RELIABILITYFIRST

CIP in the Cloud

Lew Folkerth, BSEE, PE, LPI, CISSP, CCSP, CISA, GCFA, GPEN, ITPM

Principal Reliability Consultant

RF Tech Talk, September 12, 2022

Much of this presentation is speculative in nature, since no NERC Reliability Standards currently permit operational services in the cloud environment.

Overview

- **Quick Review of Cloud Computing Concepts (adapted from NIST SP 800-145)**
  - Essential Characteristics of Cloud Computing
  - Deployment Models
  - Service Models
  - Shared Responsibility Model
- **Drivers of Cloud Computing**
  - IT
  - OT
- **Challenges of Cloud Computing**
  - Operational Challenges
  - CIP Compliance
- **Path Forward**
  - Develop Use Cases
  - Identify and Resolve Operational Challenges
  - Identify and Resolve CIP Compliance Challenges

Cloud Concepts

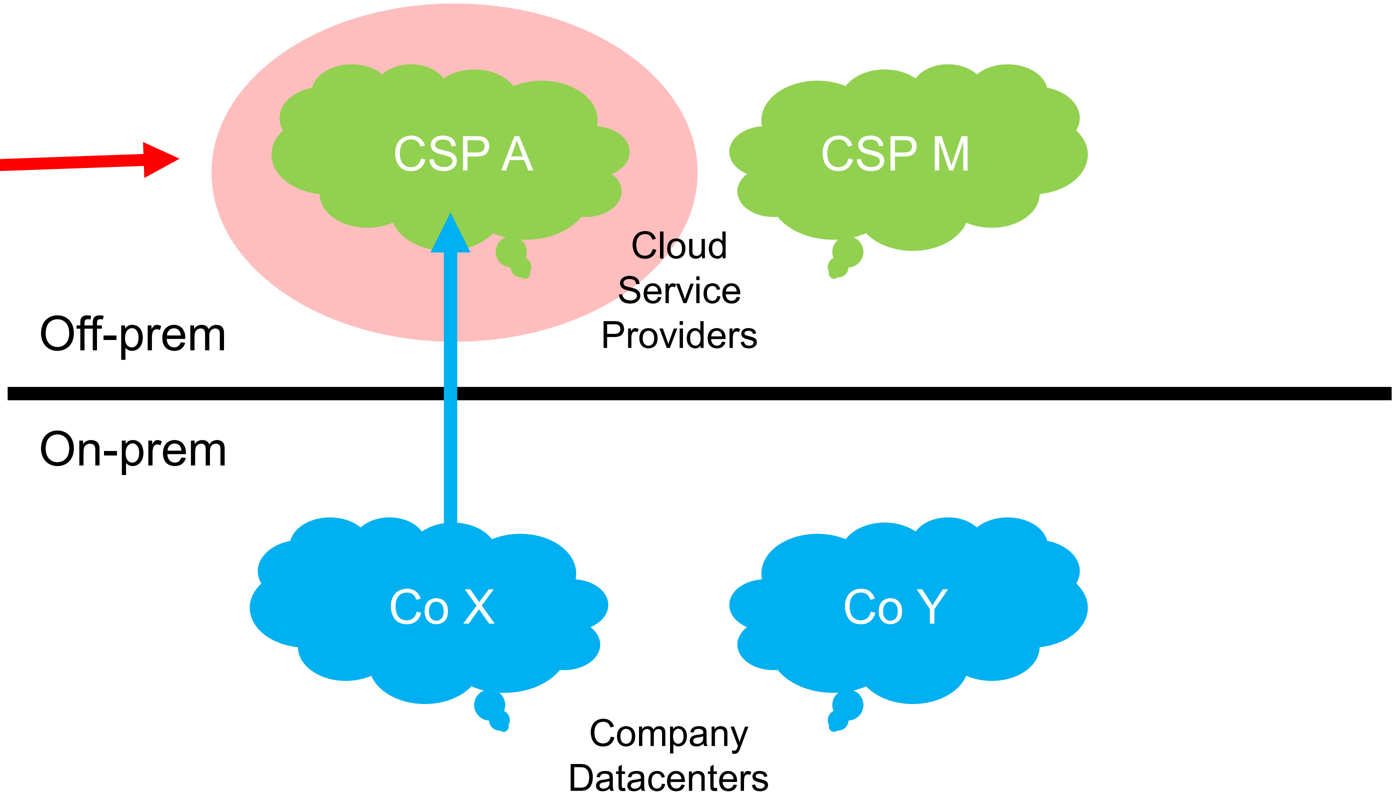
➢ Essential Characteristics of Cloud Computing

- **Self provisioning**: A cloud user can create and modify computing resources without vendor or administrative assistance.
- **Network access**: Computing resources are available to the cloud user over a network (public or private).
- **Resource pooling**: A collection of hardware resources is pooled and made available to the cloud user.
- **Rapid elasticity**: A cloud user can increase (or decrease) the use of cloud resources easily and quickly.
- **Measured service**: Cloud resource usage can be monitored and controlled in order to manage the cloud environment..

