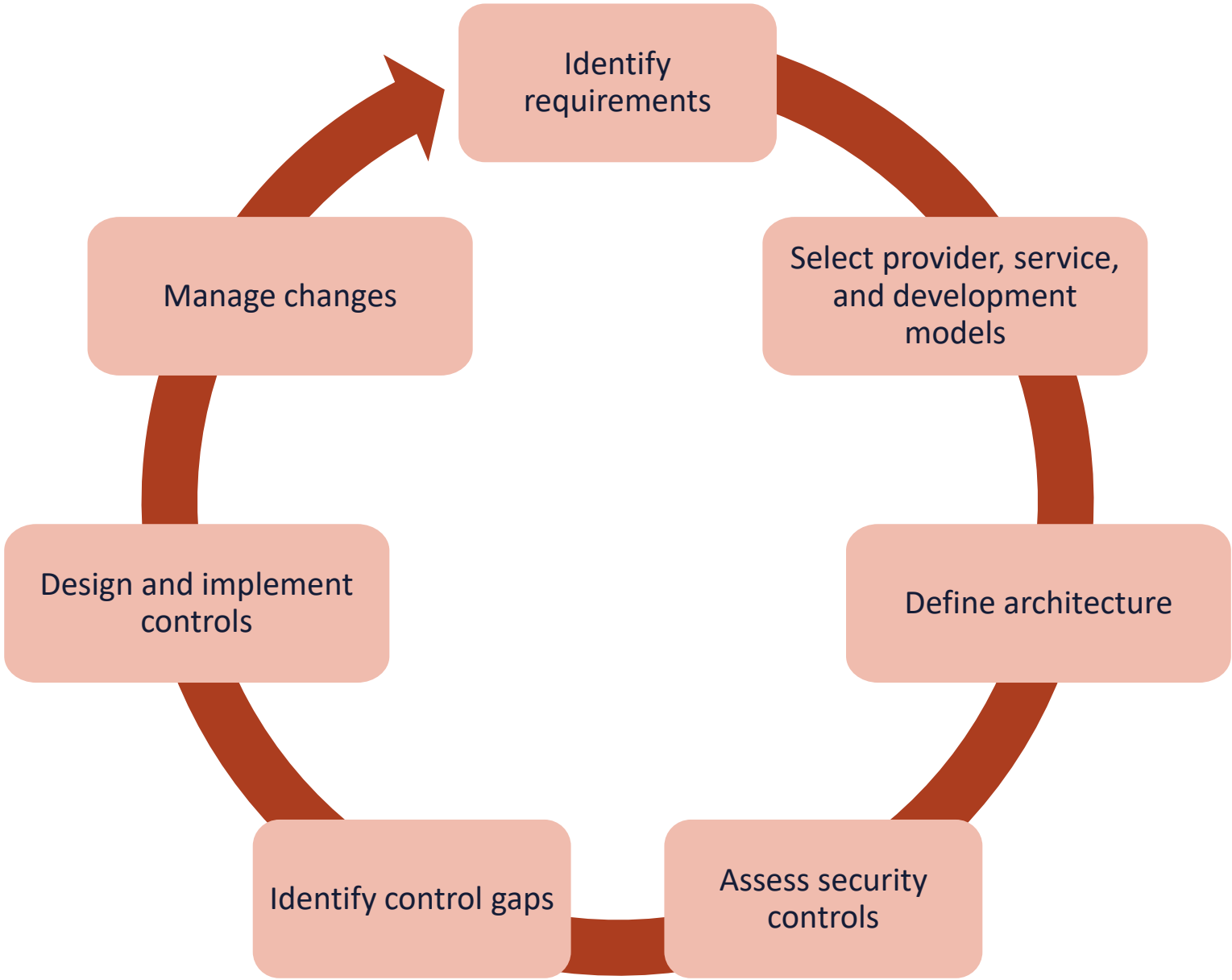
Infrastructure Services

(TOGAF)

Security & Risk Management

(Jericho) (Zero Trust)

CSA Cloud Security Process Model



Defining Risk

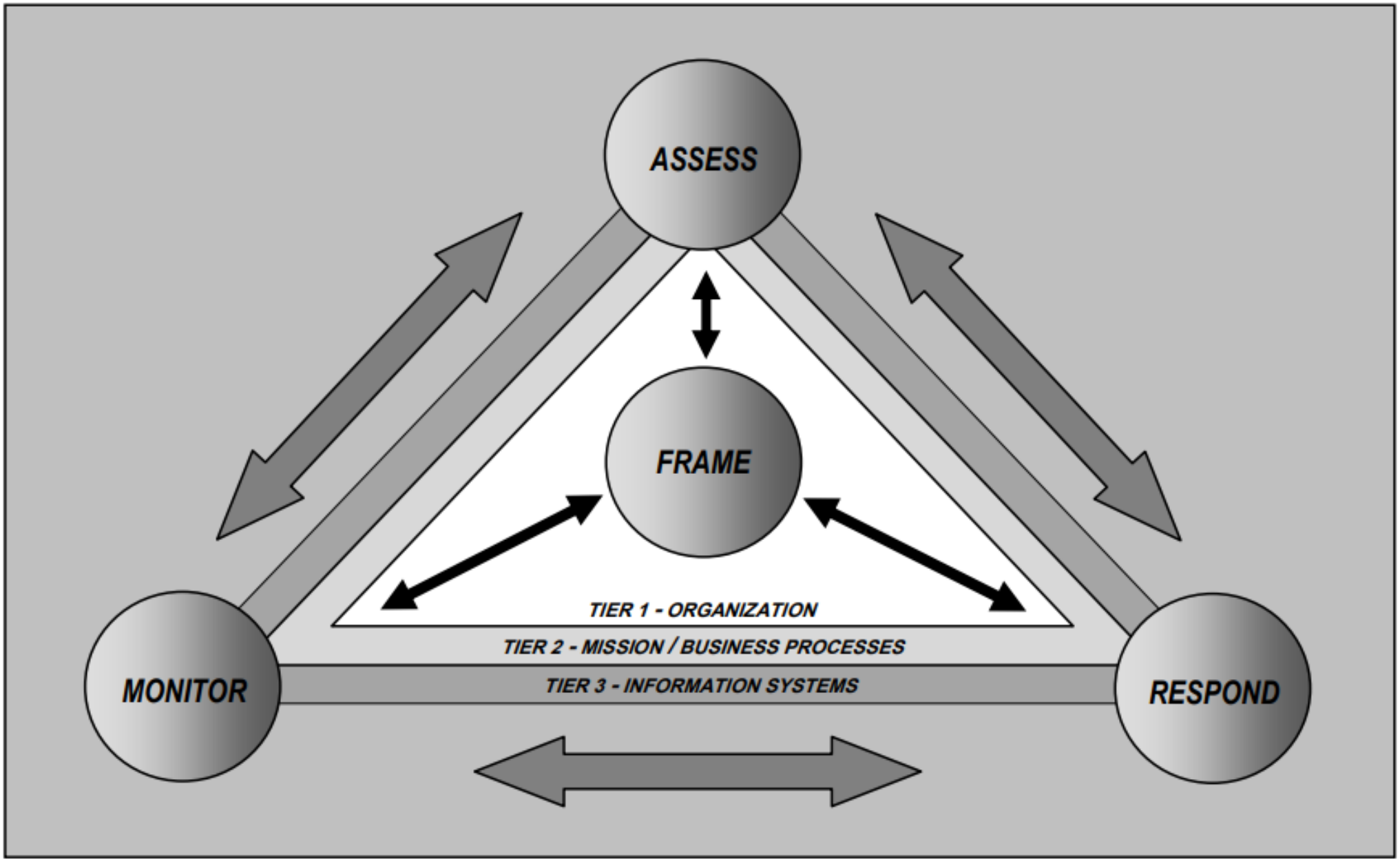
- Inherent (total) risk
  - Risk the organization faces if safeguard is not implemented
- Residual risk
  - Risk that remains once safeguard is in place
- Residual = inherent risk - safeguards (controls)

Risk Treatment

Also called risk handling or appetite

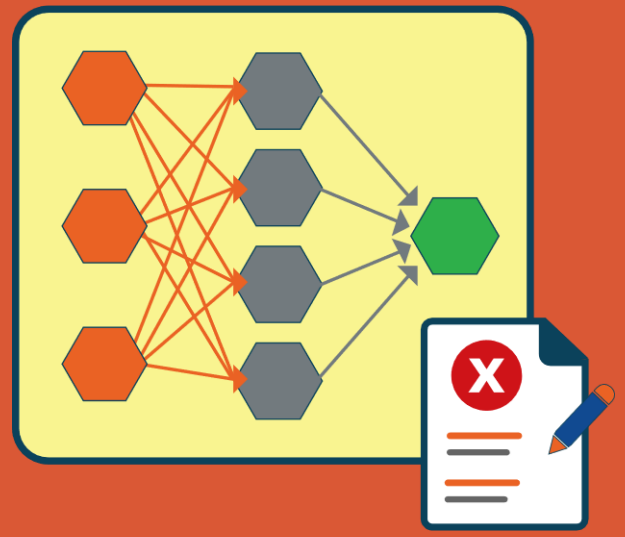
- Risk **acceptance**
  - Do not implement any safeguards
  - Justification in writing is often required
- Risk **avoidance**
  - Choose not to undertake actions that introduce risk
- Risk **transference/sharing**
  - Pass the risk to a third-party, such as an insurance company or a cloud service provider
- Risk **mitigation**
  - Implement safeguards that will eliminate or reduce risk exposure - risk may exist, but impact is reduced

NIST SP 800-39



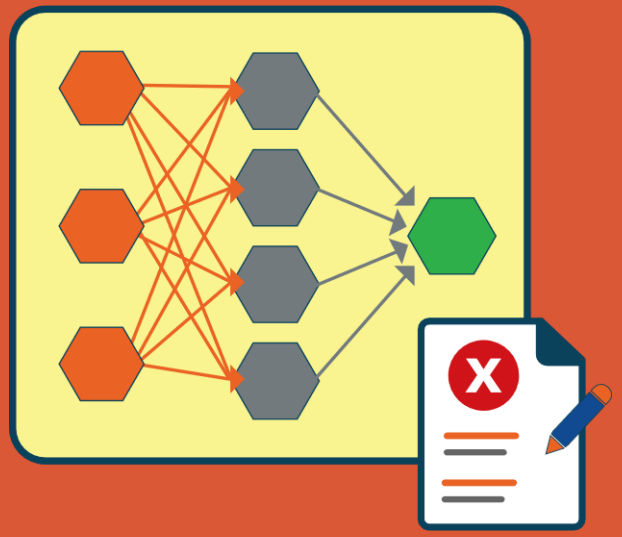
Managing Information Security Risk (NIST SP 800-39)

- **Step 1: Risk Framing**
  - Risk framing establishes the context and provides a common perspective on how organizations manage risk
  - As its principal output, it produces a risk management strategy that addresses how organizations intend to assess risk, respond to risk, and monitor risk
- **Step 2: Assessing Risk**
  - Risk assessment identifies, prioritizes, and estimates risk to organizational
  - Risk assessments use the results of threat and vulnerability assessments to identify and evaluate risk in terms of likelihood of occurrence and potential adverse impact (i.e., magnitude of harm) to organizations, assets, and individuals



Managing Information Security Risk (NIST SP 800-39)

- **Step 3: Responding to Risk**
  - Risk response identifies, evaluates, decides on, and implements appropriate courses of action to accept, avoid, mitigate, share, or transfer risk to organizational operations and assets, individuals, other organizations, and the country, resulting from the operation and use of information systems
- **Step 4: Monitoring Risk**
  - Risk monitoring provides the means to: verify compliance; determine the ongoing effectiveness of risk response measures; and identify risk-impacting changes to organizational information systems and environments of operation
  - Analysis gives organizations the capability to maintain awareness of the incurred risk, highlight the need to revisit other steps in the risk management process, and initiate process improvement activities as needed



Qualitative Risk Analysis

The most common method used in risk and security

- Descriptive approach using subjective opinions, history, and scenarios to determine risk levels
  - Expert judgement
  - Best practices
  - Experience
  - Intuition
- Often involves interviewing people (Delphi) regarding assets, known risks, known vulnerabilities, common threats, and historical impacts

Qualitative Heat Map

Likelihood			Impact				
			Negligible	Minor	Moderate	Critical	Disastrous
			1	2	3	4	5
	Frequent	5	Medium	Medium	High	High	High
	Likely	4	Medium	Medium	Medium	High	High
	Occasional	3	Low	Medium	Medium	Medium	High
	Seldom	2	Low	Low	Medium	Medium	Medium
	Improbable	1	Low	Low	Low	Medium	Medium

Semi-Quantitative Risk Analysis

Impact

- Negligible = 1 (no impact)
- Minor = 2 (< $1 million)
- Moderate = 3 (≥ $1 million)
- Critical = 4 (≥ $100 million)
- Disastrous = 5 (complete)

Likelihood

- Improbable = 1 (almost never)
- Seldom = 2 (not in 5 years)
- Occasional = 3 (once in last 5 years but not in last year)
- Likely = 4 (once in last year)
- Frequent = 5 (several times a year)

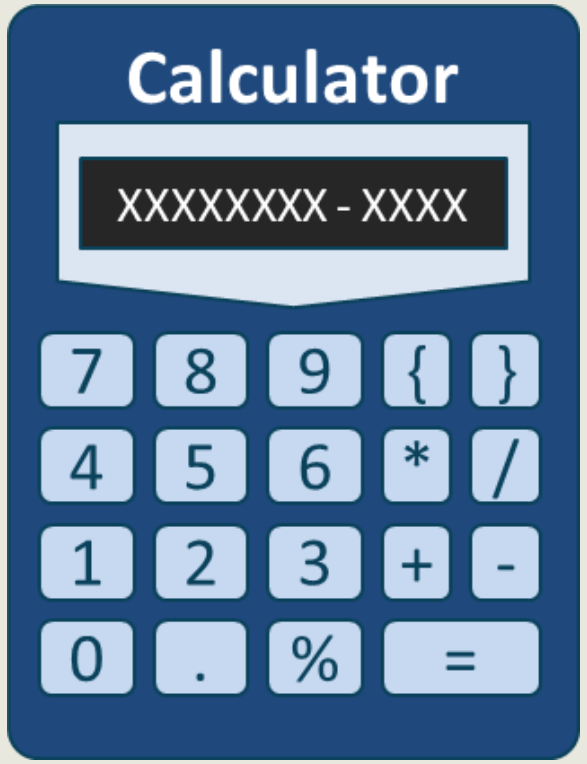
Risk of event = 4 (material impact) X 3 (moderate likelihood) = 12

Quantitative Risk Analysis

Rapidly gaining popularity due to FAIR analysis

- Scientific/mathematical approach to getting monetary and numeric results based on the following:
  - Asset values
  - Impact and magnitude
    - Severity of incident
  - Probability and likelihood of occurrence
    - Threat frequency
  - Costs and effectiveness of safeguards
  - Probabilities based on percentages and calibrated estimation
    - **Goal is to find the 90 percentile**

Classic Quantitative Analysis (Whitman)

