



Welcome to CYBRARY: CCSP (Certified Cloud Security Professional)

Kelly Handerhan, Instructor
CCSP, CISSP, PMP, CISM, CRISC, CEH, CISA

Welcome and Introduction

- Kelly Handerhan, Instructor, Owner CyberTrain.IT
- Over twenty years experience in Information Assurance, and Cybersecurity
- Award-winning technical instructor
- Certified in:
CCSP, CCSP, CISM, CRISC, PMP, Security+, etc.



KELLY HANDERHAN,
Instructor, Owner of
CyberTrain.IT

KellyH@CyberTrain.IT

Before we get started.....

- Class hours
- Breaks
- Courseware
- Additional resources
 - Cybrary.it
 - [Https://Tinyurl.com/KellysCCSP](https://tinyurl.com/KellysCCSP)
- Your Name/Job Role
 - Information Security Experience
 - Cloud Experience
 - Other Certifications

Introductions

- Your Name?
- Security/Cloud Experience?
- CISSP?
- Exam Date?

Domain 0

Course Introduction and Exam Specifics

The 6 Domains of CCSP

CCSP Course Syllabus:

- Domain 0: Introduction and Exam Specifics
- Domain 1: Architectural Concepts and Design Requirements
- Domain 2: Cloud Data Security
- Domain 3: Cloud Platform and Infrastructure
- Domain 4: Cloud Application Security
- Domain 5: Operations
- Domain 6: Legal and Compliance

CCSP Exam Specifics

Exam Specifics

- Length of exam: 3 hours
- Number of questions: 125
- Question format: multiple choice
- Passing grade: 700 out of 1000 points
- Exam Language: English
- Testing Center - Pearson Vue Testing Center

Exam Requirements (Prior to Exam)

Candidates must meet the following requirements prior to taking the examination:

- Submit the examination fee
- Understand the experience requirements described in the next slide as they relate to the endorsement process
- Attest to the truth of his or her assertions regarding professional experience
- Legally commit to abide by the (ISC)2 Code of Ethics
- Answer four pre qualification questions regarding criminal history and related background
- *******OR HAVE THE CISSP CERTIFICATION*******

Exam Requirements (After Taking the Exam)

- In addition to successfully passing the exam, CCSP candidates must have a minimum of five (5) years of cumulative paid full-time information technology experience, of which three (3) years must be in information security and one (1) year in one of the six (6) domains of the CCSP examination. Earning the Cloud Security Alliance's CCSK certificate may be substituted for one (1) year in one of the six (6) domains of the CCSP examination. Earning the CCSP credential may be substituted for the entire CCSP experience requirement. Candidates who do not meet these experience requirements may still choose to sit for the exam and become an Associate of (ISC)2.

Introductions

Name?

Background in Cybersecurity?

Experience working with the cloud?

Other Certifications?

The CCSP Exam

What to Expect

CCSP Domains

- Cloud Concepts, Architecture and Design.
- Cloud Data Security.
- Cloud Platform & Infrastructure Security.
- Cloud Application Security.
- Cloud Security Operations.
- Legal, Risk and Compliance.



The CCSP Mindset

Part 1

The CCSP Mindset: Part 1

- A mile wide and an inch deep!!!—If it's something you can Google, it's probably not on the test
- Your Role is a Risk Advisor--Do NOT fix Problems
- Who is accountable (ultimately responsible) for security?
- How much security is enough?
- All decisions start with risk management. Risk management starts with the identification and valuation of your assets.
- If all the answers seem good, revisit the question.
- Always start with business requirements. That will drive technical requirements

The CCSP Mindset: Part 2

- Process not Problem
- Think “End Game”
- “Security Transcends Technology”
- Physical safety is always the first choice.
- Technical questions are for managers.
- Do NOT memorize things you can Google
- Any Answer that has you conduct risk analysis is a good one!
- Incorporate security into the design, as opposed to adding it on later.
- Layered Defense!

Domain 1

Architectural Concepts and Design Requirements

Domain 1 Architectural Concepts and Design Requirements Agenda

- ▶ Introduction to Cloud Concepts
- ▶ Cloud Deployment Models
- ▶ Cloud Service Models
- ▶ Cloud Computing Standards Roadmap (NIST SP 500-291)
- ▶ General Security Requirements
- ▶ Identity and Access Management
- ▶ Virtualization

Introduction to Cloud Concepts

Traditional Managed Service Providers

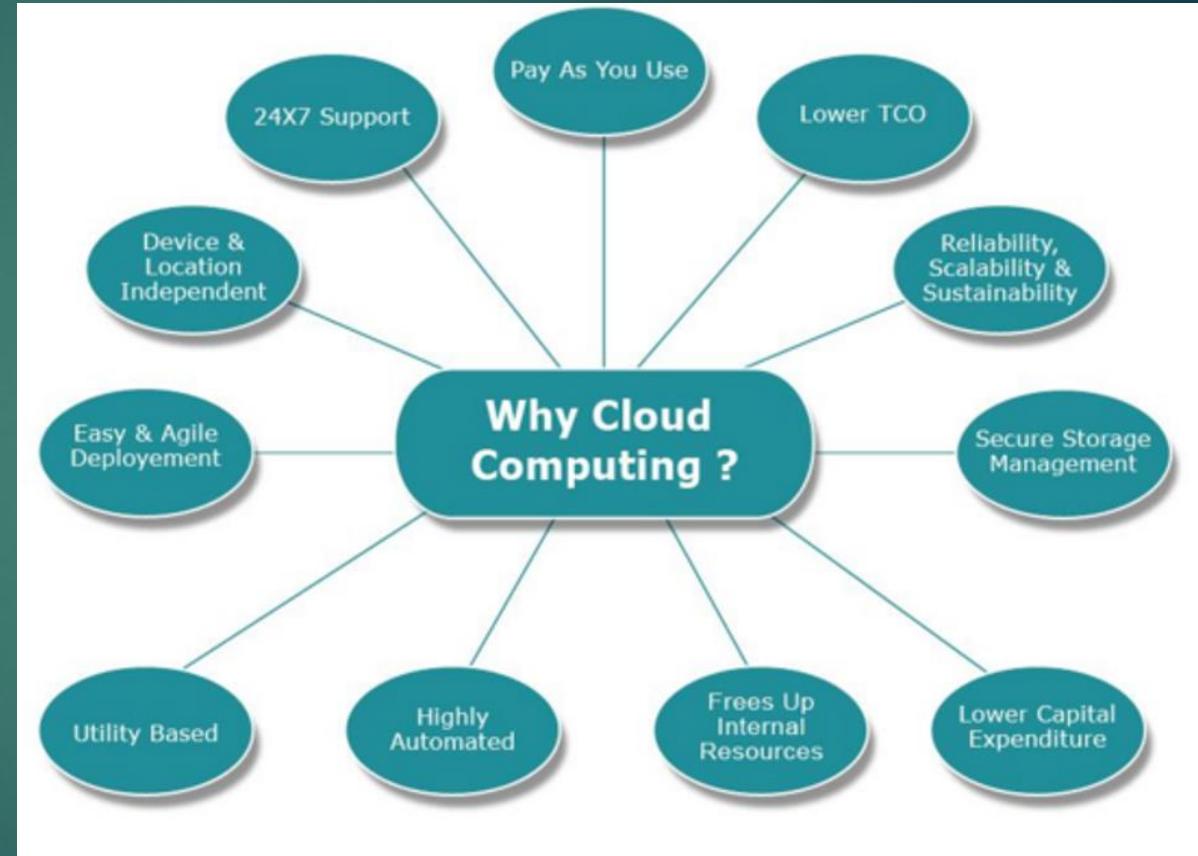
- A managed service provider (MSP) is a company that remotely manages a customer's IT infrastructure and/or end-user systems, typically on a proactive basis and under a subscription model.
- Client maintains control/ownership over the technology and operating procedures
- Smaller companies may not have budget to support Full-time IT
- Larger companies may supplement their existing staff
- Offers a predictable monthly cost for IT services

- ▶ “Cloud computing is a model for enabling ubiquitous, convenient on-demand network access to a shared pool of configurable computing resources (e.g., networks, server, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

--NIST Definition of Cloud Computing

Cloud Drivers

- ▶ Your Name/Job Role
- ▶ Scalability
- ▶ Mobility
- ▶ Elasticity
- ▶ Cost-Savings
- ▶ Risk Transference/Reduction
- ▶ Reduced Infrastructure
- ▶ Less Overhead
- ▶ Pay as you go
- ▶ Shifting Capital Expenditure to Operational Expenditure



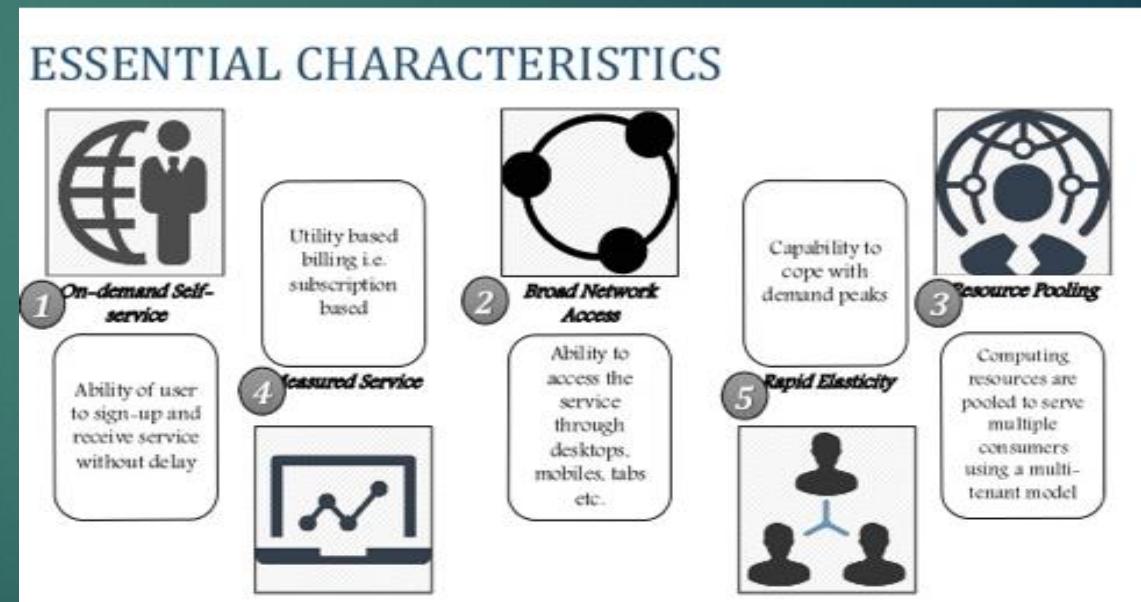
5 Characteristics of Cloud Computing

- Broad network access: Bandwidth should not be a bottleneck. Through advanced technologies and techniques, bandwidth should be virtually unlimited
- On-demand services: customers should be able to scale their compute/storage resources without CSP involvement
- Resource pooling: CSP shares physical resources across multiple tenants. Can include storage, processing, memory, and network bandwidth
- Measured or “metered” service: The CSP measures or monitors the provision of services for various reasons, including billing, effective use of resources, or overall predictive planning.
- Rapid Elasticity: the ability to scale resources both up and down as needed. To the consumer, the cloud appears to be infinite, and the consumer can purchase as much or as little compute/storage/network as they need..

NIST's 5 Key Requirements of Cloud Computing

On-demand self-service - ability of user to sign-up and receive service without delay

- Broad network Access - ability to access the service through desktops, mobiles, tabs, etc.
- Resource pooling - computing resources are pooled to serve multiple consumers using a multi-tenant model
- Rapid elasticity - capability to cope with demand peaks
- Measured Service - utility based billing i.e. subscription based

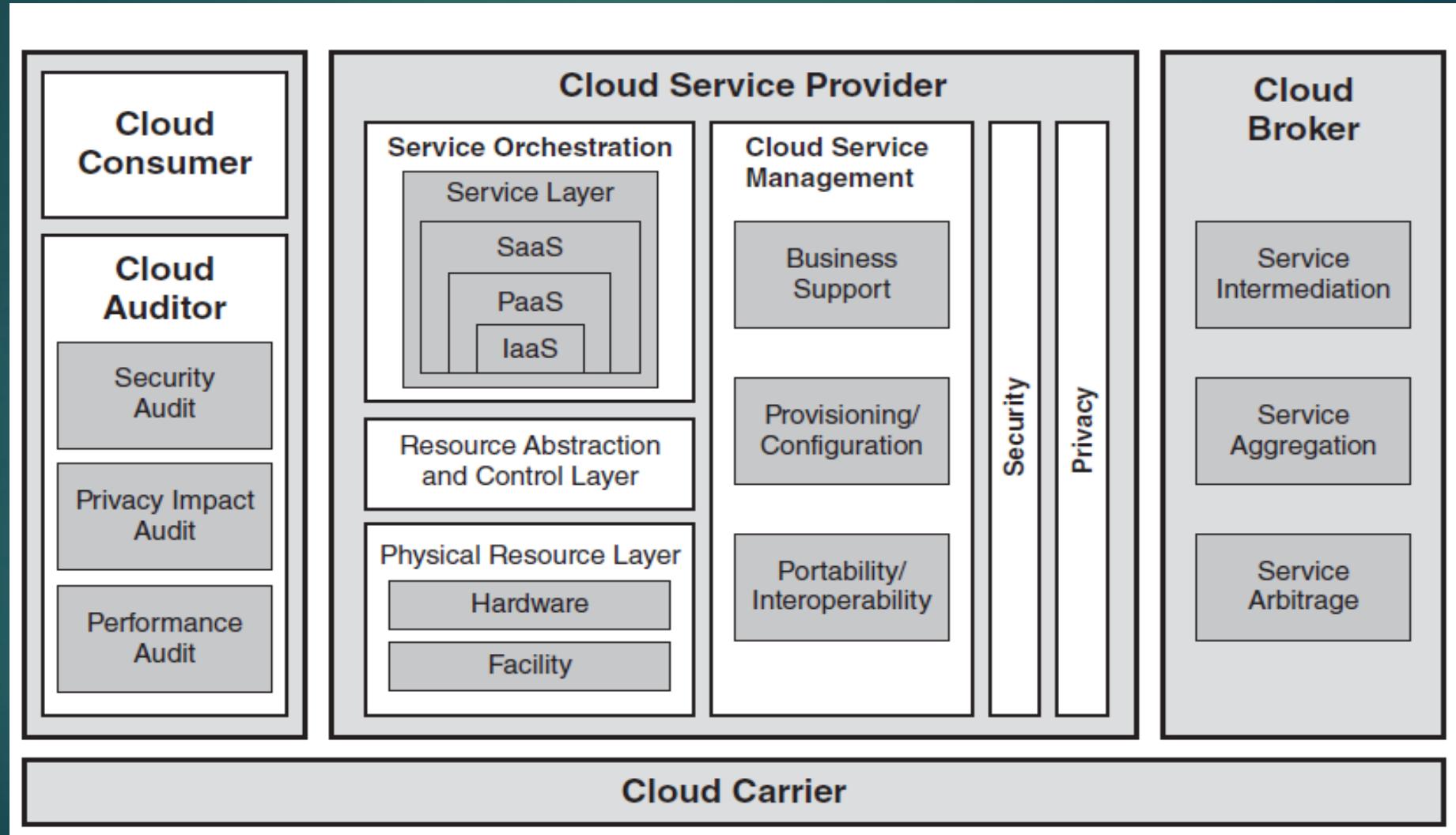


NIST's 5 Cloud Actors

- **Cloud Service Consumer:** Individual or entity that utilizes or subscribes to cloud-based services or resources
- **Cloud Service Provider (CSP):** The company that provides the cloud-based platform or services
- **Cloud Carrier:** the intermediary that provides connectivity and transport of cloud services between the CSPs and the cloud service consumers
- **Cloud Services Broker:** A third-party entity which acts as a liaison between customers and CSPs ideally selecting the best provider for each customer. The CSB acts as a middleman to broker the best deal and customize services
- **Cloud Service Auditor:** Third-party organization that verifies attainment of SLAs

**Per NIST SP 500-291 (Cloud Computing Standards Roadmap)

Cloud Actors and Functions



• Security Risks

- Multitenancy
 - Shared physical resources make incident response, forensics, destruction, are difficult
- Distributed
 - Laws vary from jurisdiction to jurisdiction
- Responsibility cannot be transferred
 - Customer is still legally liable for protection of the resource—Data Owner Maintains Responsible in All Cloud Models
- Privacy
 - The degree of privacy enforcement must be specified in SLA
- CSP may have higher requirements than the enterprise, BUT THE ONLY GUARANTEE IS IN THE SLA

Cloud Deployment Models

Deployment Models

- Public
- Private
- Hybrid
- Community

Public Cloud

What is a public cloud?

- Public clouds are the most common of deploying cloud computing. The cloud resources (like servers and storage) are owned and operated by a third party cloud service provider and delivered over the internet. Microsoft Azure is an example of a public cloud. With a public cloud, all hardware, software, and other supporting infrastructure is owned and managed by the cloud provider. In a public cloud, you share the same hardware, storage, and network devices with other organizations of cloud “tenants.” You access services and manage your account using a web browser. Public cloud deployments are frequently used to provide web-based email, online office applications, storage, and testing and development environments.

Public Cloud (2)

Advantages of public clouds:

- Lower costs - no need to purchase hardware and software, and you only pay for the service you use.
- No maintenance - your service provider provides the maintenance.
- Near unlimited scalability - on demand resources are available to meet your business needs.
- High reliability - a vast network of servers ensures against failure

Private Cloud

What is a private cloud?

- A private cloud consists of computing resources used exclusively by one business or organization. The private cloud can be physically located at your organization's on-site datacenter, or it can be hosted by a third party service provider. But in a private cloud, the services and infrastructure are always maintained on a private network and the hardware and software are dedicated solely to your organization. In this way, a private cloud can make it easier for an organization to customize its resources to meet specific IT requirements. Private clouds are often used by government agencies, financial institutions, and other mid-to-large size organizations with business critical operations seeking enhanced control over the environment.

Private Cloud (2)

Advantages of private clouds:

- More flexibility - your organization can customize its cloud environment to meet specific business needs.
- Improved security - resources are not shared with others, so higher levels of control and security are possible.
- High scalability - private clouds still afford the scalability and efficiency of a private cloud.

Hybrid Cloud

What is a hybrid cloud?

- Often called “the best of both worlds,” hybrid clouds combine on-premises infrastructure, or private clouds, with public clouds so organizations can reap the advantages of both. In a hybrid cloud, data and applications can move between private and public clouds for greater flexibility more deployment options. For instance, you can use the public cloud for high-volume, lower-security needs such as web based email, and the private cloud (or other on-premises infrastructure) for sensitive, business-critical operations such as financial reporting. In a hybrid cloud, “cloud bursting” is also an option. This is when an application or resource runs in the private cloud until there is a spike in demand (during an event like seasonal shopping or tax filing), at which point an organization can “burst through” to the public cloud to tap into additional computing resources.

Hybrid Cloud (2)

Advantages of hybrid clouds:

- Control - your organization can maintain a private infrastructure for sensitive assets.
- Flexibility - you can take advantage of additional resources in the public cloud if you need them
- Cost effectiveness - with the ability to scale to the public cloud, you pay for extra computing power only when needed.
- Ease - transitioning to the cloud doesn't have to be overwhelming because you can migrate gradually - phasing in workloads.

Community Cloud

- The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g. mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations , a third party, or some combination of them, and it may exist on or off premises.

Cloud Deployment Model Summary

| Deployment Model | Description | Best suited for | Offers | Challenges |
|------------------|---|---|---|---|
| Public cloud | -Provisioned for general public use -Externally hosted by a service provider | -Variable workloads -Test & Dev | -The lowest TCO, rapid elasticity& flexibility, faster deployments | -Data security&privacy, service availability |
| Private cloud | -Use for a single organization -Can be internally or externally deployed | -Sensitive data -Legal compliance | -Security and control, higher customizability, performance | -High cost of ownership -Required skill set |
| Community cloud | -Shared by several organizations -Typically externally hosted -Can be hosted internally by one of the organizations or distributed | -Collaboration between universities -Multiple business enterprises apply shared Services model (e.g group of hospitals or clinics) | -Lower TCO than private cloud, elasticity | -Complex IT governance -Required skill set |
| Hybrid cloud | -Composition of 2 or more clouds that remains unique entities but are bound together -Make use of the scalability and cost-effectiveness of public cloud offers without exposing mission-critical apps and data to third party vulnerabilities | -Cloud bursting -On demand access -Sensitive data -Storage as a service for non sensitive data | -Lower TCO -High elasticity -Security&control -Performance -Customizability | -Portability -Interoperability -Integration -Migration |

Cloud Service Models

Pizza as a Service



Traditional
On-Premises
Deployment

Kitchen

Oven

Gas

Pizza Dough

Toppings

Cook the Pizza

Made In-House

Infrastructure
as a Service
(IaaS)

Kitchen

Oven

Gas

Pizza Dough

Toppings

Cook the Pizza

Kitchen-as-a-
Service

Platform
as a Service
(PaaS)

DLLs

Tools

Runtime
Environment

Database

Toppings

Cook the Pizza

Create An App so
users can order pizza

Software
as a Service
(SaaS)

Kitchen

Oven

Gas

Pizza Dough

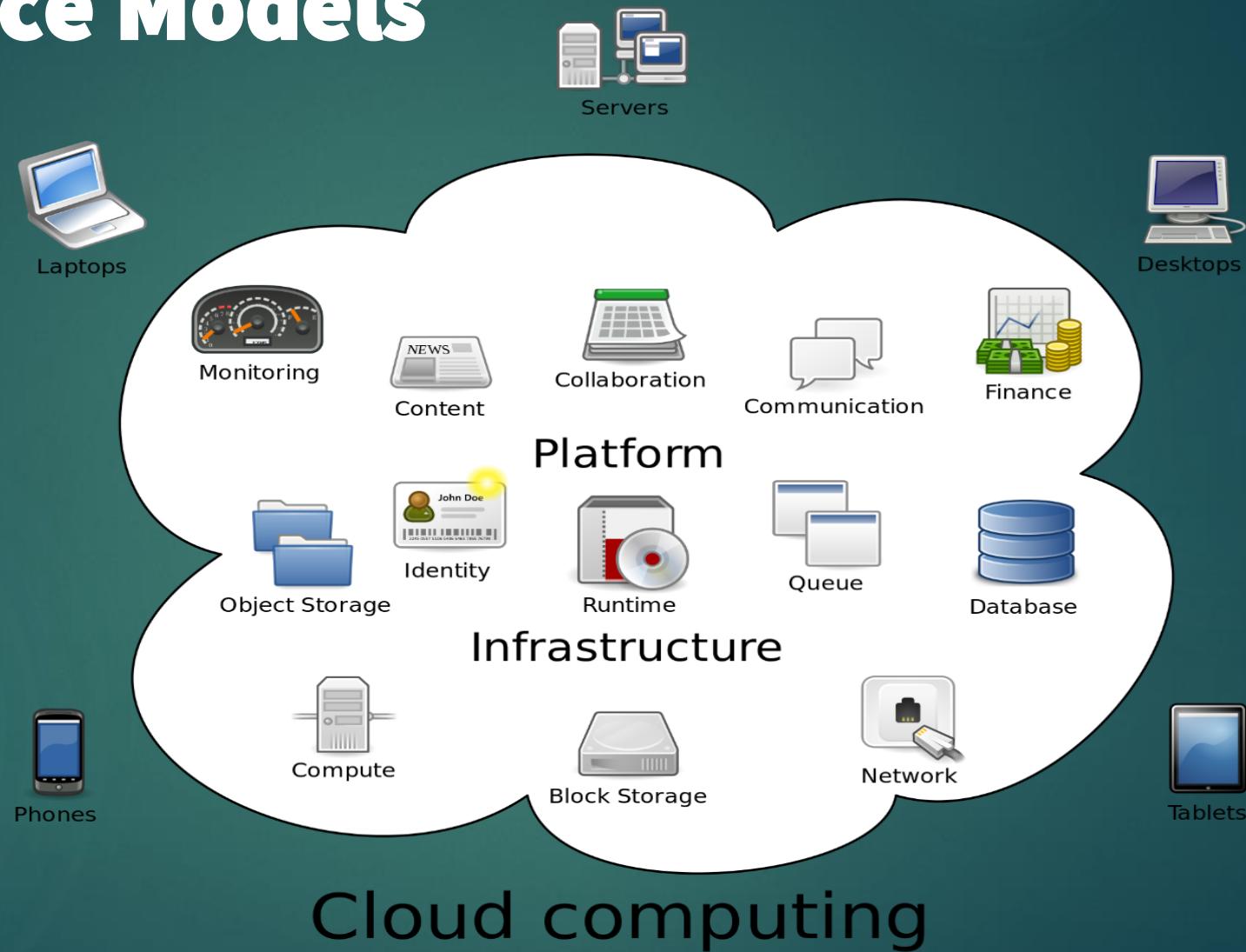
Toppings

Cook the Pizza

Pizza-as-a-
Service

Cloud Service Models

- SaaS
- PaaS
- IaaS



SaaS

- Software as a Services provides the consumer the ability to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through an interface like a web browser or a program interface



SaaS Offers

- Users can access their applications and data from anywhere, anytime
- Reduced TCO—reduced the need for advanced hardware. Redundancy and storage are provided
- Rather than purchasing licenses, software is leased
- Pay-per-use
- Elasticity
- Updates and Patch management is the responsibility of the provider
- Standardization—all users have the same version of software

Security for SaaS

- ▶ SaaS Involves 3 main issues
 - ▶ Data Segregation
 - ▶ Data Access and Policies
 - ▶ Web Application Security

PaaS

- Platform as a Service: provides the customer the capability to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services and tools supported by the provider.



PaaS Offers:

- Support for multiple languages and frameworks allowing developers to code in whichever programming language they prefer
- Multiple hosting environments: the ability to offer a wide variety and choice for the underlying hosting environments
- Flexibility: Focus on open standards and allowing relevant plugins to be quickly introduced to the platform. The goal is to reduce “lock-in” that comes with proprietary source code
- Automatic scalability: The application to seamlessly scale up and down as required by the platform.