Cloud Concepts

➢ Cloud Computing Deployment Models

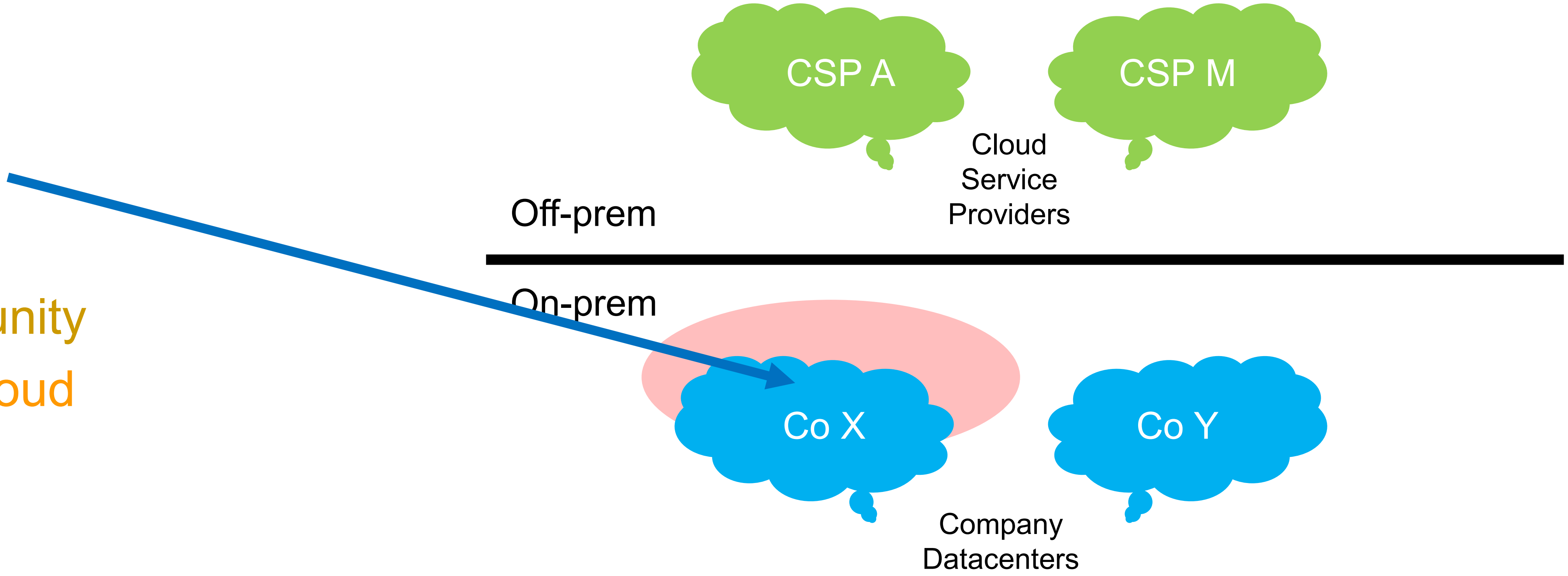
- Public
- Private
- Hybrid
- Community
- Multi-cloud