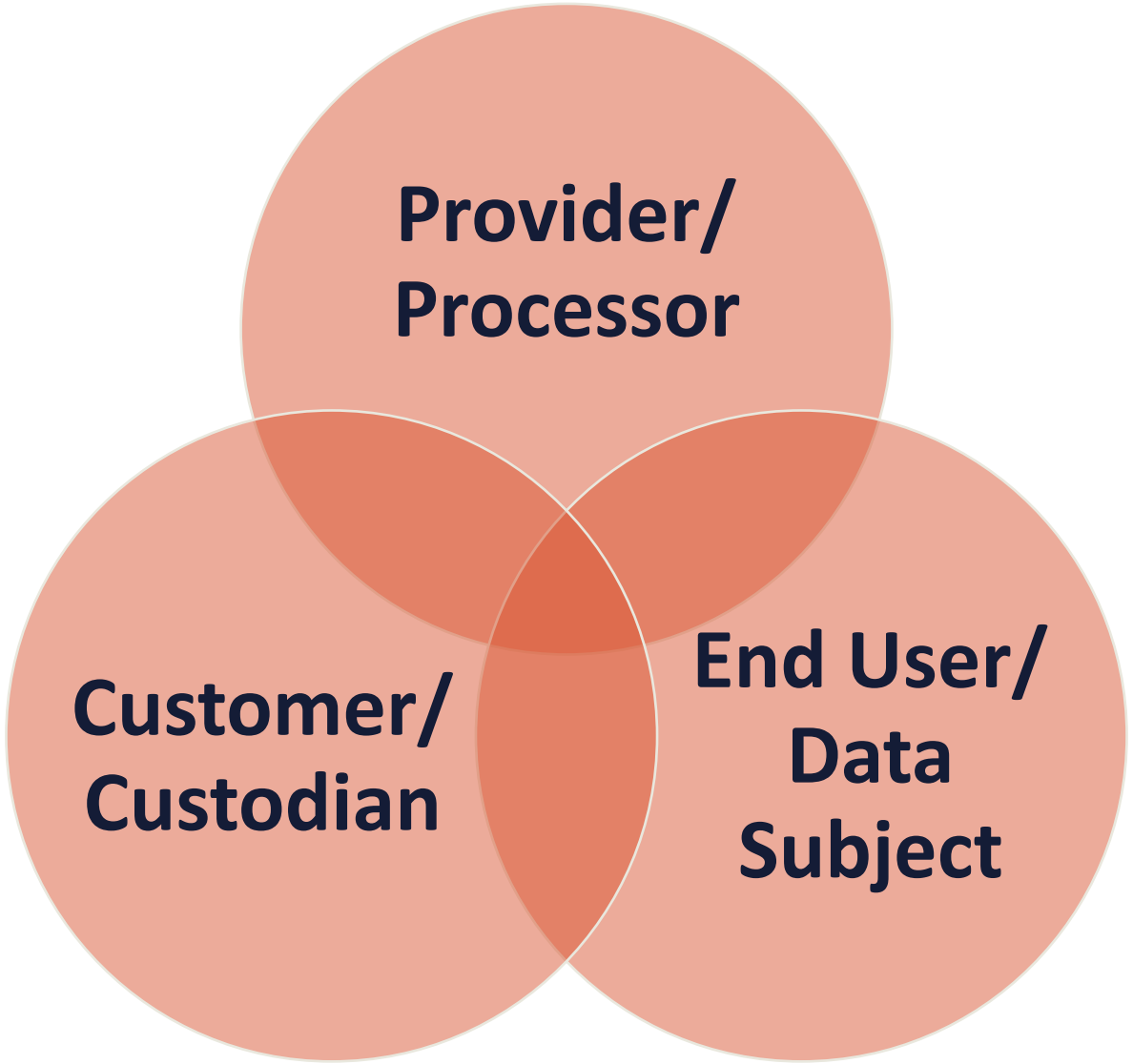


- AV (asset value)
  - Value of the asset according to the organization
- EF (exposure factor)
  - Percentage of asset loss caused by identified threat
- SLE (single loss expectancy)
  - Potential loss if attack occurs
  - (Asset value * exposure factor)
- ARO (annualized rate of occurrence)
  - Estimated frequency the threat will occur within a single year
- ALE (annualized loss expectancy) = (SLE * ARO)

Classic Quantitative Analysis (Whitman)

Risk analysis						
Asset	**Threat**	**Asset value**	**Exposure factor**	**Single loss expectancy**	**Annualized rate of occurrence**	**Annualized loss expectancy**
SRV_1	Fire	$15000	100%	$15000	0.1	$1500
SRV_2	Fire	$20000	100%	$20000	0.1	$2000
SRV_1	Flood	$15000	100%	$15000	0.0001	$1.5
SRV_2	Flood	$20000	100%	$20000	0.0001	$2.0
SRV_1	Virus (no AV software)	$15000	10%	$1500	365	$547,500
SRV_1	Virus (with AV software)	$15000	10%	$1500	1	$1500

Cloud Services Legal Entities



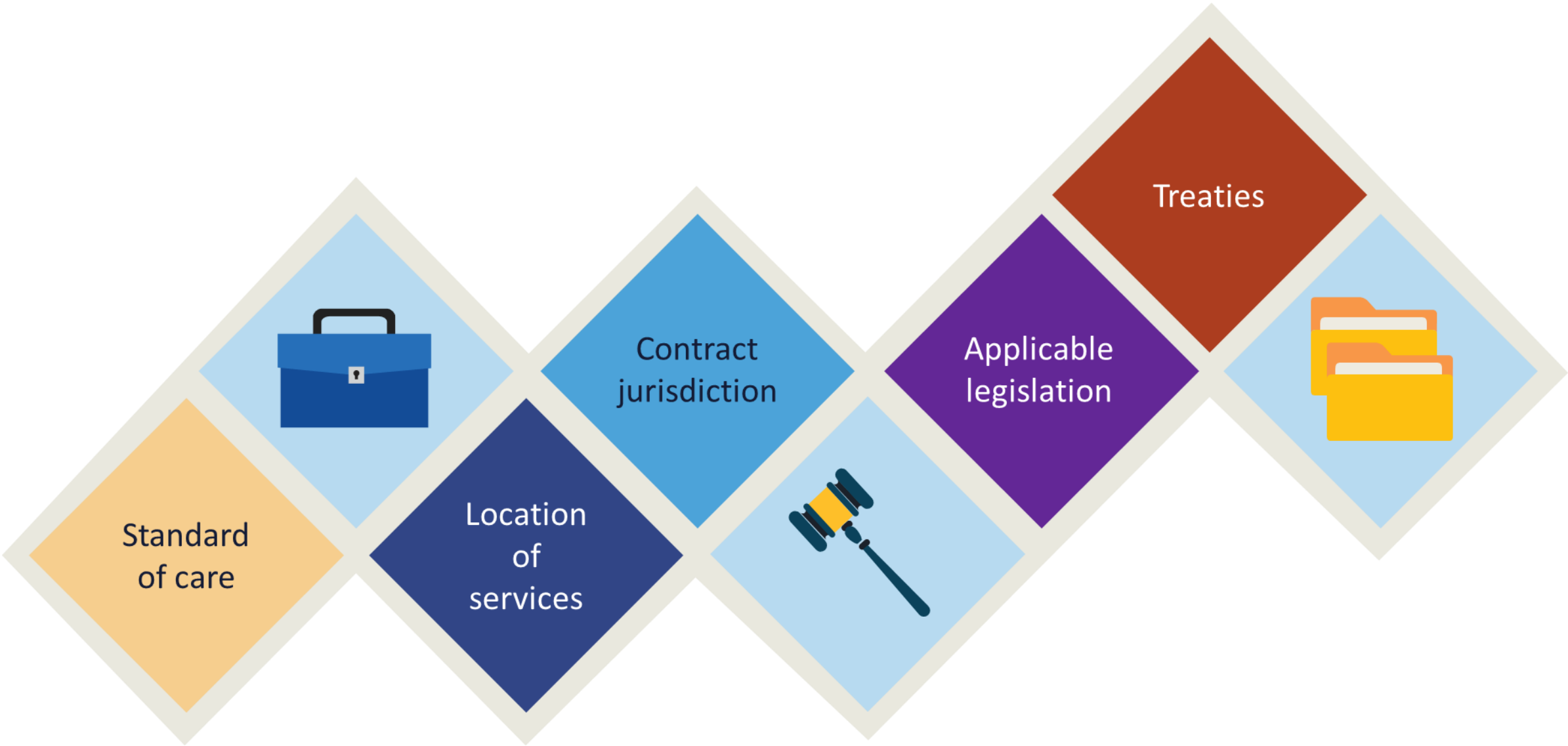
Cloud Services Legal Entities

- **Provider/Processor**
  - The cloud IaaS, PaaS, SaaS, MSSP, or CASB provider
- **Custodian/Controller**
  - The entity that stores the end-user data and applications
  - Legally responsible for properly securing digital assets (depends on service type)
  - Must follow all jurisdictional laws and regulations (i.e., GDPR)
- **End User/Data Subject**
  - The subject whose data is being held by a controller/custodian

PROCESS OF SETTING LEGAL AND REGULATORY REQUIREMENTS

1. Understand the law and relevant regulations that apply to the organization
2. Classify data or operations that might require special attention
3. Establish provider contractual negotiation guidelines
4. Set provider evaluation criteria
5. Understand requirements coming from contractual obligations

Legal Facets when using Cloud Services



Standard of Care

- The standard of care is a legal term that is applied to determine if a person or company should be held responsible for harming others and thus should be made to compensate victims
- A standard of care exists when people or companies engage in certain activities or provide certain services
- **A common practical example would be a cloud-based healthcare system or community cloud**

Cloud Governance Tools

Contracts

- In addition to bilateral instruments, contracts include (but are not limited to):
  - Awards and notices of awards
  - Job orders or task letters issued under basic ordering agreements
  - Letter contracts
  - Orders, such as purchase orders, under which the contract becomes effective by written acceptance or performance
  - Bilateral contract modifications

Common Contract Documents

- **Terms and Conditions** – Key document that defines service situations, data usage, termination options, warranties, legalities, and more
- **Acceptable Use Policy (AUP)** – states how the services can be utilized
- **Service Terms** – provider-specific contractual agreements
- **SLA/OLAs** – defines performance metrics for external and internal vendors and providers
  - SLA is also called Master Service Agreements (MSA)
- **Specific Clauses**

Service Level Agreements (SLAs)

- Define the precise responsibilities of the service provider and set customer expectations
- Also clarify the support system (service desk) response to problems or outages for an agreed level of service
- Can be internal between business units or departments, as well as external
- Should be used with new third-party vendors or cloud providers (SaaS, IaaS, PaaS) for 24-hour support

Master Service Agreement (MSA)

- As part of due diligence in your BCP, you should confirm any/all expectations with the candidate service provider and ensure that they are documented in your MSA/SLAs
- A master service agreement (MSA) is a contract two parties enter into during a service transaction
- This agreement details the expectations of both parties
- The goal of a master service agreement is to make the contract process faster
- It also should make future contract agreements simpler

Organizational Level Agreements (OLAs)

- An OLA documents the pertinent information for regulating the relationship between internal service recipients and an internal IT area (service provider)
- The difference between an SLA and an OLA is what the service provider is promising the customer (SLA) vs. what the functional IT groups promise each other (OLA)
- An OLA often corresponds to the structure of an SLA with a few specific differences based on the enterprise

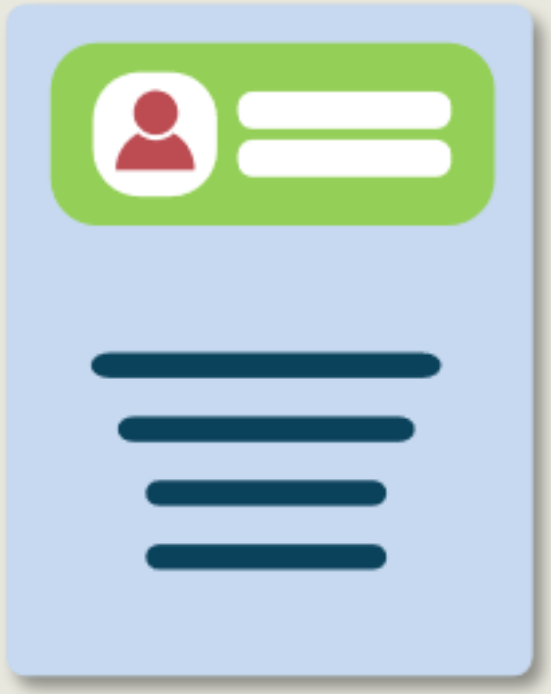
Non-Disclosure Agreements (NDAs)

- Also called "Confidentiality Agreements"
- Legal contract between two or more parties
  - Confidential relationship that is often strictly enforced
  - Business to business/business and employee
- Identifies confidential information they wish to share with each other
  - IP, trade secrets, technologies, campaigns, ideas, new processes, new products, and services
  - Restricts the sharing of that information with others
- Commonly used during interview process and then legally enforced for “leavers”

Memorandum of Understanding (MOUs)

- Also called a Memorandum of Agreement (MOA) or "letter of intent"
- A formal MOU (or MOA) usually precedes a more formal agreement or contract ISA
- It defines common courses of action and high-level roles and responsibilities in management of a cross-domain connection
- It will usually terminate the customer's provider search process so that subsequent time and resources can be dedicated to the next steps of the formal contract process

Reciprocal Agreements



- A reciprocal agreement is between two organizations with similar infrastructure and technology – often difficult to legally enforce
- The most common goal is that one can be a recovery site for the other in case of a disaster or lengthy outage
- Also seen with data backup and escrow services whereby two departments or organizations agree to store one each other's backup data on their computers

Evaluation of Legal Risks Specific to Cloud Computing

- Data Privacy and Security (GDPR, PCI-DSS, HIPAA)
- Data Ownership
  - Intellectual property rights and DRM/IRM in various agreements and contracts
- Liability for copyright infringement, data breaches, and privacy violations
- Primary and secondary loss
- Legal issues resulting from counter-attack active defense
- Jurisdictional Issues (import-export, cultural sensitivities)

Treaties

- Treaties are binding agreements between two political authoritative entities and nations and become that part of international law
- Treaties to which the United States is a party also have the force of federal legislation, forming part of what the Constitution calls "the supreme Law of the Land.”