Security for PaaS

- ▶ PaaS requires addressing 4 main issues
 - ▶ System/Resource isolation
 - ▶ User-level permissions
 - ▶ User Access Management
 - ▶ Protection against malware

IaaS

- The capability provided is to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run software including applications and operating systems. The consumer doesn't control the infrastructure, but does control the OS, storage, deployed apps and configuration settings.
- CPU
- Memory
- Disk storage local or SAN
- Operating
- Switches, all or part of the VLAN



IaaS Offers:

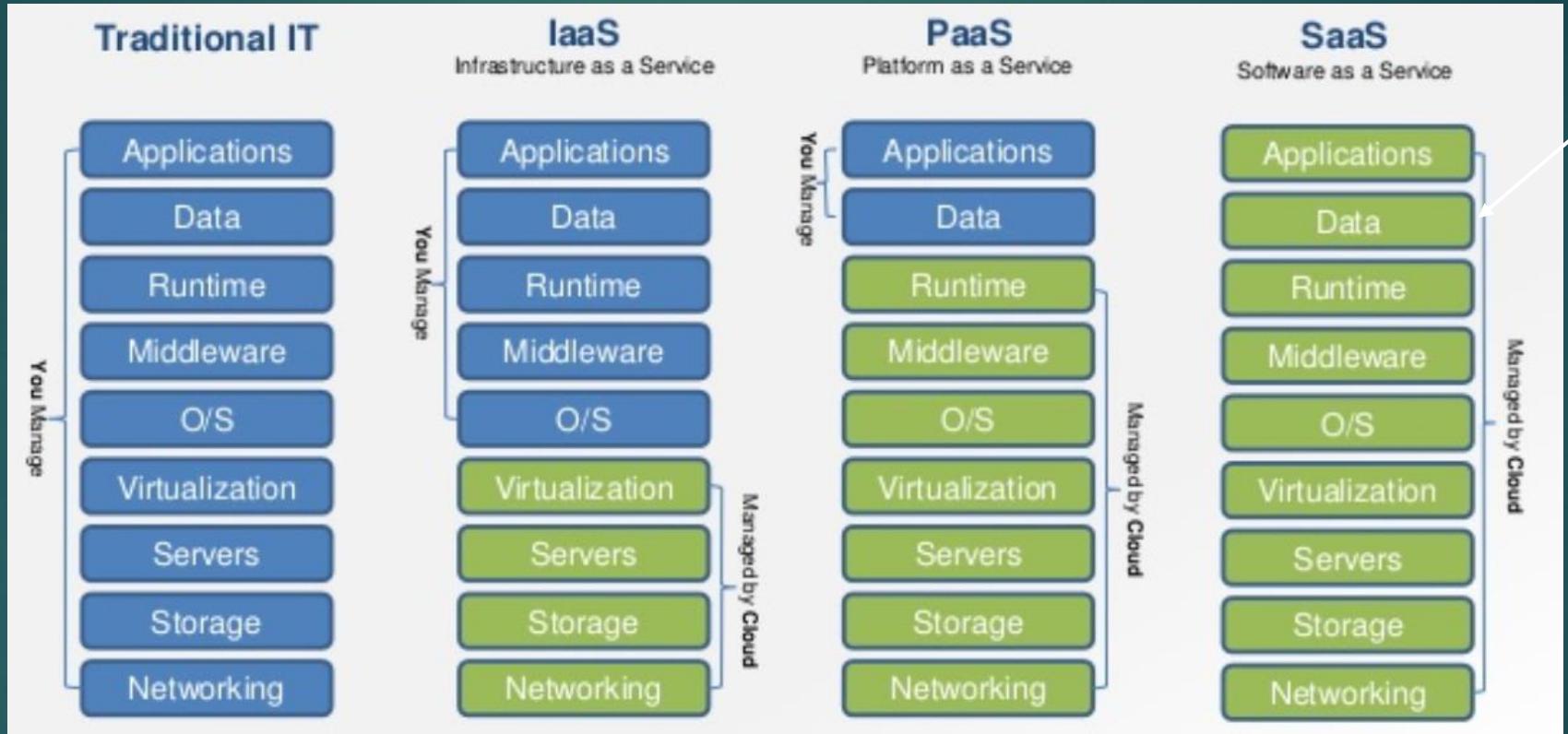
- Usage metered and priced on the basis of units consumed
- Upwards or Downwards scalability as needed
- Reduced TCO: No need to buy any assets, as day-to-day efforts are provided within the cloud. Reduced cost of maintenance and support, and no loss of asset value
- Reduced energy and cooling costs along with green IT environment
- Reduced in-house IT staff

Security for IaaS

- ▶ IaaS requires focus and understanding of the layers of the architecture from architecture to virtualization components.
Concerns include
 - ▶ VM Attacks
 - ▶ Virtual Switches/Network,
 - ▶ VM Based Rootkits/malicious hypervisor
 - ▶ Single point of access (A single NIC may provide access to numerous VMs)

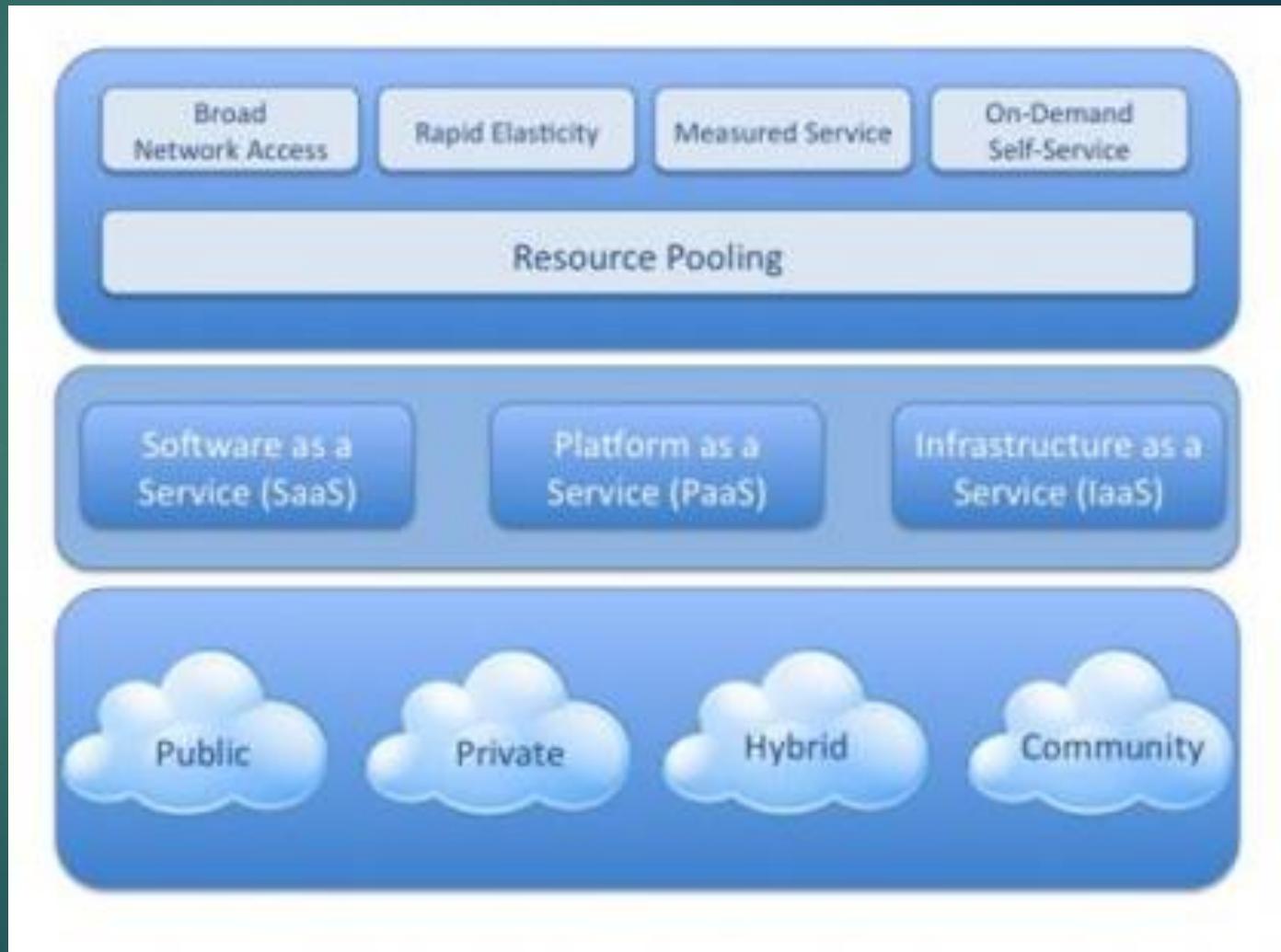
SaaS, PaaS, IaaS

Management Responsibility



The Big Picture

- Essential Characteristics
- Delivery Models
- Deployment Models



Cloud Computing Standards Roadmap (NIST SP 500-291)

Cloud Computing Standards Roadmap

- A cloud technology roadmap allows cloud providers to develop standardized, secure and interoperable identity, access & compliance management configurations & practices
- Designed to help assess current state for internal IT and cloud providers and plan how to meet needs of the future

** [NIST-SP 500-291](#)



The Cloud Services Roadmap

- Interoperability
- Availability
- Privacy
- Performance
- Service-level agreements (SLAs)
- Regulatory
- Portability
- Security
- Resilience
- Regulatory
- Auditability

Interoperability

- ▶ Standards-driven (vendor lock-in is the opposite)
- ▶ Helps ensure that enterprise investments do not become prematurely obsolete
- ▶ Components should be able to be replaced by new or different components from other providers and continue to work



Portability

- ▶ The ease with which application components can be used and reused elsewhere regardless of platform, provider, operating system, infrastructure, location, storage or format
- ▶ Important to consider as portability can help prevent vendor lock-in
- ▶ Can also enhance redundancy by allowing identical deployments to occur in other CSPs



Availability

- ▶ Resources can be accessed, as needed in a timely fashion, as authorized
- ▶ SLAs should specify the uptime required
- ▶ 99.999 is not unusual and can result in penalties, reimbursement of fees if not provided



Security

- ▶ Many cloud providers list their typical or baseline levels of security. They likely will not indicate specific controls or technologies
- ▶ Some Contracts might require particular security controls and techniques. These are usually seen as “extras” and will incur additional cost.
- ▶ Smaller companies will find moving to the cloud may enhance their security profile
- ▶ Regardless of the degree of security needed, it is almost always available with the right provider and for the right price.
- ▶ Don't assume security levels. SLAs should document needs



Privacy

- ▶ No consistent federal laws or directives in the US
- ▶ Laws vary based on location of stored data and pathways that data travels
- ▶ European Union sees privacy as a human right
- ▶ Laws and standards such as GLBA, HIPAA, and PCI DSS have requirements for protecting the privacy of information. These responsibilities are not transferred to the CSP
- ▶ Privacy vs. Confidentiality
 - ▶ Privacy: Owner's right to determine to whom information is disclosed
 - ▶ Security: Controller (processor) must provide security controls to enforce Privacy



Resilience

- ▶ Resiliency describes the ability to continue operating in the event of a disruption.
- ▶ Disruption could be caused by power outage, equipment failure, natural disaster, etc.
- ▶ Multiple layers of redundancy and fault tolerance must be in place
- ▶ Typically CSPs are capable of providing greater redundancy than most small organizations are capable of.



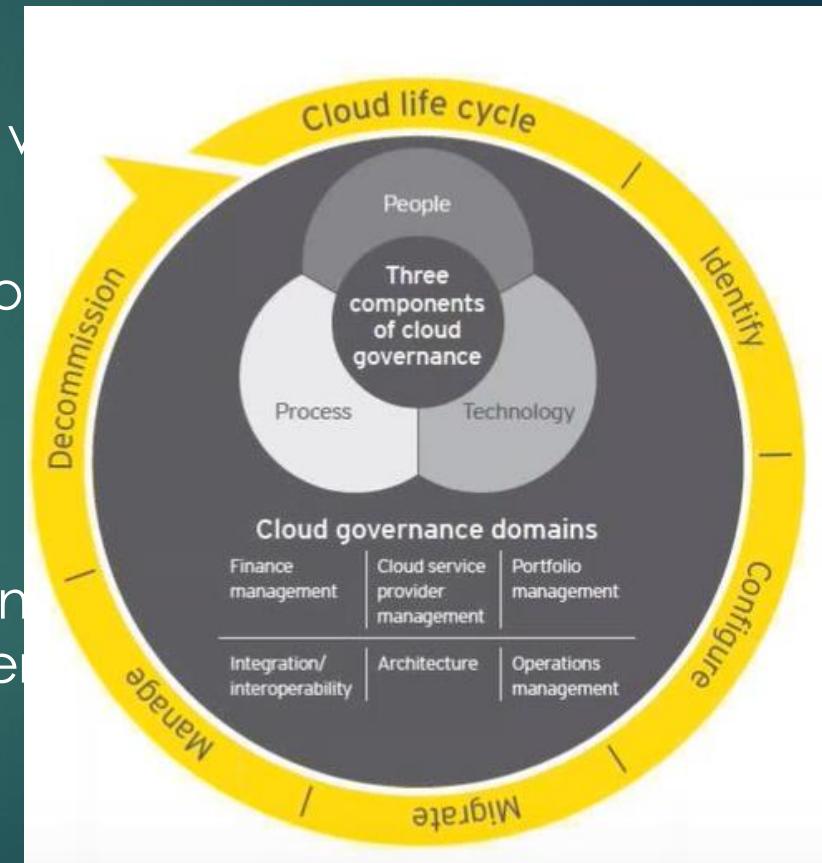
Performance

- ▶ Cloud computing should provide high performance at all times
- ▶ Capabilities are based on the
 - ▶ Network
 - ▶ Compute
 - ▶ Storage
 - ▶ Data



Governance

- ▶ Defining the actions, assigning the responsibilities and verifying performance
- ▶ Often an extension of existing organizational or traditional enterprise governance
- ▶ Must take into account risk management
- ▶ Many CSPs provide reporting, metrics, stats related to usage/actions/activities/updates, etc. This information streamline the process of oversight and facilitate governance



Service Level Agreements

- ▶ Availability (e.g. 99.997)
- ▶ Performance (e.g. maximum response times)
- ▶ Security / privacy of the data (e.g. encrypting all stored and transmitted data)
- ▶ Disaster Recovery expectations (RTO/RPO)
- ▶ Location of the data (e.g. consistent with local legislation)
- ▶ Access to the data (e.g. data retrievable from provider in readable format)



Service Level Agreements (2)

- ▶ Portability of the data (e.g. ability to move data to a different provider)
- ▶ Process to identify problems and resolution expectations (e.g. call center)
- ▶ Change Management process (e.g. changes – updates or new services)
- ▶ Dispute mediation process (e.g. escalation process, consequences)
- ▶ Exit Strategy with expectations on the provider to ensure smooth transition



Regulatory

- ▶ Compliance is an enterprise's requirement to adhere to relevant laws, regulations, standards, guidelines and specifications relevant to its business.
- ▶ Failure to comply may result in legal action, fines, loss of contracts, or business stoppage



Auditability

- ▶ Allows for users and the organization to access, report on, and document evidence of actions, processes, controls carried out by a particular user
- ▶ Most CSPs offer access to standard audit trails and system logs
- ▶ Increases transparency at the CSP
- ▶ Allows stakeholders to review, assess, and report user and system activities



Business Requirements

Business Requirements

- ▶ Cloud migration should be driven by business goals
 - ▶ Access
 - ▶ Availability
 - ▶ Performance
 - ▶ Security
 - ▶ Cost reduction

Inventory of Assets

- ▶ What does the business value?
 - ▶ Hardware
 - ▶ Software
 - ▶ Non-Tangibles
- ▶ Configuration Management/Change Management

Valuation of Assets

- ▶ Value of the asset
 - ▶ Value to the organization
 - ▶ Loss if compromised
 - ▶ Legislative drivers
 - ▶ Liabilities
 - ▶ Value to competitors
 - ▶ Acquisition costs
- ▶ FIPS 199/FIPS 200
 - ▶ Security Categorization
 - ▶ High Water Mark

Determination of Criticality

- ▶ Understanding of business objectives and organizational goals
- ▶ Sensitivity vs. Criticality
- ▶ Business Impact Analysis
 - ▶ Identifies business processes/paths/assets/etc. and prioritizes them based on criticality
 - ▶ Defines Metrics for Recovery
 - ▶ MTD/MAD: Length of time where an interruption of service would render the company unable to continue to operate
 - ▶ RTO: Goal for recovery of full operational capacity
 - ▶ RPO: Tolerance for data loss

Understanding Risk



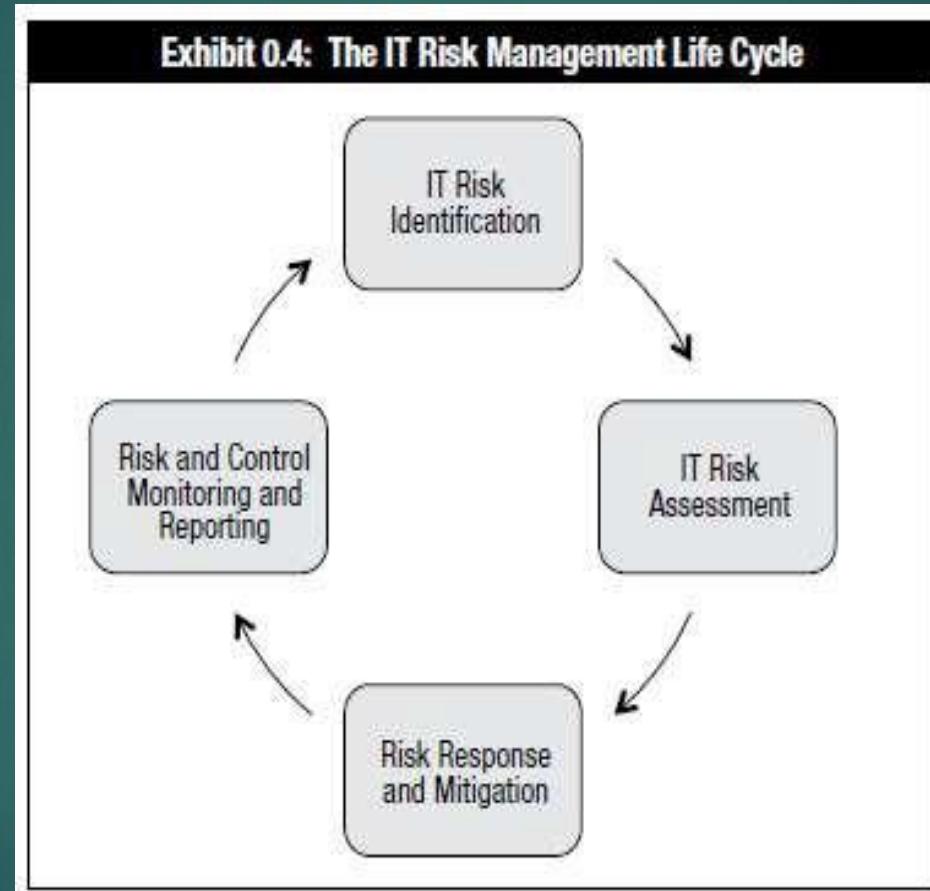
Risk Definitions

- ▶ **Asset:** Something of tangible or intangible value and is worth protecting
- ▶ **Vulnerability:** A weakness in the design, implementation, operation or internal control of a process that could expose a system to adverse threats
- ▶ **Threat:** Something that could pose loss to all or part of an asset
- ▶ **Threat Agent:** What carries out the attack
- ▶ **Exploit:** An instance of compromise
- ▶ **Risk:** The combination of the probability of an event and its consequence. Risks are often seen as an adverse event that can threaten an organization's assets or exploit vulnerabilities and cause harm
- ▶ **Inherent Risk:** With all business endeavors there is some degree of risk

Risk Definitions Continued

- ▶ **Residual Risk:** Risk that remains after a control has been implemented. Ultimately, risk should be mitigated until the residual risk is within the level that management is willing to accept (management's risk tolerance)
- ▶ **Secondary Risk:** One risk response may cause a second risk event
- ▶ **Risk Appetite:** Level amount of type of risk that the organization is willing to take on
- ▶ **Risk Tolerance:** The acceptable level of variation that management is willing to allow for any particular risk
- ▶ **Risk capacity:** The objective amount of loss an enterprise can tolerate without risking its continued existence. Defined by board and executive management at the enterprise level
- ▶ **Risk Threshold:** A quantified limit beyond which your organization is not willing to go
- ▶ **Controls:** Proactive and Reactive mechanisms put in place to manage risks

Risk Management Lifecycle



Risk Identification: The Risk Register

- ▶ AV * Threat * Vulnerability = Risk
- ▶ This may also appear as AV * Threat * Vulnerability
- ▶ At this stage, risks are ONLY being identified.

| Risk Identification | | Qualitative Rating | | | | Quantitative Rating | Risk Response | | Trigger (KRI—Key Risk Indicator) | Risk Owner | Status |
|---------------------|---------------|--------------------|--------|------------|--------------|-------------------------------|---------------|--|---|------------|--------|
| Risk Description | Risk Category | Probability | Impact | Risk Score | Risk Ranking | EMV (Expected Monetary Value) | Risk Response | | | | |
| DDoS | Technical | 3 | 5 | 15 | 1 | \$ 8,000.00 | FW, IDS/IPS | | Network utilization > 70% for more than 5 minutes consecutive | Mylo | |
| | | | | 0 | 2 | | | | | | |
| | | | | 0 | 3 | | | | | | |
| | | | | 0 | 4 | | | | | | |
| | | | | 0 | 5 | | | | | | |
| | | | | 0 | 6 | | | | | | |
| | | | | 0 | 7 | | | | | | |
| | | | | 0 | 8 | | | | | | |
| | | | | 0 | 9 | | | | | | |
| | | | | 0 | 10 | | | | | | |
| | | | | 0 | 11 | | | | | | |
| | | | | 0 | 12 | | | | | | |
| | | | | 0 | 13 | | | | | | |
| | | | | 0 | 14 | | | | | | |
| | | | | 0 | 15 | | | | | | |
| | | | | 0 | 16 | | | | | | |
| | | | | 0 | 17 | | | | | | |
| | | | | 0 | 18 | | | | | | |
| | | | | 0 | 19 | | | | | | |
| | | | | 0 | 20 | | | | | | |
| | | | | 0 | 21 | | | | | | |
| | | | | 0 | 22 | | | | | | |
| | | | | 0 | 23 | | | | | | |
| | | | | 0 | 24 | | | | | | |
| | | | | 0 | 25 | | | | | | |
| | | | | 0 | 26 | | | | | | |
| | | | | 0 | 27 | | | | | | |
| | | | | 0 | 28 | | | | | | |
| | | | | 0 | 29 | | | | | | |
| | | | | 0 | 30 | | | | | | |

Threat Modeling

| STRIDE (Threats) | DREAD (Vulnerabilities) |
|-------------------------|--------------------------------|
| Threat | Damage potential |
| Spoofing | Reproducibility |
| Tampering | Exploitability |
| Repudiation | Affected user base |
| Information Disclosure | Discoverability |
| Denial of Service | |
| Escalation of Privilege | |

Risk Assessment

- Justifies a mitigation strategy
 - Analysis--Value
 - Probability X Impact
 - Qualitative
 - Quantitative
 - Evaluation of Risk
 - Cost of Control vs Potential for loss

Risk Mitigation and Response

- Reduce: Lessen probability and/or impact of risk
- Avoidance: If probability and/or impact is reduced to zero, the risk is avoided
- Transfer: Share the loss potential--THINK SLA or Insurance
- Accept: If risk is within levels of tolerance, we may accept the risk, or we often accept risk when the cost of the control exceeds the potential for
- Rejection: Ignore the risk

Risk Monitoring and Reporting

- Because of the changing nature of risk and associated controls, ongoing monitoring is an essential step of the risk management life cycle.
- KRI: Key Risk Indicator
- KPI: Key Performance Indicator

Risk Review

- **Risk Identification**
 - Identify and determine the value of assets
 - Identify threats and vulnerabilities
- **Risk Assessment (Value)**
 - Analysis (Probability X Impact = Loss Potential)
 - Qualitative vs. Quantitative
 - Evaluation (Loss Potential vs. Cost of Countermeasure)
- **Risk Mitigation/Response**
 - Reduce
 - Accept
 - Transfer
 - Avoid
 - Reject
- **Ongoing Controls Evaluation**
 - KRI
 - KPI

Boundaries of Cloud Models

Boundaries

- ▶ Defining the demarcation point is more difficult with cloud-based environment—lines are blurred
- ▶ Data resides outside our perimeter in environment owned by someone else
- ▶ Remember: Cloud customer maintains legal liability for loss of data
 - ▶ SLAs may offer restitution

Boundaries: IaaS

- ▶ CSP is responsible for:
 - ▶ Facility
 - ▶ Hardware
 - ▶ Power
 - ▶ Connectivity
 - ▶ Hypervisor
- ▶ Customer
 - ▶ Operating Systems
 - ▶ Application
 - ▶ Data Management

- ▶ CSP is additionally responsible for:
 - ▶ Installation, maintenance, administration of operating system(s)
- ▶ Customer is responsible for applications running on the operating system
 - ▶ Review/monitor application issues
 - ▶ Updates to the applications
 - ▶ Data

- ▶ CSP is responsible for:
 - ▶ Most elements of the environment
- ▶ Customer is responsible for
 - ▶ Identity and Access Management
 - ▶ Data

Boundary Summary

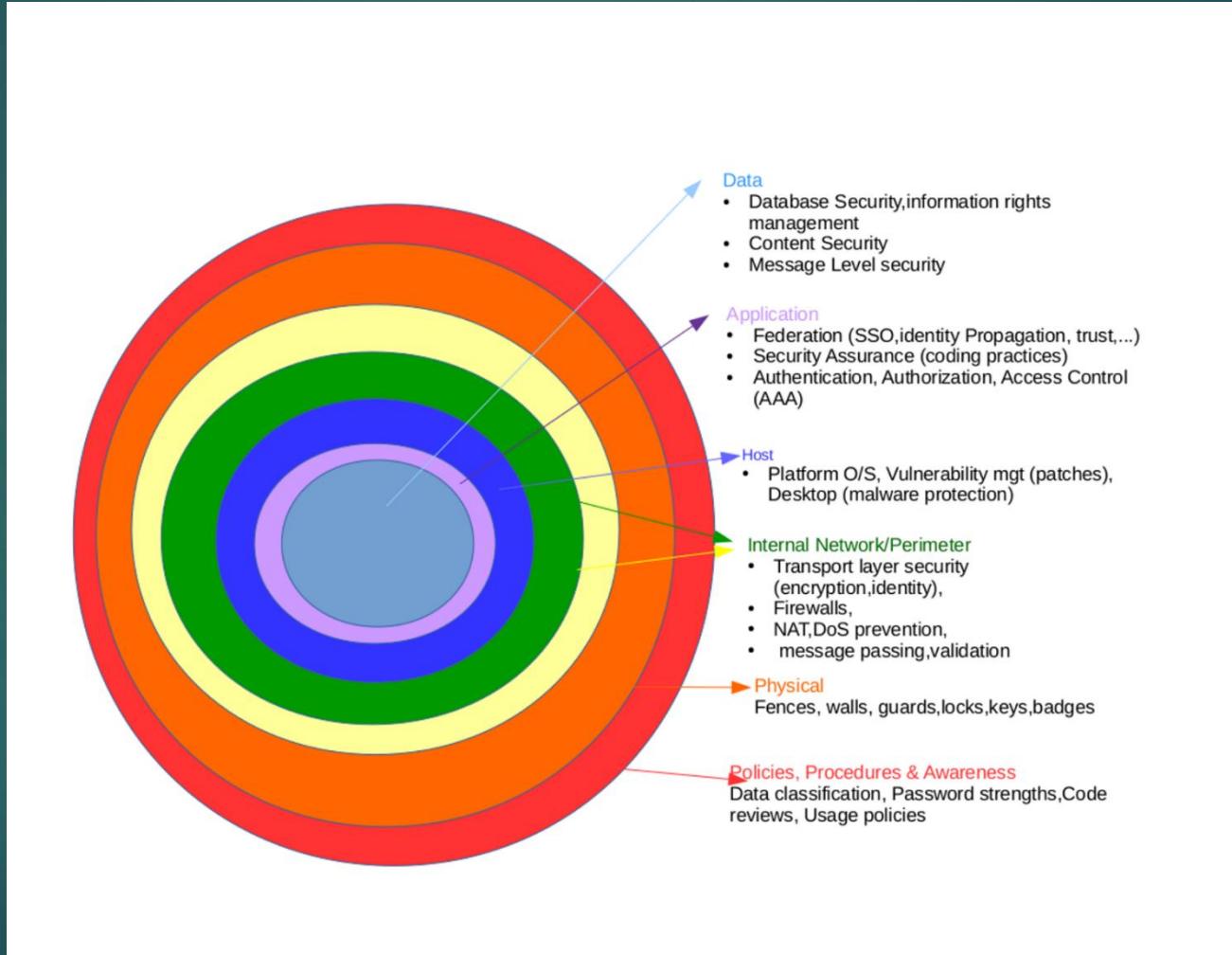
| Responsibility | On-Prem | IaaS | PaaS | SaaS |
|--------------------------------------|----------------|----------------|----------------|----------------|
| Data classification & accountability | Cloud Customer | Cloud Customer | Cloud Customer | Cloud Customer |
| Client & end-point protection | Cloud Customer | Cloud Customer | Cloud Customer | Cloud Provider |
| Identity & access management | Cloud Customer | Cloud Customer | Cloud Provider | Cloud Provider |
| Application level controls | Cloud Customer | Cloud Customer | Cloud Provider | Cloud Provider |
| Network controls | Cloud Customer | Cloud Provider | Cloud Provider | Cloud Provider |
| Host infrastructure | Cloud Customer | Cloud Provider | Cloud Provider | Cloud Provider |
| Physical security | Cloud Customer | Cloud Provider | Cloud Provider | Cloud Provider |

Legend: █ Cloud Customer █ Cloud Provider

Defense in Depth

Defense in Depth

90



Hardening Devices

- Remove or rename guest accounts
- Removing Unnecessary Services/protocols/ports
- Reconfigure Default configurations that may result in security compromise
- Use strong passwords/secure protocols
- Audit admin privileges
- Limit physical access
- Patch, maintain, update systems

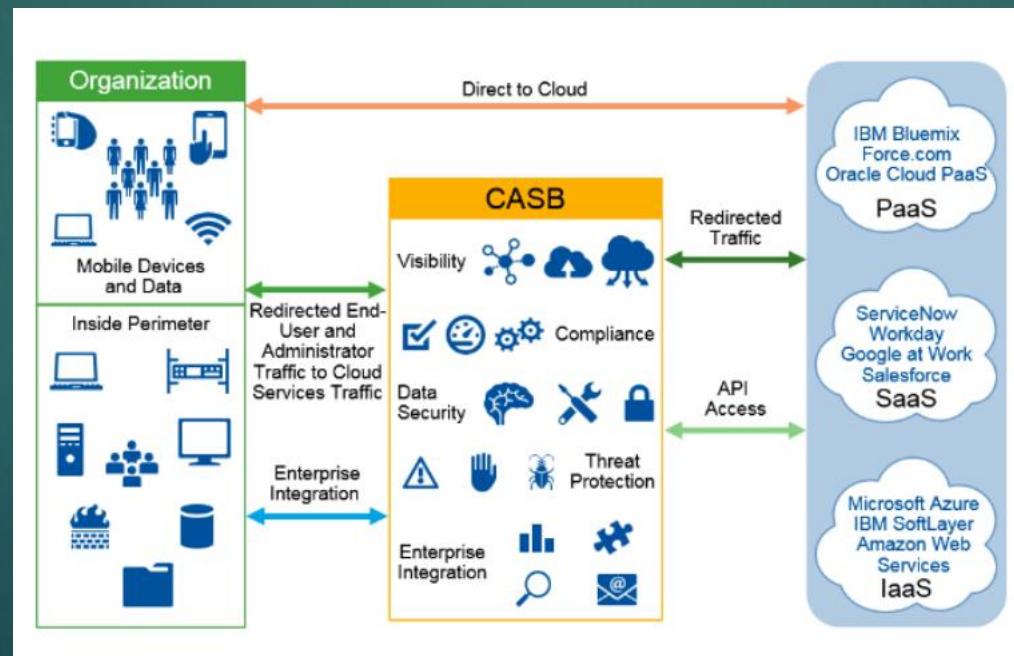
***Applies to virtual systems also

Data Protection

- ▶ Data at Rest (DAR)
 - ▶ Encryption, Redundancy
- ▶ Data in Motion (DIM)
 - ▶ Separation/Isolation, Transport Security, VLANs
 - ▶ SSL/TLS create an encrypted tunnel
 - ▶ IPSec tunnel mode is also a good solution
- ▶ Data in Use (DIU)
 - ▶ Protection of APIs, digital signatures and encryption, restricted access
 - ▶ Homomorphic encryption. The idea is that if we could keep a dataset encrypted while being manipulated in memory or shared with another application, we would then never have to decrypt it, making the data transaction safer

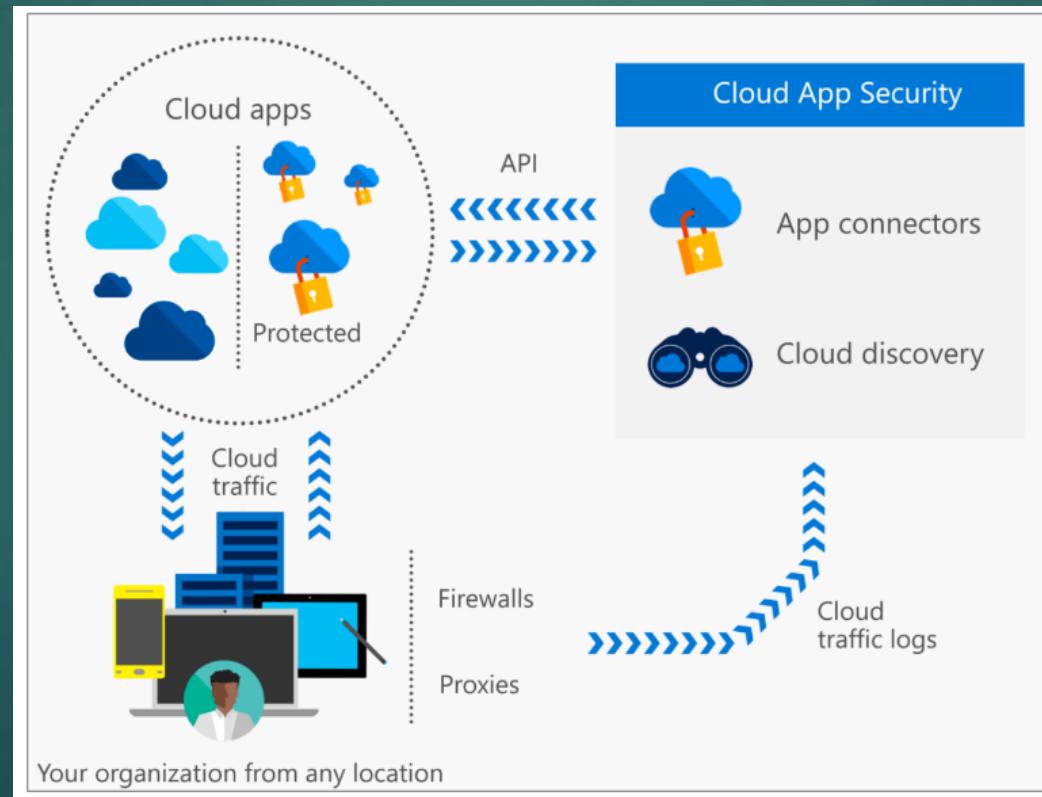
CASB (Cloud Access Security Brokers)

- ▶ Cloud Access Security Broker(CASB) is an on-premises or cloud-based security policy enforcement point that is placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as cloud-based resources are accessed



CASP (Cloud Application Security Platforms)

- ▶ CASP: API-based model of a CASB leveraging APIs while providing detection, remediation and user education instead of in-line inspection of cloud application traffic.