Cloud Concepts

➢ Cloud Computing Deployment Models

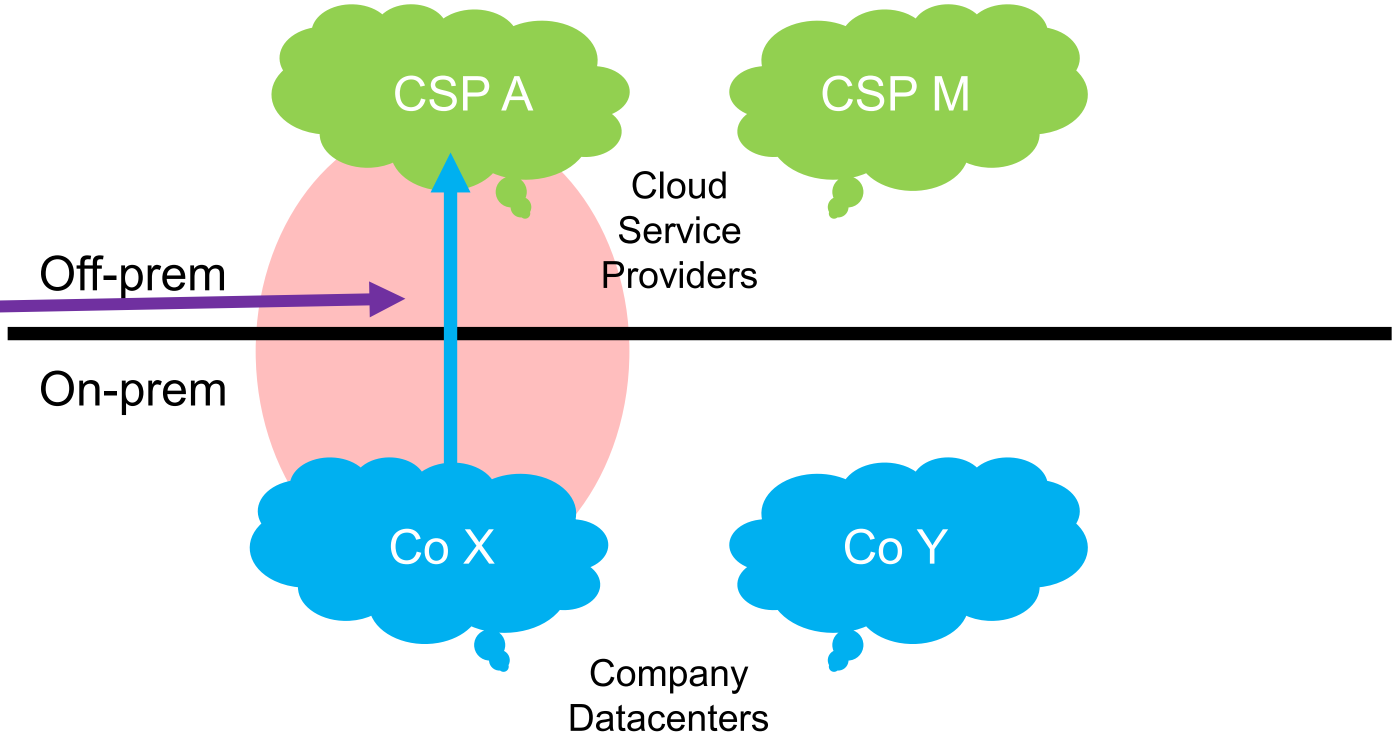
- Public
- Private
- Hybrid
- Community
- Multi-cloud



Cloud Concepts

➢ Cloud Computing Deployment Models

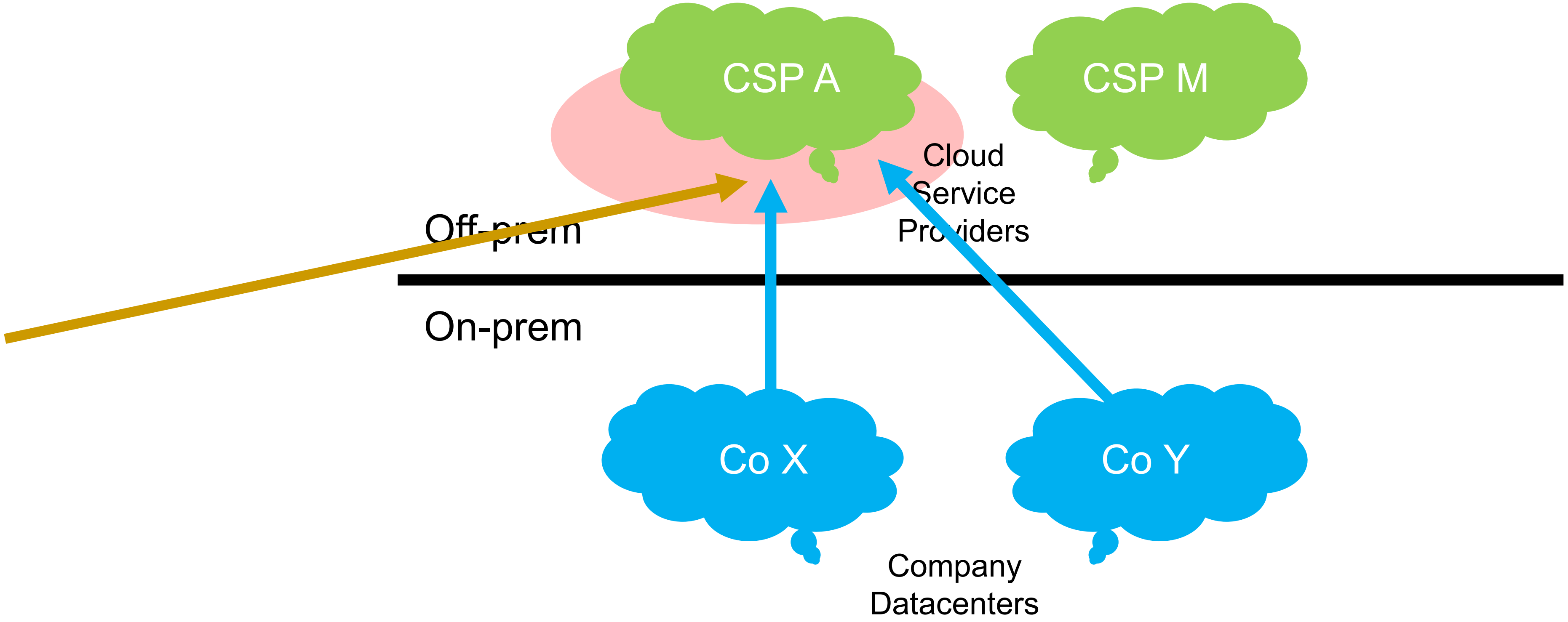
- Public
- Private
- Hybrid
- Community
- Multi-cloud