Cross-border Data Transfer Issues

- Many countries restrict data being used and stored outside of their national boundaries
- Without existing treaties, the situation will be more complex for cloud security managers
- Organizations must carefully consider content distribution to various regions, zones, and edge locations
- Data importer and exporter may sign end user privacy rights agreements

SAMPLE: INTERNATIONAL SANCTIONS AND EXPORT COMPLIANCE POLICY

1. **Statement and Policy** – To provide guidance on export controls and sanctions laws and regulations, policies, and how they relate to the corporate work and to assist officers, directors and employees in complying with these policies, laws and regulations, and direct where to go for help navigating complex legal requirements
2. **Trade Sanctions** - Sanctions restrict or prohibit dealings, directly or indirectly, with certain targeted countries, governments, groups, or persons. The nature and extent of sanctions vary depending on the intended target and the intended objective

SAMPLE: INTERNATIONAL SANCTIONS AND EXPORT COMPLIANCE POLICY

- **Types of Trade Sanctions**
  - **Sanctioned Territories** – From a US perspective, presently may represent areas such as Cuba, Iran, North Korea, Syria, and regions of Ukraine
  - **Sanctioned Parties**: - Certain individuals, entities, and even vessels or aircraft (“Sanctioned Parties”) are targets of U.S. sanctions under a variety of U.S. sanctions programs.
    - Certain parties are deemed to be associated with restrictive regimes or undermining democracy in various countries or territories under "list-based" programs
  - **Significant Sanctions Regimes** - Other significant sanctions apply to for example: U.S. Persons are also restricted from engaging in commercial activity with the Government of Venezuela

SAMPLE: INTERNATIONAL SANCTIONS AND EXPORT COMPLIANCE POLICY

3. **Export Controls** - Regulations that are applicable to the transfer of items (i.e., goods, software, technology) and for U.S. purposes apply to exports from the United States, re-exports from other countries, and transfers (in-country) of US origin/content items
    - Various licensing requirements can apply to these activities depending on the sensitivity and export classification of the item at issue, the country of destination (not limited to Sanctioned Territories), the end-user, and the end-use
    - The U.S. export controls applicable to this company are primarily the **EAR**, which are administered and enforced by the U.S. Department of Commerce's **BIS** licenses the export, re-export, and transfer of U.S.-origin and certain U.S. content “dual use”

SAMPLE: INTERNATIONAL SANCTIONS AND EXPORT COMPLIANCE POLICY

- U.S. export controls apply to items that are subject to the jurisdiction of the Export Administration Regulations (EAR) and include:
  - items **exported** from the US
  - items **manufactured in** the US
  - items **manufactured outside** of the US that incorporate above applicable de minimis levels of controlled US origin content (i.e., 10% for most comprehensively sanctioned countries, and 25% for all other destinations)
  - in some cases, certain foreign direct products of certain controlled US technology or software

SAMPLE: INTERNATIONAL SANCTIONS AND EXPORT COMPLIANCE POLICY

- There are **five** basic questions you should be asking whenever you are entering into an export transaction:
  - **WHAT** is the item being exported (i.e., what is the classification)?
  - **WHERE** is the item going (i.e., what is the destination country and any intermediate country)?
  - **WHO** will use the item (i.e., who is the ultimate end-user)?
  - **WHY** do they want the item (i.e., what is the ultimate end use)?
  - **WHAT other activities** is the customer/end-user engaged in (i.e., this goes to risk of diversion to high-risk

SAMPLE: INTERNATIONAL SANCTIONS AND EXPORT COMPLIANCE POLICY

4. **Anti-Boycott Laws -** Of particular concern to business in the Middle East, some are required to comply with U.S. anti-boycott laws and regulations
   - Anti-boycott laws can be seen as the reverse of sanctions laws: they essentially prohibit a party from complying with someone else's sanctions
   - U.S. companies are prohibited from participating in foreign boycotts that aren't supported by the U.S. Government
5. **Record Keeping**
6. **Reporting Obligations and Non-retaliation**
7. **Consequences of Violation of Policies**
8. **Frequently Asked Questions (FAQ)**

Data Discovery

- Data discovery is a methodology that often serves two goals:
  - The enterprise is performing an initial asset assessment and inventory of data ownership
  - The organization is performing e-discovery as part of a digital forensic investigation
- There are three main forms of data discovery
  - **Content-based** – dataset contents such as terms and pattern-matching
  - **Label-based** – discovery is based on existing labels an/or tagging that is applied to physical and logical assets both on-prem and in the cloud
  - **Metadata-based** – leveraging the extensible metadata available on data stored as objects – i.e., using APIs against data in AWS S3, Google Cloud Storage, Azure Blob storage

ISO/IEC 27050

- Information Technology Electronic Discovery Package offers guidance methods on establishing the electronic discovery process
- The ISO/IEC 27050 series enables the user to identify, collect, preserve, process, review, and analyze electronically stored information
- Electronic discovery often serves as a driver for investigations as well as evidence acquisition and handling activities
- **Exam: It is not intended to contradict or supersede local jurisdictional laws and regulations**

Internal Due Diligence

- Custodian/controller may be responsible for legal repercussions if due diligence is not performed
- Customers and Providers must both consider all processes, needs, and constraints as well as legal and compliance requirements
- You must always consider the cloud-enabled nature of data and applications
- Continuous monitoring, testing, and upgrading must be conducted

External Due Diligence

- Evaluations of all pertinent cloud documentation must be performed
  - Example: AWS Artifact documents and reports
- All service level agreements must be analyzed
- Audits of supply chains should be performed
  - Supply Chain Management
- CSA CCM is a vital resource for the exam

RACI Charts for Mapping Roles

R – Responsible **A** – Accountable **C** – Consulted **I** - Informed

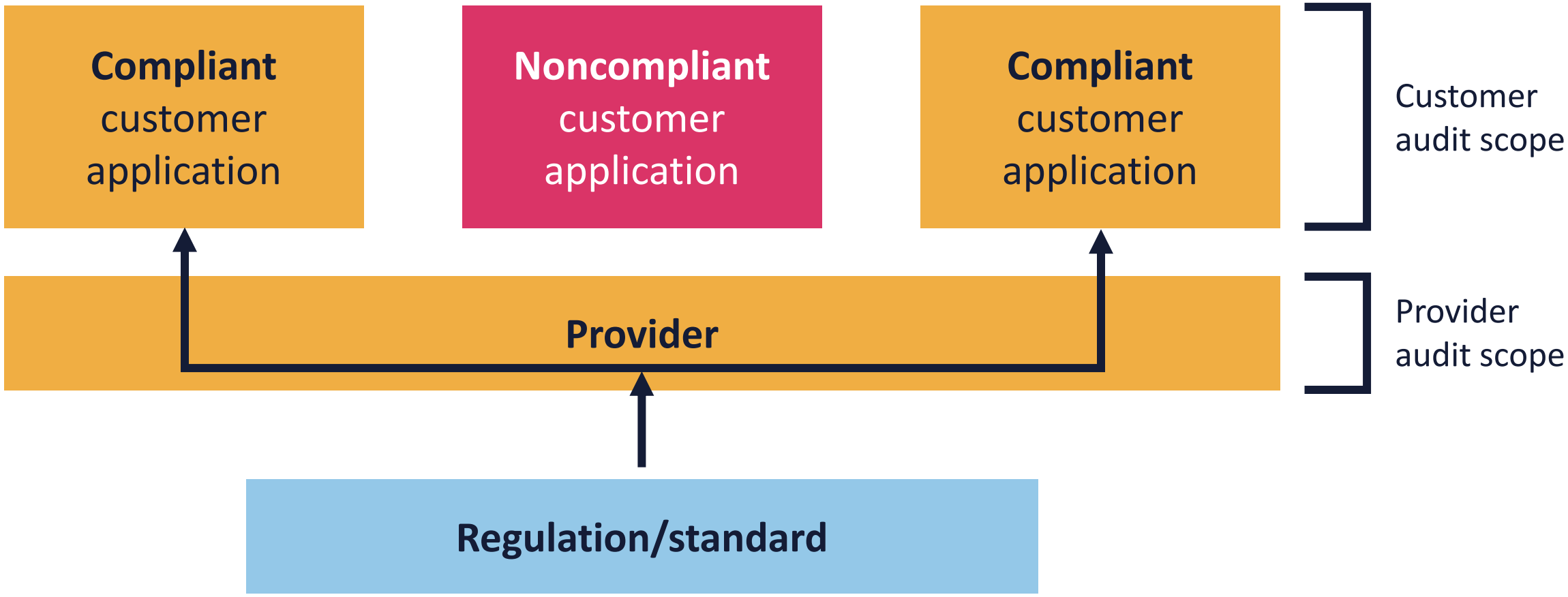
	GRC* Department	Legal Department	Security Team	IT Operations
Establish the provider requirements	R/A	C	C	I
Build the governance scheme	R/A	C	C	I
Assess cloud vendor	A	I	R	R
Build the architecture	I	I	A/R	R
Conduct cloud migration	I	I	C	A/R

**GRC – Governance, Risk, and Compliance*

Compliance Considerations

- Considerations of exports of data to foreign jurisdictions
- Application of the Shared Responsibility Model
- Complexity and disruptions of the cloud supply chain
- Obtaining documentation, reports, and artifacts from the providers
- Scope of audits and assessments
- Maturity of compliance testing and management
- Provider experience with regulatory entities
- Inheritance of compliance from an IaaS to a SaaS

Inheriting Compliance

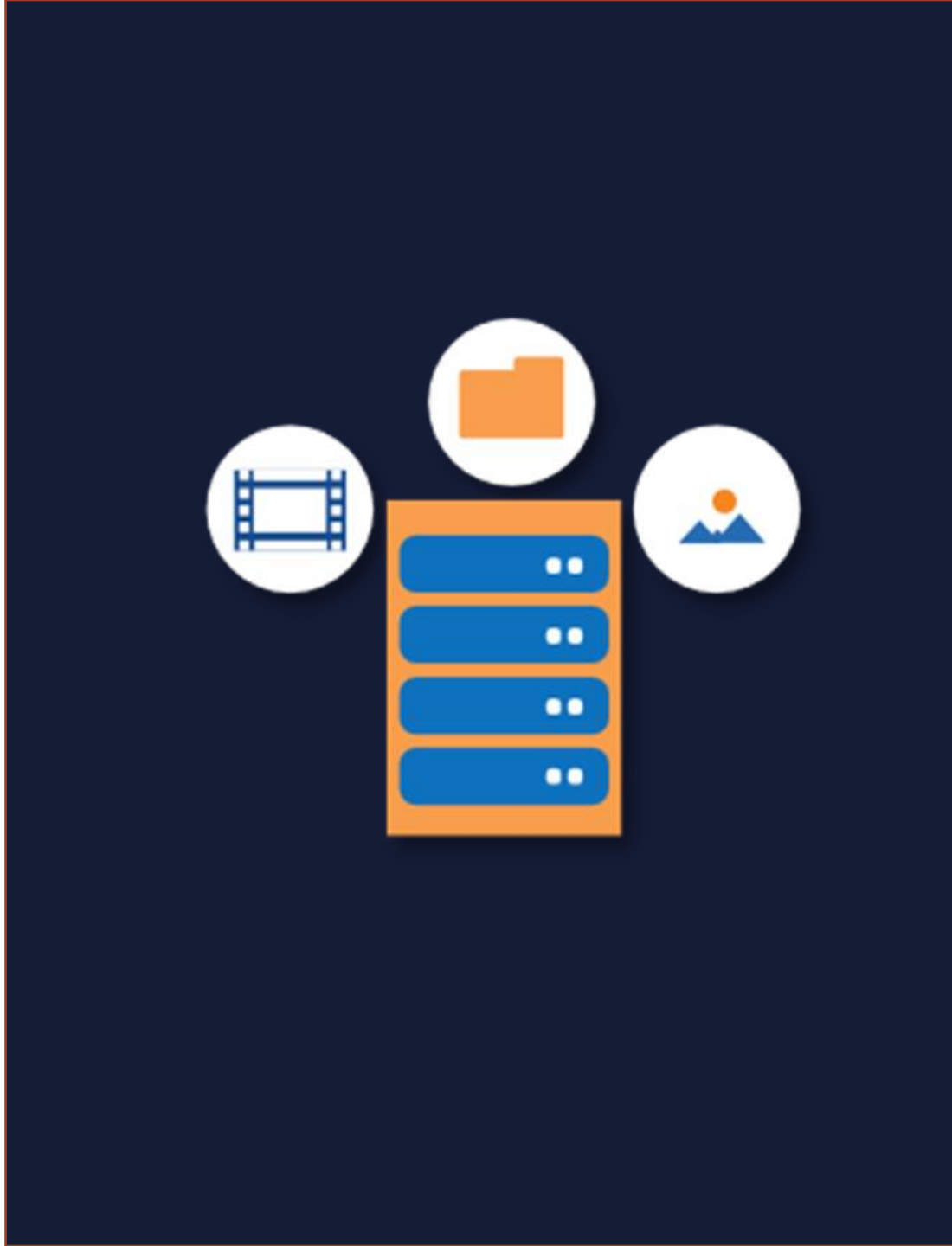


Statement on Standards for Attestation Engagements (SSAE)

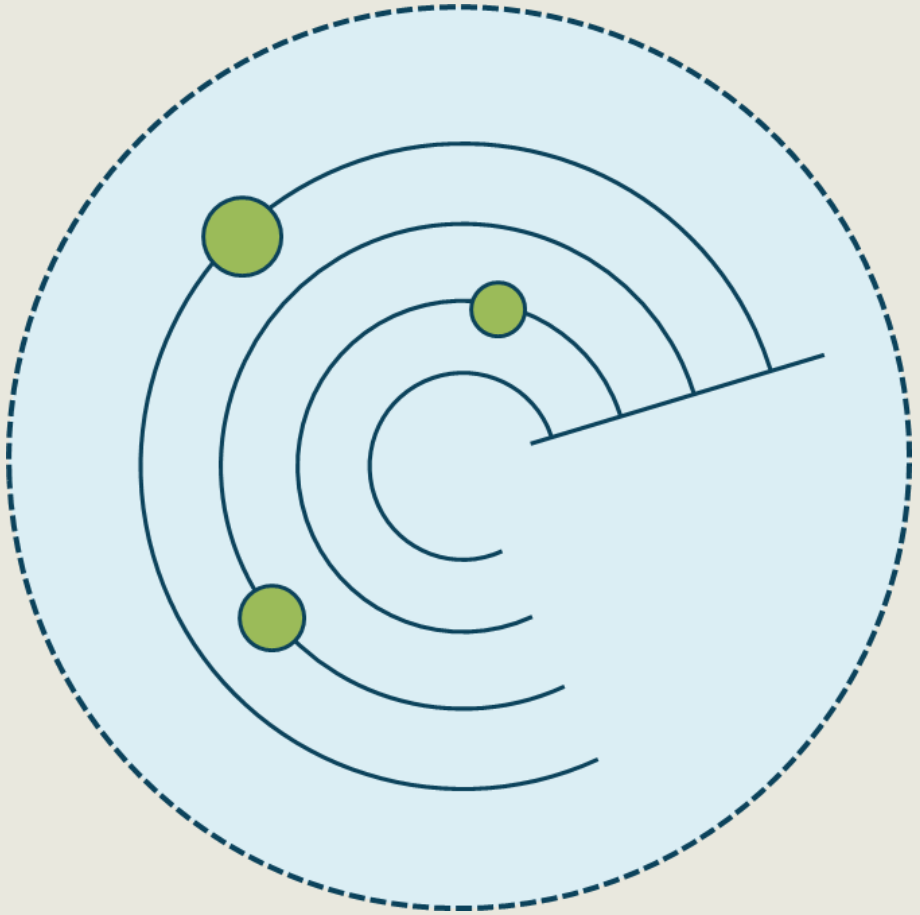
- Statement on Standards for Attestation Engagement (SSAE) 18 is an American auditing standard issued by the American Institute of Certified Public Accountants (AIPCA)
- It addresses engagements undertaken by a service auditor for reporting on controls at service organizations that provide services to user entities, for which a service organization's controls are likely to be relevant to a user entities internal control over financial reporting
- The SSAE 18 standard is used to produce three types of System and Organization Controls (SOC) reports - SOC 1, 2 and 3

Service and Organizational Controls

- SOC 1
  - Report used for Internal Control over Financial Reporting (ICFR) and auditing financial statements
- **SOC 2**
  - **Called "Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy"**
- SOC 3
  - Publicly available "high-level" statement from a CPA that a SOC engagement was conducted



Audit Management in the Cloud



- Assures that the initiatives and directives are implemented in an optimal way
  - Internal and/or external auditors
  - Purpose and goal of audit
  - Scope of the audit
  - Contribution to risk management and analysis
  - Audit standard operating procedures and processes
  - Available physical and digital resources
  - Scheduling and other logistics (project management)

Audit Mechanisms

Involves tools and techniques

- Various logs (system, application, firewall, etc.) and activity reporting (DAM)
- Simple Network Management Protocol (SNMP) traps and informs
- NetFlow v5 and v9 collections
- Security information and event management (SIEM) and Security Orchestration, Automation, and Response (SOAR) systems
- Next-Gen IPS and IPS
- Change and configuration management
- Cloud-based ML and AI visibility/analysis

Relevant ISO/IEC Compliance Standards

- 27001 - The world's best-known standard for information security management systems (ISMS) and their requirements – has an appendix with list of controls
- 27002 – Code of practice catalog for ISMS that lists controls (over 130) and guidance serving as best practice recommendations
- 27005 – Information security risk management guidelines document to assist with 27001 compliance
- 27017 – Set of security controls from 27002 that are modified for cloud services by adding cloud-specific controls (cloud service extended control set)
- 27018 – The code practice for protection of personal data (PII) in cloud computing environments