Domain 1 Architectural Concepts and Design Requirements Review

95

- ▶ Introduction to Cloud Concepts
- ▶ Cloud Deployment Models
- ▶ Cloud Service Models
- ▶ Cloud Computing Standards Roadmap (NIST SP 500-291)
- ▶ Business Requirements
- ▶ Boundaries in the Cloud
- ▶ Layered Defense

Domain 2: Cloud Data Security

Domain 2 Cloud Data Security

- ▶ Data Inventory and Discovery
- ▶ Data Lifecycle Security
- ▶ Storage Architectures
- ▶ Unauthorized User Access
- ▶ Liability Issues
- ▶ Denial of Service
- ▶ Integrity Issues
- ▶ Cloud Security Alliance Cloud Controls Matrix

Data Roles

- ↳ Data Subject: an identifiable subject who can be identified by reference to an id number, or one or more factors specific to the his physical, physiological, mental, economic, cultural, or social identity (Telephone number, SSN, IP address, etc.)
- ↳ Data Owner/Controller: organization that has collected or created the data. Within an organization the owner is often the line of business. Responsible for determining sensitivity and access for data. Also known as the controller.
- ▶ Data Custodian/Processor: Performs routine operations on data—collection, recording, organization, storage, etc.

The cloud customer is the controller of the data and is **RESPONSIBLE for all the legal duties addressed in Privacy and Data Protection (P&DP) applicable laws. The service provider supplies

Data Security Lifecycle

- The Cloud Security Alliance has incorporated the data security lifecycle which enables the organization to map the different phases in the data lifecycle against the required controls that are relevant to each phase.
- Create:** This is probably better named Create/Update because it applies to creating or changing a data/content element, not just a document or database. Creation is the generation of new digital content, or the alteration/updating of existing content.
 - Store:** Storing is the act committing the digital data to some sort of storage repository, and typically occurs nearly simultaneously with creation.
 - Use:** Data is viewed, processed, or otherwise used in some sort of activity.



Data Security Lifecycle (2)

4. **Share:** Data is exchanged between users, customers, and partners.
5. **Archive:** Data leaves active use and enters long-term storage.
6. **Destroy:** Data is permanently destroyed using physical or digital means

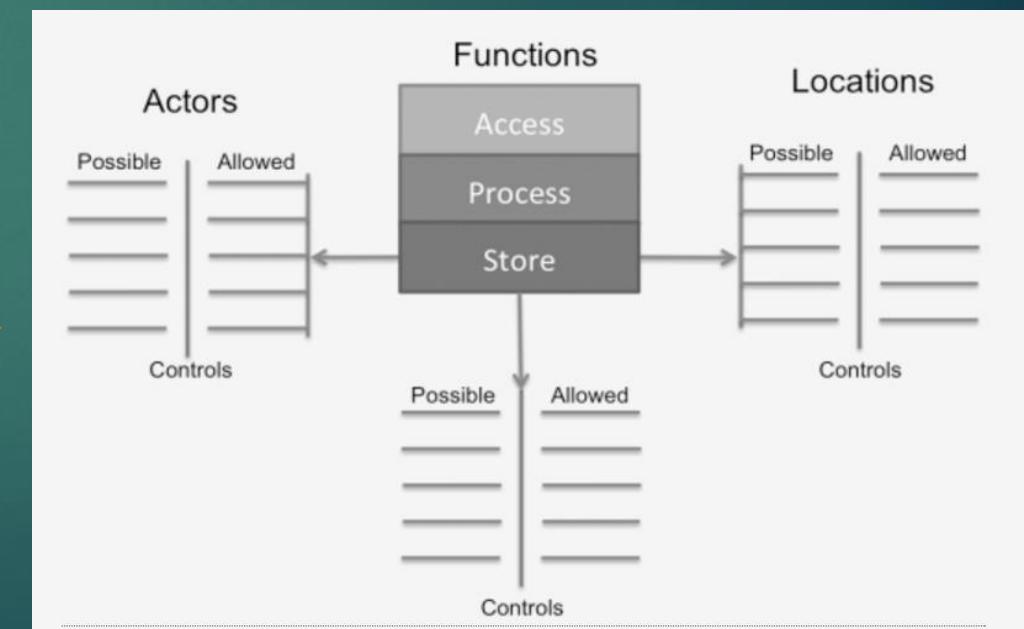


Data Creation Phase

- ▶ Categorize: Organization of data
 - ▶ Legal/regulatory
 - ▶ Business function
 - ▶ Department
 - ▶ Project or program
- ▶ Classify:
 - ▶ Value to the organization
 - ▶ CIA Triad
 - ▶ Jurisdictional
- ▶ Label: Provides information on confidentiality, handling, dissemination, limitations, etc on the data

Threat Modeling with the Data Security Lifecycle

- ▶ At this point, we are able to produce a high-level mapping of data flow, including device access and data locations. For each location, we can determine the relevant function and actors. Once this is mapped, we can better define what to restrict from which actor and by which control

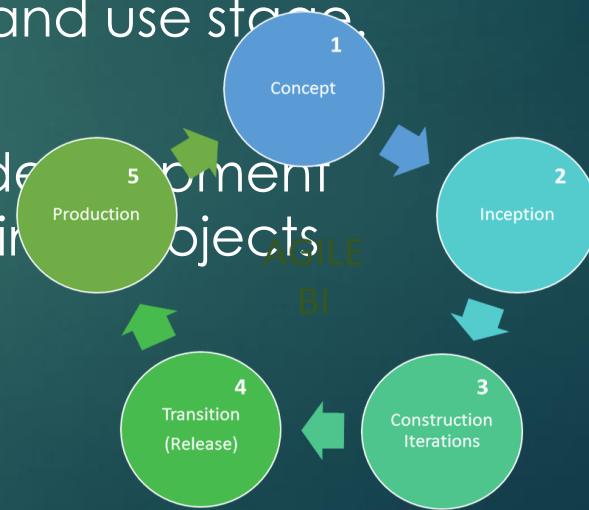


Data Discovery/Analytics

Data Discovery Techniques

- ▶ **Data Discovery** is a user-driven process of searching for patterns or specific items in a data set. Data Discovery applications use visual tools such as geographical maps, pivot-tables, and heat-maps to make the process of finding patterns or specific items rapid and intuitive.
- ▶ Data Discovery may leverage statistical and data mining techniques to accomplish these goals. There are several different ways Data Discovery tools make their analysis
 - ▶ **Metadata** provides data its meaning and describes its attributes
 - ▶ **Labels** provide a logical grouping of data elements and gives them a “tag” describing the data
 - ▶ **Content** analysis examines the data itself

- ▶ **Data mining:** A process used by companies to turn raw **data** into useful information. By using software to look for patterns in large batches of **data**, businesses can learn more about their customers to develop more effective marketing strategies, increase sales and decrease costs.
- ▶ Real-time analytics: Data mining during the creation and use stage. Resource intensive
- ▶ Agile Business Intelligence: Utilization of the software development methodology known as, “agile development” for use in business objects



Data Control

Backups and Archives

- Keep Data Retention Requirements in mind
- Select Backup methods appropriate with Business Objectives
- Use Numbers from BIA: RTO and RPO
- Remember security of backup media
- Backups are copies of current data, intended for fault tolerance
- Archives are data considered to be out of use, but preserved in the event that it is required at a later time
- ▶ ***Don't forget to consider media type and format

Data Protection policies: Retention

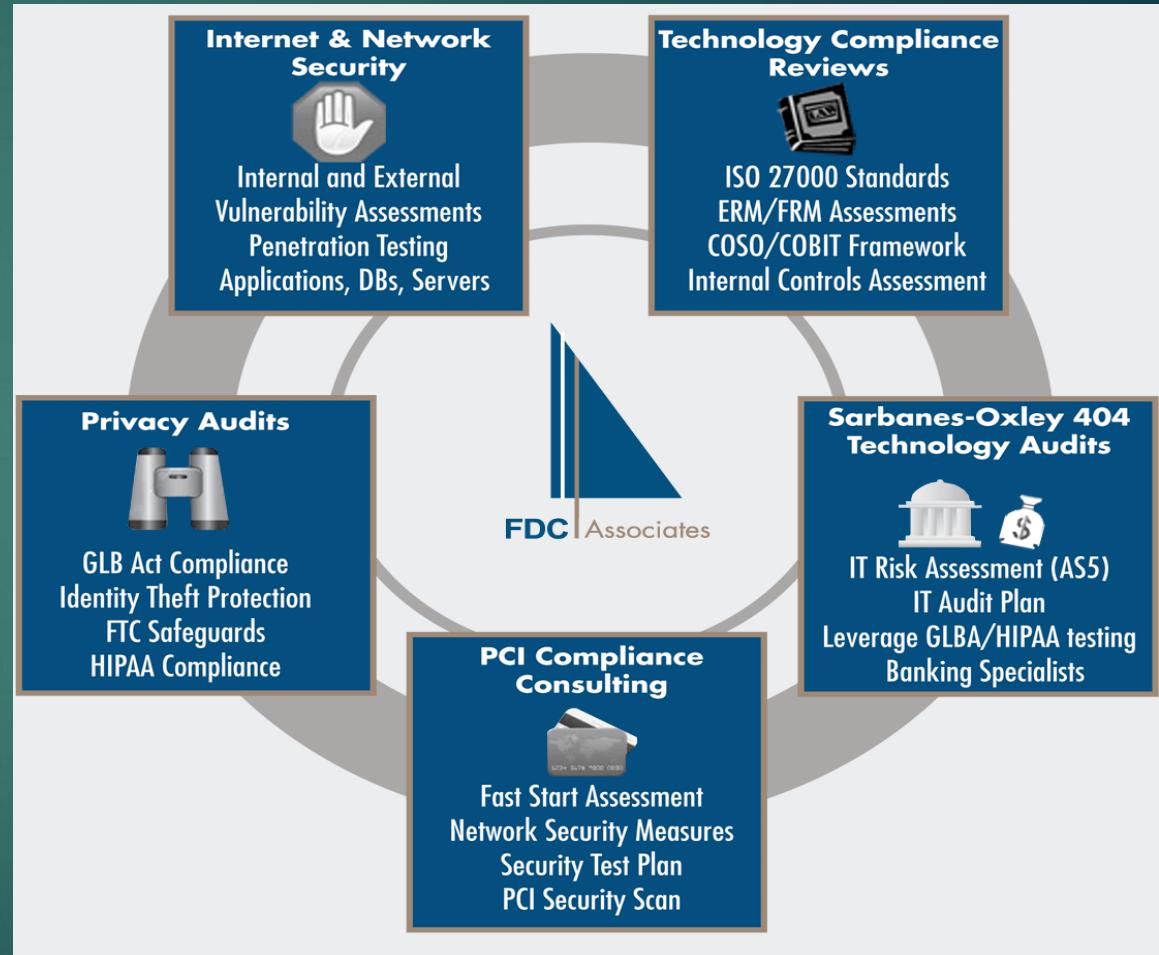
- Data retention: Established protocol for keeping information for operational or regulatory compliance needs.
- Cloud considerations:
 - Legal, regulatory and standards requirements must be well-documented and agreed upon
 - Data mapping should map all relevant data in order to understand formats, data types and data locations
 - Data Classification based on locations, compliance requirements, ownership and business usage
 - Each category's procedures should be followed based on appropriate policy that governs the data type

Data Protection policies: Data archiving

- Data archiving is the process of identifying and moving inactive data out of current production systems and into specialized long-term archival storage systems. Considerations include:
 - Encryption
 - Monitoring
 - Granular retrieval
 - **Electronic discovery** (also called **e-discovery**) any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case
 - Backup and recovery
 - Media Type
 - Restoration procedures

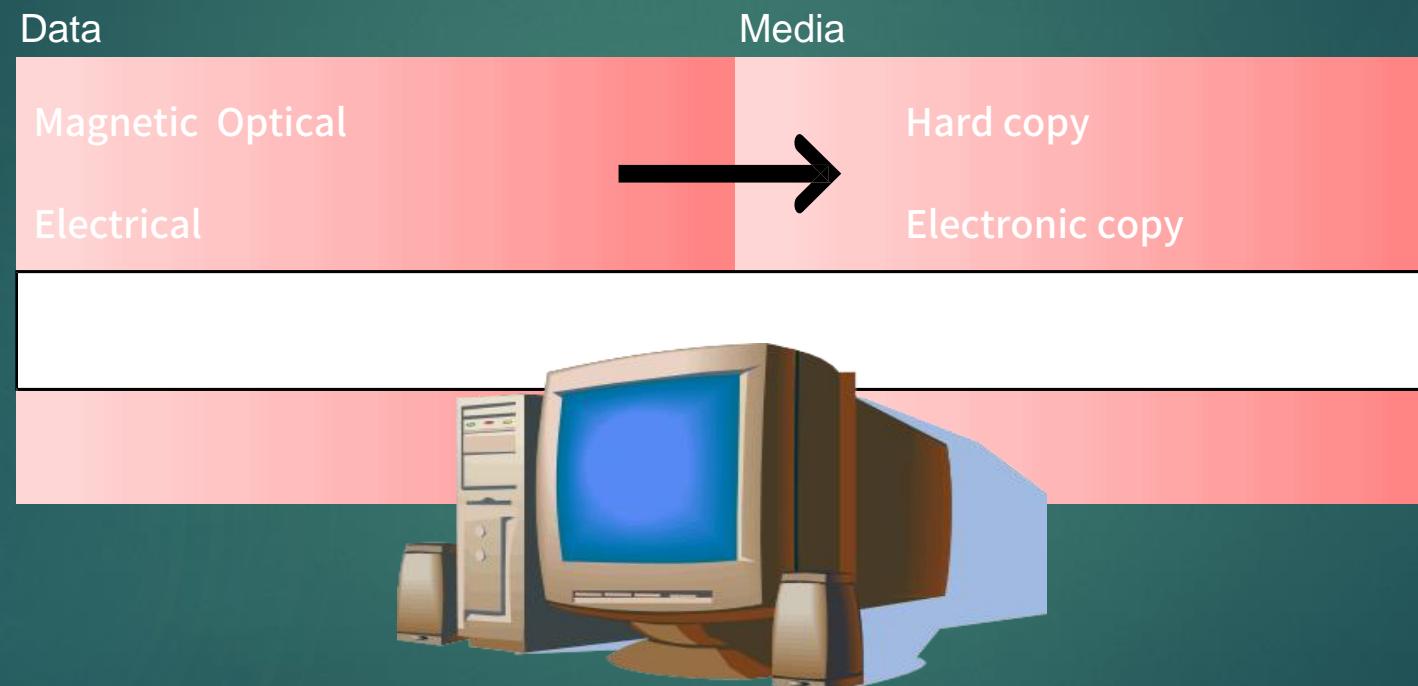
Audits

- ▶ Associate Audits with compliance:
 - Compliance with policy
 - Compliance with Standards
- ▶ Remember Auditors do not need write protection
- ▶ Also, auditors do not provide suggestions on remediation



Media Sanitation

111



Removing Data Remnants Disposal

- Clearing—overwriting—renders data in accessible by normal means
- Purging—degaussing—renders media unusable by normal means
- Destruction—Physical destruction Irreversible by all known techniques
- Cryptoshredding—Best option in the cloud. Encrypting the remnants with strong, publicly known algorithm and destroying the key

Domain 2: Cloud Data Security

Data Security Lifecycle: Create

- The Cloud Security Alliance has incorporated the data security lifecycle which enables the organization to map the different phases in the data lifecycle against the required controls that are relevant to each phase.
- **Create:**
 - Data Created Remotely: Data created by the user should be encrypted before uploading to the cloud.
 - FIPS 140-2
 - Data Created within the Cloud: Encryption
- Activities related to Classification of data begin at this phase and continue into the next phase—See next slides



Data Security Lifecycle: Store

Store:

- Storing is the act committing the digital data to a storage repository, and typically occurs nearly simultaneously with creation.
- To comply with the federal standards organizations:
 1. Determine the security category of their information system in accordance with [FIPS 199](#), (Standards for Security Categorization of Federal Information and Information Systems,)
 2. Derive the information system impact level from the security category in accordance with [FIPS 200](#),
 3. Apply the appropriately tailored set of baseline security controls in [NIST SP 800-53](#), Security and Privacy Controls for Federal Information Systems and Organizations



Data Security Lifecycle: Use

- Data is processed or otherwise used in some sort of activity, NOT including modification
- Data is particularly vulnerable as in order to be processed, it must be encrypted
 - DLP
 - IRM
 - File Monitoring
 - VM Controls



Data Security Lifecycle: Share

- Information is made accessible to others (users, customers, partners)
 - Secure Transport
 - IPsec
 - SSL/TLS
 - SSH
 - VPNs
 - DLP: Data Loss Prevention—Prevent/Monitor Data exfiltration
 - IRM: Information Rights Management

**Consider jurisdictional issues—Export/Import Regulations may prohibit certain types of data to be shared/stored in different locations – See Next Slide



Data Security Lifecycle: Archive

- ▶ Archival period is determined by policy
- ▶ Often policy is the result of external drivers such as legal requirements
- ▶ Certain Industries require data be retained for a certain time period
- ▶ At the end of the archival period, data should be destroyed across all locations in a manner consistent with policy



Data Security Lifecycle: Destruction

- Clearing—overwriting—renders data inaccessible by normal means
- Purging—degaussing—renders media unusable by normal means
- Destruction—Physical destruction Irreversible by all known techniques
- Crypto-shredding: Encrypt the drive with a strong, publicly known algorithm and algorithm and destroy the key.



Data Classification

Classification Schemes

Figure 1—Sample Data Categorization Scheme

| Security Objective | Level 1 | Level 2 | Level 3 |
|------------------------|---|---|--|
| Confidentiality | Loss of access restrictions or unauthorized disclosure would have a high impact on enterprise goals. | Loss of access restrictions or unauthorized disclosure would have a medium impact on enterprise goals. | Loss of access restrictions or unauthorized disclosure would have a low impact on enterprise goals. |
| Integrity | Improper information modification or destruction would have a high impact on enterprise goals. | Improper information modification or destruction would have a medium impact on enterprise goals. | Improper information modification or destruction would have a low impact on enterprise goals. |
| Availability | Loss of timely and reliable access would have a high impact on enterprise goals. | Loss of timely and reliable access would have a medium impact on enterprise goals. | Loss of timely and reliable access would have a low impact on enterprise goals. |

Figure 2—Sample Questions

| | |
|---|---|
| Confidentiality —Would unauthorized disclosure... | <ul style="list-style-type: none">• affect health and safety?• have a monetary impact (e.g., intellectual property)?• have a reputational impact (e.g., personally identifiable information [PII])?• have a legal/regulatory impact (e.g., PCI DSS)? |
| Integrity —Would unauthorized modification or destruction... | <ul style="list-style-type: none">• affect critical business decisions?• affect health and safety?• have a monetary impact?• have a reputational impact?• have a legal/regulatory impact? |
| Availability —Would nonavailability... | <ul style="list-style-type: none">• have a reputational impact?• affect health and safety?• have a monetary impact?• have a legal/regulatory impact? |

FIPS 199-STANDARDS FOR SECURITY Categorization

FIPS 199 defines three levels of potential IMPACT on organizations or individuals should there be a breach of security (i.e., a loss confidentiality, integrity, or availability).

- ▶ The potential impact is LOW if – The loss of confidentiality, integrity, or availability could be expected to have a LIMITED adverse effect on organizational operations, organizational assets, or individuals.
- ▶ The potential impact is MODERATE if – The loss of confidentiality, integrity, or availability could be expected to have a SERIOUS adverse effect on organizational operations, organizational assets, or individuals
- ▶ The potential impact is HIGH if – The loss of confidentiality, integrity, or availability could be expected to have a SEVERE OR CATASTROPHIC adverse effect on organizational operations, organizational assets, or individuals
- ▶ Example: A SCADA system includes a SC sensor data = {(confidentiality, NA), (integrity, HIGH), (availability, HIGH)},
 - ▶ and
 - ▶ SC administrative information = {(confidentiality, LOW), (integrity, LOW), (availability, LOW)}.
 - ▶ The resulting security category of the information system is initially expressed as:
 - ▶ **SC SCADA system = {(confidentiality, LOW), (integrity, HIGH), (availability, HIGH)}**,

Potential Impact

| Security Objective | POTENTIAL IMPACT | | |
|--|---|---|--|
| | LOW | MODERATE | HIGH |
| <i>Confidentiality</i> 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. |
| <i>Integrity</i> 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. |
| <i>Availability</i> 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. |

FIPS 199-STANDARDS FOR SECURITY Categorization

- ▶ FIPS describes the following
 - ▶ *Low-impact system* is an information system in which all three of the security objectives are low.
 - ▶ *Moderate-impact system* is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate.
 - ▶ *High-impact system* is an information system in which at least one security objective is high.

**High Water Mark (HWM): FIPS 200 introduced the concept of the high water mark (HWM) which must be used to determine the overall impact level of the information system.

Addresses the minimum-security requirements for information and information systems supporting the executive agencies of the federal government and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements.

- ▶ Access control
- ▶ Awareness and training
- ▶ Audit and accountability
- ▶ Certification accreditation, and security assessments
- ▶ Configuration management
- ▶ Contingency planning
- ▶ Identification and authentication
- ▶ Incident response
- ▶ Maintenance
- ▶ Media protection
- ▶ Physical and environmental protection
- ▶ Planning
- ▶ Personnel security
- ▶ Risk assessment
- ▶ Systems and services acquisition
- ▶ System and communications protection
- ▶ System and information integrity

NIST 800-53 rev 4

- ▶ FIPS 800-53 Rev 4 Security and Privacy Controls for Federal Information Systems and Organizations Specifies
 - ▶ MULTITIERED RISK MANAGEMENT
 - ▶ SECURITY CONTROL STRUCTURE
 - ▶ SECURITY CONTROL BASELINES
 - ▶ SECURITY CONTROL DESIGNATIONS
 - ▶ EXTERNAL SERVICE PROVIDERS
 - ▶ ASSURANCE AND TRUSTWORTHINESS

NIST 800-53 Rev4 Control Structure and Baselines

127

| ID | FAMILY |
|----|---------------------------------------|
| AC | Access Control |
| AT | Awareness and Training |
| AU | Audit and Accountability |
| CA | Security Assessment and Authorization |
| CM | Configuration Management |
| CP | Contingency Planning |
| IA | Identification and Authentication |
| IR | Incident Response |
| MA | Maintenance |
| MP | Media Protection |
| PE | Physical and Environmental Protection |
| PL | Planning |
| PS | Personnel Security |
| RA | Risk Assessment |
| SA | System and Services Acquisition |
| SC | System and Communications Protection |
| SI | System and Information Integrity |
| PM | Program Management |

| CNTL NO. | CONTROL NAME <i>Control Enhancement Name</i> | WITHDRAWN | ASSURANCE | CONTROL BASELINES | | |
|----------|---|-----------|-----------------------------------|-------------------|-----|------|
| | | | | LOW | MOD | HIGH |
| AC-1 | Access Control Policy and Procedures | | X | X | X | X |
| AC-2 | Account Management | | | X | X | X |
| AC-2(1) | ACCOUNT MANAGEMENT AUTOMATED SYSTEM ACCOUNT MANAGEMENT | | | | X | X |
| AC-2(2) | ACCOUNT MANAGEMENT REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS | | | | X | X |
| AC-2(3) | ACCOUNT MANAGEMENT DISABLE INACTIVE ACCOUNTS | | | | X | X |
| AC-2(4) | ACCOUNT MANAGEMENT AUTOMATED AUDIT ACTIONS | | | | X | X |
| AC-2(5) | ACCOUNT MANAGEMENT INACTIVITY LOGOUT | | | | | X |
| AC-2(6) | ACCOUNT MANAGEMENT DYNAMIC PRIVILEGE MANAGEMENT | | | | | |
| AC-2(7) | ACCOUNT MANAGEMENT ROLE-BASED SCHEMES | | | | | |
| AC-2(8) | ACCOUNT MANAGEMENT DYNAMIC ACCOUNT CREATION | | | | | |
| AC-2(9) | ACCOUNT MANAGEMENT RESTRICTIONS ON USE OF SHARED / GROUP ACCOUNTS | | | | | |
| AC-2(10) | ACCOUNT MANAGEMENT SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION | | | | | |
| AC-2(11) | ACCOUNT MANAGEMENT USAGE CONDITIONS | | | | | X |
| AC-2(12) | ACCOUNT MANAGEMENT ACCOUNT MONITORING / ATYPICAL USAGE | | | | | X |
| AC-2(13) | ACCOUNT MANAGEMENT DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS | | | | | X |
| AC-3 | Access Enforcement | | | X | X | X |
| AC-3(1) | ACCESS ENFORCEMENT RESTRICTED ACCESS TO PRIVILEGED FUNCTIONS | X | Incorporated into AC-6. | | | |
| AC-3(2) | ACCESS ENFORCEMENT DUAL AUTHORIZATION | | | | | |
| AC-3(3) | ACCESS ENFORCEMENT MANDATORY ACCESS CONTROL | | | | | |
| AC-3(4) | ACCESS ENFORCEMENT DISCRETIONARY ACCESS CONTROL | | | | | |
| AC-3(5) | ACCESS ENFORCEMENT SECURITY-RELEVANT INFORMATION | | | | | |
| AC-3(6) | ACCESS ENFORCEMENT PROTECTION OF USER AND SYSTEM INFORMATION | X | Incorporated into MP-4 and SC-28. | | | |
| AC-3(7) | ACCESS ENFORCEMENT ROLE-BASED ACCESS CONTROL | | | | | |
| AC-3(8) | ACCESS ENFORCEMENT REVOCATION OF ACCESS AUTHORIZATIONS | | | | | |
| AC-3(9) | ACCESS ENFORCEMENT CONTROLLED RELEASE | | | | | |
| AC-3(10) | ACCESS ENFORCEMENT AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS | | | | | |
| AC-4 | Information Flow Enforcement | | | X | X | |
| AC-4(1) | INFORMATION FLOW ENFORCEMENT OBJECT SECURITY ATTRIBUTES | | | | | |
| AC-4(2) | INFORMATION FLOW ENFORCEMENT PROCESSING DOMAINS | | | | | |
| AC-4(3) | INFORMATION FLOW ENFORCEMENT DYNAMIC INFORMATION FLOW CONTROL | | | | | |
| AC-4(4) | INFORMATION FLOW ENFORCEMENT CONTENT CHECK ENCRYPTED INFORMATION | | | | | |
| AC-4(5) | INFORMATION FLOW ENFORCEMENT EMBEDDED DATA TYPES | | | | | |
| AC-4(6) | INFORMATION FLOW ENFORCEMENT METADATA | | | | | |
| AC-4(7) | INFORMATION FLOW ENFORCEMENT ONE-WAY FLOW MECHANISMS | | | | | |
| AC-4(8) | INFORMATION FLOW ENFORCEMENT SECURITY POLICY FILTERS | | | | | |
| AC-4(9) | INFORMATION FLOW ENFORCEMENT HUMAN REVIEWS | | | | | |
| AC-4(10) | INFORMATION FLOW ENFORCEMENT ENABLE / DISABLE SECURITY POLICY FILTERS | | | | | |

Import/Export of Data

Export and Import Restriction: Wassenaar Agreement

- ▶ The Wassenaar Arrangement was established in July 1996 at the end of the cold war. It was created to advance regional and international security and stability. It attempts to accomplish this stability by promoting transparency in the transfers of conventional arms and dual-use goods.
- ▶ The Wasenaar Agreement is not enforced by any agency or regulatory Committee
- ▶ Because of this all U.S. export compliance is enforced by the various U.S. agencies. The U.S. Department of Commerce's Bureau of Industry and Security for items falling under the Export Administration Regulations (EAR) and the Directorate of Defense Trade Controls (DDTC) for items falling under the International Trade in Arms Regulations (ITAR).