Cloud Concepts

➢ Cloud Computing Deployment Models

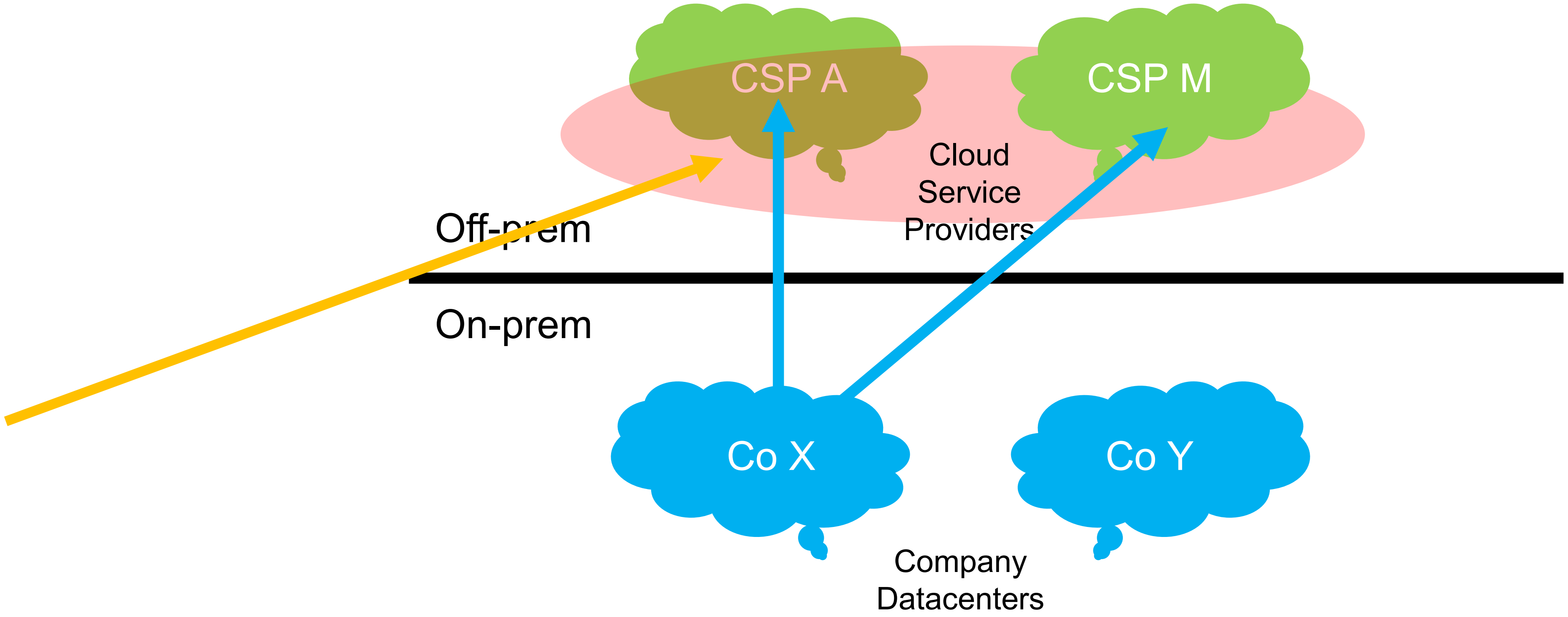
- Public
- Private
- Hybrid
- Community
- Multi-cloud



Cloud Concepts

➢ Cloud Computing Deployment Models

- Public
- Private
- Hybrid
- Community
- Multi-cloud



Cloud Concepts

➢ Service Model Components

User Permissions	Authorization to access services and data
Data	Customer data
Application	Software used for the task
Operating System	Windows, Linux, etc.
Virtual Network	Software-defined network, usually a function of the hypervisor
Virtual Machine	A software instance that acts like a physical computer
Server	Computer hardware and software providing virtualization services
Storage	Hardware and software providing data storage services, not the data itself
Physical Network	Network connecting storage and servers
Physical Facilities	Building, grounds, HVAC, etc.