Cloud Information Governance Domains

- Ownership and custodian/controller responsibilities
- Data and asset classification schemas
- Information management policies (AUP, DRP, IRM, DRM related to PII, PHI, and IP)
- Jurisdictional and regional locality policies
- Authorizations and exceptions
- Applicable contractual controls
- Applicable security controls for confidentiality, integrity, authenticity, availability, and non-repudiation

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Data Classification

- **Government/Military**: Top Secret > Secret > Confidential > Sensitive But Unclassified (SBU) > Unclassified
- **Commercial/Private sector**: Confidential > Private > Sensitive > Public
- **User-based**
- **Content-based**
- **Context-based**

Management Plane Protection

- Historically speaking, protection was configured locally on often overlapping control, management, and data planes (Cisco) on individual infrastructure devices
- Devices were configured in-band and out-of-band with management VLAN's, or IPsec AH protected production management traffic
  - There was a heavy reliance on device hardening and secure management protocols though access servers with local or centralized AAA using access control or identity services engines
- Principles such as Least Privilege, Segregation of Duties, and Dual Operator in a "Trust but Verify" environment was common
- **Today, modern private and public cloud data centers rely on Zero Trust, Software-Defined Networking (SDN) and Orchestration technologies (SD-WAN and SD-MAN)**

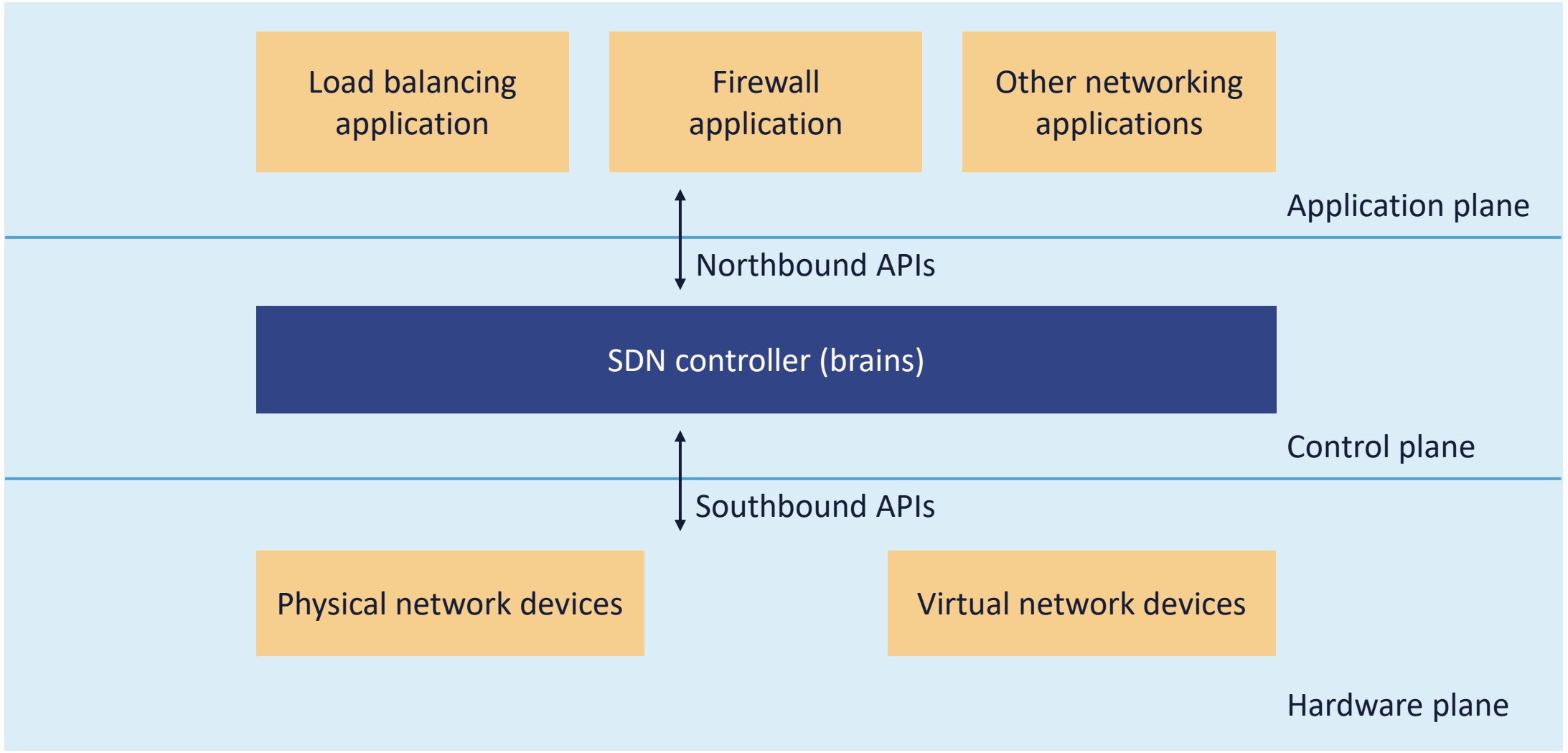
Software-Defined Networking (SDN)

- Directly programmable
  - Network control is directly programmable because it is decoupled from forwarding functions
- Agile
  - Abstracting control from forwarding lets administrators dynamically adjust network-wide traffic flow to meet changing needs
- Centrally managed
  - Network intelligence is (logically) centralized in software-based SDN controllers that maintain a global view of the network, which appears to applications and policy engines as a single, logical switch

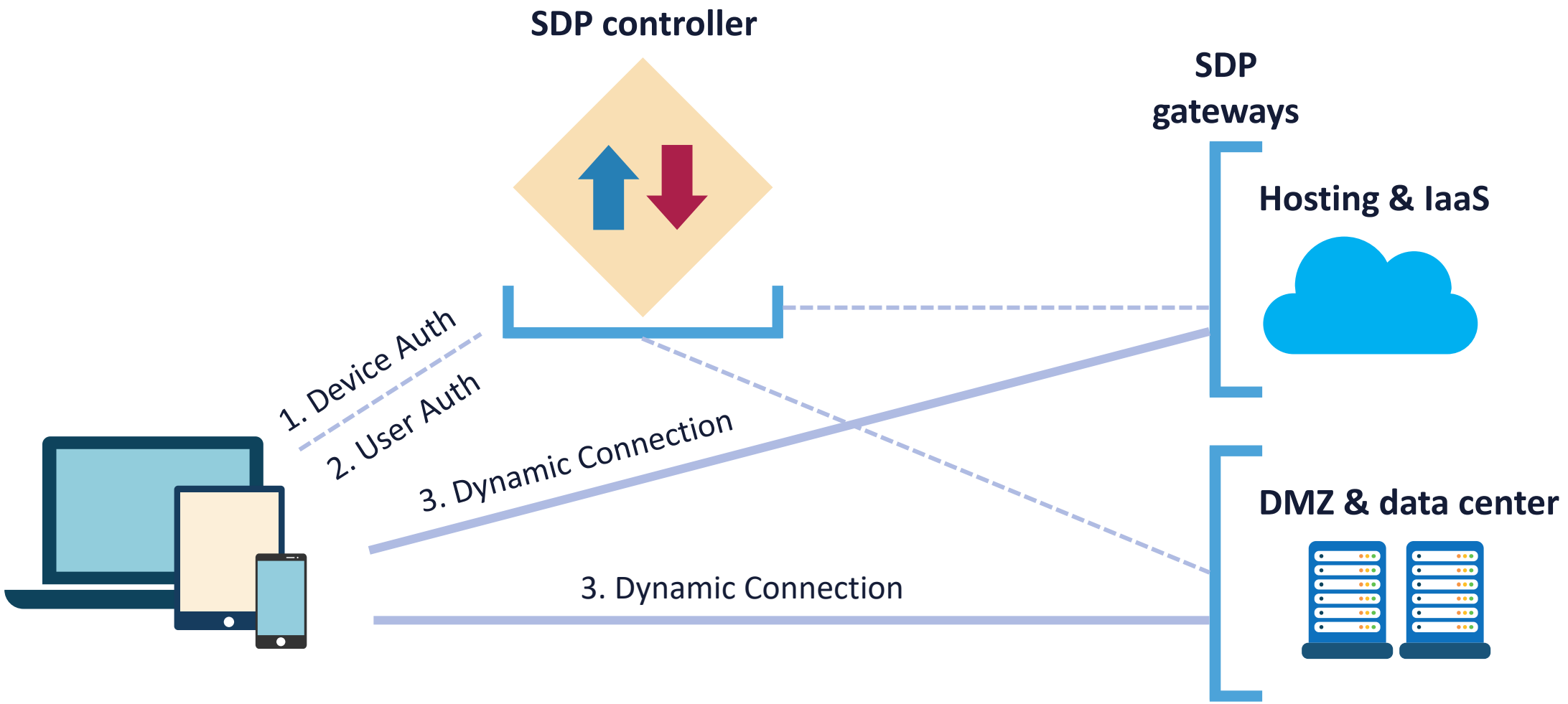
Software-Defined Networking (SDN)

- Programmatically configured
  - SDN lets network managers configure, manage, secure, and optimize network resources very quickly via dynamic, automated SDN programs, which they can write themselves because the programs do not depend on proprietary software
- Open standards-based and vendor-neutral
  - When implemented through open standards (OpenFlow), SDN simplifies network design and operation because instructions are provided by SDN networking controllers instead of multiple, vendor-specific devices and protocols

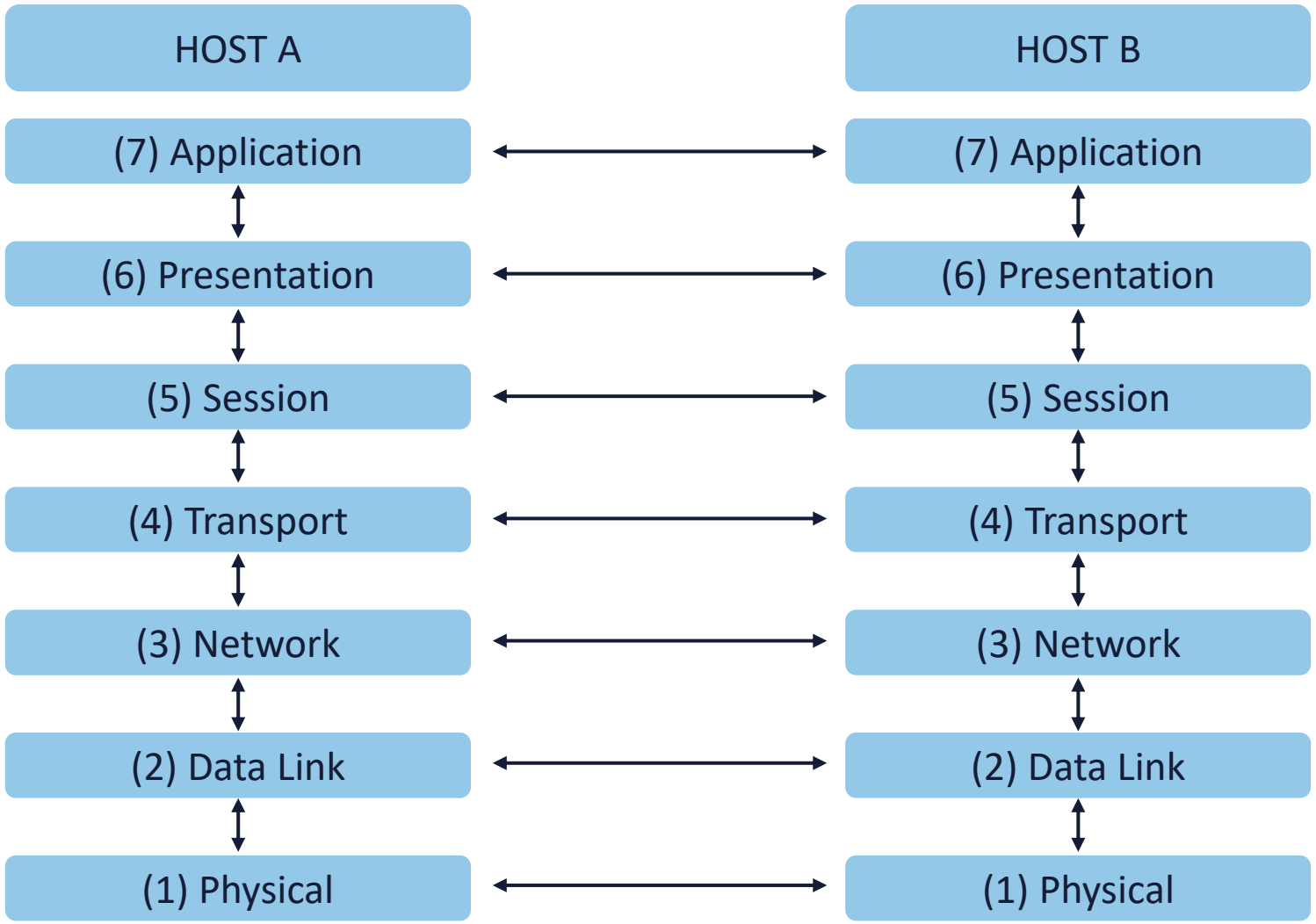
SDN Enterprise



SDN Enterprise



The ISO OSI 7-Layer Model



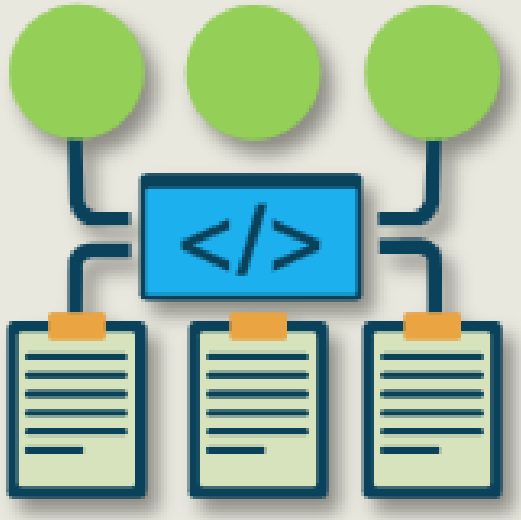
Cloud Datacenter Network Types

Management network	Storage network	Service network
• Management plane to pools (using APIs)	• Storage volumes to instances	• Internet to instances • Instance to instance

All three of these networks should run on different physical networks

Software-defined Security (SDS)

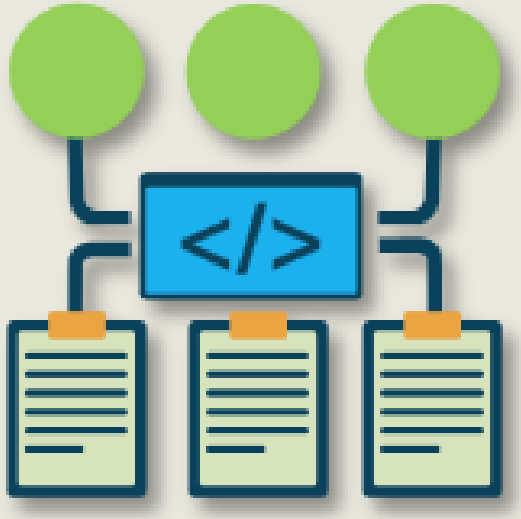
Used with Software-defined Networks



- Software-defined Security (SDS) is a model in which the information security is highly controlled often using virtualization
- The functionality of network security devices, such as next-gen firewalls, intrusion detection and prevention, identity and access controls, and network segmentation are removed from hardware devices to a software layer

Software-defined Security (SDS)

Used with Software-defined Networks



- SDS exploits the software-defined networking (SDN) initiative to enhance network security
- The concept of software-defined security is envisioned to define IT infrastructure security services as a transition from hardware based to a software-defined solution