Export and Import Restriction

131

- ▶ United States
 - ▶ ITAR (International Traffic in Arms Regulation) Prohibits export of defense-related information
 - ▶ EAR (Export Administration Regulations) govern the export and re-export of items for reasons of national security, non-proliferation, foreign policy, and short supply. Covers civilian and dual-use systems
- ▶ Various Countries
 - ▶ Laws restricting imports of strong cryptosystems
 - ▶ Wassenaar Agreement: Multilateral export control organization that regulates national security controlled items among member states

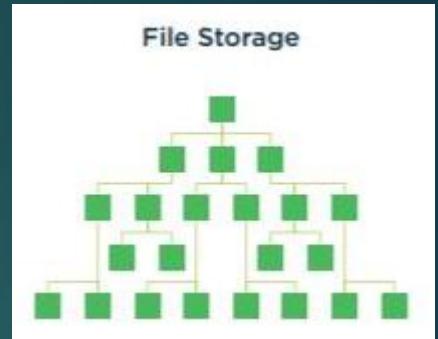
Cloud Storage Architectures

Cloud Storage

- ▶ Cloud storage is data storage made available as a service via a network
- ▶ CSPs provide a range of storage options to meet various service level objectives
- ▶ Storage type varies by service type

Storage Architectures: File-Based

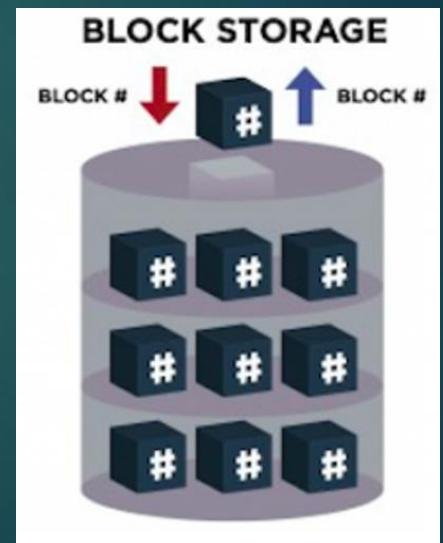
- ▶ Includes volumes/data stores attached to IaaS instances, usually a virtual hard drive
 - ▶ **File-based:** presented with traditional folder/file level hierarchy.
 - ▶ Centralized, highly accessible, hierarchy of files and folders
 - ▶ File storage uses metadata and directories to organize files
 - ▶ Low cost, but not a very robust solution



Storage Architectures: Block-Based

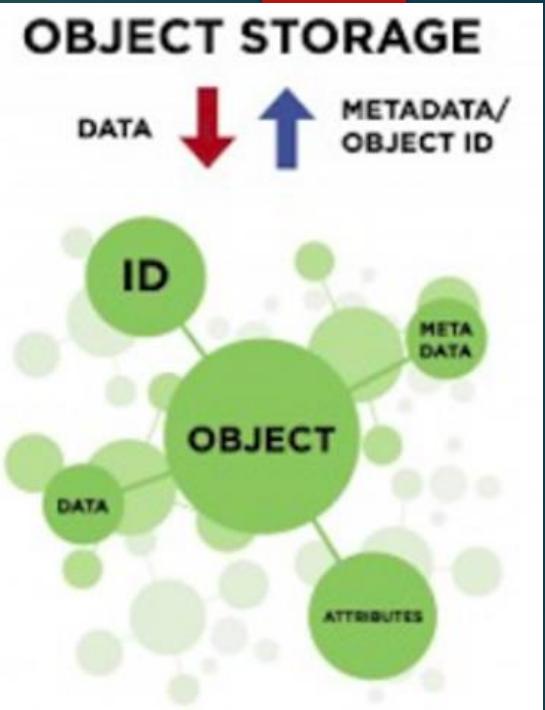
135

- ▶ **Block** : Each storage volume acts as an individual hard drive that is configured by the storage administrator. In the block storage model, data is saved to the storage media in fixed-sized chunks called blocks. Each block is associated with a unique address
 - ▶ Storage blocks are controlled by the server-based operating system and are generally accessed by iSCSI, Fibre Channel or Fibre Channel over Ethernet (FCoE) protocols.
 - ▶ Ideal for high-performing, mission-critical applications that require consistent input/output (I/O) performance and low latency and is often used in storage-area network (SAN) environments in place of file storage.



Storage Architectures: IaaS—Object-Based Storage

- ▶ Relatively low performance/low-cost option
- ▶ Extremely large amounts of storage available unstructured data
- ▶ **Particularly good for archival of data or unstructured data**
- ▶ **Four necessary elements for each object:**
 - ▶ The data or content of the object—any type of file
 - ▶ A unique identifier: 128 bit GUID
 - ▶ Metadata: contains contextual information about data such as its name, size, content-type and URL
 - ▶ Security Attributes
- ▶ Objects go in “buckets” and buckets are accessed via an API



Use Case for Object-Based Storage

137

- Off-site backups
- Storing and serving user content (e.g. profile pictures)
- Storing artifacts (e.g. JAR files, startup scripts) to be deployed to VMs
- Distributing static content (e.g. video content for your users)
- Caching intermediate data (e.g. individual frames from a render farm before assembly into output video)
- Accepting input or providing output to a web service (as accepting data by POST can be difficult/inefficient for large input files).
- archiving data for regulatory purposes

Storage Architectures: IaaS

138

| Object vs. file vs. block storage | | | |
|-----------------------------------|--|--|---|
| | OBJECT STORAGE | FILE-BASED STORAGE | BLOCK-BASED STORAGE |
| Transaction units | Objects, that is, files with custom metadata | Files | Blocks |
| Supported type of update | No in-place update support; updates create new object versions | Supports in-place updates | Supports in-place updates |
| Protocols | REST and SOAP over HTTP | CIFS and NFS | SCSI, Fibre Channel, SATA |
| Metadata support | Support of custom metadata | Fixed file-system attributes | Fixed system attributes |
| Best suited for | Relatively static file data and as cloud storage | Shared file data | Transactional data and frequently changing data |
| Biggest strength | Scalability and distributed access | Simplified access and management of shared files | High performance |
| Limitations | Ill-suited for frequently changing transactional data; doesn't provide a sharing protocol with a locking mechanism | Difficult to extend beyond the data center | Difficult to extend beyond the data center |

Data Storage: PaaS

- ▶ Databases:
 - ▶ Structured: Highly organized, such that inclusion in a relational database is seamless and readily searchable
 - ▶ Unstructured: Information that doesn't reside in a traditional row-column database—text, multimedia content, email, etc

Data Storage: SaaS

- ▶ Information Storage and Management: Data is entered into the system via the web interface and stored with the SaaS application (often a backend database)
- ▶ Content/file storage is stored within the application
- ▶ Content Delivery Network: content is stored in object storage, and then distributed to geographically distributed nodes to improve performance

Cloud Data Security Foundational Strategies

Encryption

- ▶ The types and implementation of encryption are driven by the CIA objectives determined for the data. However, encryption generally involves the following:
 - ▶ Data—what needs to be protected
 - ▶ Encryption engine—element that performs the encryption operation
 - ▶ Encryption keys—safe-guarding the keys is an essential element of successful cryptography

Types of Encryption (2)

- ▶ Object storage encryption
 - File-level encryption—DRM/IRM allows creator of file to embed permissions based on attributes. These restrictions protect the file regardless of 3rd party access.
 - Application-level—encryption engine resides in the application utilizing the object storage, or can be implemented on a customer gateway/proxy
- ▶ Database Encryption—can use file or application level encryption. Also most DBMS can provide transparent encryption that is seamless to the user, with the engine residing within the database

Key Management

- Protection: Keys must be stored securely and (if needed) transmitted in a secure fashion
- Key Archival/Recovery
 - Dual Control
 - M of N control
- Key Distribution:
 - PKI
 - Out of Band
 - Session Keys and PFS
- Key Revocation
- Key Escrow
- Key Management
 - Customer
 - 3rd Party

Key Management

- ▶ RKMS (Remote Key Management Service): Customer owns KMS on premise but it is managed remotely by the service provider allowing customer to control the confidentiality while the provider provides support remotely
- ▶ Client Side Key Management: Similar to RKMS the client side approach puts the customer in control of encryption/decryption keys. KMS resides on customer's premises.

Encryption Best Practices

- ▶ Use Open and validated formats (Algorithms should be strong and publicly known)
- ▶ All encryption keys should be stored within the enterprise, as opposed to with the cloud provider. Keying material should never be stored on same volume as encrypted data
- ▶ Identity-based key assignment and protection of private keys
- ▶ Use strong encryption
- ▶ Follow Key management best practices for location of keys
- ▶ Separation of Duties would require that key management functions should be conducted separately from the cloud provider

Masking, Obfuscation, Anonymization, and Tokenization

- ▶ Obfuscation is the process of hiding, replacing or omitting sensitive information
 - ▶ Masking is the process of using specific characters to hide certain parts of a specific dataset. For instance, displaying asterisks for all but last 4 digits of SSN.
- ▶ Data Anonymization is the process of either encrypting or removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous
- ▶ Tokenization: Public cloud service can be integrated and paired with a private cloud that stores sensitive data. The data sent to the public cloud is altered and contains a reference to the data residing the in the private cloud.

Tokenization

148

HOW DOES A TOKENIZED TRANSACTION WORK?

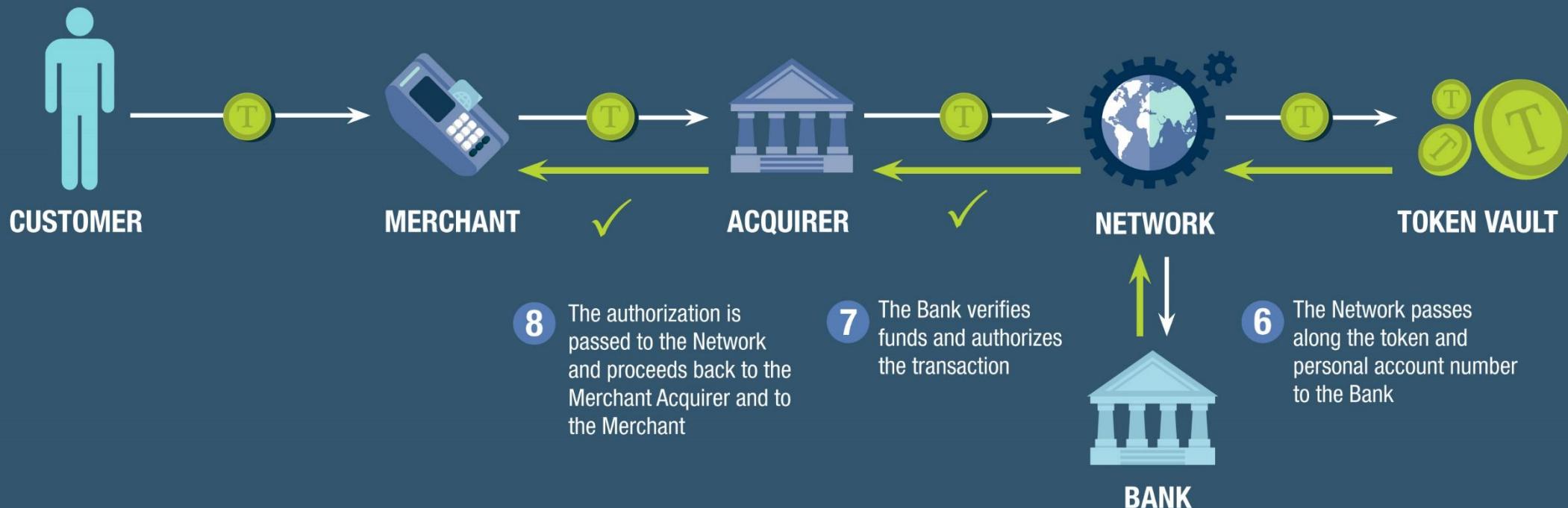
- 1 When paying—either via online purchase or tap-to-pay—the token goes to the Merchant

- 2 The Merchant passes the token along to their Merchant Acquirer

- 3 The Merchant Acquirer passes the token to the Network

- 4 Once passed to the Network, the data is within the secure bank vault

- 5 The network consults its “Token Vault” to match the token with the customer’s account number



Monitoring: Security and Event Management

- ▶ Software and products combining security information management and event management. It provides real-time analysis of security alerts generated by network hardware and applications. SEIM Systems often provide:
 - ▶ Aggregation from many sources
 - ▶ Correlation across common attributes
 - ▶ Alerting to a predefined entity responsible for monitoring
 - ▶ Dashboard tools to take event data and organize into charts or other formats
 - ▶ Compliance tools automate the gathering of compliance data
 - ▶ Retention employs long term storage of historical data to facilitate correlation of data over time to provide the retention necessary for compliance
 - ▶ Forensic analysis provides the ability to search across logs on different nodes and time periods based on specific criteria

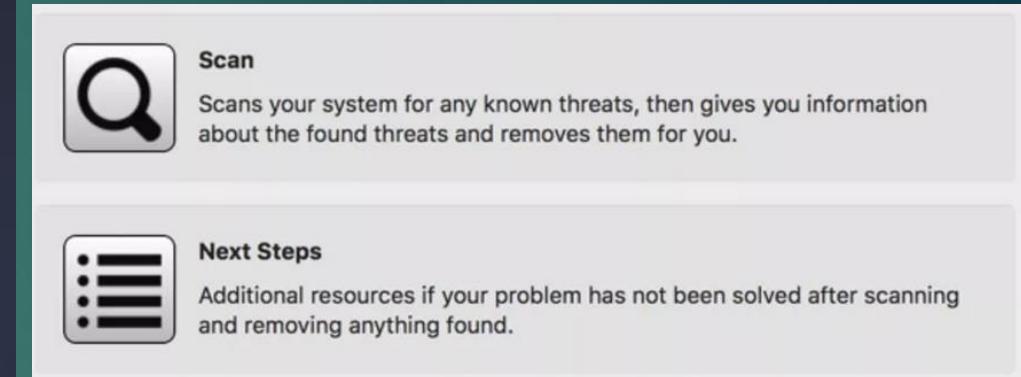
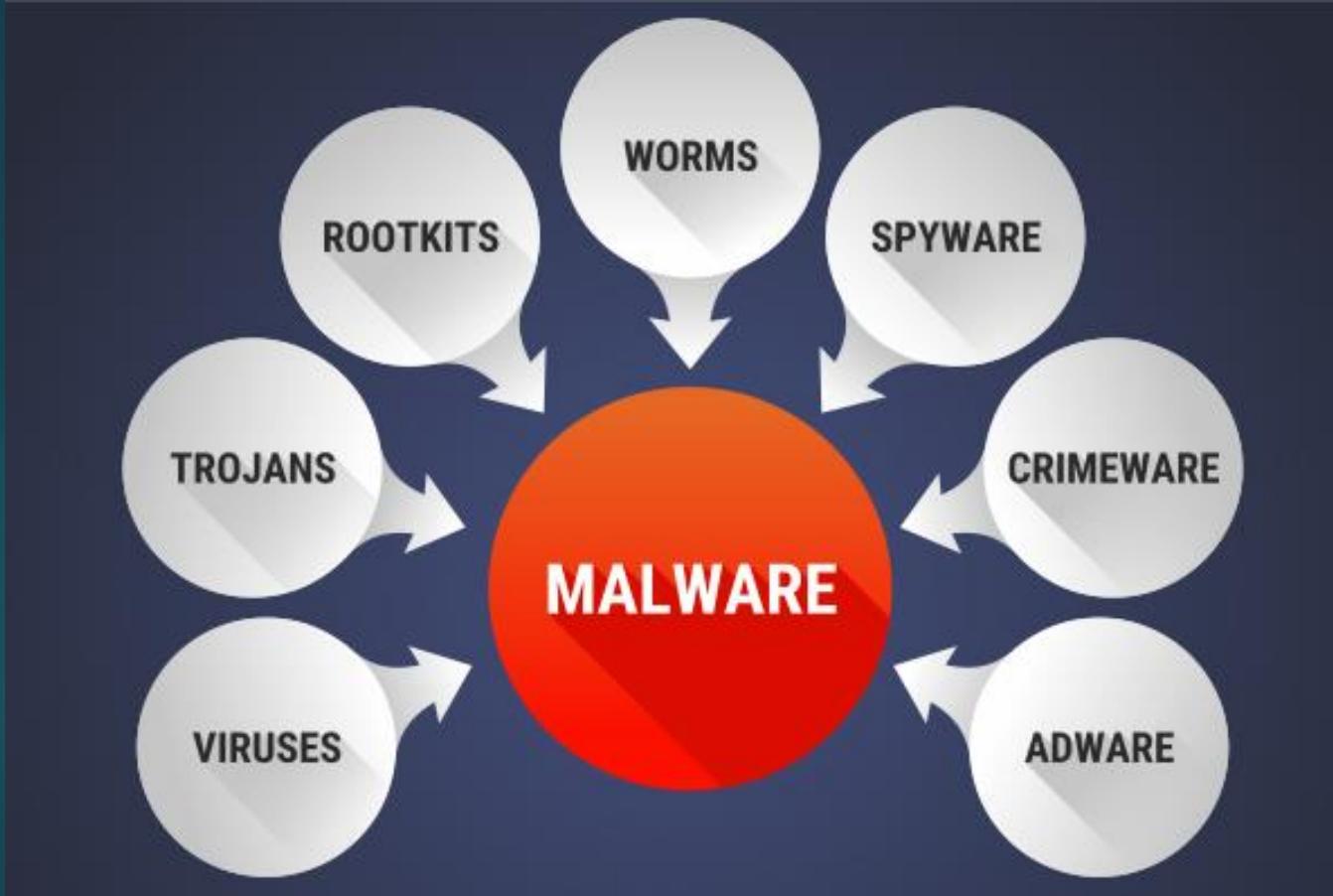
Data Loss Prevention DLP

- ▶ Can also be known as Data Leakage Prevention describes the controls put in place by an organization to ensure that certain types of data (SSNs, Account Numbers, etc) remain under organization controls in line with policies, standards, and procedures
- ▶ Detects exfiltration of certain types of key data (SSNs, Account number, etc.)
- ▶ Help ensure compliance with regulations like HIPAA, PCI-DSS and others

***Often Integrated with IRM tools

Anti-Malware

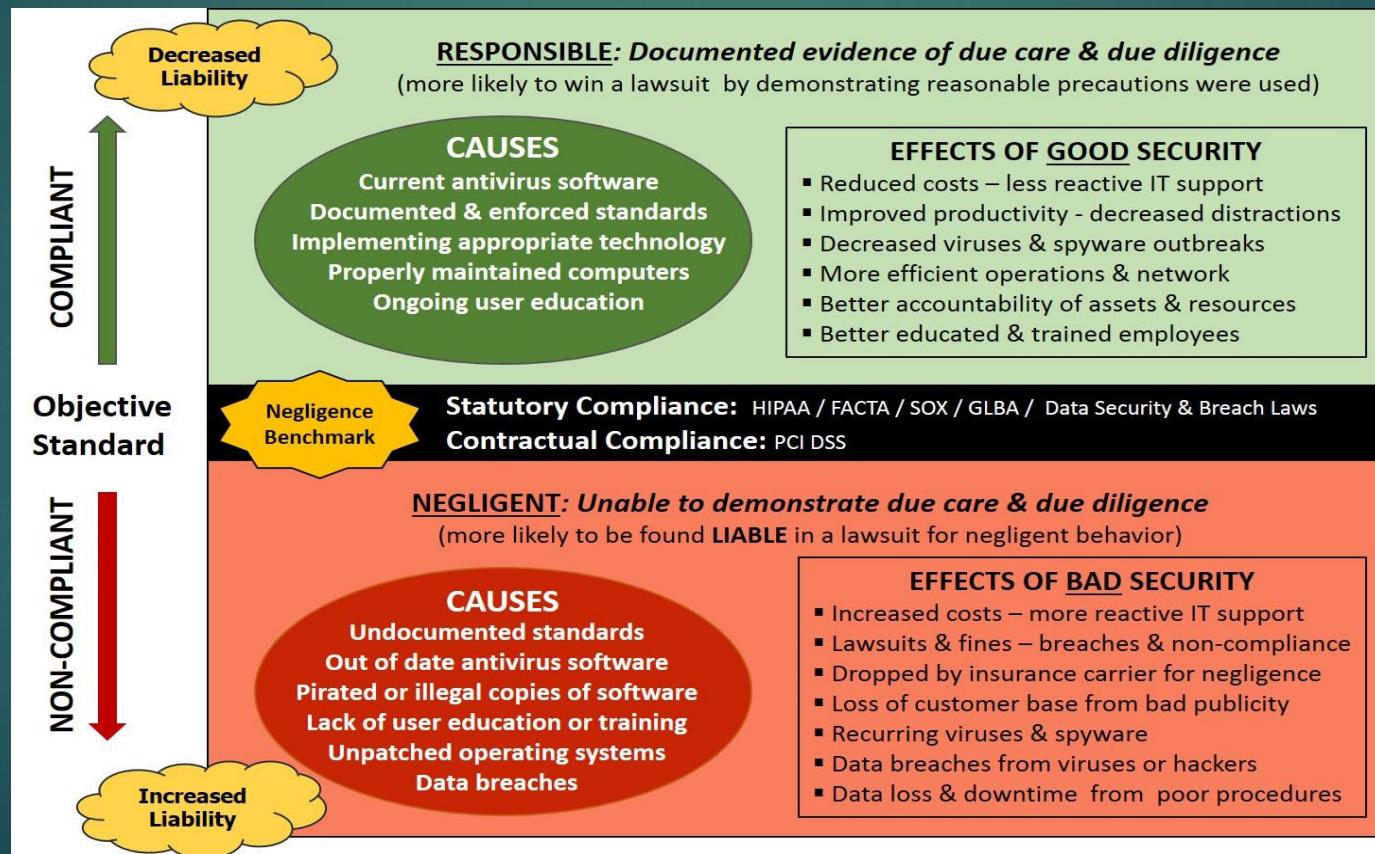
151



Additional Security Considerations in the Cloud

Compliance

Compliance refers to the act of responding favorable to an explicit or implicit request
 Could be an external or internal requirement



Due Diligence and Due Care

Corporate policies, standards, procedures and guidelines show and implement **due diligence** and **due care**.

- ▶ **Due Diligence:** An organization's attempt to understand the risk it faces. Research and risk analysis are two way an organization demonstrates due diligence. Think: **research**
- ▶ **Due Care:** An organization's attempt to minimize risks and protect its assets. Implementing and enforcing policies, procedures and standards demonstrate due care. Think: **action**

Common Threats

- ▶ “Treacherous 12”

Cloud Computing Risks by Deployment Model

- ▶ Self-Hosted: Organization is responsible for the entire infrastructure
- ▶ Overhead
- ▶ Provider-Hosted:
 - ▶ Skillset of employees/Personnel
 - ▶ Physical Security
 - ▶ Hypervisor, etc.
- ▶ Disasters
 - ▶ Natural
 - ▶ Man-made
 - ▶ Technical
- ▶ Attacks
- ▶ Liability and Non-Compliance
- ▶ Malware

Community Cloud Risks

- ▶ Multi-tenancy
 - ▶ Lack of Consistency across tenants
 - ▶ Can't enforce centralized policy
 - ▶ Access Control
 - ▶ Lack of access to centralized reporting and performance information

- ▶ Vendor lock-In: describes situation where proprietary formats, technology, etc. make it more difficult to move data out of the cloud or from one provider to another
- ▶ Vendor Lock-Out: Provider goes out of business
- ▶ Jurisdictional Risks—location of data
- ▶ Multitenancy
 - ▶ Conflicts of interest/lack of separation of duties
 - ▶ Privilege escalation
 - ▶ Information Bleed
 - ▶ Legal—search and seizure

Cloud Computing Risks by Service Model

IaaS Risks

- Personnel: Cloud environment requires that we redefine “internal” employees
- External Threats (not isolated to the cloud) malware, hacks, ransomware, MITM, etc.
- Lack of Specific Skillsets: Most network operations and security responsibility reside with the customer. Can IT staff “scale-up” their skills for the cloud?

PaaS

- In addition to risks with IaaS
- Interoperability Issues
 - Applications are designed to operate on specific platforms (NET, Java, PHP, Python, Ruby, etc.) Each platform uses specialized libraries and routines--moving application to another platform will require extensive changes3
- Persistent backdoors
- Virtualization risks—most PaaS offerings use virtual Oss---more later!
- Programs run by the customer will operate on the same devices used by other customers
- Shared Resources: side-channel attacks, resource utilization issues, information bleed

SaaS Risks

- Vendor Lock-in for data
- Virtualization risks
- Web vulnerabilities
 - Browser
 - APIs
 - Identity and Access Management

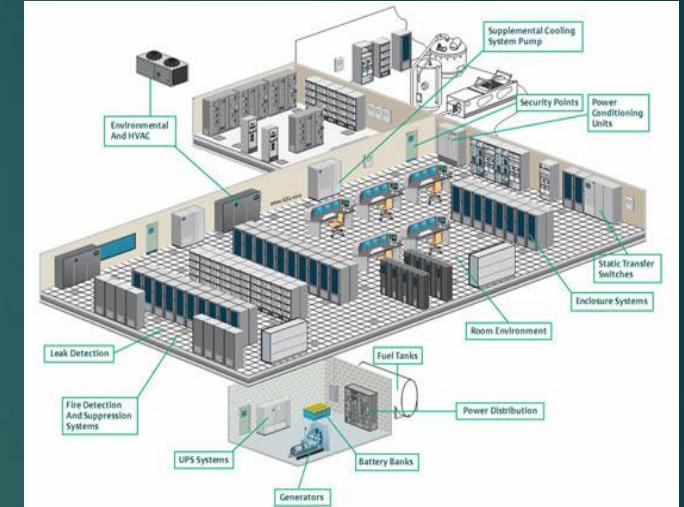
Domain 3 Cloud Platform and Infrastructure Security

Domain 3 Cloud Platform and Infrastructure Security

- ▶ Physical environment of the data center
- ▶ Network Communications
- ▶ Compute
- ▶ Storage
- ▶ Cloud Infrastructure components
- ▶ Risk Management
- ▶ Design and plan security controls
- ▶ Disaster Recovery and Business Continuity

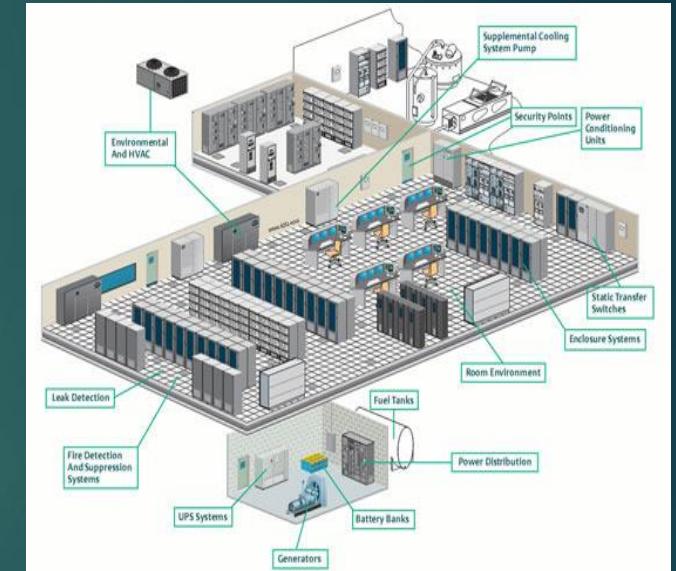
Physical Environment of the CSP

- ▶ Expensive hardware—hundreds of thousands of servers
- ▶ Massive density of power
- ▶ Downtime affects all dependent businesses
 - ▶ Redundancy on all levels is essential
- ▶ Power, Pipe (cooling) Ping (connectivity) limitations
- ▶ **Temperature:** Sensors will measure the heat being generated by equipment as well as the air-conditioning system's intake and discharge.
- ▶ **Humidity and moisture:** Sensors ensure high moisture levels won't corrode electronic elements and low levels won't cause static electricity. They also monitor for leaks in cooling equipment, pipes, etc.