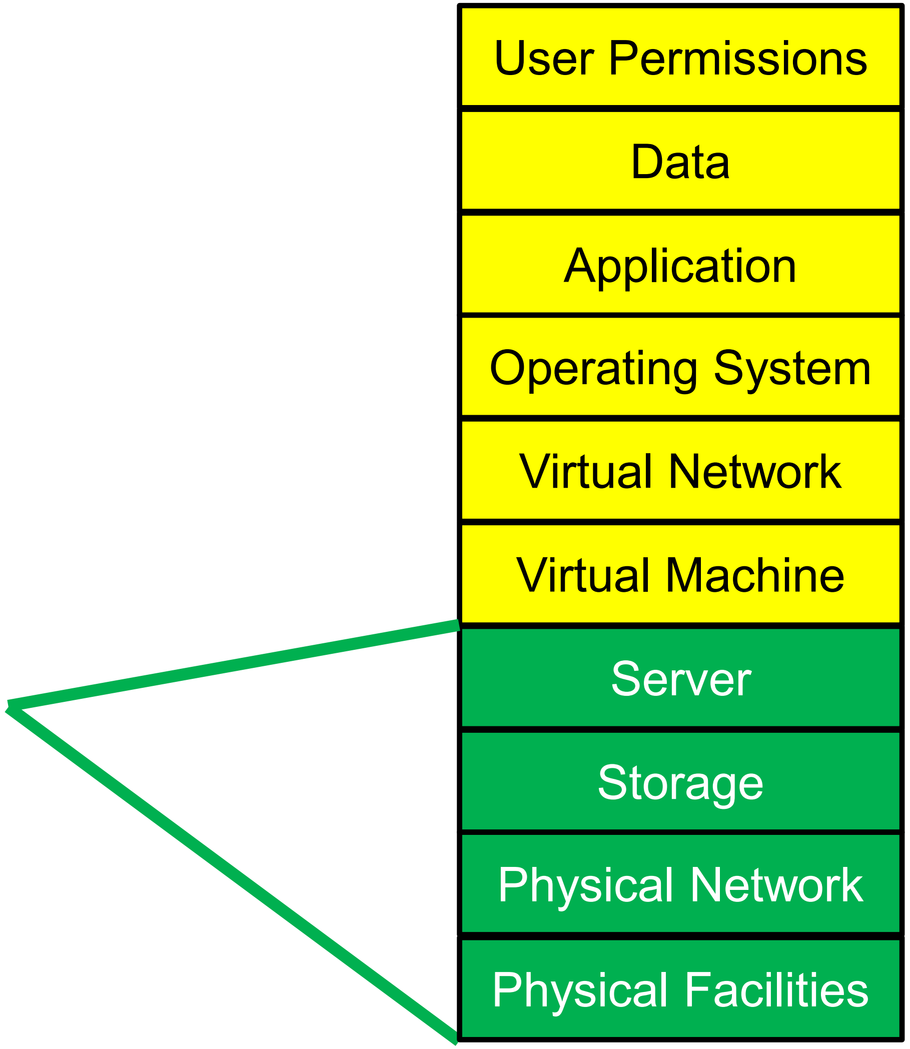
Cloud Concepts

➢ Service Models

Software as a Service (SaaS)

Platform as a Service (PaaS)

Infrastructure as a Service (IaaS)