Advantages of SDS

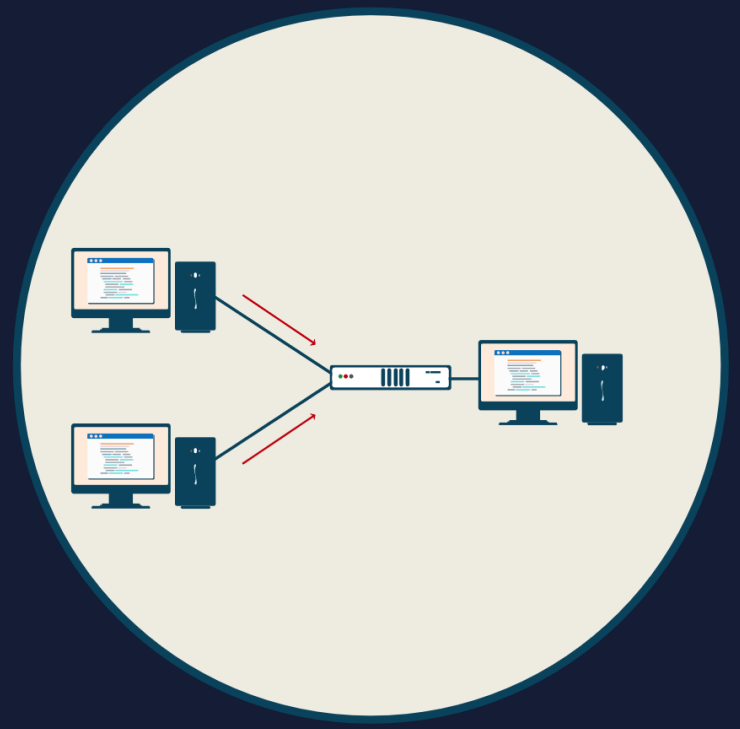
- Offers resourceful and dynamic countermeasures to security attacks
- Separates security away from traditional hardware vulnerabilities
- Ability to dynamically configure existing network nodes allows for rapid attack mitigation from zero-day attacks
- Synchronized view of logical security policies exist within the SDN controller model (not tied to any server or specialized security device)

Advantages of SDS

- Visibility of information provided from one source
- Integration with emerging technology to correlate events in a simpler way and respond more efficiently and intelligently to threats
- Enables centralized management of security, which is implemented, controlled, and managed by security software through the SDN controller
- Facilitates IoT & BYOD connectivity and security

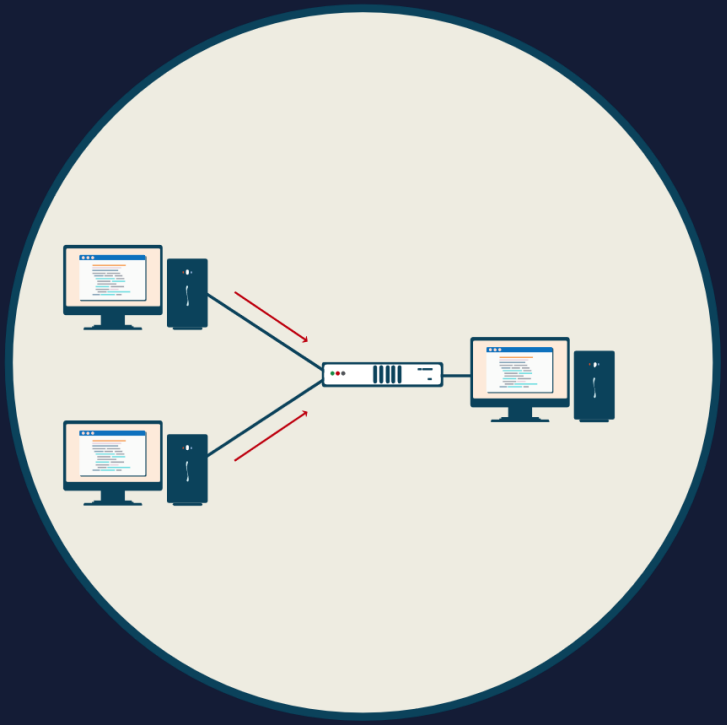
Virtual Extensible LAN (VXLAN)

- VXLAN is technically an encapsulation protocol that offers data center connectivity using tunneling to stretch Layer 2 connections over a Layer 3 network
- VXLAN solutions from a variety of vendors decouple the physical hardware from the network map in order to support virtualization
  - This uncoupling allows the data center network to be deployed programmatically



Virtual Extensible LAN (VXLAN)

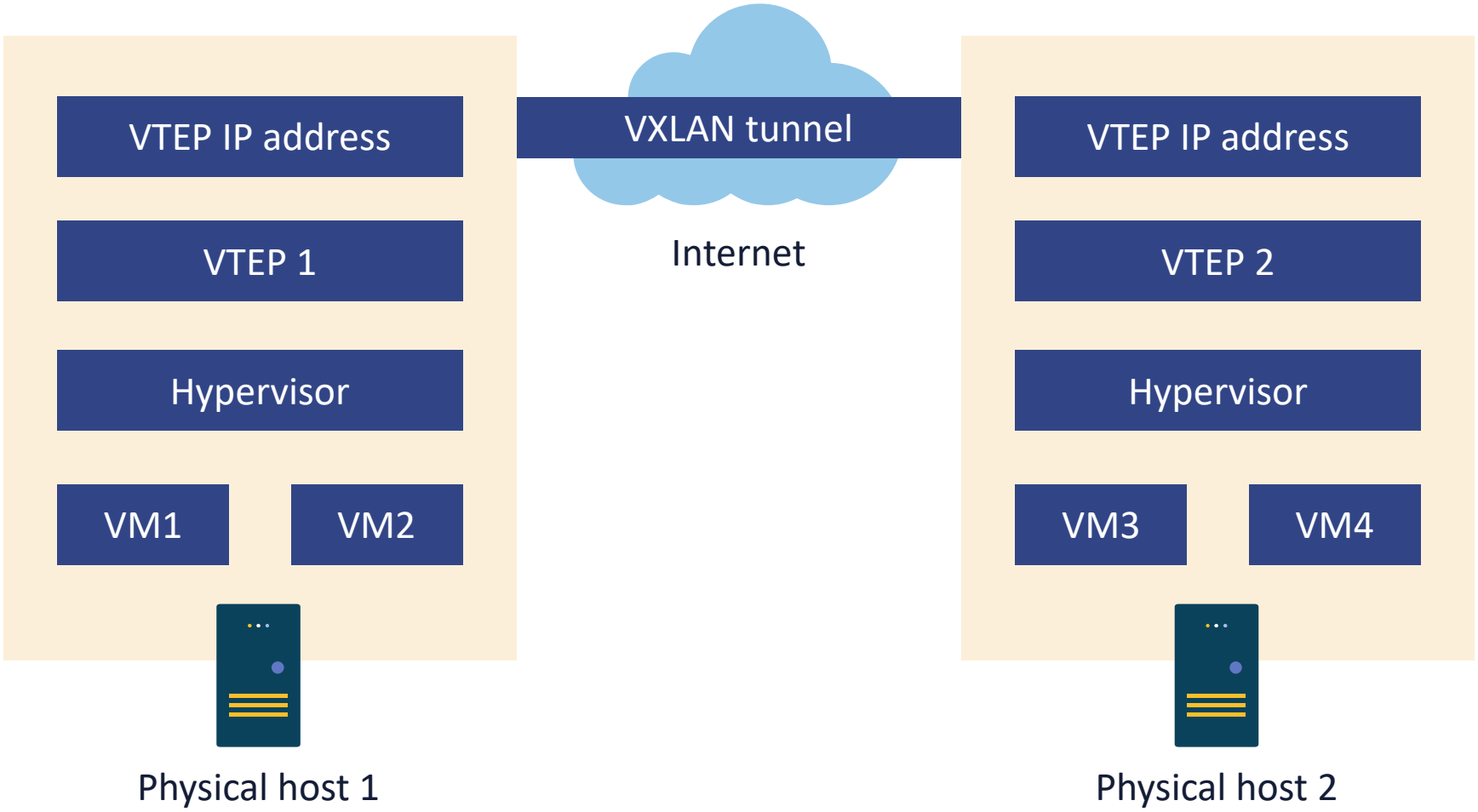
- It allows both Layer 2 and Layer 3 transport between VMs and bare-metal servers
- VXLAN supports the virtualization of the data center network while addressing the needs of multi-tenant data centers by offering the necessary scalable segmentation
- The traditional 802.1Q frame with the 12-bit VLAN identifier is replaced with a 24-bit VXLAN frame so one can theoretically create as many as 16 million VXLANs in an administrative domain



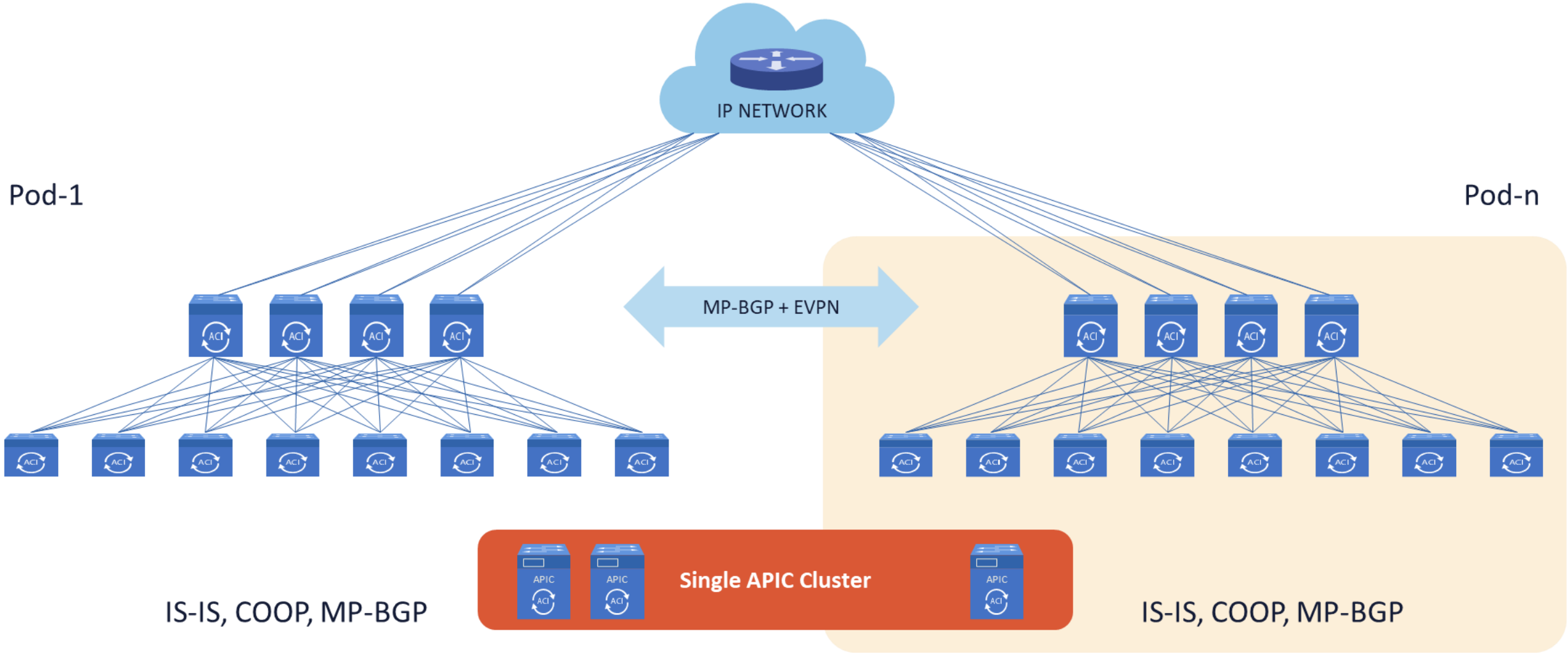
VXLAN Frame

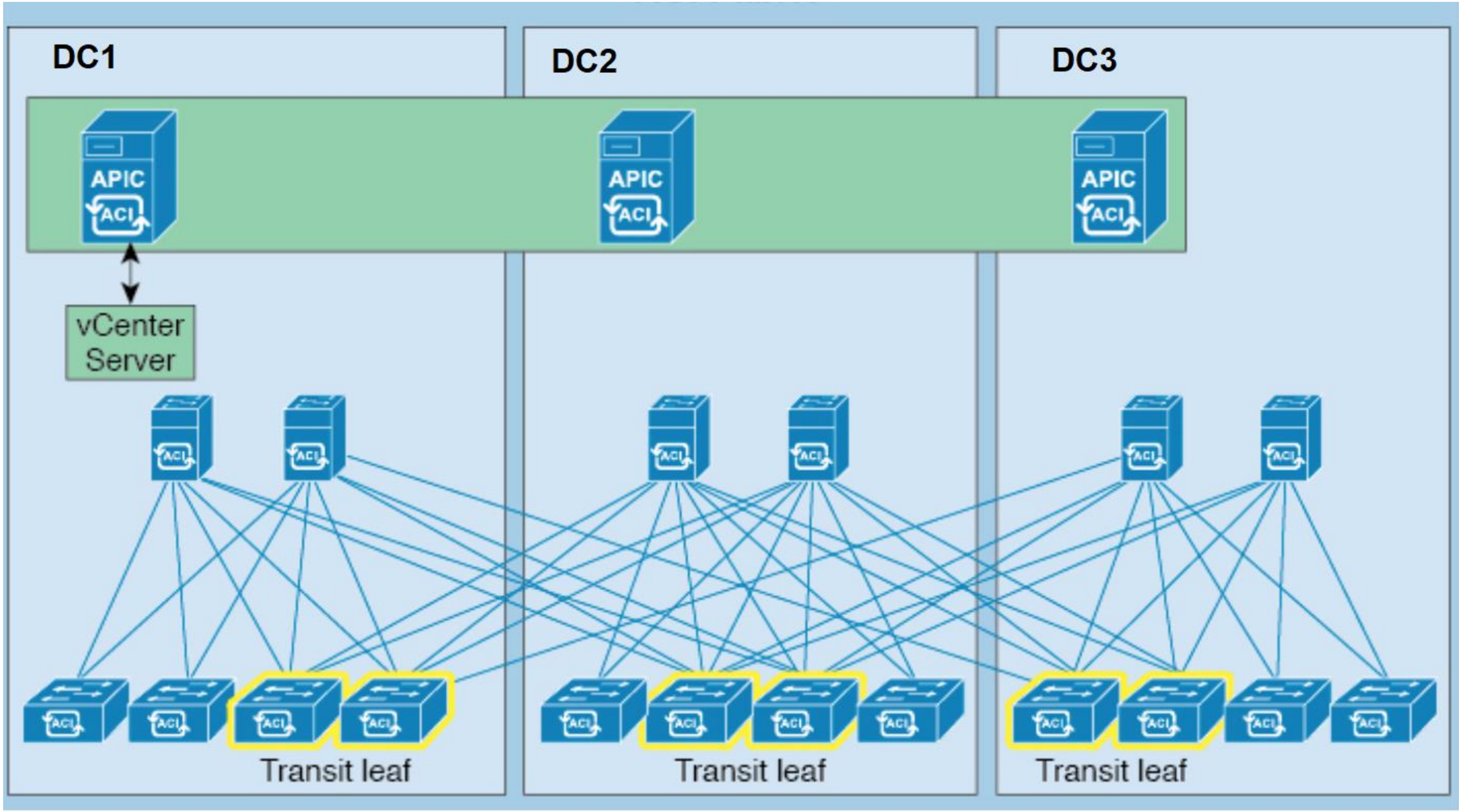
- The VXLAN tunnel endpoint (VTEP) is the device that is responsible for encapsulating and de-encapsulating the layer 2 traffic
- This device is the connection between the overlay and the underlay network
- The VTEP comes in two forms:
  - Software (host-based)
  - Hardware (gateway)