Physical Environment of the Cloud Infrastructure (2)

- ▶ **Airflow:** Sensors ensure air is properly flowing through racks and to/from the air-conditioning system.
- ▶ **Voltage:** Sensors detect the presence or absence of line voltage.
- ▶ **Power:** Monitoring systems ensure proper current coming into facility and detect failures.
- ▶ **Smoke** Detection of smoke/heat/flames and communication with emergency services.
- ▶ **Video surveillance:** Real-time surveillance of data center activities



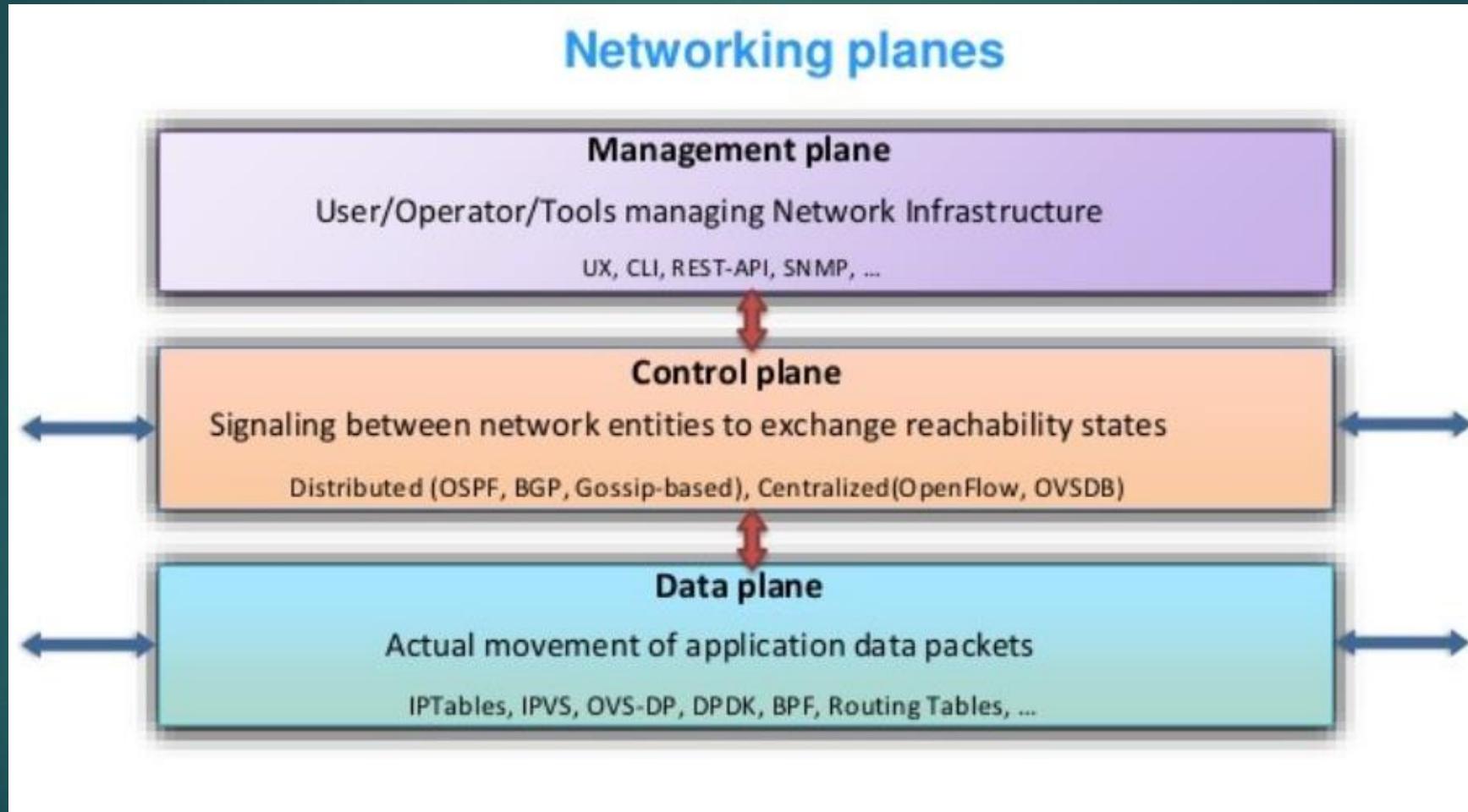
Network Functionality

- ▶ Address Allocation ensuring that cloud resources are assigned IP addresses statically or dynamically
- ▶ Access Control: Regulation of subject/object access (physical, administrative, technical)
- ▶ Sufficient Bandwidth Allocation: control the amount of traffic between systems or interfaces
- ▶ Filtering: block or allow content or access
- ▶ Routing: Directing the flow of traffic

Software Defined Networking

- ▶ In a software-defined network, a network engineer or administrator can shape traffic from a centralized control console without having to touch individual switches in the network. A centralized SDN controller directs the switches to deliver network services wherever they're needed, regardless of the specific connections between a server and devices.
- ▶ This process is a move away from traditional network architecture, in which individual network devices make traffic decisions based on their configured routing tables. SDN has played a role in networking for a decade now and has influenced many innovations in networking.

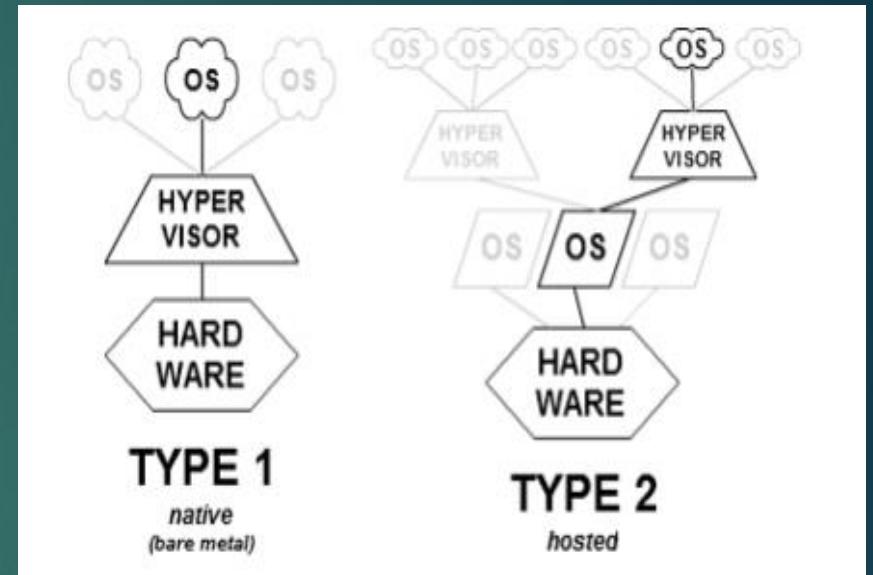
Software Defined Networking: Data Planes



Hypervisors

► TYPE I

- ▶ Known as bare metal, embedded, or native hypervisor
- ▶ Works directly with the hardware and can monitor the overlying guest OS
- ▶ Smaller and faster, primarily manages sharing and managing hardware between the guest OS
- ▶ Examples VMWare ESX, XEN
- ▶ TYPE II
- ▶ Installed “on top” of the guest operating system
- ▶ Dependent upon the host OS
- ▶ More vulnerable
- ▶ Examples VM workstation, VirtualBox, MS Virtual PC



Securing the Hypervisor

- ▶ Install all updates to the hypervisor as they are released by the vendor. Centralized patch management solutions can also be used to administer updates.
- ▶ Restrict administrative access to the management interfaces of the hypervisor.
- ▶ Protect all management communication channels using a dedicated management network
- ▶ Synchronize the virtualized infrastructure to a trusted authoritative time server.
- ▶ Disconnect unused physical hardware from the host system (external drives, NICs.)

Securing the Hypervisor (2)

- ▶ Disable all hypervisor services such as clipboard- or file-sharing between the guest OS and the host OS unless they are needed
- ▶ Consider using introspection capabilities to monitor the security of each guest OS and their interactions
- ▶ Carefully monitor the hypervisor itself for signs of compromise. This includes using self-integrity monitoring capabilities that hypervisors may provide, as well as monitoring and analyzing hypervisor logs on an ongoing basis.

Securing the Guest OS

- ▶ Follow the recommended practices for managing the physical OS, e.g., time synchronization, log management, authentication, remote access, etc.
- ▶ Install all updates to the guest OS promptly. All modern OSs have features that will automatically check for updates and install them.
- ▶ Back up the virtual drives used by the guest OS on a regular basis, using the same policy for backups as is used for non-virtualized computers in the organization.

Securing the Guest OS (2)

- ▶ In each guest OS, disconnect unused virtual hardware. This is particularly important for virtual drives (usually virtual CDs and floppy drives), but is also important for virtual network adapters other than the primary network interface and serial and/or parallel ports.
- ▶ Use separate authentication solutions for each guest OS unless there is a particular reason for two guest OSs to share credentials.
- ▶ Ensure that virtual devices for the guest OS are associated only with the appropriate physical devices on the host system, such as the mappings between virtual and physical NICs.

Virtualization Concerns

- ▶ Inter-VM attacks
 - ▶ traffic between the VMs traverses a virtual network and are invisible to the physical security elements and is sometimes referred to as the “Blind Spot”
 - ▶ Monitoring of the virtual network is as essential as that of the physical
- ▶ Performance:
 - ▶ Many security tools affect performance, perhaps more so on VMs
 - ▶ Understanding the virtual environment and the use of proper sizing, planning and balancing the needs of the environment
- ▶ VM Sprawl:
 - ▶ The increasing number of VMs in use leaves the potential for oversights and misconfigurations
 - ▶ Automation and proper governance and long term framework to

Virtualization Concerns Continued

- ▶ Instant-On Gaps
 - ▶ Vulnerabilities exist from when a VM is powered on and when its security rules can be updated
 - ▶ Best practices include network based security and “virtual patching” that inspects traffic for known attacks before it can get to a newly provisioned or newly started VM. It is also possible to enforce NAC (Network Access Control)-like capabilities to isolate stale VMs until their rules and pattern files are updated and a scan has been run.
- ▶ VM Theft or Modification
 - ▶ VM Encryption is necessary as VMs are susceptible to modification or theft, but it can affect performance

Virtualization Concerns Continued

- ▶ Data Commingling:
 - ▶ Data of different classifications could potentially be stored on the same physical device
 - ▶ combination of VLANs, firewalls, and IDS/IPS to ensure VM isolation as a mechanism for supporting mixed mode deployments. We also recommend using data categorization and policy based management to prevent this. In Cloud Computing environments, the lowest common denominator of security could potentially be shared by all tenants in the multi-tenant virtual environment.

Recommendations for Virtualization

- ▶ Evaluate, negotiate and refine the licensing agreements with major vendors for virtualized environments---SLAs
- ▶ Secure each virtualized OS by using software in each guest or using an inline virtual machine combined with hypervisor-based APIs such as VMware vShield.
- ▶ Virtualized operating systems should be augmented by built-in security measures, leveraging third party security technology to provide layered security controls and reduce dependency on the platform provider alone.

Recommendations for Virtualization (2)

- ▶ Secure by default configuration must be assured by following or exceeding available industry baselines.
- ▶ Encrypt virtual machine images when not in use.
- ▶ Explore segregating VMs and creating security zones by type of usage (e.g., desktop vs. server), production stage (e.g., development, production, and testing) and sensitivity of data on separate physical hardware components such as servers, storage, etc.
- ▶ Make sure that the security vulnerability assessment tools or services cover the virtualization technologies used.

Risk Assessment and Analysis in the Cloud

- ▶ Policy and Organizational Risks
- ▶ General Risks
- ▶ Virtualization Risks
- ▶ Cloud-Specific Risks
- ▶ Non-Cloud-Specific Risks
- ▶ Legal Risks

Policy and Organizational Risk

- ▶ Provider lock-in/lock-out
- ▶ Loss of governance
- ▶ Compliance issues
- ▶ Provider Exit

General Risks

- ▶ Requirements issues
- ▶ Consolidation of Infrastructure
- ▶ Changing environment
- ▶ Scalability requires skill at CSP
- ▶ Technical controls shift to CSP

Cloud-Specific Risks

- ▶ Breach of management plane (compromise of management interfaces)
- ▶ Resource exhaustion
 - ▶ DDoS
 - ▶ Traffic analysis
 - ▶ Manipulation/interception of data
- ▶ Isolation control failures
- ▶ Insecure or incomplete data deletion
- ▶ Control conflicts between stakeholders
- ▶ Software risks

Non-Cloud-Specific Risks

- ▶ Traditional IT risks are still applicable to the cloud. Enterprise Risk Management requires that a comprehensive risk approach is implemented with the continued focus of alignment with business objectives
- ▶ Resource exhaustion
 - ▶ DDoS
- ▶ Data Protection
 - ▶ PII, PHI, PFI have special requirements. SLAs must include contractual obligations to maintain necessary compliance
- ▶ Jurisdiction
- ▶ Law enforcement
 - ▶ Who is responsible
 - ▶ Seizure and Examination of equipment
- ▶ Licensing
 - ▶ Will licensing agreements suffice if software is moved elsewhere.
 - ▶ Based on CPU vs. Users, etc

Further Attack Vectors

- ▶ New technology for federated identities, provisioning, virtualization, automation, etc.
- ▶ External service providers
- ▶ Guest breakout
- ▶ Identity compromise at provider
- ▶ API compromise
- ▶ Attacks on provider infrastructure
- ▶ Attacks on underlying cloud carrier infrastructure

Countermeasures Across the Cloud

- ▶ Layered defense should always be implemented
- ▶ Redundancy configured for continuous uptime
 - ▶ Resiliency
 - ▶ Component updates without disruption
- ▶ Automation of Controls
 - ▶ Consistency
 - ▶ Minimize human element
 - ▶ Integrate security into VM builds (baseline security, configuration management, encryption of files, etc.)
- ▶ Access Controls
 - ▶ Cache CSR on customer-premises availability (on-prem)

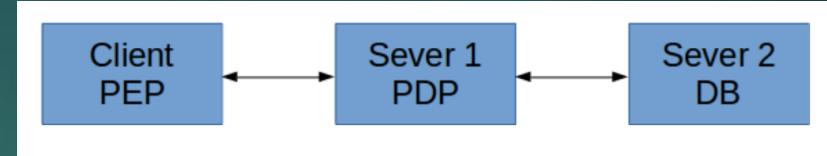
Virtualization Systems Controls

- ▶ Isolation/Separation of Zones
 - ▶ DMZ, VLANs, Physical Segmentation
- ▶ Encryption
- ▶ Secure Images with DLPs, firewalls, auto-generated logs
- ▶ Secure data transit protocols
- ▶ Protected management plane
- ▶ Detective controls
 - ▶ IDS/IPS
 - ▶ Honeypots
 - ▶ Enticement vs. entrapment

IAAA in The Cloud Infrastructure

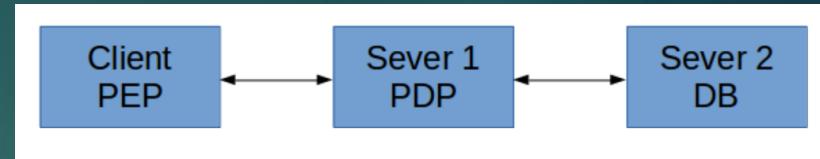
- ▶ Identity
 - ▶ Identity providers in the cloud are using OpenID and Oauth.
 - ▶ Internal corporate environments may use Active Directory
- ▶ Authentication
 - ▶ Function of the Identity Provider
 - ▶ Multi-Factor is best
- ▶ Authorization
 - ▶ Based on identity, roles, attributes, context
 - ▶ Enforced at policy enforcement point
- ▶ Auditing

PEPs, DBs and PDP



- ▶ Policy Enforcement Point (PEP): Invoked by client programs for security policy enforcement. These gatekeepers are embedded directly into their host thus require platform specific bindings. The less impact to their host, the better.
- ▶ Database (DB): Invoked by PDPs to store security credentials, attributes and activity logs. An important concern is speed; to be used correctly, it's used often. Another important concern is reliability; the integrity of its data is mission critical. Example: Active Directory or other LDAP database

PEPs, DBs and PDP (2)



- ▶ Policy Decision Point (PDP): Invoked by PEPs and dependent on a DB. CA Siteminder, Tivoli Access Manager, Oracle Access Manager, Shibboleth, CAS and many others. Responsible for computing:
 - ▶ authentication – with passwords or keys
 - ▶ authorization – with attributes or permissions
 - ▶ audit trail – identify subjects, decisions, time/date/locations, and resources

Business Continuity and Disaster Recovery

Business Continuity and Disaster Recovery

- ▶ BCP allows an enterprise to plan what is necessary to ensure that its key products and services will continue to be available in the event of a disaster, and that disruption to the business is minimized as much as possible
- ▶ DRP addresses what an enterprise needs to be done in the immediacy of the disaster and how to restore business processes in order to recover from the event

BCDR Scenarios

- ▶ On-premises, cloud as BCDR
 - ▶ Infrastructure is on premises, whereas the CSP provides alternate capabilities. This has traditionally been most common
 - ▶ Concerns: Different environment in the cloud. For instance, may need to convert workload on physical systems to virtual machines
- ▶ Cloud service consumer, primary provider BCDR
 - ▶ Infrastructure is already located at a CSP
 - ▶ The risk being considered is a failure of part of CSP's infrastructure
 - ▶ Failover would occur to another part of the CSP infrastructure
 - ▶ Concern: What is functionality of the redundant CSP location—load balancing? Bandwidth? Ability to meet SLA?

BCDR Scenarios (2)

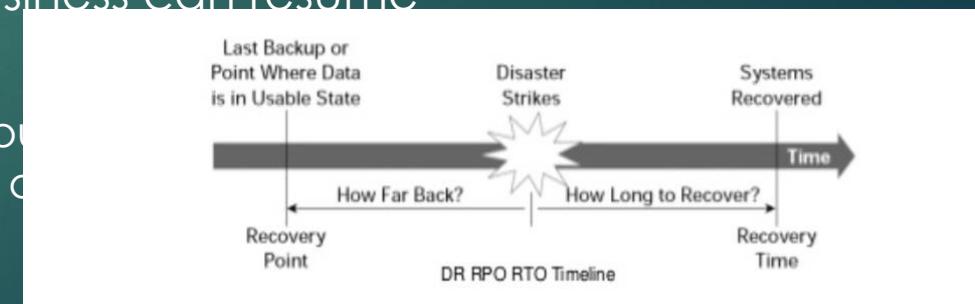
- ▶ Cloud service consumer, alternative provider
 - ▶ Infrastructure is already located at a CSP
 - ▶ The risk being considered is a failure of part of CSP's infrastructure
 - ▶ Failover is to a secondary provider
 - ▶ Concern: Same as scenario 2 above plus need for processes to switch providers. MOUs should be considered to clearly identify expectations

The Business Impact Analysis (BIA)

- Identifies and prioritizes business processes based on criticality
- Establishes metrics to be integrated into the infrastructure and the SLAs
 - Service Level Objectives
 - RPO (Recovery Point Objective):
 - MTD (Maximum Tolerable Downtime) aka RTO (Recovery Time Objective)
 - RSL Recovery Service Level is a percentage of how much computing power is necessary based on the percentage of the production system needed during a disaster

The Business Impact Analysis (BIA) (2)

- RPO & RTO
 - ▶ Recovery Point Objective (RPO): Amount of acceptable data loss measured in terms of how much data can be lost before the business is too adversely affected.
 - ▶ RPO indicates the point in time a business is able to recover data after a systems failure, relative to the time of the failure itself
 - ▶ Recovery Time Objective (RTO): Amount of systems downtime defining the total time of the disaster until the business can resume operations
 - ▶ Quantifies how much data loss is acceptable without affecting the business due to business transactions or processes



Business Continuity Planning

- ▶ Disaster recovery and continuity planning deal with uncertainty and chance
 - ▶ Must identify all possible threats and estimate possible damage
 - ▶ Develop viable alternatives
- ▶ Threat Types:
 - ▶ Man-made
 - ▶ Strikes, riots, fires, terrorism, hackers, vandals
 - ▶ Natural
 - ▶ Tornado, flood, earthquake
 - ▶ Technical
 - ▶ Power outage, device failure, loss of a T1 line, dated technology

Strategy Risks

- ▶ Complexity is added with redundancy/failover
 - ▶ Qualified Staff
 - ▶ Budget
 - ▶ Compatibility
- ▶ Need for protection at all layers
 - ▶ Data/Hard drives/Clusters/Images/Zones/Networks, etc.
- ▶ DR site may be geographically remote
 - ▶ Latency
 - ▶ Bandwidth
 - ▶ Regulatory compliance may vary across jurisdictions

Phases of Business Continuity Planning

- ▶ Define: Determine Scope , Gather Requirements
- ▶ Analyze: Conduct Business Impact Analysis
- ▶ Assess Risk: Determine Probability and Impact of risks in relation to BIA
- ▶ Design: Write the Plan
- ▶ Test, Implement, Maintain

Creating the BCP

- ▶ Scope—Should be embedded in an information security strategy and includes roles, risk assessment, classification, policy, awareness, and training
- ▶ Gathering requirements and context
 - ▶ Identification of critical business processes and dependencies
 - ▶ Risks and threats, including failures at CSP
 - ▶ Requirements may come from organization, industry standards, or legal/regulatory compliance obligations

Creating the BCP

- ▶ Scope—Should be embedded in an information security strategy and includes roles, risk assessment, classification, policy, awareness, and training
- ▶ Gathering requirements and context
 - ▶ Identification of critical business processes and dependencies
 - ▶ Risks and threats, including failures at CSP
 - ▶ Requirements may come from organization, industry standards, or legal/regulatory compliance obligations

Creating the BCP (2)

- ▶ Plan Analysis
 - ▶ Translation of BCDR requirements into inputs to the design phase
 - ▶ Requirements and threat modeling should be used to ensure completeness
- ▶ Risk Assessment
 - ▶ See earlier evaluations of CSP risks
- ▶ Plan Design
 - ▶ Should address technical alternatives, procedures, workflow, staff, other business necessities
 - ▶ Invocation responsibilities
 - ▶ Automation
 - ▶ Testing of BCP

Testing the Plan

- ▶ Evaluating the plan for accuracy and completeness
 - ▶ Expectations for business units to demonstrate ability to achieve objectives within metrics specified in BIA (RTO, RPO, RSL)
 - ▶ Degree of testing to be accomplished
 - ▶ Roles and responsibilities
 - ▶ Testing of internal and external dependencies
 - ▶ Justification for testing strategy
 - ▶ Objectives should be measurable, with clear expectations defined
 - ▶ Testing strategy should be reviewed and approved by senior management

Types of BCDR Tests

- ▶ Checklist Test
 - ▶ Copies of plan distributed to different departments
 - ▶ Functional managers review
- ▶ Structured Walk-Through (Table Top) Test
 - ▶ Representatives from each department go over the plan
- ▶ Simulation Test
 - ▶ Going through a disaster scenario
 - ▶ Continues up to the actual relocation to an offsite facility

Types of BCDR Tests

- ▶ Parallel Test
 - ▶ Systems moved to alternate site, and processing takes place there
- ▶ Full-Interruption Test
 - ▶ Original site shut down
 - ▶ All of processing moved to offsite facility

Post-Incident Review

- ▶ Results should be published
- ▶ Action Items should be identified to address issues
- ▶ Action items should be tracked until resolved
- ▶ Plan should be updated
- ▶ Plan should be reviewed at least once per year, or as risk dictates

Physical and Environmental Controls

- ▶ Regulations like PCI DSS, HIPAA, and other regulations may apply
 - ▶ Policies to maintain a safe and secure facility/office/room/secure area
 - ▶ Physical access restrictions
 - ▶ Perimeter security, physical authentication/auditing techniques

Physical and Environmental Controls (2)

- ▶ Redundancy
 - ▶ UPS/Generators
 - ▶ Systems
 - ▶ Hard Drives
 - ▶ Network Devices
 - ▶ Cable
 - ▶ Software
 - ▶ Backup Staff (Continuous cross-training and assessment of skills)

Backup and Recovery Considerations

- ▶ CSPs should provide assurance in securing customer data backed up to the cloud for the purpose of fault tolerance and disaster recovery.
- ▶ Solutions might include
 - ▶ SSL/TLS secure transfers
 - ▶ Encrypted storage
 - ▶ Password protections
 - ▶ Geo-redundant storage
 - ▶ Continuous backup
 - ▶ Express restore
 - ▶ Deduplication (finding and removing duplication within data without compromising its fidelity or integrity allowing a more intelligent form of data compression)

Physical Location of Cloud Infrastructure

- ▶ Physical location of CSP should be evaluated for location in relation to
 - ▶ Regions with a high rate of natural disasters (flood, landslides, seismic activity, etc.)
 - ▶ Regions of high crime, social/political unrest
 - ▶ Frequency of inaccessibility

Data Center Operations

- Cloud providers running data center operations should demonstrate to customers their compliance to current regulations and standards.
- CSPs can/should share results of independent audits
 - Cloud Trust Protocol is intended to establish digital trust between a cloud computing customer and provider and create transparency about the provider's configurations, vulnerabilities, access, authorization, policy, accountability, anchoring and operating status conditions.
 - Cloud Audit: Provides automated audit, assertion, assessment, and assurance
 - CSA STAR is the industry's most powerful program for security assurance in the cloud. STAR encompasses key principles of transparency, rigorous auditing, and harmonization of standards. STAR certification provides multiple benefits, including indications of best practices and validation of security posture of cloud offerings.

Domain 3 Cloud Platform and Infrastructure Security

- Physical environment of the data center
- Network Communications
- Compute
- Storage
- Cloud Infrastructure components
- Risk Management
- Design and plan security controls
- Disaster Recovery and Business Continuity

Domain 4: Cloud Application Security

Domain 4 Cloud Application Security

- Determining Data Sensitivity
- Cloud Application Architecture
- Security Responsibilities Across Models
- The Software Development Lifecycle
- OWASP Top Ten Vulnerabilities
- IAM and Federated identity management
- Application Security Testing

Determining Data Sensitivity

- Six key questions in relation to determining data sensitivity. What would the impact be if:
 - Information was widely distributed
 - An employee of cloud provider accessed the application
 - The process was manipulated by an outsider
 - The process failed to provide the expected result
 - The information was unexpectedly changed
 - The application or information was unavailable for a period of time

Cloud Application Architecture

- Application Programming Interfaces
- Multitenancy
- Cryptography
- Sandboxing
- Application Virtualization

APIs

- Programming code that governs how a web service can request information or services. APIs define 3 primary elements:
- Access: who is allowed to ask for data or services.
- Request: what data or services can be asked for (e.g., if I give you an address can you tell me how to get there?). Requests have two main parts:
 - Methods: the type of questions you can ask, assuming you have access (it also defines the type of responses available).
 - Parameters: additional details you can include in the question or response.
- Response: the data or service for your request.

APIs Continued

- The map we left her and the fact that the coffee shop was open gave her access to the API.
- When she got to the coffee shop, she had access to the menu with all the different options. She knew what you can ask for (methods) and the options and details (parameters). This told her how to place her request for food. Once Rachel placed her request, the barista played the role of the API and sent a message to the kitchen.
- Rachel then just had to wait for the response in the form of food and beverage, which the barista, acting as the API, delivered to her with a smile (nice folks at The Grin)



Types of APIs

- SOAP Simple Object Access Protocol is a protocol specification providing for the exchange of structured information or data in web services
 - Similar to an envelope and is based on the WS Standards (widely implemented and provide standards for security, addressing, messaging, etc.)
 - Uses Web Services Description Language (WSDL) to describe services and how to access them
 - Overhead comes with the envelope
- RESTful APIs: Representational State Transfer is a software architecture style consisting of guidelines and best practices for creating scalable web services.