User Permissions

Data

Application

Operating System

Virtual Network

Virtual Machine

Server

Storage

Physical Network

Physical Facilities

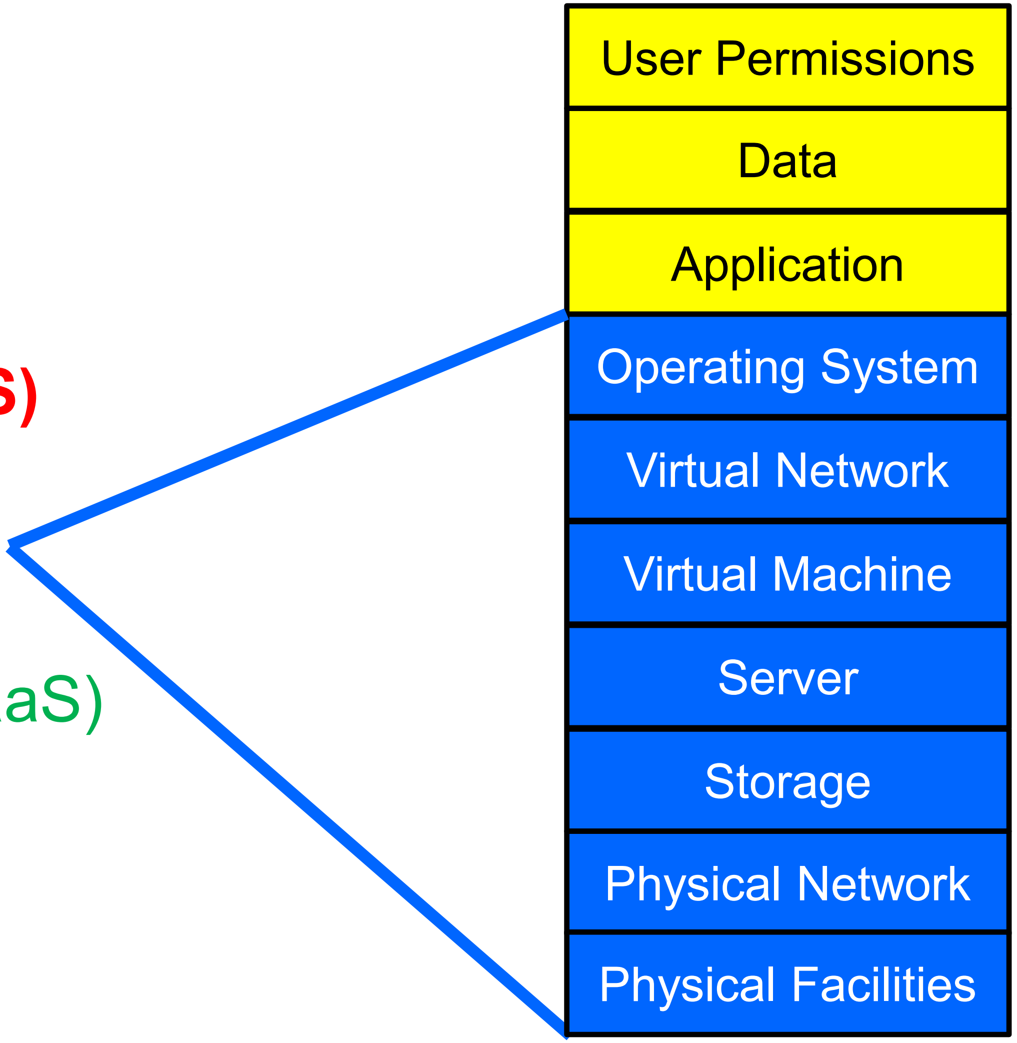
Cloud Concepts

- **Service Models**

Software as a Service (SaaS)

Platform as a Service (PaaS)

Infrastructure as a Service (IaaS)



User Permissions

Data

Application

Operating System

Virtual Network

Virtual Machine

Server

Storage

Physical Network

Physical Facilities

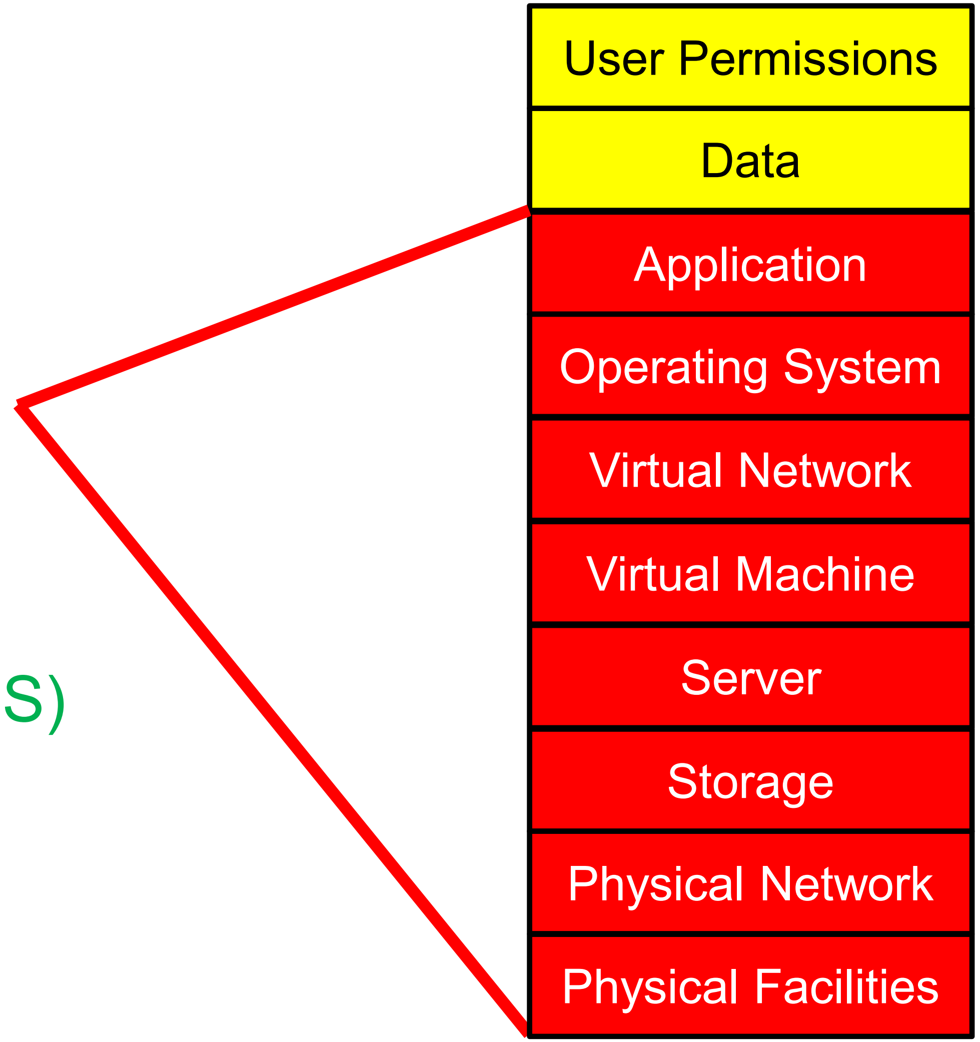
Cloud Concepts

➢ Service Models

Software as a Service (SaaS)