VXLAN Topology



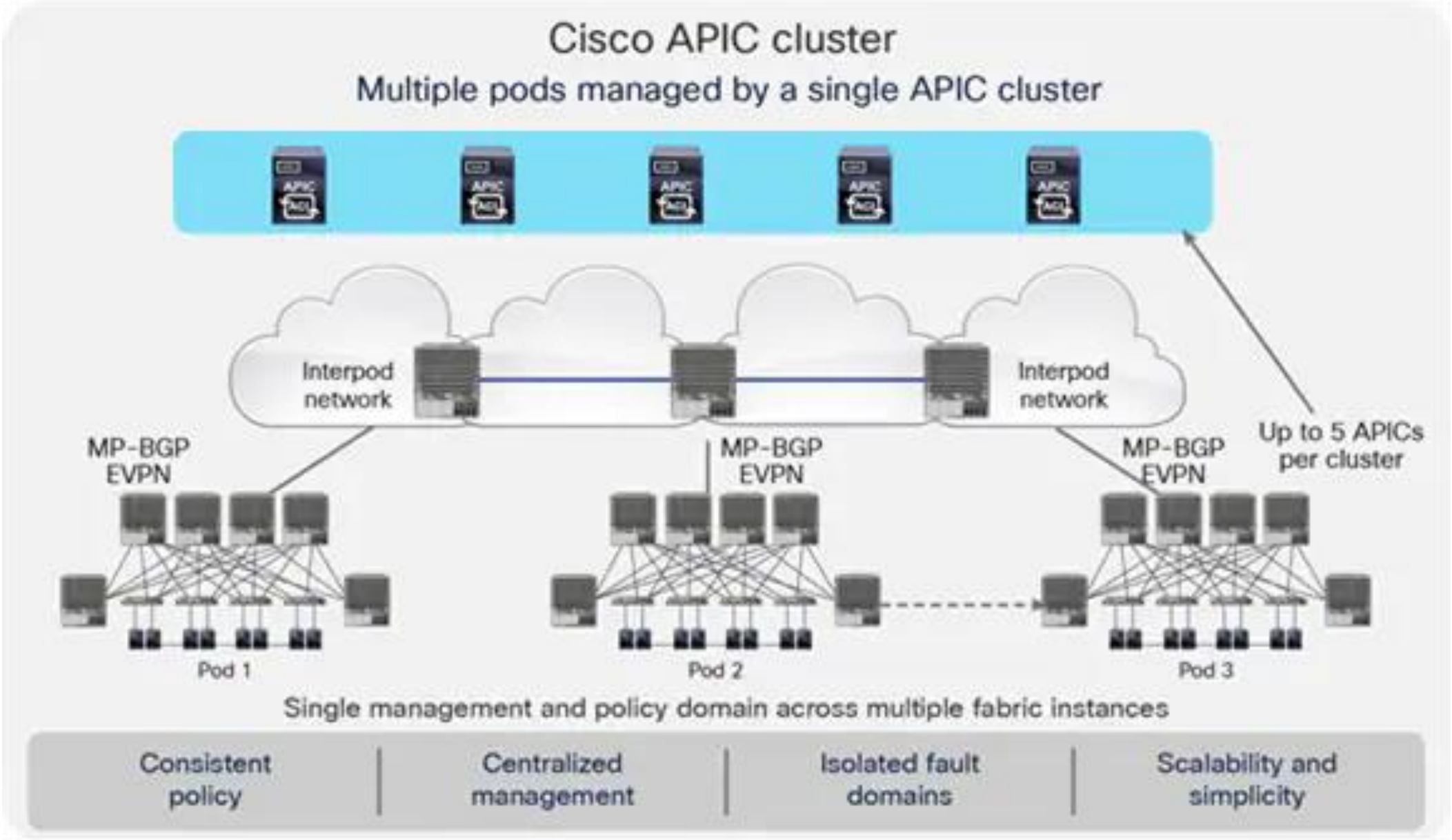
Datacenter VXLAN Topology





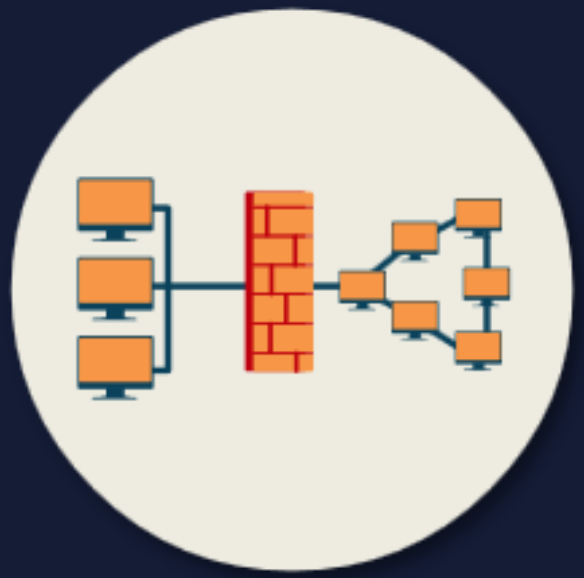
CSP Availability Zone

Cisco ACI APIC Architecture



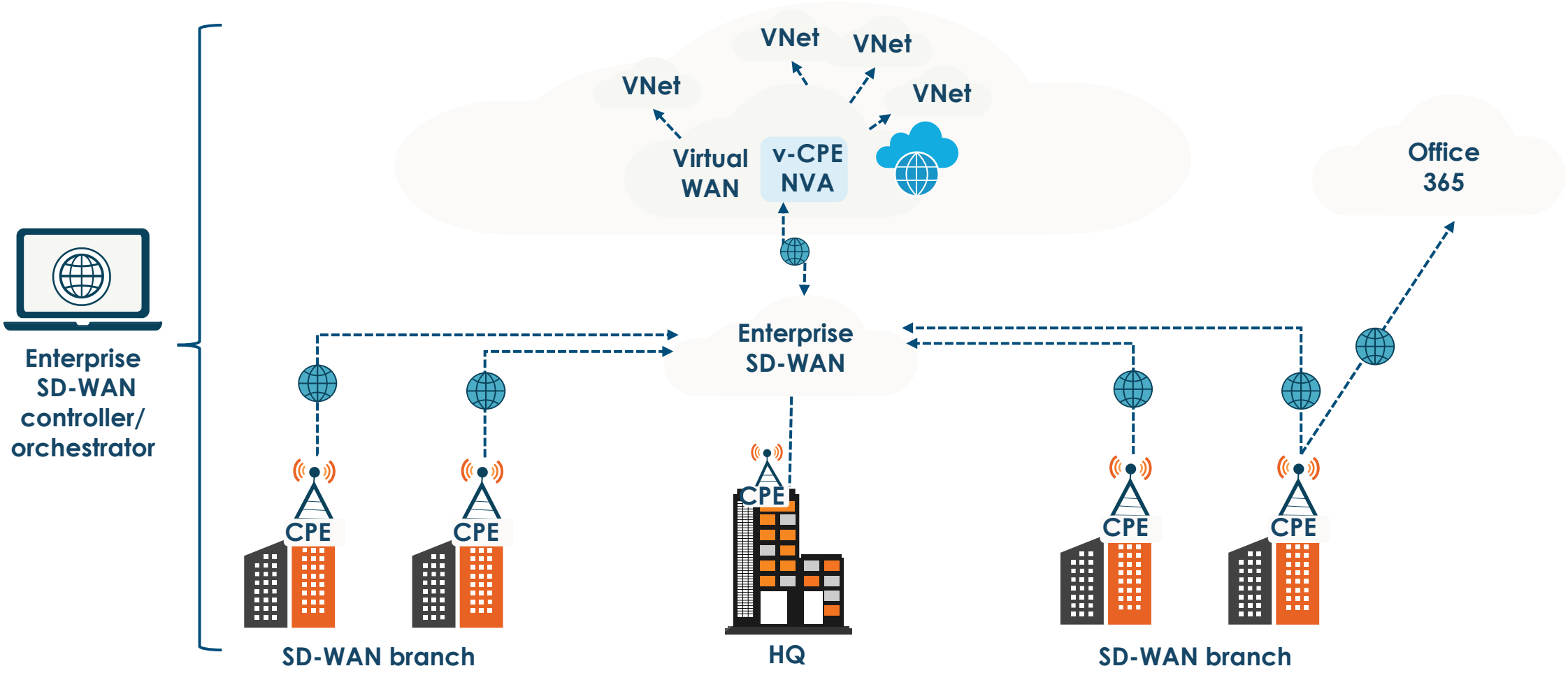
SD-WAN

Software-defined Wide Area Networks



- Software Defined Wide Area Network is an SDN approach that raises network traffic management away from the hardware and premises to next-generation software in the cloud for superior agility, control, and visibility
- It is commonly used with Cloud Providers in metropolitan area solutions
- Incorporates a centralized control function with user-defined application and routing policies to deliver highly secure, robust, application-aware network traffic management

Microsoft Azure SD-WAN Solution

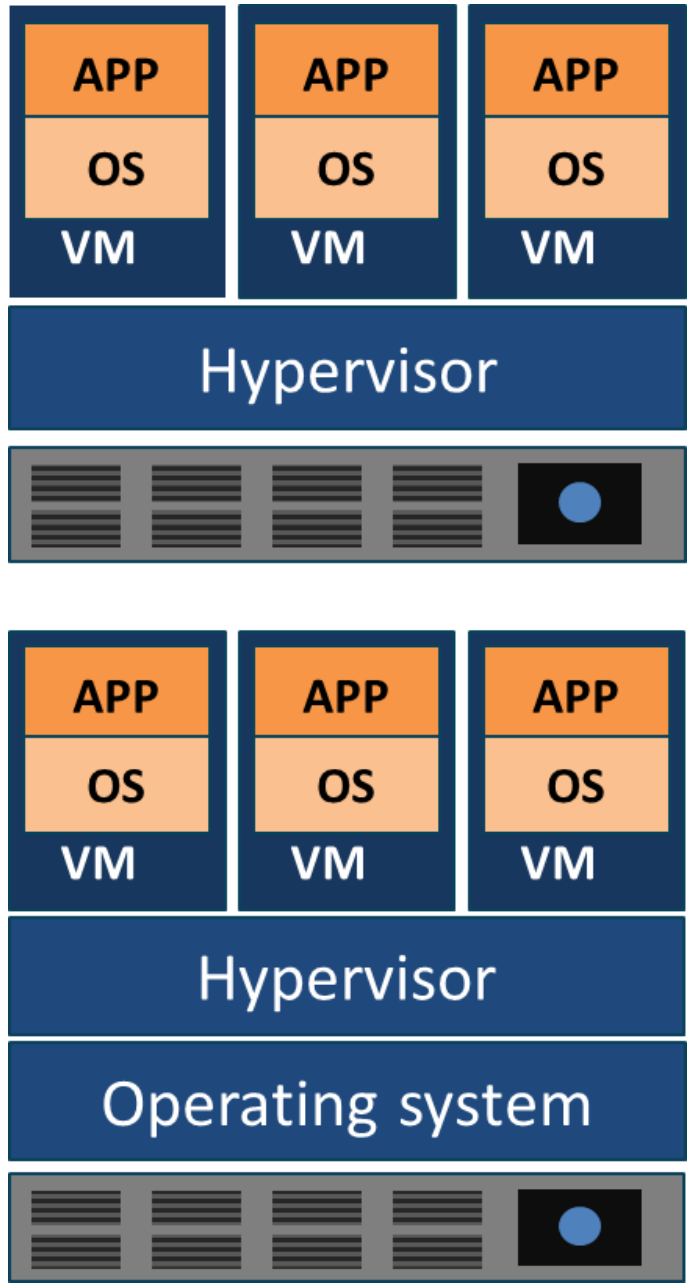


Virtualization (VMs)

- Virtualization is the process of running a virtual instance of a computer system in a layer abstracted from the underlying hardware server
- It most often refers to running multiple operating systems on a computer system simultaneously
- To the applications running on top of the virtualized machine, it can seem as if they are on their own dedicated operating system with libraries, DLLs, and associated programs

Hypervisors

- Software that runs virtual machines
- Controls interaction between the VMs and the hardware
- **Type I - bare metal or native**
  - Runs directly on the underlying hardware
  - XenServer, KVM, Hyper-V, ESXi
- **Type II - hosted**
  - Runs on the OS installed on the hardware
  - Oracle VirtualBox 6, VMWare Player/Workstation

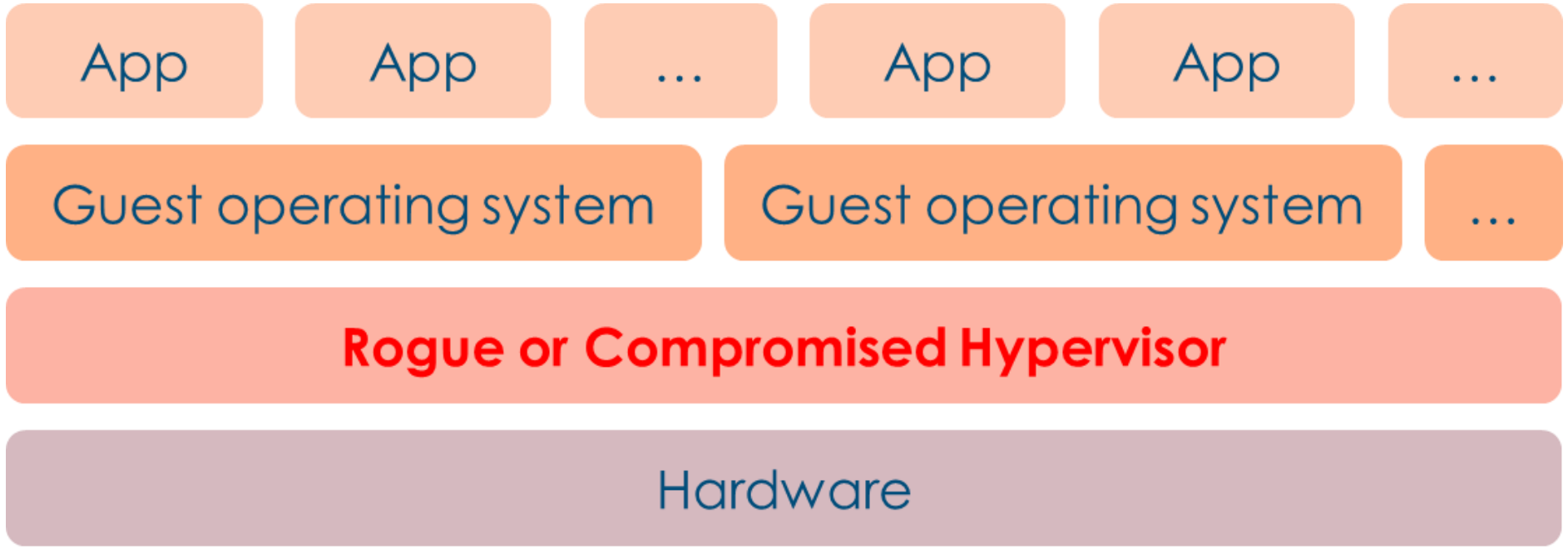


Virtualization Vulnerabilities

- **VM sprawl**
  - When the number of VMs overtakes the administrator's ability to manage them and the available resources
- VM sprawl avoidance
  - Enforce a strict process for deploying VMs
  - Have a library of standard VM images
  - Archive or recycle under-utilized VMs
  - Use a Virtual Machine lifecycle management tool or a cloud service provider-managed service
- **VM escape**
  - A serious threat where a process running in the guest VM interacts directly with the host OS
- VM escape protection
  - Patch VMs and VM software regularly
  - Only install what you need on the host and the VMs
  - Install verified and trusted applications only
  - Strong access control policies and passwords