APIs: SOAP

- Standards-based
- Reliant on XML
- Highly intolerant of errors
- Slower
- Built-in error handling
- Some examples of where SOAP works or fits in better are
 - Asynchronous processing
 - Format contracts
 - Stateful operations

APIs

RESTful APIs

REST is a framework, not a protocol, therefore its not bound to

- It's lightweight—best choice for mobile applications
- It uses simple URLs.
- It is not reliant on XML.
- It's scalable.
- It outputs in many formats (CSV, JSON, and so on).
- It's efficient, which means it uses smaller messages than XML.
- Some examples of situations where REST works well are
 - When bandwidth is limited
 - When stateless operations are used
 - When caching is needed

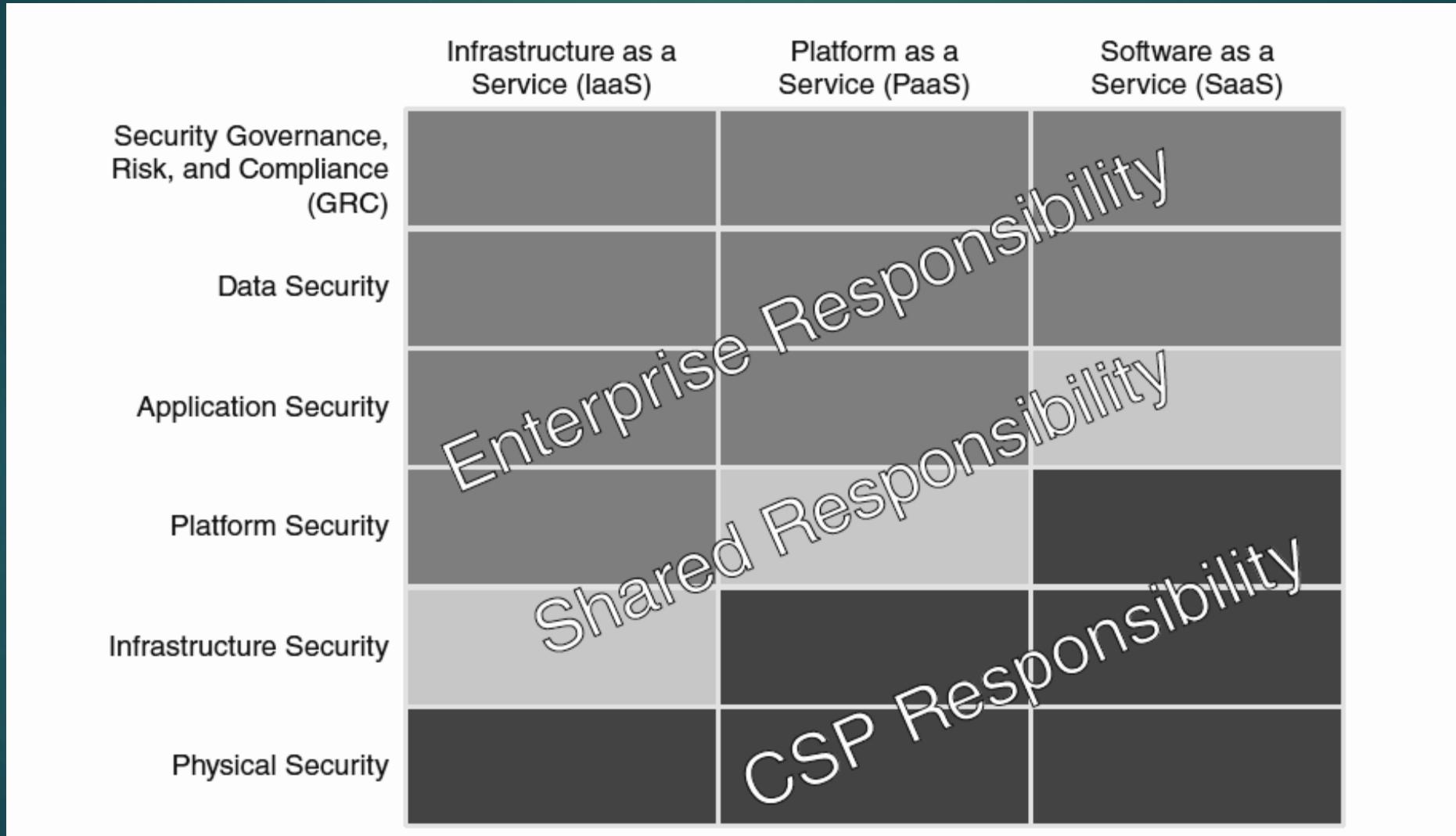
Common Pitfalls of Cloud Security Application Deployment

- On-Premise does not always transfer to the cloud
 - Current configurations and applications may be difficult, as they may not have been designed for the cloud environment
- Cloud development and testing can be difficult in hardened, secure environments
- Learning curve for new environment can be steep
- Lack of standardization across web apps
- Multitenancy
- 3rd party administrators

Multitenancy

- Mode of operation of software where multiple independent instances share the same environment
- Physical environment is generally shared
 - Segmentation: Separating tenant resources/data/applications, etc.
 - Isolation: Logical isolation is often provided through virtualization
 - Governance: Propose a data governance framework to ensure the privacy, availability, integrity and overall security of data in different cloud models
 - Service Levels: Document minimum expected performance
 - Chargeback and metering refers to the ability of an IT organization to track and measure the IT expenses per business unit and charge them back accordingly.

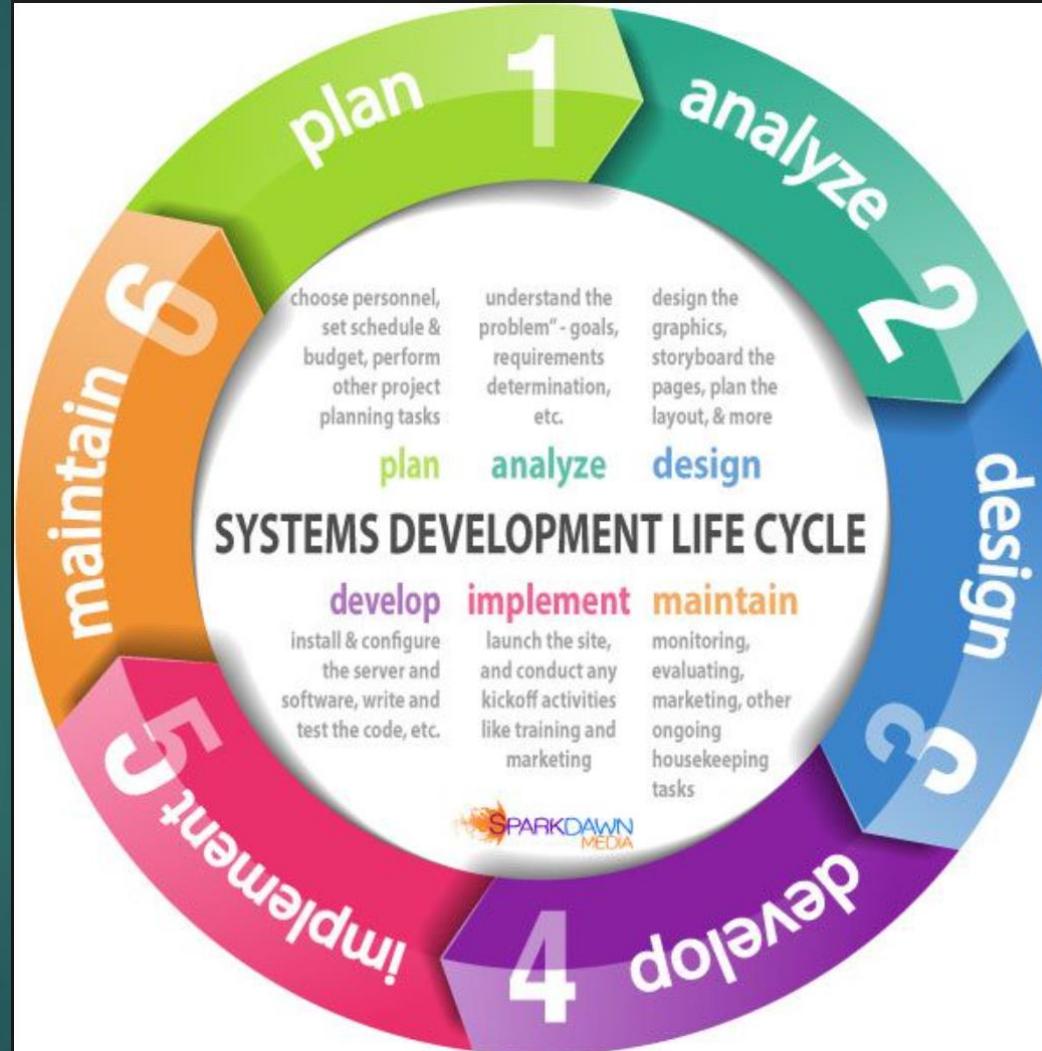
Security Responsibilities Across Models



THE SDLC (Software Development Life-Cycle) for the Cloud

- Planning and Requirements analysis: All business requirements should be defined and risks should be identified
- Analyzing/Defining: Clearly defines the requirements, such as language and platform through a requirement specification document
- Designing: Specifies hardware and system requirements and helps determining overall architecture
- Developing: Work is divided into modules and the actual coding starts
- Testing: Code is tested against requirements: Unit testing, integration testing, system testing and user acceptance testing, certification and authorization
- Implement/Operate: Install systems in production environment
- Maintenance: Continuous monitoring and updates as needed

Systems Development Lifecycle



Vulnerability Databases and Resources

- OWASP (Open Web Application Security Project) Top Ten
- CVE (Common Vulnerabilities and Exposures)
- CWE (Common Weakness Enumeration)
- NVD (National Vulnerability Database)
- US CERT (Computer Emergency Response Team) Vulnerability Database

OWASP (Open Web Application Security Project) Top Ten

- OWASP is an international non-profit organization
- OWASP (Open Web Application Security Project) Top Ten
- Offers a broad consensus on the most common security flaws/exploits
- Designed to raise awareness and stress the need for security in web-based applications

**A1:2017-
Injection**

Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

**A2:2017-Broken
Authentication**

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

**A3:2017-
Sensitive Data
Exposure**

Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

**A4:2017-XML
External
Entities (XXE)**

Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

**A5:2017-Broken
Access Control**

Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

**A6:2017-Security
Misconfiguration**

Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.

**A7:2017-
Cross-Site
Scripting (XSS)**

XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

**A8:2017-
Insecure
Deserialization**

Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

**A9:2017-Using
Components
with Known
Vulnerabilities**

Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

**A10:2017-
Insufficient
Logging &
Monitoring**

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

OWASP 1. Code Injection

- Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization

OWASP 2. Broken Authentication & Session Management

- Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities

OWASP 3. Sensitive Data Exposure

- Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser
- Primary reasons for sensitive data exposure:
 - Insufficient data-in-transit protection
 - Insufficient data-at-rest protection and
 - Electronic social engineering

OWASP 4. XML External Entities

- Attackers can exploit vulnerable XML processors if they can upload XML or include hostile content in an XML document, exploiting vulnerable code, dependencies or integrations
- Numerous public XXE issues have been discovered, including attacking embedded devices. XXE occurs in a lot of unexpected places, including deeply nested dependencies. The easiest way is to upload a malicious XML file, if accepted.

OWASP 5. Broken Access Control

- Exploitation of access control is a core skill of attackers. SAST (Static Application Security Testing) and DAST (Dynamic Application Security Testing) tools can detect the absence of access control but cannot verify if it is functional when it is present. Access control is detectable using manual means, or possibly through automation for the absence of access controls in certain frameworks

OWASP 6. Security Misconfigurations

- Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date

OWASP 7. XSS (Cross-Site Scripting)

- XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites

OWASP 8. Insecure Deserialization

- Serialization is the process of turning some object into a data format that can be restored later. People often serialize objects in order to save them to storage, or to send as part of communications. Deserialization is the reverse of that process -- taking data structured from some format, and rebuilding it into an object. Today, the most popular data format for serializing data is JSON. Before that, it was XML.
- However, many programming languages offer a native capability for serializing objects. These native formats usually offer more features than JSON or XML, including customizability of the serialization process. Unfortunately, the features of these native deserialization mechanisms can be repurposed for malicious effect when operating on untrusted data. Attacks against deserializers have been found to allow denial-of-service, access control, and remote code execution attacks.

OWASP 9. Known Vulnerable Component

Usage

- Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts
- deprecated, insecure and banned APIs

OWASP 10 Insufficient Logging and Monitoring

- Exploitation of insufficient logging and monitoring is the bedrock of nearly every major incident. Attackers rely on the lack of monitoring and timely response to achieve their goals without being detected.



Organizational Normative Framework

- Specified in ISO 27034
- Defines components of application security best practices
 - Business Context
 - Regulatory Context
 - Technical Context
 - Specifications
 - Roles
 - Processes
 - ASC Library (application security control)

Application Normative Framework

- ▶ Used in conjunction with the ONF and is created for specific applications
- ▶ Think of best practices for applications within the context of the organization

Identity and Access Management

IAAA of Access Control

The components of Access Control that we are about to discuss are:

- Identification:

- Make a claim (userid etc)

- Authentication:

- Provide support (proof) for your claim

- Authorization:

- What rights and permissions you have

- Auditing:

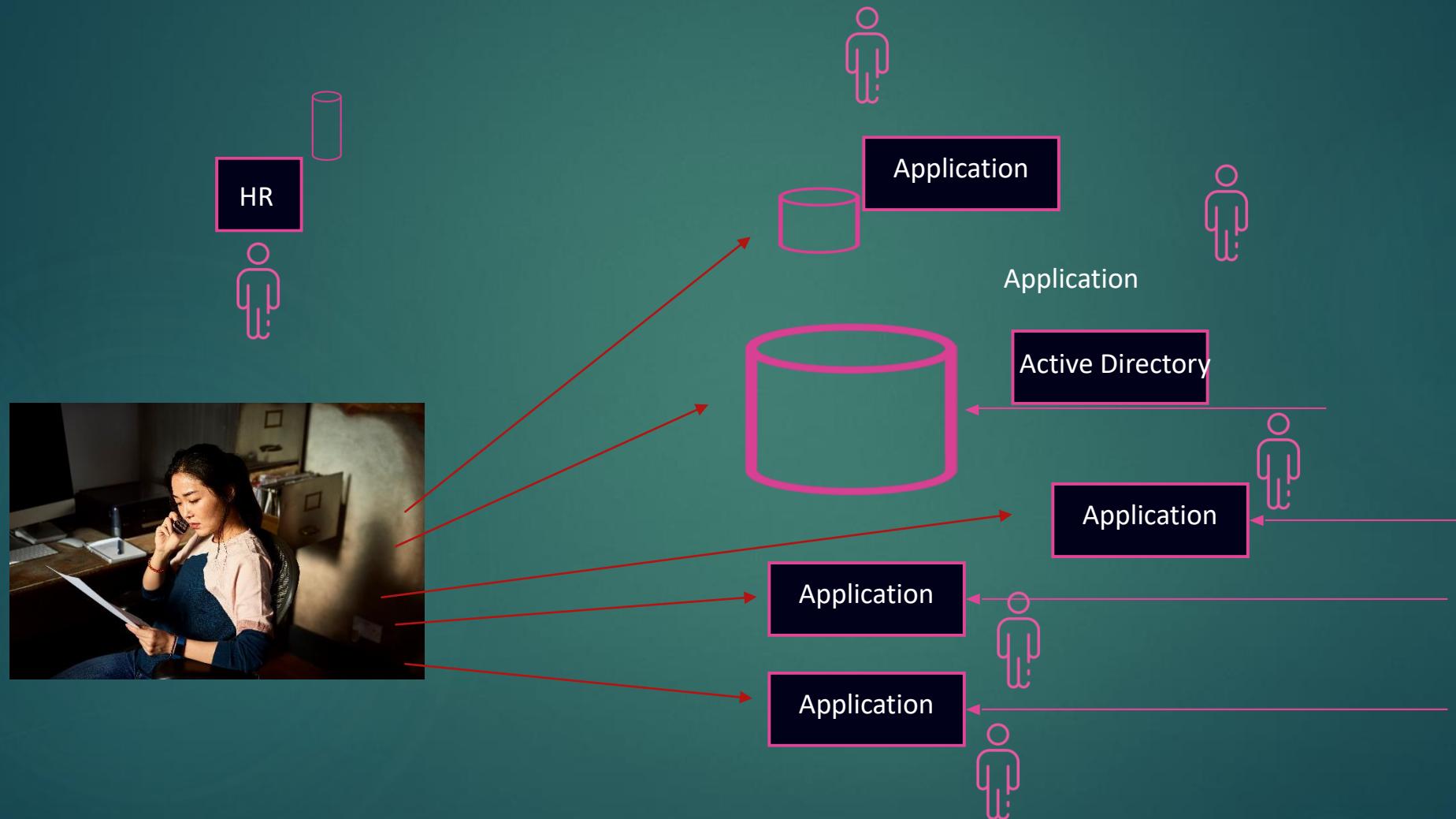
- Accountability—matching actions to subjects

Identity Proofing

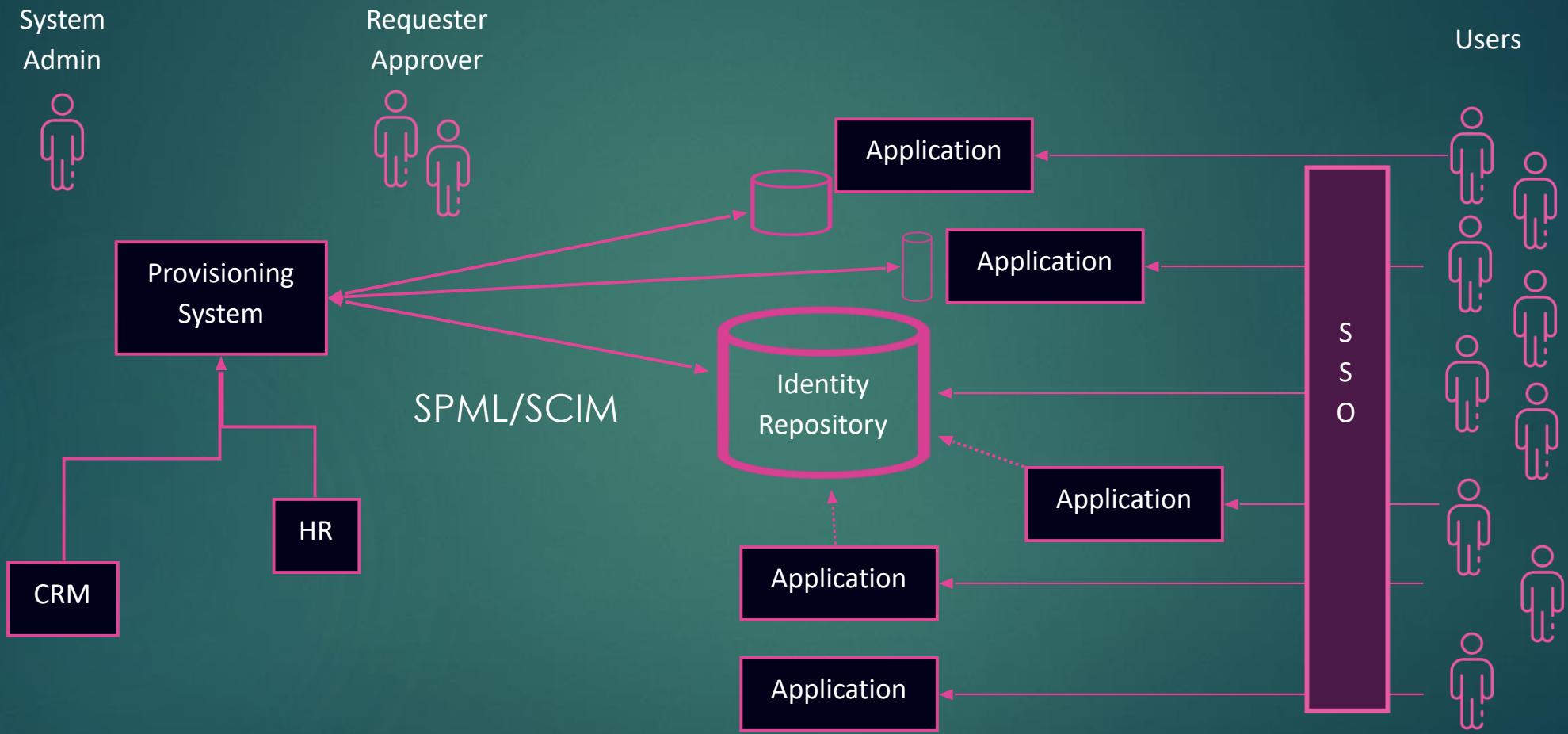
- Precedes the creation of a user account
- Not the same as authentication
- Requires the prospective employee to prove their identity to the employer.
- Long before an employee is given a user account to identify with on the network, they have proven their identity to their employer



Identity/Account Provisioning



Identity/Account Provisioning



SPML and SCIM

SPML concepts

Service Provisioning Markup Language (SPML) is an XML-based framework developed by OASIS for exchanging user, resource and service provisioning information between cooperating organizations. The Service Provisioning Markup Language is the open standard for the integration and interoperation of service provisioning requests. The goal of SPML is to allow organizations to securely and quickly set up user interfaces for Web services and applications, by letting enterprise platforms such as Web portals, application servers, and service centers generate provisioning requests within and across organizations. This can lead to automation of user or system access and entitlement rights to electronic services across diverse IT infrastructures, so that customers are not locked into proprietary solutions.

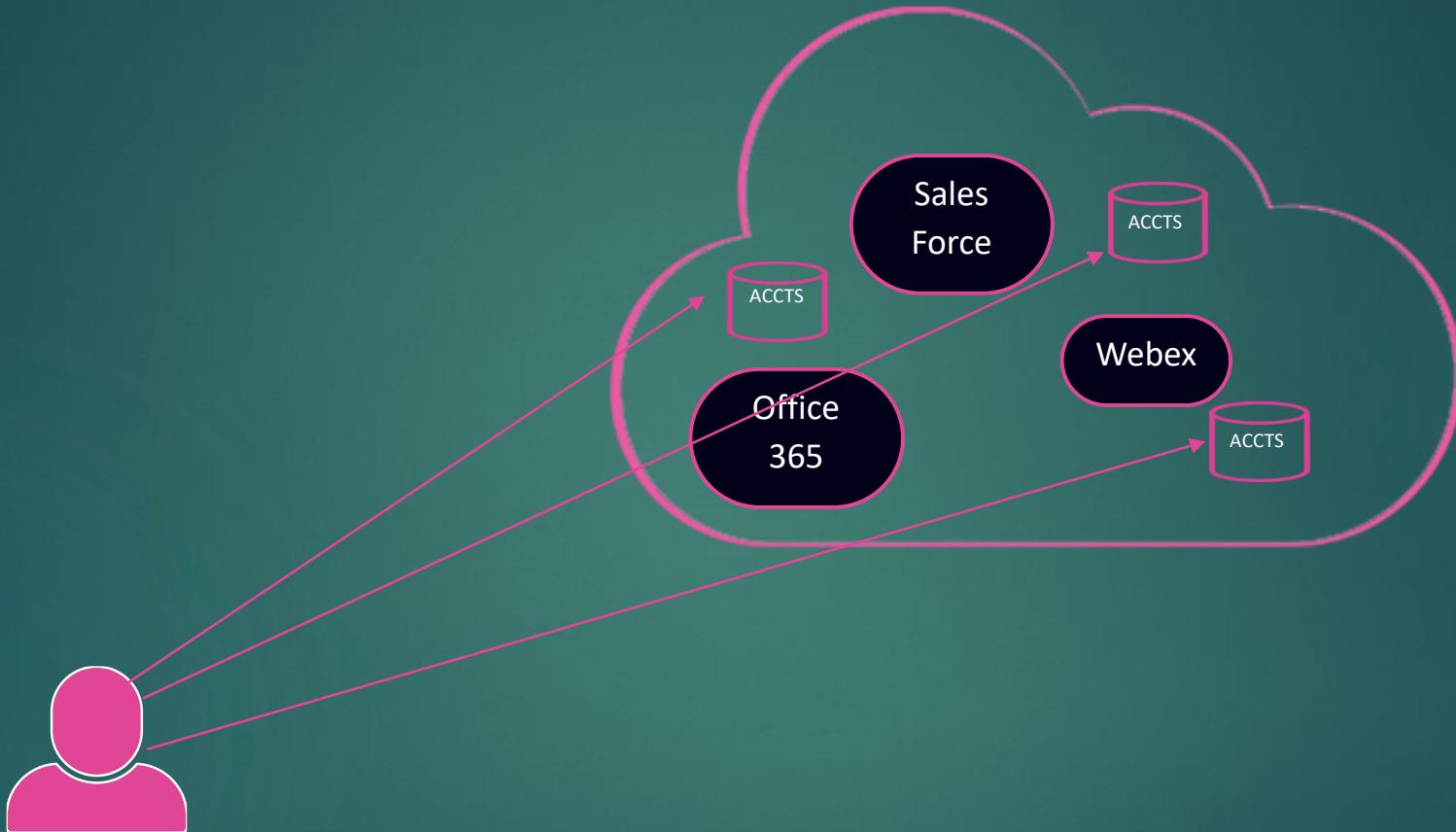
SCIM concepts

The System for Cross-domain Identity Management (SCIM) specification is designed to make managing user identities in cloud based applications and services, easier. Identity provisioning is a key aspect of any Identity Management Solution. In simple terms, it is to create, maintain and delete user accounts and related identities in one or more systems or applications in response to business processes which are initiated either by humans directly or by automated tasks.

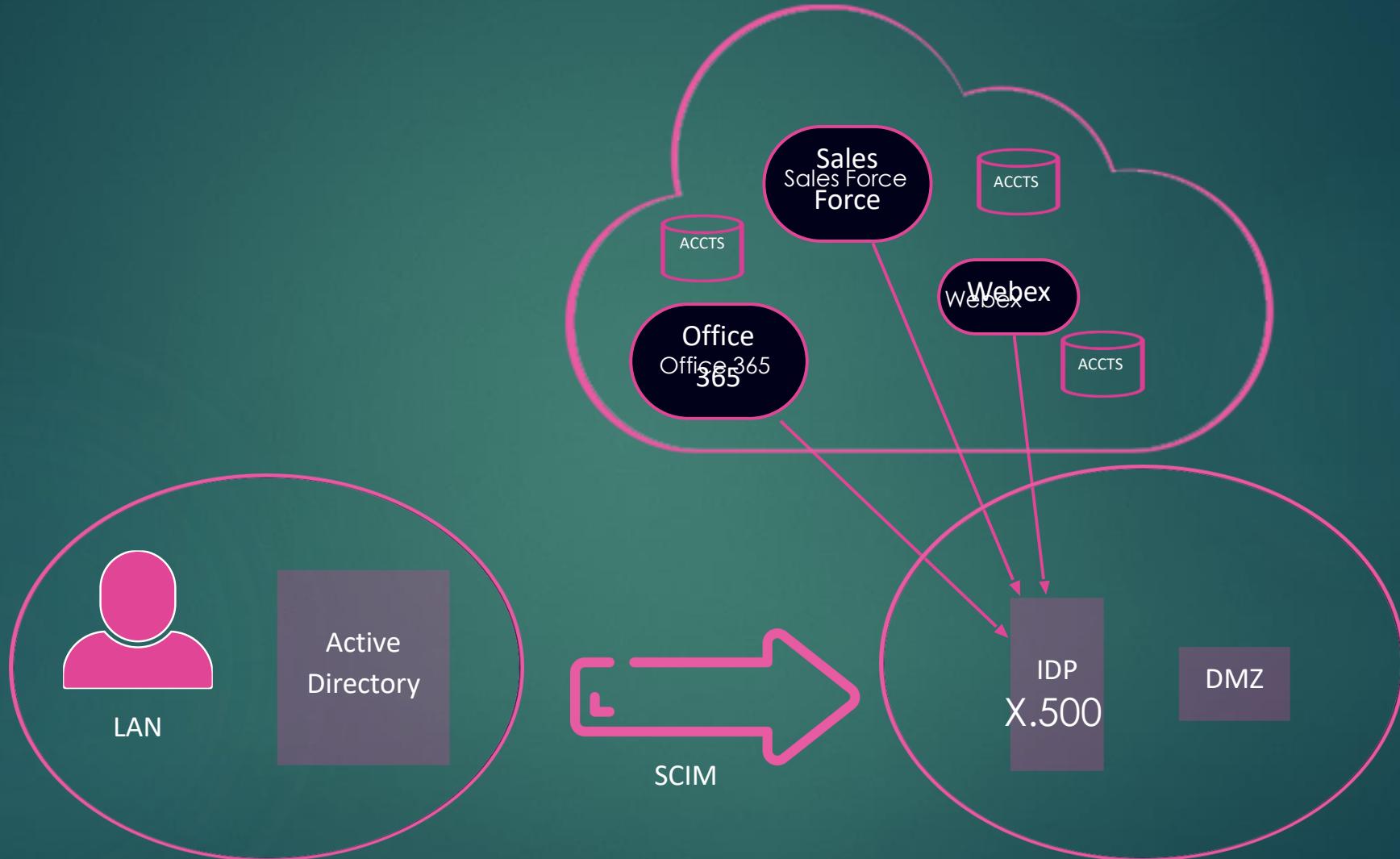
Identity Management: Provisioning/Deprovisioning

- Traditionally, different cloud vendors used non-standard provisioning APIs
- Enterprises to develop and maintain proprietary connectors to integrate with multiple SaaS providers
- Alternatively, Provisioning can be managed easier through
 - Service Provisioning Markup Language (SPML)
 - Older, seldom implemented due to the inflexibility and lack of vendor support
 - System for Cross-domain Identity Management...or...Simple Cloud Identity Management (SCIM)
 - Defines a schema and an API for managing identities
 - System for Cross-domain Identity Management (SCIM) is an open standard for automating the exchange of user identity information between identity domains, or IT systems.