Platform as a Service (PaaS)

Infrastructure as a Service (IaaS)



User Permissions

Data

Application

Operating System

Virtual Network

Virtual Machine

Server

Storage

Physical Network

Physical Facilities

Cloud Concepts

➢ Cloud Shared Responsibility Model

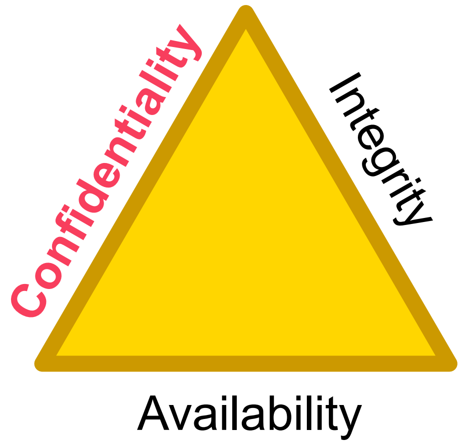
Service Model Components	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
User Permissions	Customer	Customer	Customer
Data	Customer	Customer	Customer
Applications	Customer	Customer	CSP
Operating Systems	Customer	CSP	CSP
Virtual Networks	Customer	CSP	CSP
Virtual Machine	Customer	CSP	CSP
Servers	CSP	CSP	CSP
Storage	CSP	CSP	CSP
Physical Networks	CSP	CSP	CSP
Physical Facilities	CSP	CSP	CSP

CSP – Cloud Service Provider

IT and OT

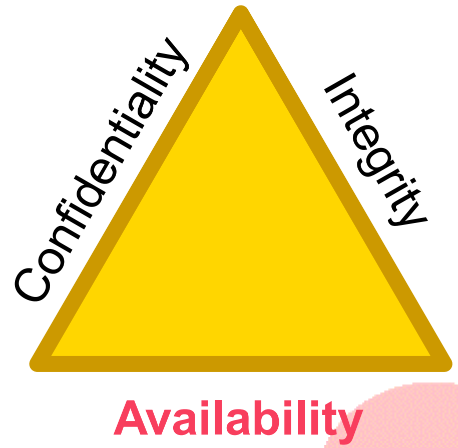
➢ Information Technology (IT)

- Typical business systems – email, accounting, etc.
- Information-focused
- Primary concern is confidentiality
- Not typically time sensitive



➢ Operational Technology (OT)

- Runs physical processes – power plants, substations, etc.
- Control-focused
- Primary concern is availability
- Real-time or near-real-time systems



Purdue Model

- **Level 4 – Enterprise/business systems**
  - Email, web, word processing, spreadsheets
- **Level 3 – Supervisory systems**
  - “within 15 minutes” – BES Cyber Asset
  - 2 to 4 second scan rate – SCADA, DCS
- **Level 2 – Control systems**
  - Milliseconds – Relays, PLCs, Safety systems
- **Level 1 – Physical interfaces**
  - Temperature and pressure sensors, valve actuators
- **Level 0 – Physical devices**
  - Breakers, valves, pumps, turbines, inverters

Purdue Model

IT

OT

- **Level 4 – Enterprise/business systems**
  - Email, web, word processing, spreadsheets
- **Level 3 – Supervisory systems**
  - “within 15 minutes” – BES Cyber Asset
  - 2 to 4 second scan rate – SCADA, DCS
- **Level 2 – Control systems**
  - Milliseconds – Relays, PLCs, Safety systems
- **Level 1 – Physical interfaces**
  - Temperature and pressure sensors, valve actuators
- **Level 0 – Physical devices**
  - Breakers, valves, pumps, turbines, inverters

Purdue Model

- **Level 4 – Enterprise/business systems**
  - Email, web, word processing, spreadsheets

Current Cloud Usage

- **Level 3 – Supervisory systems**
  - “within 15 minutes” – BES Cyber Asset
  - 2 to 4 second scan rate – SCADA, DCS
- **Level 2 – Control systems**
  - Milliseconds – Relays, PLCs, Safety systems
- **Level 1 – Physical interfaces**
  - Temperature and pressure sensors, valve actuators
- **Level 0 – Physical devices**
  - Breakers, valves, pumps, turbines, inverters

Purdue Model

- **Level 4 – Enterprise/business systems**
  - Email, web, word processing, spreadsheets
- **Level 3 – Supervisory systems**
  - "within 15 minutes" – BES Cyber Asset
  - 2 to 4 second scan rate – SCADA, DCS

This Discussion

- **Level 2 – Control systems**
  - Milliseconds – Relays, PLCs, Safety systems
- **Level 1 – Physical interfaces**
  - Temperature and pressure sensors, valve actuators
- **Level 0 – Physical devices**
  - Breakers, valves, pumps, turbines, inverters