Virtualization Vulnerabilities

- **Hyperjacking**
  - A hyperjacking attack is an attempt by an attacker to take control of the hypervisor, using a rootkit installed on a virtual machine



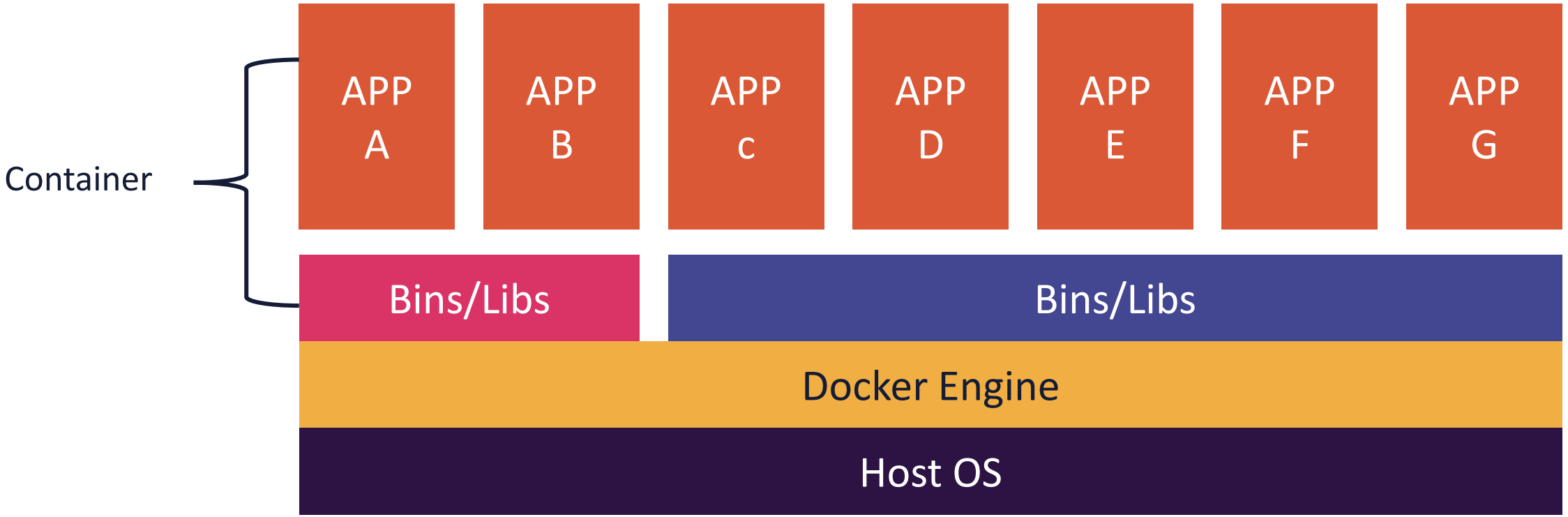
Virtualization Concepts

- **Ephemeral Computing**
  - Ephemeral computing is the process of creating a virtual computing environment on an ad-hoc temporary basis and then disposing of the environment when necessary or the resources are no longer in demand
  - The consumer only pays for what is used
  - Examples would be functions-as-a-service with AWS Lambda and Azure Functions
- **Serverless Technology**
  - Functions are a form of serverless technology
  - These are technologies for running code, managing data, and integrating applications, all without managing Windows, Linux, and MacOS servers
  - Serverless technologies feature automatic scaling, built-in high availability, and a pay-for-use billing model to increase agility and optimize costs

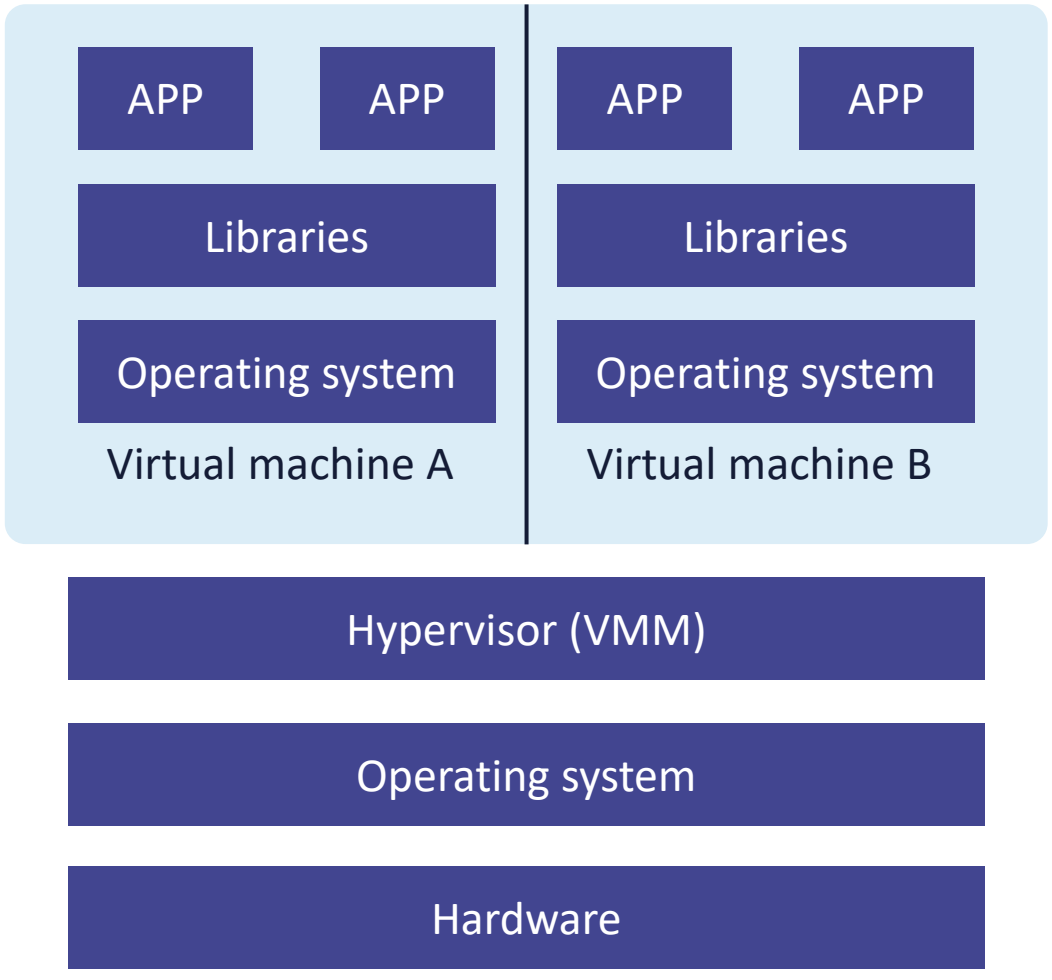
Containers

- A method for packaging and securely running an application within an application virtualization environment
- A container is a discrete modular and portable environment that includes the application binaries, software dependencies, and hardware requirements wrapped up into an independent, self-contained unit
- You can also use containers for processes and workflows in which there are important requirements for security, reliability, and scalability
- All cloud providers offer managed container development, automation and orchestration services
- Containers can be server-based or serverless (AWS Fargate)

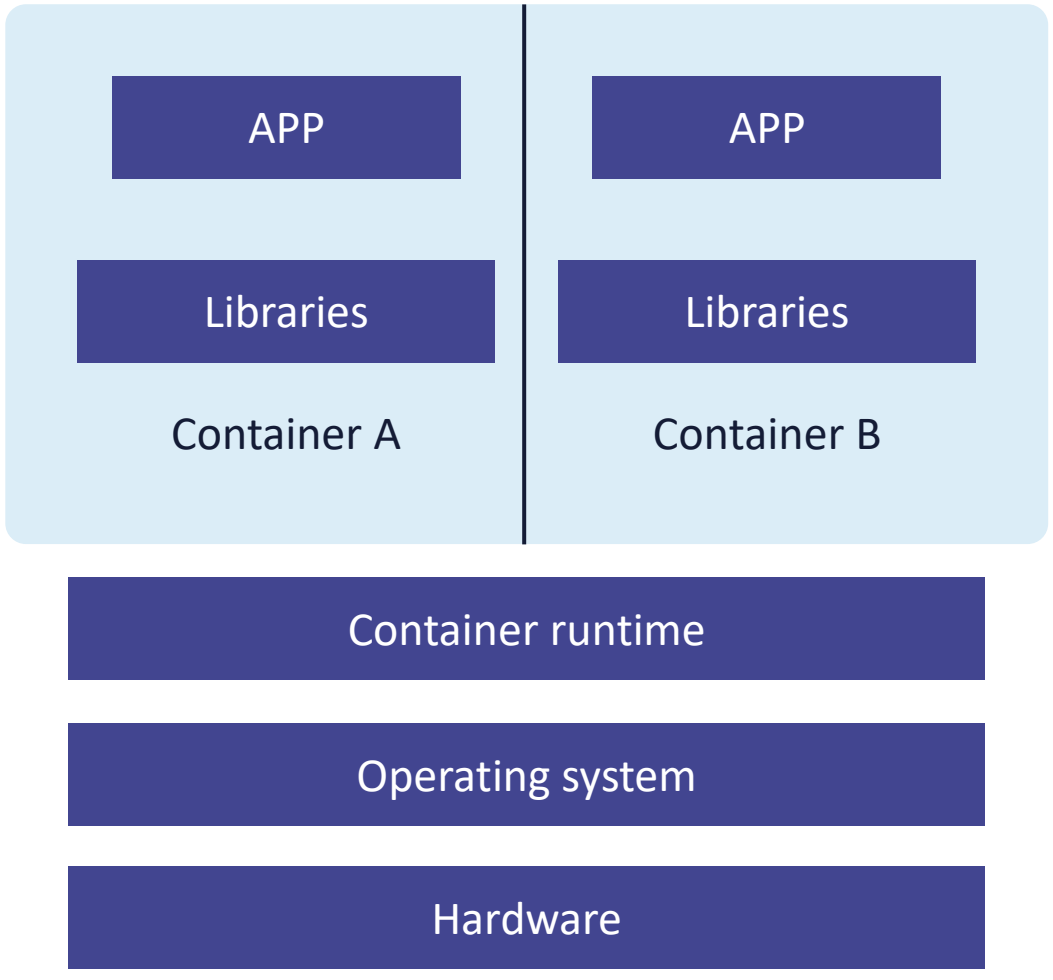
APPLICATION CONTAINERS



Virtual Machines vs. Containers



Traditional Virtual Machines on VMM



Container Example

Docker vs. Kubernetes

- **Docker** is a containerization platform
- The Docker Engine is the runtime that allows you to build and run containers
- Docker is currently the most popular container platform, and over 30% of enterprises currently use Docker in their AWS environment

- **Kubernetes** is an orchestrator for container platforms
- It is a comprehensive system for automating deployment, scheduling, and scaling of containerized applications
- It is the industry leader and supports many container tools, such as Docker

Docker vs. Kubernetes

Life of an application

How do you package and distribute an application?

Docker

How do you scale, run, and monitor an application

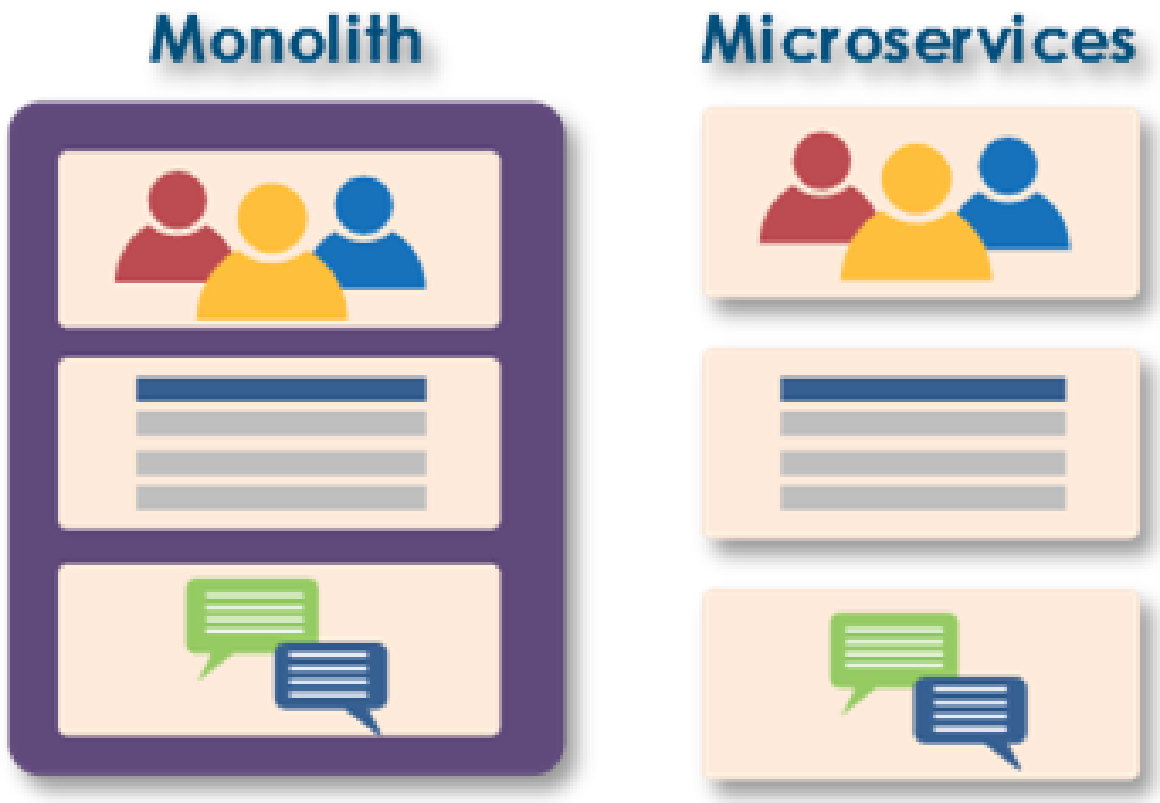
Kubernetes

Microservices

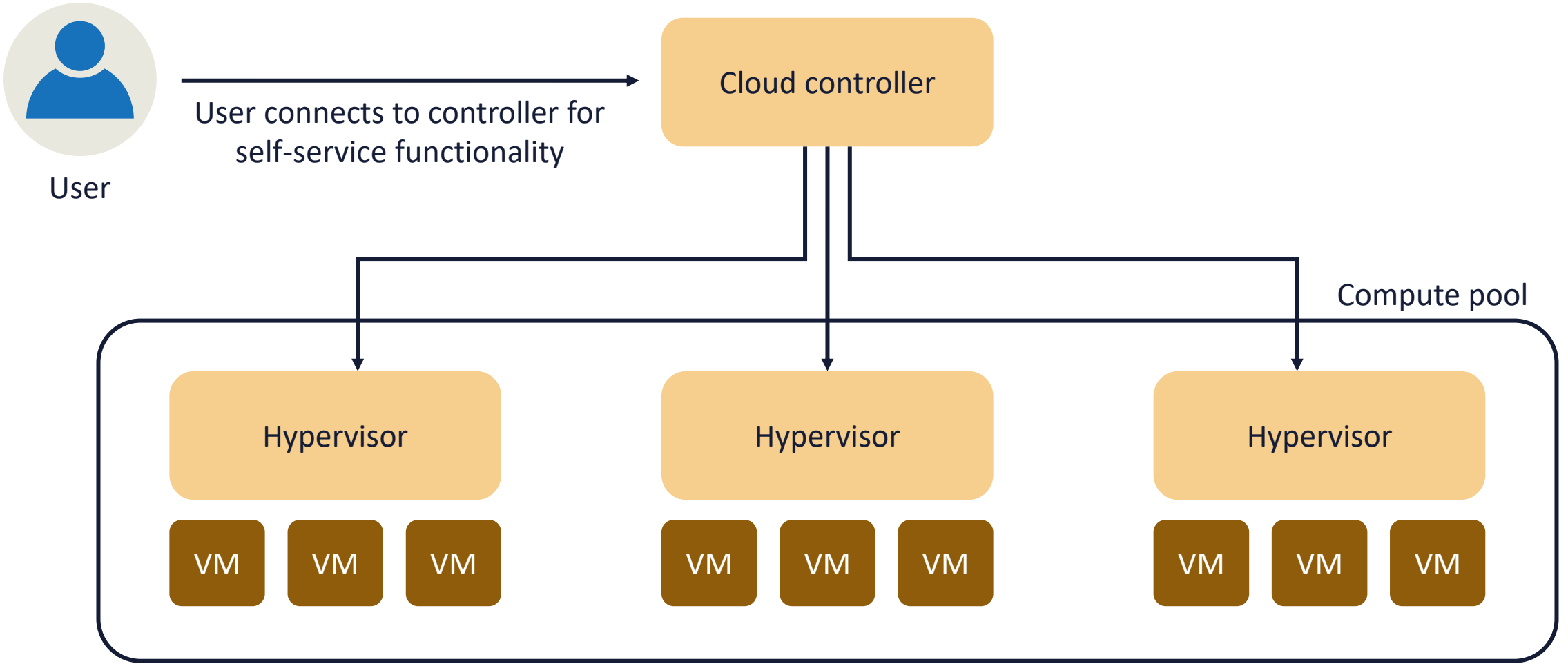
- Microservices are specific service-oriented application components
- An architectural approach to software development where the results are made up of small independent services that communicate over well-defined APIs
- These services are typically maintained by small, self-contained teams of developers
- Microservices architectures make applications faster to develop and easier to scale
- They enable innovation and fast-tracked delivery of new application features