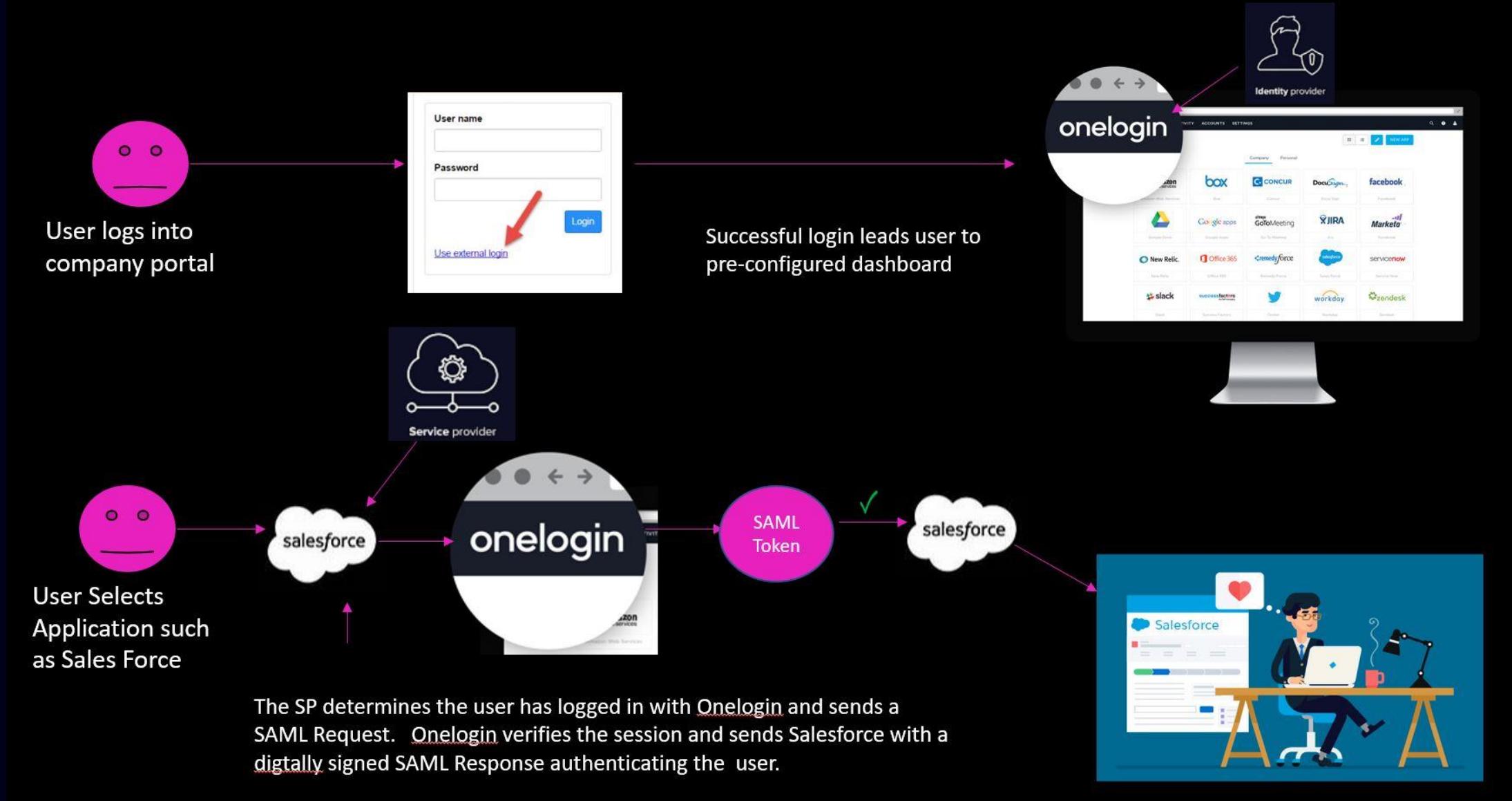
The Problem with Authentication



The Problem with Authentication



The Solution Through SAML/OPenID Connect



Managing the IAAA in the Cloud through Federations

• Web Identity Protocols

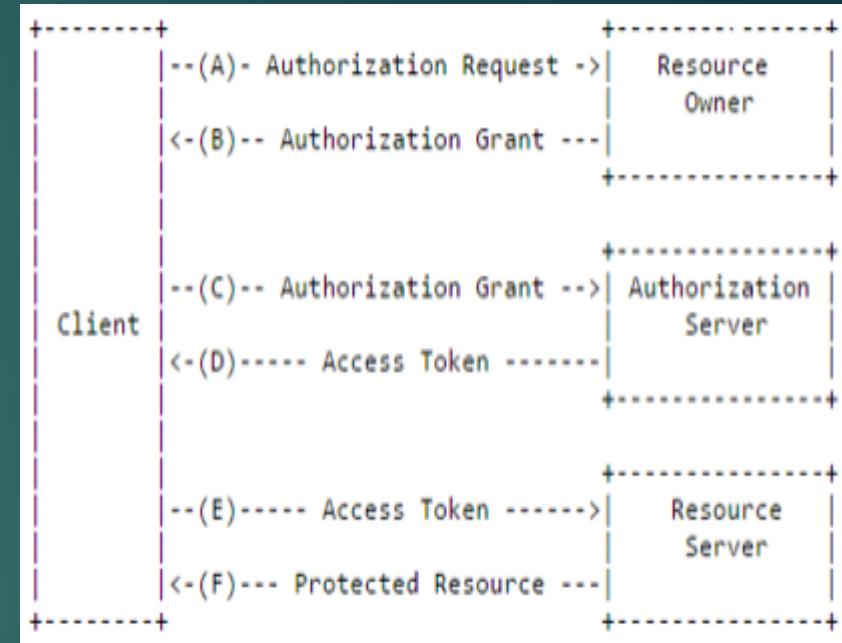
1. WS-Federation: Defines mechanisms to allow different security realms to federate, such that authorized access to resources managed in one realm can be provided to security principals whose identities reside in other realms
2. SAML: XML-based framework designed to communicate user authentication, entitlement and attribute information to other entities
3. OpenID Connect: based on OAuth 2.0 allowing developers authenticate their users across we sites and apps without having to own and manage password files. Allows information from an Identity provider to be used.
4. OAuth 2.0: Included in OpenID and enables a third party application to obtain limited access to an HTTP service on behalf of a resource owner by managing an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its behalf

Oauth 2.0

- OAuth (Open Standard for Authorization) has different intent
- Not designed for SSO
- Provides delegation of rights to applications
- In simplest terms, it means giving your access to someone you trust, so that they can perform the job on your behalf. E.g. updating status across Facebook, Twitter, Instagram, etc. with a single click.
- Could go to the sites manually, but easier to delegate access to an app that connects the above platforms
- Authenticate yourself to Facebook, Facebook provides a consent page stating you are about to give this app rights to update status on your behalf. If you agree, the app gets an opaque access token from Facebook, app stores that access token, send the status update with access token to Facebook
- Facebook validates the access token (easy in this case as the token was issued by Facebook itself), and updates your status.

Oauth 2.0

- OAuth refers to the parties involved as Client, Resource Owner (end-user), Resource Server, and Authorization Server.
- In our Facebook example, Client is the application trying to do work on your behalf.
- Resource owner is you (you own the Facebook account),
- Resource Server is the Facebook (holding your account),
- Authorization Server is also Facebook (in our case Facebook issues the access token using which client can update status on Facebook account).
- It perfectly ok for Resource Server and Authorization Server to be managed by separate entities, it just means more work to establish common ground for protocols and token formats

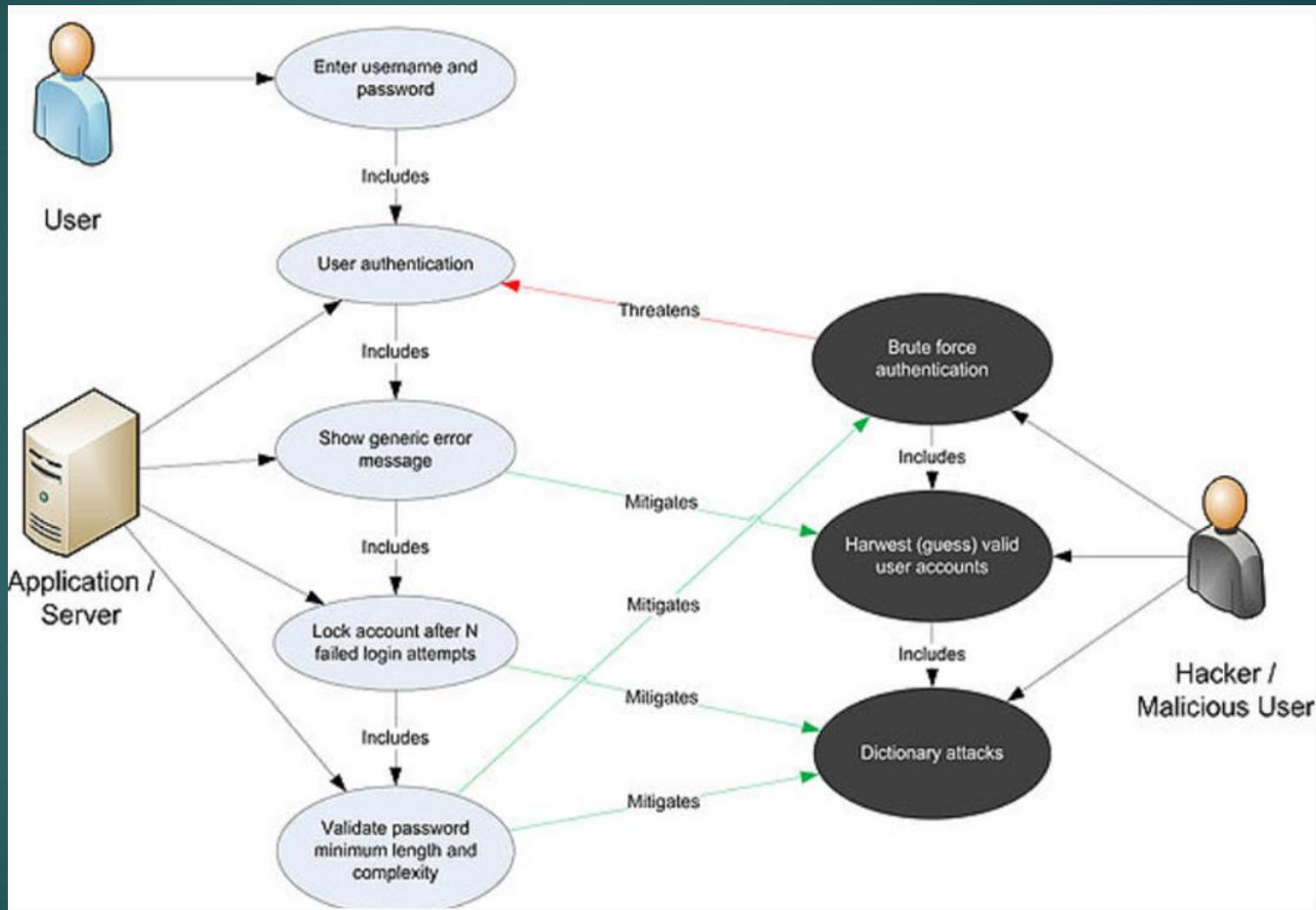


Threat Modeling for Applications

Threat Modeling

- Identify Security Objectives
 - Legislative Drivers
 - Contractual Requirements
 - Alignment with Business Objectives
- CIA Triad
- Tools for Threat Modeling
 - Data Flow Diagrams
 - Use/Misuse Cases

Use/Misuse Cases



Threat Modeling: Stride

| Threat | Mitigation |
|-------------------------|---|
| Spoofing | Authentication |
| Tampering | Integrity Verification (Message Digests/CRCs) |
| Repudiation | Non-Repudiation (Digital Signatures, Keys) |
| Information Disclosure | Confidentiality Through Encryption |
| Denial of Service | High Availability/Redundancy/Fault Tolerance |
| Escalation of Privilege | Authorization |

Risks in Design

- Code Reuse
- Flaws vs. Bugs
 - Flaw: Inherent fault with the design of code
 - Bug: Implementation fault
- Open vs. Closed Design

Controls Evaluation

- Efficacy of Controls
- Economy of Mechanism
- Cost/Benefit Analysis
- Psychological Acceptability

Supplemental Security Devices

- WAF Web Application Firewall is Layer 7 firewall that can understand HTTP traffic and help prevent DoS attacks
- DAM Database Activity Monitoring is a layer 7 monitoring device that understands SQL commands and can limit code injection
- XML Gateways transform how services and sensitive data are exposed as APIs to developers and users and can implement DLPs, antivirus and anti-malware
- Firewalls can be configured across the SaaS, PaaS and IaaS
- API Gateways filter APIs and can implement access control, rate limiting, logging, metrics and filtering
- DLP Data Loss Prevention Systems help detect exfiltration of data

Application Security Testing

- SAST Static Application Security Testing: Whitebox test used to determine structure and logic and to detect coding errors without executing the code. Should be done early in the life cycle
- DAST Dynamic Application Security Testing is used with applications in their running state and is considered a black-box test
- RASP Runtime Application Self Protection: enables applications to protect themselves by identifying and blocking attacks in real time. Unlike firewalls, which rely solely on network data to work, RASP leverages the application's intrinsic knowledge of itself to accurately differentiate attacks from legitimate traffic, stopping only malicious traffic

Domain 4 Cloud Application Security Review

- Determining Data Sensitivity
- Security Responsibilities Across Models
- The Software Development Lifecycle
- OWASP Top Ten Vulnerabilities
- IAM and Federated identity management
- Application Security Testing

Domain 5

Cloud Security Operations

Domain 5 Operations Overview

- Datacenter
- Implement Build, Run, and Manage Physical Infrastructure for Cloud Environment
- Build, Run and Manage Logical Infrastructure for Cloud Environment
- Ensure Compliance with Regulations and Controls
- Conduct Risk Assessments to Logical and Physical Infrastructure
- Collection, Acquisition and Preservation of Digital Evidence
- Manage Communication with Relevant Parties

Datacenter design

- Factors impacting Data Center Design
 - Location and Users
- Type of services – PaaS/ IaaS/ SaaS
- Operating standards – ISO, ITIL etc.
- Automation, consolidation, MTTR and MTBF

Logical Design

- Multi-Tenancy
- Management Plane
- Virtualization Technology
- Logical Design Levels – Compute, Management, Storage, Control
Plane, Network
- Physical Design
- Service Model – IaaS, PaaS, SaaS

Physical Design

- Temperature and Humidity Guidelines: 64-80 Degrees roughly 40-60% humidity
- HVAC Considerations: redundancy, energy efficient, filtration
- Air Management: air should be able to circulate freely
- Cable Management: Under floor or overheard can leave hot spots due to poor circulation
- Aisle Separation and Containment Hot/cold aisles

Uptime Institute's Data Center Site

Infrastructure provides a standard that many enterprises use to evaluate their data center's design

- Tier I Basic Data Center Site Infrastructure
- Tier II Redundant Site Infrastructure Capacity Components
- Tier III Concurrently Maintainable Site Infrastructure
- Tier IV Fault-Tolerant Site Infrastructure

| FEATURE | TIER I | TIER II | TIER III | TIER IV |
|---|--------|---------|-----------------------------|----------------------------|
| Active capacity components to support the IT load | N | N+1 | N+1 | N after any failure |
| Distribution paths | 1 | 1 | 1 active and 1 alternate | 2 simultaneously active |
| Concurrently maintainable | No | No | Yes | Yes |
| Fault tolerance | No | No | No | Yes |
| Compartmentalization | No | No | No | Yes |
| Continuous cooling | No | No | No | Yes |

Enterprise operations

- Isolate security zones—trusted, semi-trusted, untrusted → Zero Trust
- Separation of outsourced resources from internal environment
- Regulatory Compliance—HIPAA, PCI DSS, GLBA, SOX
- Service provider separation of billing, CRM, payment systems, portals and hosted environments
- Financial organization specific needs
- Government agencies

Secure hardware configuration Storage

- Server Best Practices
 - Secure Build and Initial Configuration--Baselining
 - Host hardening, patching and lock-down
 - Block non-privileged access
 - Limit remote access; Ensure security protocols are used if remote administration is needed
 - Host-based firewall/IDS/IPS
 - Secure ongoing configuration maintenance
 - Patch management
 - Vulnerability assessments/penetration tests

Secure hardware configuration Storage

- Storage Networks
 - Initiators: server with host bus adapter that initiates the connection to a port on the storage system
 - Targets: the ports on the storage system that deliver the storage volumes, as LUNs (logical unit numbers)
 - Avoid Oversubscription in iSCSI
 - iSCSI Implementation
 - Dedicated network to reduce latency
 - iSCSI traffic is unencrypted---Encryption must be added through IPSec and IKE
 - Authentication
 - Kerberos/ SRP(secure remote password)/ SPKM 1&2(secure public key ,management)/ CHAP

Virtual Switches

- Virtual Switch best practice
 - Key virtual networking component
 - Network Isolation
 - Limit access to management plane
 - Redundancy
 - Isolation between internal and external networks—create separate virtual switch with its own physical network interface cards---never mix internal and external traffic

Best Practices

- Leading Practices
 - Defense in Depth
 - Access Control
 - Auditing/ Monitoring
 - Maintenance

When Assessing the Physical Infrastructure of a CSP, Consider the following

- Legal
- Compatibility
- Control
- Log Data
- Upgrades and changes, change management
- Failover technology

When Assessing the Physical Infrastructure of a CSP, Consider the following (2)

- Compliance
- Regulations
- Outsourcing
- Placement of Security
- Virtualization
 - Operating system and app files
 - Data fluidity

Securing Virtual Machines

- Access Control and Secure KVM (kernel-based VMs)
- Kernel-based Virtual Machine (KVM) is an open source [virtualization](#) technology built into Linux®. Specifically, KVM lets you turn Linux into a [hypervisor](#) that allows a host machine to run multiple, isolated virtual environments called guests or virtual machines (VMs).
 - Isolated data channels: makes it impossible for data to be transferred between connected computers via the KVM
 - Tamper warning labels/Housing intrusion detection: Provide indication if enclosure has been compromised
 - Fixed firmware: Can't be modified
 - Tamper-proof circuit board: Can't be modified
 - Safe buffer design: Does not use a buffer and keyboard buffer is cleared after transmissions preventing transfer of keystrokes
 - Selective USB access: Only allows human interface device (keyboards, mice, etc.)
 - Push-button control: Requires physical access to switch between connected systems

Benefits of a KVM

- Security: KVM uses a combination of security-enhanced Linux (SELinux) and secure virtualization (sVirt) for enhanced VM security and isolation. SELinux establishes security boundaries around VMs. sVirt extends SELinux's capabilities, allowing Mandatory Access Control (MAC) security to be applied to guest VMs and preventing manual labeling errors.
- Storage: KVM is able to use any storage supported by Linux, including some local disks and network-attached storage (NAS). Multipath I/O may be used to improve storage and provide redundancy. KVM also supports shared file systems so VM images may be shared by multiple hosts. Disk images support thin provisioning, allocating storage on demand rather than all up front.
- Performance and scalability: KVM inherits the performance of Linux, scaling to match demand load if the number of guest machines and requests increases. KVM allows the most demanding application workloads to be virtualized and is the basis for many enterprise virtualization setups, such as data centers and private clouds (via OpenStack®).

Secure network configuration

- Network Isolation
- Protecting VLANs
 - VLAN Communication
 - VLAN Advantages
- Using Transport Layer Security (TLS)
- Using Domain Name System (DNS)
 - DNS Security Extensions (DNSSEC)

Network Isolation/Security Zones

- Protection:
 - A ‘Managed Boundary’ for all user access to application and systems
 - Implement granular role-based controls on traffic, users and assets
 - Manage Inter-Zone communications
 - Including between sub-zones
 - Enforce policy and regulations
 - Data confidentiality and integrity rules for data stored within a zone



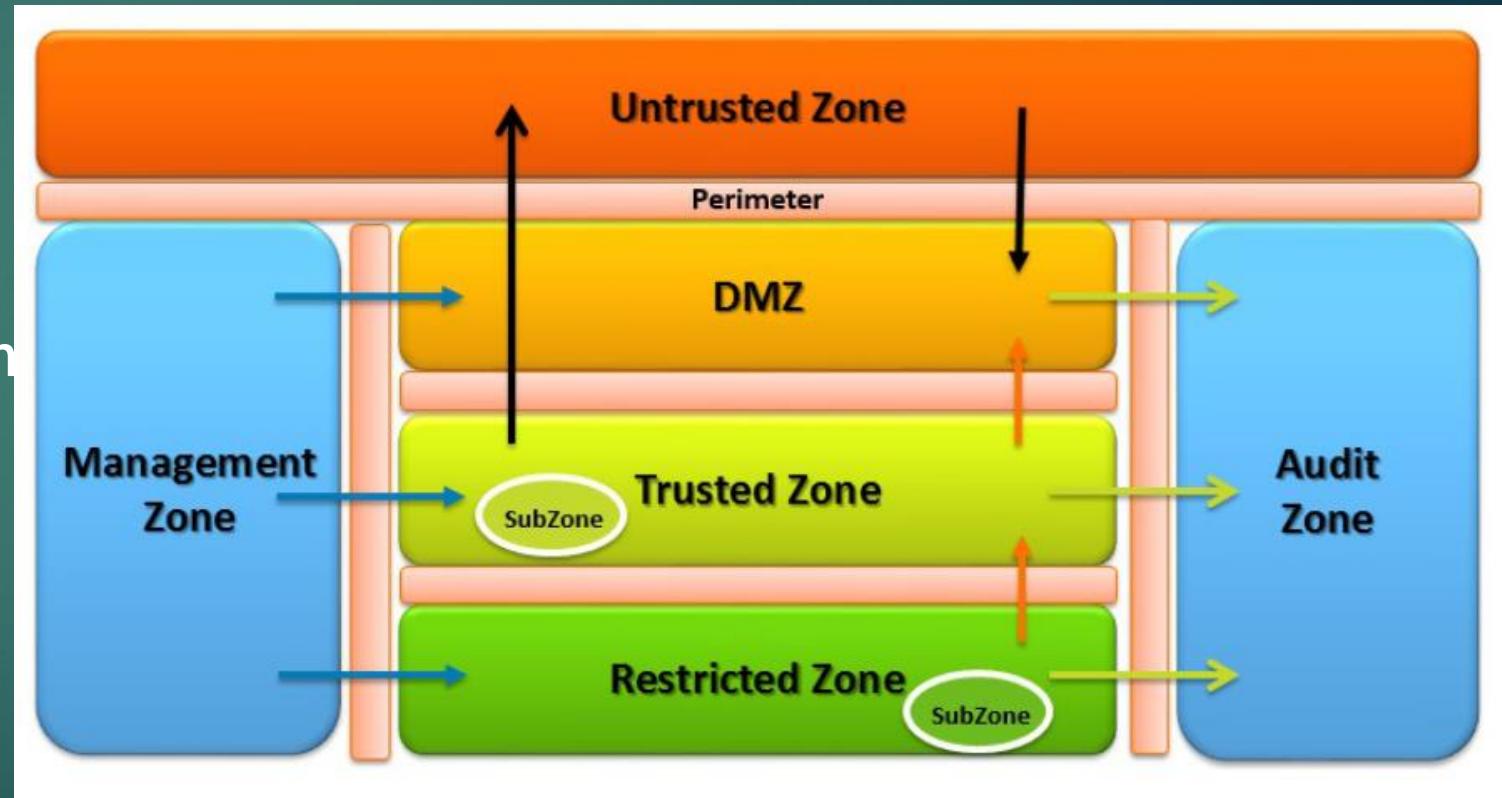
Network Isolation/Security Zones (2)

- Detection:
 - Monitor Inter-Zone communications
 - Gain visibility of traffic, users and assets
 - Logging and Event Correlation
 - Elevate alerts for events using a SIEM/Analytics
 - Prevent Inter-Zone data leakage using a DLP solution
- Containment:
 - Control communications and resources on both inbound and outbound requests
 - Set a default deny policy on all inter-segment connections



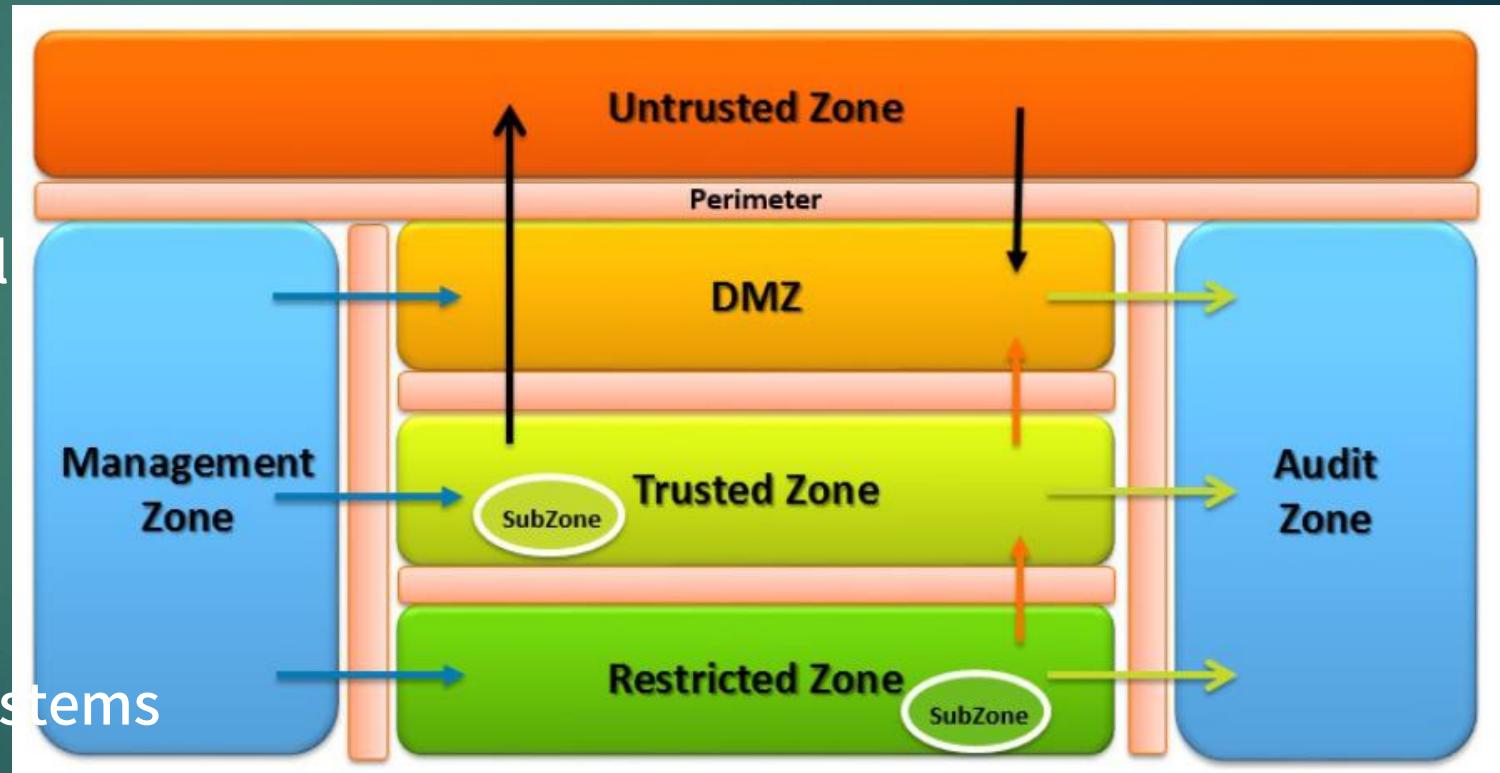
Zone Architecture

- **Untrusted Zone:**
 - External Systems (not owned by organization)
 - Internet, Public data classification
- **Semi-Trusted (DMZ):**
 - Externally-Exposed systems.
 - Public data classification
 - 3rd Party Exposed systems
 - Business Partner Systems



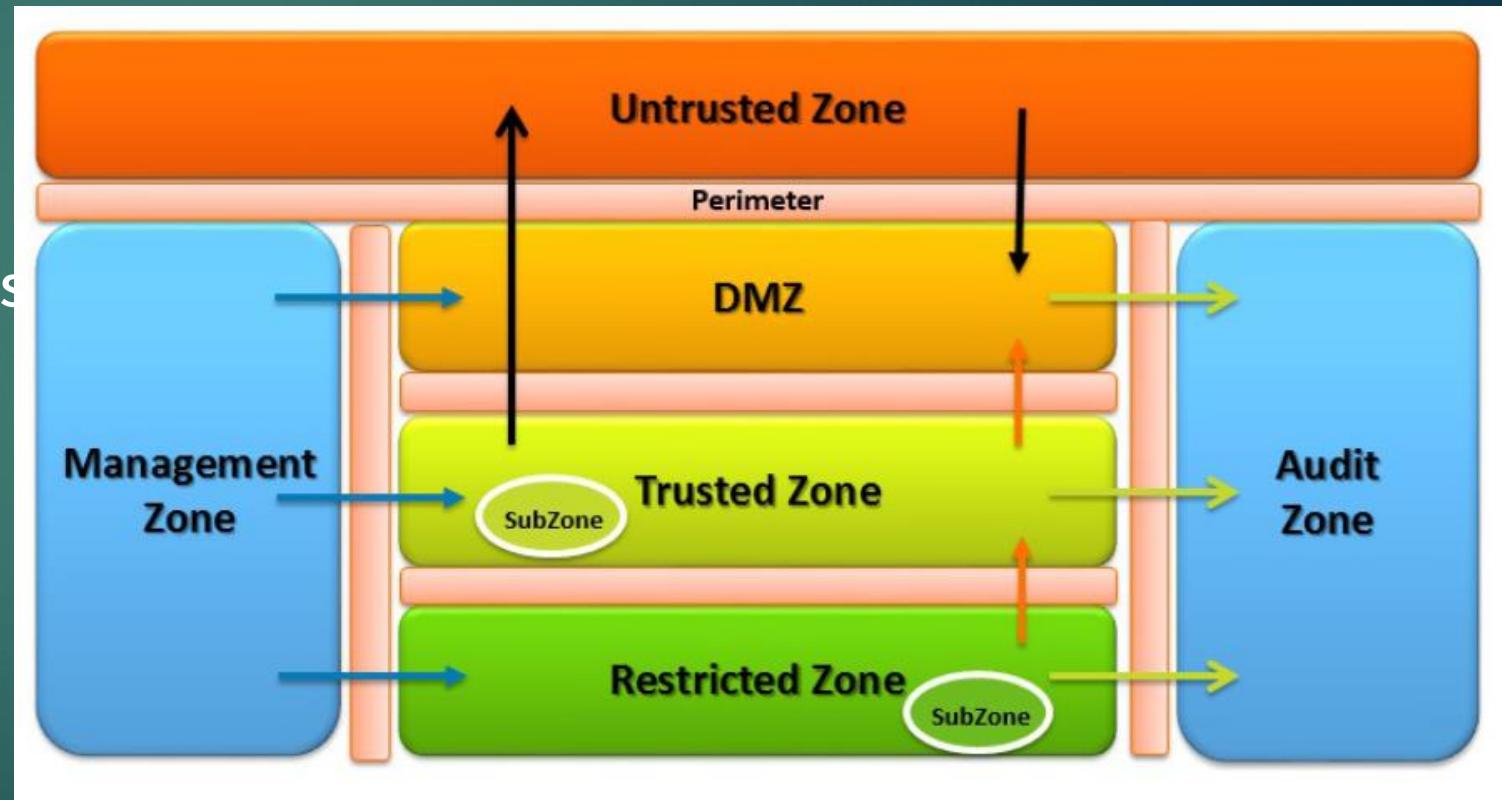
Zone Architecture (2)

- Internally-Exposed systems
 - Internal data classification
 - Confidential data classification
- **Restricted Zone:**
 - High-Risk Mission Critical systems
 - Restricted data classification
- **Management Zone:**
 - Network Management systems
 - Virtualization Management
 - Security Management systems