Purdue Model

- **Level 4 – Enterprise/business systems**
  - Email, web, word processing, spreadsheets
- **Level 3 – Supervisory systems**
  - “within 15 minutes” – BES Cyber Asset
  - 2 to 4 second scan rate – SCADA, DCS
- **Level 2 – Control systems**
  - Milliseconds – Relays, PLCs, Safety systems
- **Level 1 – Physical interfaces**
  - Temperature and pressure sensors, valve actuators
- **Level 0 – Physical devices**
  - Breakers, valves, pumps, turbines, inverters

Not Now

Cloud Drivers for IT

IT

- Easy and inexpensive setup
- Streamlined provisioning (lead time of minutes to set up a new server)
- Scalability
- Pay only for what's used
- Universal Access (Mobile, BYOD)
- Security (CSP can distribute the cost of security products and staff across many customers)

Cloud Drivers for IT

IT

- Easy and inexpensive setup
- Streamlined provisioning (lead time of minutes to set up a new server)
- Scalability
- Pay only for what’s used
- Universal Access (Mobile, BYOD)
- Security (CSP can distribute the cost of security products and staff across many customers)

IT to OT

OT

- Easy and inexpensive setup ✗
- Streamlined provisioning (lead time of minutes to set up a new server) ✗
- Scalability ?
- Pay only for what’s used ?
- Universal Access (Mobile, BYOD) ✗
- Security (CSP can distribute the cost of security products and staff across many customers) ✓

Potential Cloud Drivers for OT

- **Reliability –** Not letting problems happen
  - Geographic diversity
  - Multiplicity of physical hardware, data centers, regions
- **Resilience –** Recovering swiftly and smoothly if problems occur
  - Multi-cloud failover?
- **Security –** Ensuring availability, integrity and confidentiality
  - Data centers become a less attractive target
  - CSP provides physical and basic network security
- **Elasticity –** The ability to enhance available resources on demand
  - Adjust resource usage based on need – expand for peaks, then contract

Potential Cloud Benefits for OT

- **Non-real-time**
  - Service providers using cloud
    - Work management and ticketing
    - Generator monitoring and management
    - Document management
  - Planning and analysis
    - Many more available cores (computing resources), but:
    - Single-threaded programs may not be able to take advantage of the added cores

Potential Cloud Benefits for OT

- **Real-time (<15 min) or near-real-time systems**
  - Systems used by OT
    - Historian
    - Mapboard driver
    - State estimator (hybrid cloud?)
    - Synchrophasor (PMU) integration
    - Dynamic Line Rating integration
  - Multiply redundant hardware
  - Geographically diverse
  - Highly physically secure and attack resistant (CIP-014)
  - Elasticity – can expand use of systems quickly
    - The changing resource mix may drive new operational methods. These methods will probably be computationally intensive and may greatly benefit from cloud resources.

Potential Cloud Benefits for OT

➢ Other possible benefits

- Shared personnel
  - EMS engineers
  - OT security engineers
  - Etc.
- Security & IT administrative services provided
- QA/Development/Training in the cloud, real-time critical on local systems
- Market interface systems

Cloud Challenges for OT

➢ Operational Challenges

- Safety
- Security
  - – Different environment
    - Services
    - Training
  - – CEII/BCSI in the cloud
- Availability
  - – Focus of cloud is on capability and cost, not high availability
- Latency
  - – Measure of the delay from data generation to data consumption
- Mobile Access
  - – Cloud services are easily accessed from mobile devices – this is a problem for Control Centers and other CIP assets

Cloud Challenges for OT

➢ Financial Challenges

- On-premise systems – capital
- Cloud – operating

➢ Security Challenges

- Cyber
  - Shared infrastructure – data leakage
  - Public exposure of information or services
- Physical
  - How to ensure access to cloud services only from within a PSP?

➢ EMP/GMD Hardening

Cloud Challenges for OT

- **Compliance Challenges**
  - New standards will be required
  - Risk-based standards will be required
  - Requires a mature approach to Standards
    - Can’t get by with a letter-of-the-law approach
    - Must have compliance fully integrated into operational processes
  - Auditing concerns
    - Reasonable assurance
    - Sufficient, appropriate evidence
  - Internal controls will be much more important

Path Forward

- **Develop use cases**
  - Begin with known needs, expand to more complete cloud adoption as advisable
  - Identify and resolve operational challenges
  - Identify and resolve compliance challenges
- **Need environment to test cloud options without compliance risk**
  - Cloud Technical Advisory Group (CTAG)
  - Test cloud options in a controlled environment
  - Test compliance evidence and processes
  - Partnership between Registered Entities and ERO Enterprise
  - Perform a task in a small, controlled environment before right-sizing that task

Conclusions

- Cloud technologies may benefit reliability, but risks must be effectively managed
- Reduced cost, the primary driver of early cloud adoption, should not be a significant driver for real-time cloud migration. Rather, the leveraging of cloud technologies for improved reliability, resilience and security should be the driver.
- CIP Standards will need to be modified to address cloud risks. These modifications will need to be explicitly risk-based in order to adapt to the wide range of cloud service provider options and features.

Questions & Answers

Forward Together ReliabilityFirst