Microservices

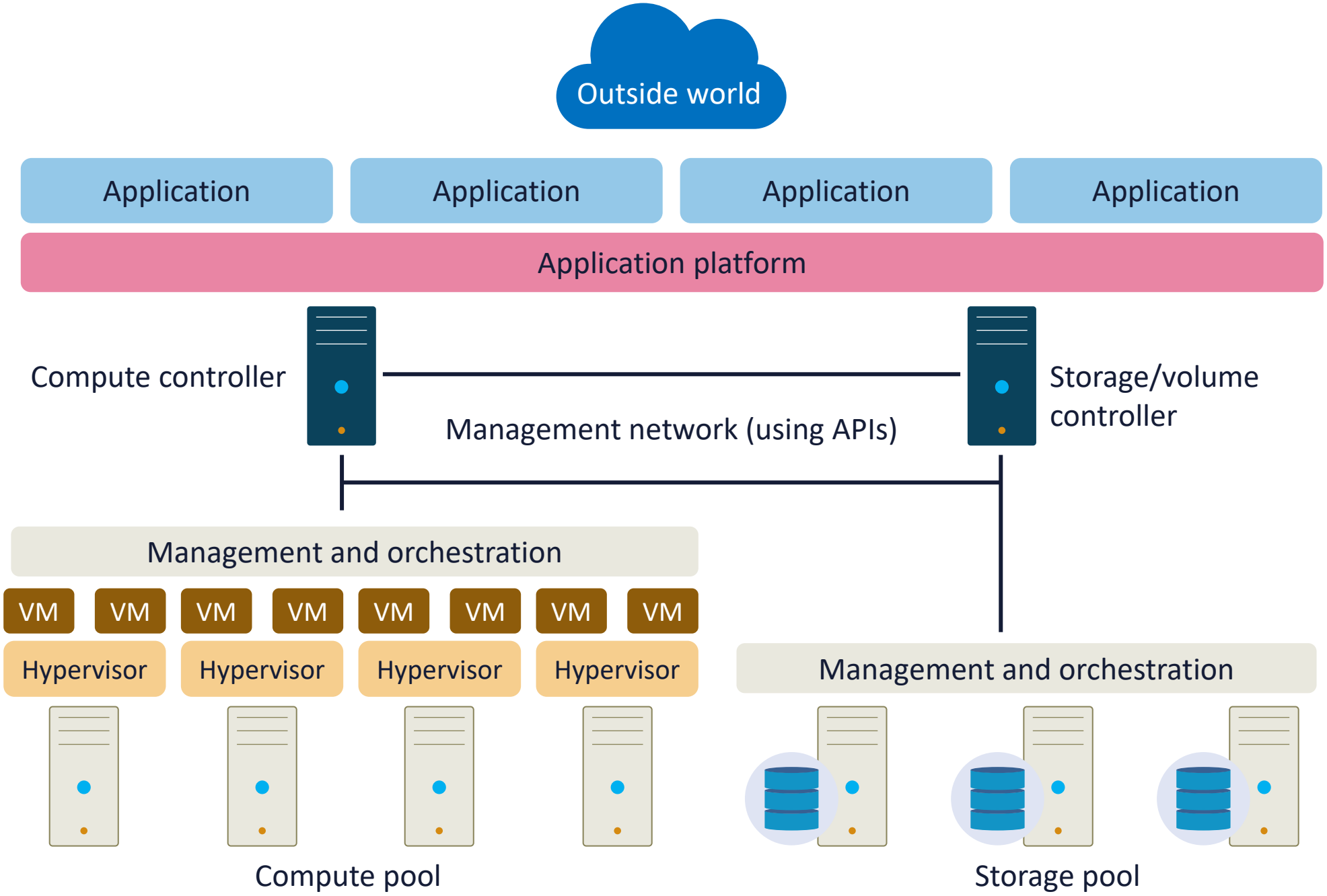
- Tightly scoped but loosely coupled
- Thoroughly modular and encapsulated
- Independently deployable
- Freely scalable
- Communicate using notification and queueing services



Cloud Controllers



Cloud Controller orchestrates access to underlying pool of resources using APIs


Outside world
Application
Application
Application
Application
Application platform
Compute controller
Management network (using APIs)
Storage/volume controller
Management and orchestration
VM
VM
VM
VM
VM
VM
VM
VM
Hypervisor
Hypervisor
Hypervisor
Hypervisor
Management and orchestration
Compute pool
Storage pool

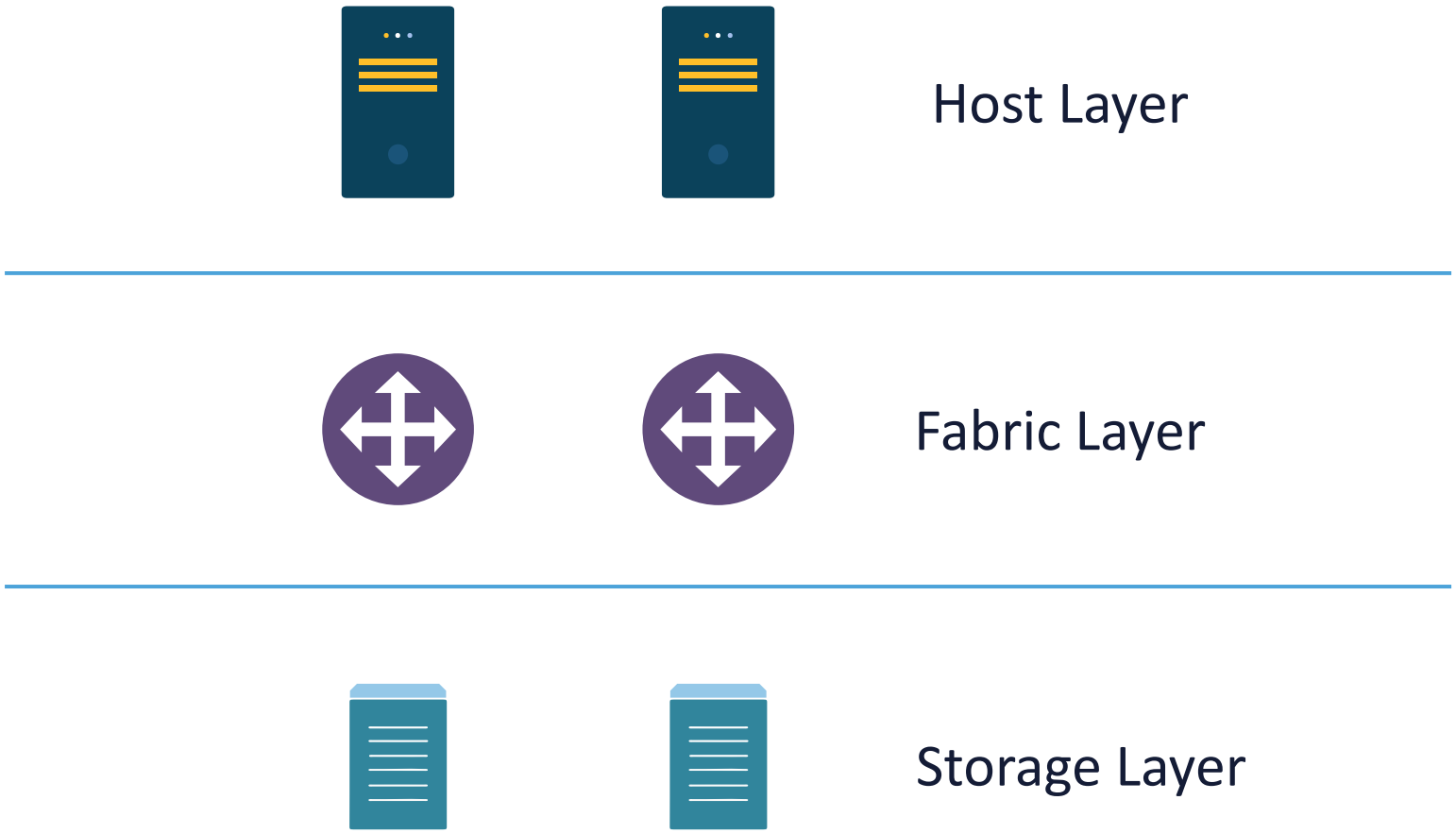
Distributed Resource Scheduling (DRS)

- DRS continually monitors your cluster utilization to assure that VMs get their resources in the most optimal fashion
- DRS is responsible for keeping the cluster balanced, so the utilization of the ESXi hosts is equal
- DRS also works closely with resource management that guarantee specific resources for your VMs
- DRS constantly monitors a lot of parameters for the peak performance and placement:
  - Host resource capacity
  - Resource reservations
  - Datastore connectivity
  - Actual resource demand from virtual machines
  - Reservations, Shares and Limits (R, L, S)

Dynamic Optimization (DO)

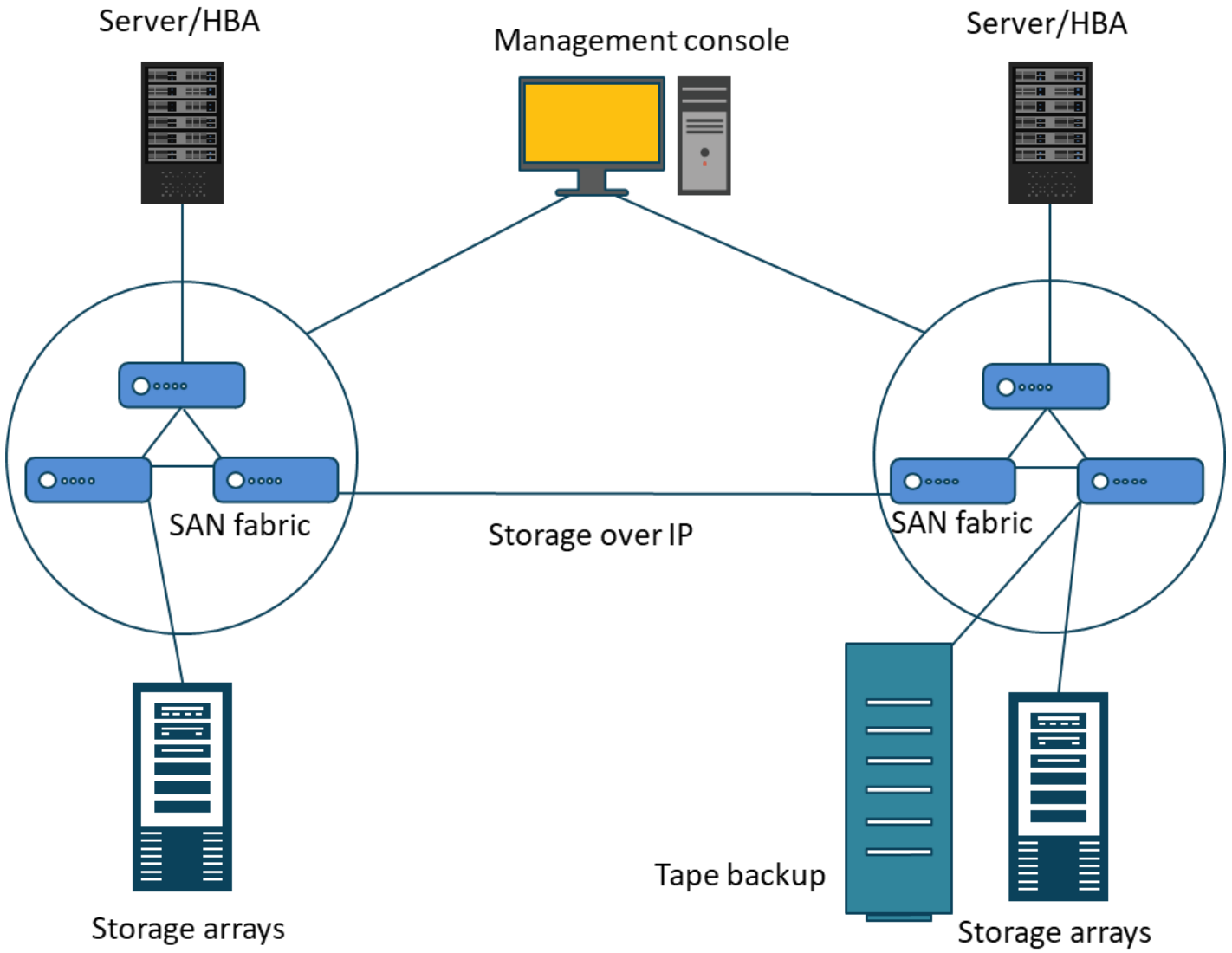
- Dynamic optimization facilitates live migration of VMs and VHDs within a host cluster
- The migration is based on designated settings to improve load balancing among hosts and cluster shared storage, and to correct the placement issues for VMs
  - **Compute Dynamic optimization** is the optimization of hosts in a cluster to optimize performance by migrating VMs across host
  - Host performance thresholds CPU and Memory
  - **Storage Dynamic Optimization** is optimization of disk space and is performed on cluster shared storage (CSV, file shares) to optimize storage space availability by migrating Virtual Hard Disks (VHD) across shared storage
  - You can set free storage space threshold on cluster shared storage

Storage Area Networking Architecture (SAN)



Securing the SAN

- Use secure management protocols on console or Software-Defined-Networking
- For securing data in transit, IPsec AH for integrity and origin authentication was used
- 802.1AE (MACsec) can provide encryption and more on the SAN frames
- Harden all switches and servers
- Encrypt data at rest with AES-256-GCM



Storage Clusters

- Storage clusters are also referred to as storage pods or Datastore clusters
- A datastore cluster is a collection of datastores with shared resources and a shared management interface
- Datastore clusters are to datastores what clusters are to hosts
- When you create a datastore cluster, you can use a tool like Storage Distributed Resource Scheduling (DRS) to manage storage resources for:
  - Space utilization load balancing
  - I/O latency load balancing
  - Anti-affinity rules