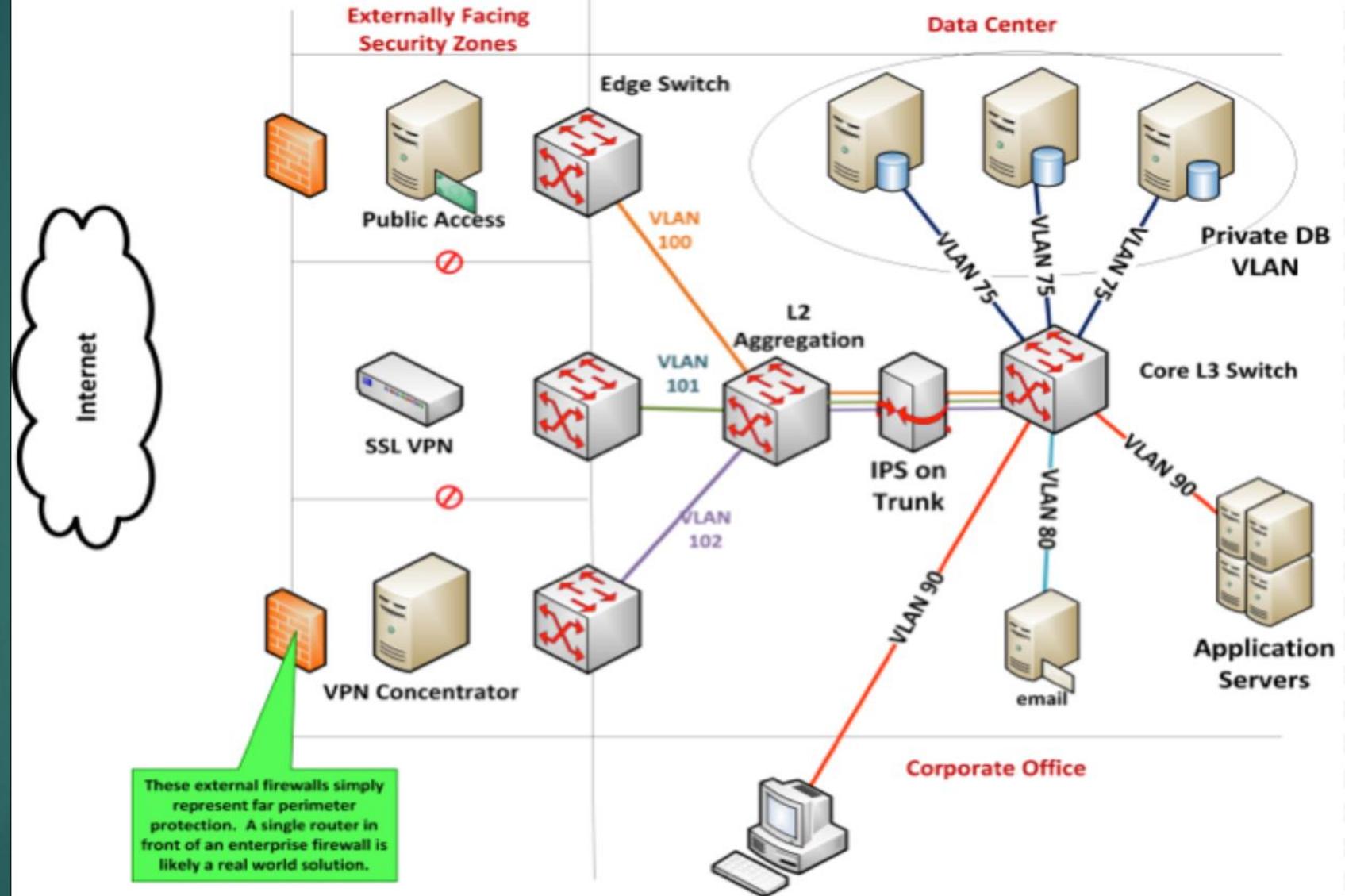
Zone Architecture (3)

- **Audit Zone:**
 - Regulatory Compliance
 - Security Logging
 - Security Monitoring (SIEM)
- **Sub-Zones:**
 - Zones divided into Subzones
 - Span Global Sites
 - Special Cases
 - Regulatory Mandated



VLANs

- Broadcast isolation on switches
- Separation of Security Zones

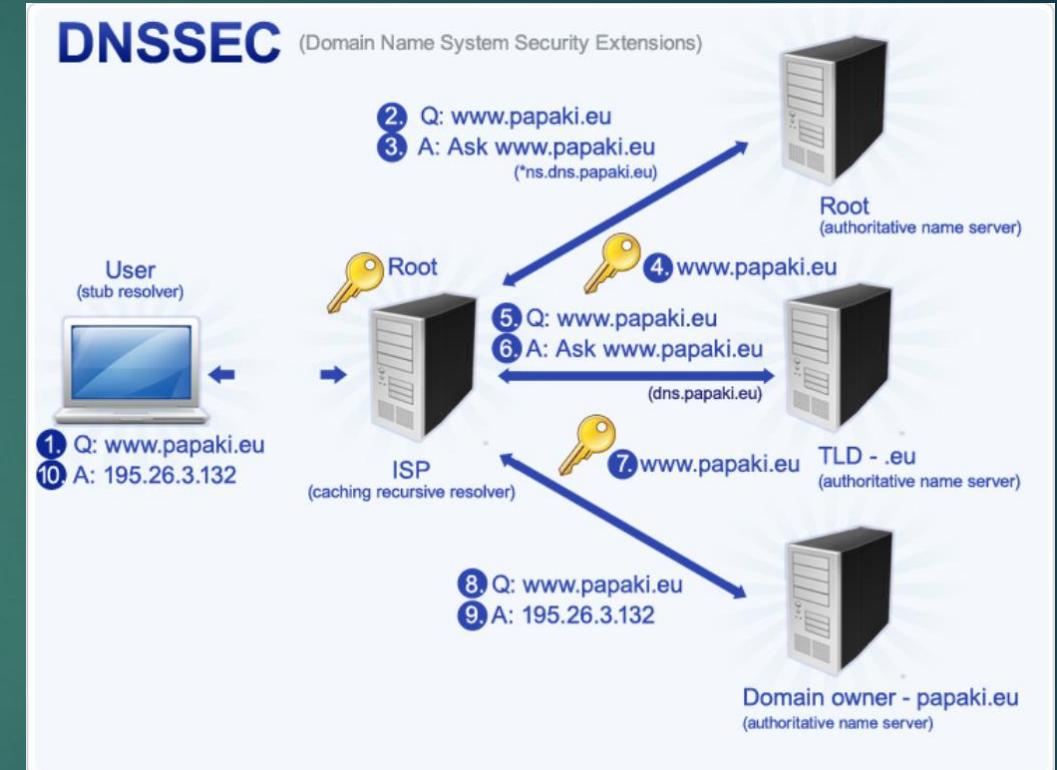


Secure network configuration: DNS

- DNS servers are desirable targets
 - Footprinting
 - Denial-of-Service Attack
 - Data modification
 - Redirection
 - Spoofing

Secure network configuration: DNS

- DNS are vulnerable to a range of threats and attacks, such as man-in-the-middle and cache poisoning. These threats use false information to redirect users to misleading sites and web addresses.
- DNSSEC records introduce **digital signatures** in the data DNS, **verify the source** and **confirm their authenticity**, as they move within the internet. This means that when a user enters an address with DNSSEC enabled, the response received, meaning the site where it is redirected, has its **authority verified for authenticity**.



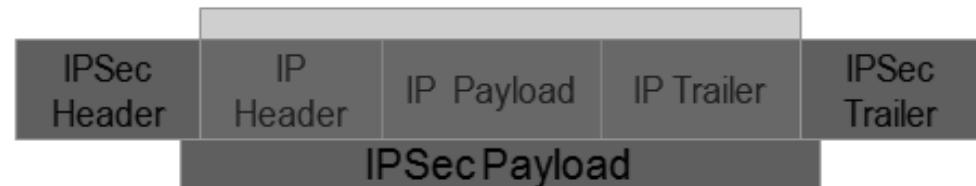
Secure network configuration

- Using Internet Protocol Security (IPSec)
- Tunnel Vs. Transport mode
- Sub-protocols

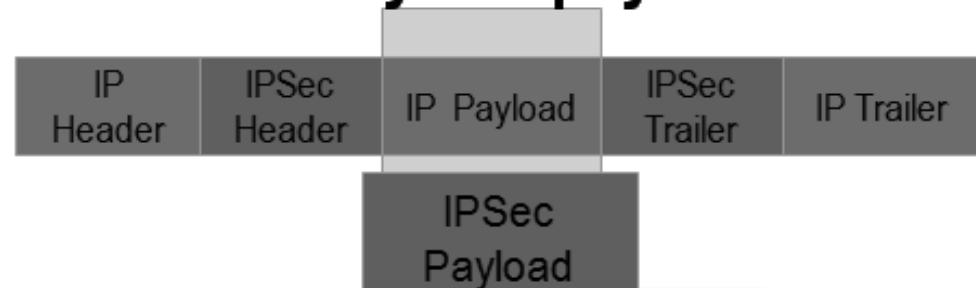
IPSEC

- IPSEC is an encapsulation framework. Tunnel vs. Transport mode dictates what portion of the IP Packet is to be encapsulated.

Tunnel Mode: Whole packet is encapsulated



Transport Mode: Only the payload is encapsulated



IPSec Sub-protocols

- AH (Authentication Header) Provides integrity, authenticity, and non-repudiation through the use of an ICV (Integrity Check Value). The ICV is run on the entire packet (header, data, trailer) except for particular fields in the header that are dynamic (like TTL, etc). NO CONFIDENTIALITY
- ESP (Encapsulating Security Payload) Provides authenticity and integrity through a MAC (no non-repudiation since a MAC is symmetric). The main service provided is ENCRYPTION. ICV is run on payload only.
- IKE: Internet Key Exchange---No Security Services. Just management of secure connection
 - Oakley: Uses Diffie Hellman to agree upon a key
 - ISAKMP (Internet Security Association and Key Management Protocol) Manages Keys, Security Associations (SAs)and Security Parameters Index (SPI)

TLS

1. Client uses https:// to initiate a secure connection
2. Server sends client its own public key
3. Client's browser generates a symmetric, session key
4. Client uses the server's public key to encrypt the symmetric session key and encrypts this symmetric session key across the network
5. Server is able to use its private key to encrypt the session key. Now both server and the client have the same symmetric key
6. Once the symmetric session key has been shared between parties, a secure “channel” has been established and all communication is encrypted with the symmetric session key



Client



Server

Administrative Controls

Types of Policy

Three main types of policies exist:

- Corporate Policy
- System Specific Policy
- Issue Specific Policy



Standards

- Mandatory
- Created to support policy, while providing more specifics details.
- Reinforces policy and provides direction
- Can be internal or external



Procedures

- Mandatory
- Step-by-step directives on how to accomplish an end-result.
- Detail the “how-to” of meeting the policy, standards, and guidelines



Guidelines

- Not Mandatory
- Suggestive in Nature
- Recommended actions and guides to users
- “Best Practices”

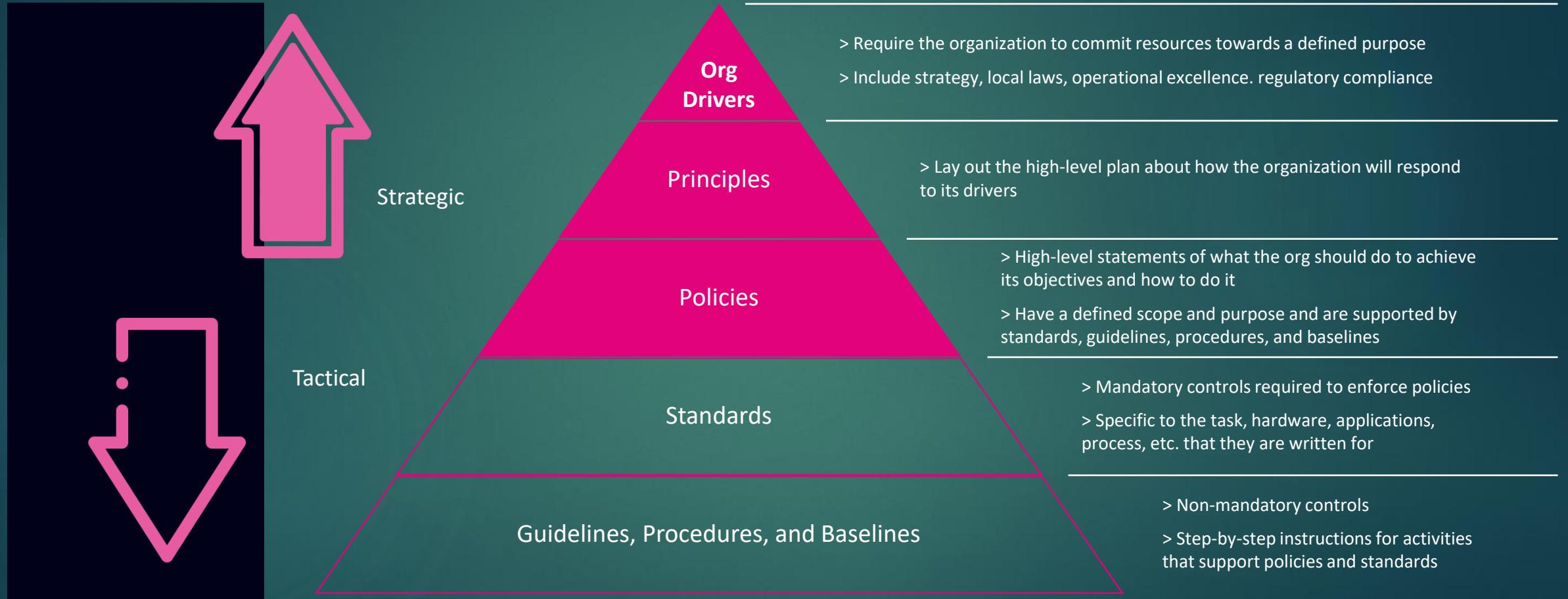


Baselines

- Mandatory
- Minimum acceptable security configuration for a system or process
- The purpose of security classification is to determine and assign the necessary baseline configuration to protect the data



Information Security Policy Framework



System and Issue Specific Policies

System Specific Policies

- Web Servers must be configured according to a consistent consistent image with baseline configuration approved by approved by Director of IT and Director of Marketing
- Multifactor authentication must always be used when accessing accessing domain controllers
- Client systems must be validated periodically against a baseline baseline image
- Etc.

Issue Specific Policies

- Change Management Policy Policy
- Acceptable Use Policy
- Privacy
- Data/System Ownership
- Separation of Duties (SOD)
- Mandatory Vacations
- Job rotation
- Least privilege
- Need to know
- Dual control
- M of N control

Patch management process

- Vulnerability detection and evaluation
- Subscription mechanism
- Severity assessment
- Applicability assessment
- Tracking records
- Customer notification
- Change Management
- Verification
- Deployment Risk Management
- Closure of tracking

Patch management automation

- Severity
- Patch or interim solution
- System entry
- Automated notification
- Considerations
 - Applicability
 - Tracking mechanisms
 - Change records
 - Verification
 - Documentation

Patch management challenges

- Standardization
- Collaboration
- Scalability
- Testing
- Multiple Time Zone
- VM Suspension and Snapshot

Performance monitoring

- Network/ Disk/ Memory/ CPU
- Outsourced Monitoring
 - References (HR)
 - SLA Terms
 - Trial runs
- Hardware Monitoring
- Redundant System Architecture
- Monitoring Functions

Defense in depth

- Firewalls
 - Host-Based Software
 - Configuration of Ports
- Layered Security
 - Intrusion Detection System
 - Network Intrusion Detection (NIDS)
 - Host Intrusion Detection (HIDS)
- Intrusion Prevention System
 - Automated reconfiguration of active controls
 - Removal of malicious content from traffic

Defense in depth

- Intrusion Detection
 - Host vs. Network
 - IDS vs. IPS
 - Analysis Engines
 - Pattern Matching
 - Profile Matching
- Utilizing Honeypots
- Conducting Vulnerability Assessments
- Log Capture and Log Management
 - External storage considerations
 - Inclusion in backup and disaster recovery plans
- Security Information and Event Management (SIEM)

Managing a Logical Infrastructure

- Access Control for Remote Access
 - Trust
 - Credentialing
- OS Baseline Compliance Monitoring and Remediation
 - Inherent (VUM/WSUS) and third party
 - Real-time or near real-time
- Backing Up and Restoring Guest OS Configuration
 - Cloning/templates

IT Service Management (ITSM)

- Portfolio Management
- Demand Management
- Financial Management
- Efficient Service Management
- Involvement and Alignment

Operations Management Security

- Information Security Management
 - Policies, Procedures, Standards and Guidelines
 - Organization
 - Assets
 - Human Resources
 - Physical and Environmental
 - Communications

Operations Management (cont.)

- Configuration Management: Security through stability
- Document, monitor, control, and audit changes to the baseline TCB
 - Development and implementation
 - Quality evaluation and compliance
 - Oversight of testing and deployment
 - Prevention of unauthorized changes

Change Management

- Change Management
 - Submit Change Request to CCB
 - Yes/No
 - Testing
 - Implementation in lab environment
 - Certification/Authorization
 - Document
 - Schedule
 - Train users

CSP Assurance

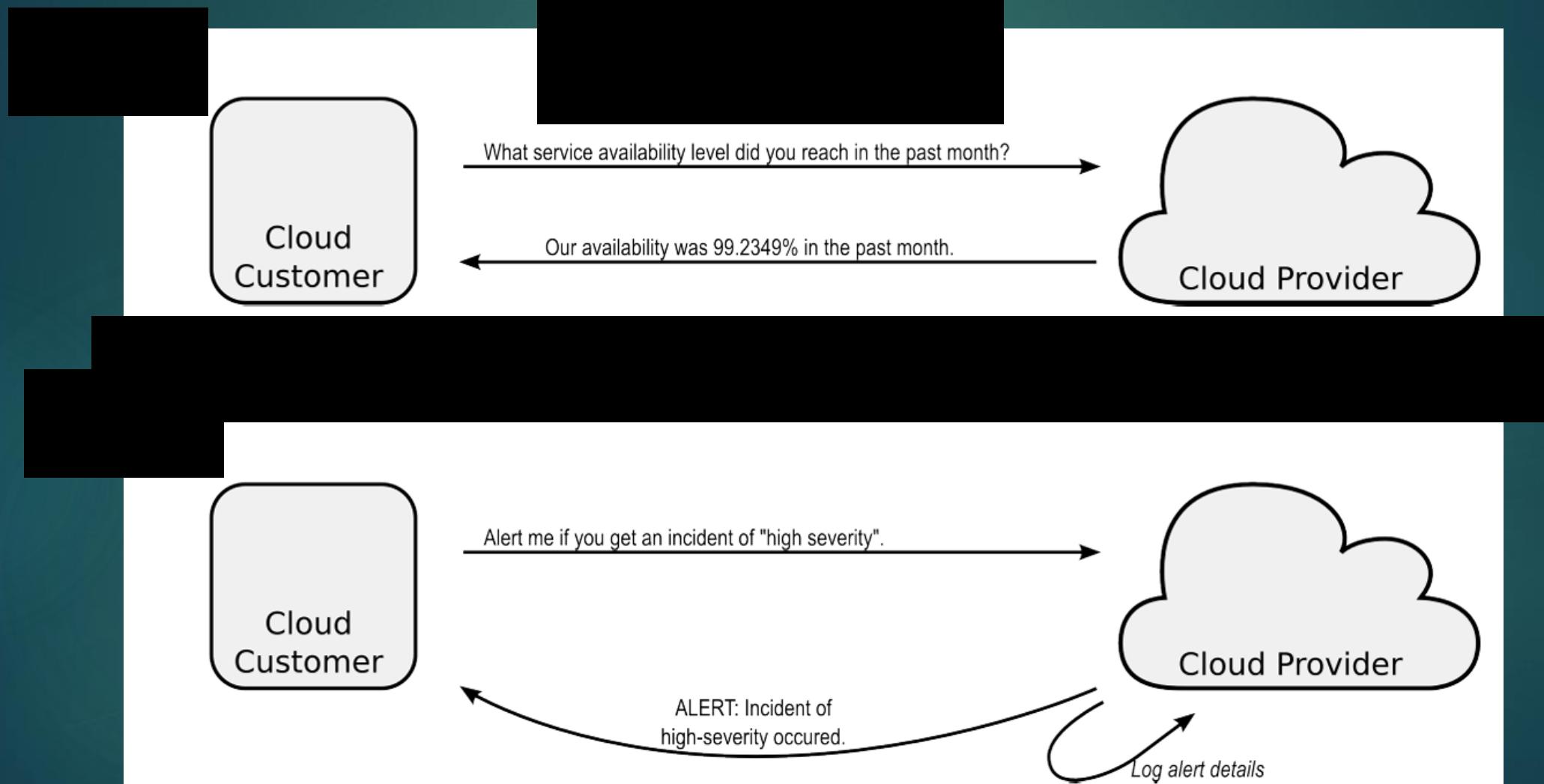
Auditing in the Cloud

- Internal and External Audits
- Types of Audit Reports
 - Service Organization Control (SOC) Reports
 - SOC 1
 - SOC 2
 - SOC 3

Assurance from CSPs

- Cloud providers running data center operations should demonstrate to customers their compliance to current regulations and standards.
- CSPs can/should share results of independent audits
 - Cloud Trust Protocol is intended to establish digital trust between a cloud computing customer and provider and create transparency about the provider's configurations, vulnerabilities, access, authorization, policy, accountability, anchoring and operating status conditions.
 - CSA STAR is the industry's most powerful program for security assurance in the cloud. STAR encompasses key principles of transparency, rigorous auditing, and harmonization of standards. STAR certification provides multiple benefits, including indications of best practices and validation of security posture of cloud offerings.

Cloud Trust Protocol (CTP)



SOURCE: chrome-extension://efaidnbmnnibpcobjpcgkclefindmkaj/https://s3.amazonaws.com/content-production.cloudsecurityalliance/h86KAm42EVh5qJ43yWd5xkVb?response-content-disposition=inline%3B%20filename%3D%22CTP-Data-Model-And-API.pdf%22%3B%20filename%2A%3DUTF-8%27%27CTP-Data-Model-And-API.pdf&response-content-type=application%2Fpdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAS6XDIRHKHO4FSU4%2F20231031%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20231031T121956Z&X-Amz-Expires=300&X-Amz-SignedHeaders=host&X-Amz-Signature=b9e3b98fda4ba5c413787daff196f16cda687636da4f60a180ffe4feacef5033

Shared Monitoring and Testing

- CSP needs to protect against
 - Data leakage
 - Side channel attacks
- May negotiate access for customer to have access to
 - Data Streams
 - Audit Logs
 - Performance Logs
 - SIEM log data
 - DLP alerts/Data

Service Organizational Control Documents

- Service Organizations are replacing traditional in-house functions (payroll processing, medical claims processing, human resources, document, workflow, and tax processing).
- SOC for Service Organizations reports help service providers build trust and confidence in their services and controls
 - SOC 1 Pertains to financial controls
 - SOC 2 Pertains to trust services (Security, Availability, Confidentiality, Process Integrity, and Privacy) Only for current customers
 - SOC 3 Also pertains to trust services (Security, Availability, Confidentiality, Process Integrity, and Privacy) PUBLICALLY AVAILABLE

Type 1 vs. Type 2 SOC Documents

A Type 1 report provides a report of procedures / controls an organization has put in place as of a point in time.

A Type 2 report has an audit period and provides evidence of how an organization operated its controls over a period of time.

It is important to understand that there are not more stringent control requirements in a Type 2 SOC Report; but rather, it describes how a company's control environment operated over its audit period (typically not less than six months). You can have the same controls in a Type 1 report as the Type 2; the only difference is that they are audited or examined over a period of time and testing results are reported in a SOC 1 and SOC 2 report.

Source: <https://www.marcumllp.com/insights/soc-report-type-1-vs-type-2-soc-1-2-3-reporting-definitions#:~:text=The%20short%20answer%20is%20that,over%20a%20period%20of%20time>.

Why do golfers like both SOC type 1 and type 2?

They like to have 2 SOCs in case they get a hole in 1



Domain 5 Operations Review

- Datacenter
- Implement Build, Run, and Manage Physical Infrastructure for Cloud Environment
- Build, Run and Manage Logical Infrastructure for Cloud Environment
- Ensure Compliance with Regulations and Controls
- Conduct Risk Assessments to Logical and Physical Infrastructure
- Collection, Acquisition and Preservation of Digital Evidence
- Manage Communication with Relevant Parties

Domain 6

Legal and Compliance

Domain 6 Legal and Compliance

- Frameworks
- Legal Concepts
- Legal Controls and CSP
- Standard Privacy Requirements
- Internal ISMS
- ERM and the Cloud
- Business Requirements
- 3rd Party Governance
- CSA STAR
- Supply Chain Management

Framework and Guidelines

Information Security Frameworks

- Provide a standard set of information security requirements which guide organizations on control implementation
- Provide unification and standardization of the behaviors and procedures that the business wishes to promote
- Generic enough to be used across various industries
- Examples: ISO 27001, CSF (Cybersecurity Framework, GDPR, etc.)

Gap Analysis



Where You
Are

Gap Analysis



Skills Needed to
Get Where You're going



Where You
Need to Be



Information Security Strategy
and Road Map

ISO 27017

- ISO/IEC 27017 is the international standard on Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
- It provides guidelines for information security controls that are applicable to providing and using cloud services by outlining: additional implementation guidance for relevant controls specified in ISO/IEC 27002 additional controls with implementation guidance that specifically relate to cloud services

ISO 27001

- Provides a framework to help organizations protect their information by adopting an Information Security Management System (ISMS).
- Based on continuous improvement
- The standard is separated into two parts. The first consists of 11 clauses, or requirements for ISO 27001 (0 to 10). The second part, called Annex A, provides a guideline for 114 control objectives and controls.

How to use The Plan-Do-Check-Act Cycle

STEP 1 – Plan:

Establish all the necessary objectives and processes to deliver results in accordance the expected output

STEP 2 – Do:

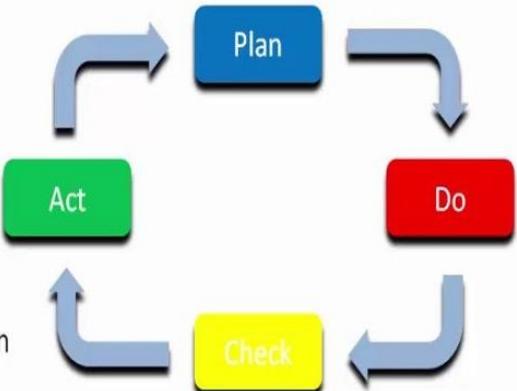
Implement the new processes. If possible on a small scale

STEP 3 – Check:

Measure the results of the new processes and hold them against the expected results in order to determine the differences

Step 4 – Act:

Analyse the differences, generated in the checking stage, to determine their cause, and decide where to apply changes for further improvement



Control Families

- A.1-A.4: Contain explanatory information
- A.5. Information Security Policies: Describe how to handle information security policies.
- A.6. Organization of Information Security: Provide the framework for the implementation and operation of information security by defining its internal organization (e.g., roles, responsibilities, etc.), and through the organizational aspects of information security.
- A.7. Human Resource Security: Ensure people are hired, trained, and managed in a secure way; also, the principles of disciplinary action and terminating the agreements are addressed.
- A.8. Asset Management: Ensure that information security assets (e.g., information, processing devices, storage devices, etc.) are identified, that responsibilities for their security are designated, and that people know how to handle them according to predefined classification levels.

Control Families

- A.9. Access Control: Limit access to information and information assets according to real business needs. The controls are for both physical and logical access.
- A.10. Cryptography: Provide the basis for proper use of encryption solutions to protect the confidentiality, authenticity, and/or integrity of information.
- A.11. Physical and Environmental Security: Prevent unauthorized access to physical areas, and protect equipment and facilities from being compromised.
- A.12. Operation Security: Information and information processing facilities should be protected from malware, data loss, and the exploitation of technical vulnerabilities.
- A.13. Communications Security: Information should be protected in networks and as it is transferred, both internally and externally to the organization.
- A.14. System Acquisition, Development, and Maintenance: Information security should be designed and implemented throughout the lifecycle of information systems.
- A.15. Supplier Relationships: Ensure that outsourced activities performed by suppliers and partners also use appropriate information security controls, and they describe how to monitor third-party security performance.

Control Families

- A.15. Supplier Relationships: Ensure that outsourced activities performed by suppliers and partners also use appropriate information security controls, and they describe how to monitor third-party security performance.
- A.16. Information Security Incident Management: Provide a framework to ensure the proper communication and handling of security events and incidents so that they can be resolved in a timely manner; they also define how to preserve evidence, as well as how to learn from incidents to prevent their recurrence.
- A.17. Information Security Aspects of Business Continuity Management: Ensure the continuity of information security management during disruptions, and the availability of information systems.
- A.18. Compliance: Provide a framework to prevent legal, statutory, regulatory, and contractual breaches, and audit whether information security is implemented and is effective according to the defined policies, procedures, and requirements of the ISO 27001 standard.

ISO 27000 Standards

- 27001: Designed to develop, build, implement, assess and improve an ISMS (Information Security Management System)
- 27002: Describes the specifics of the controls referenced in Appendix A of ISO 27001.
 - Specifies 15 domains, 35 control objectives, and 14 controls
- 27003:2017: Provides guidance for the implementation of an ISMS based on ISO/IEC 27001
- ISO/IEC 27004:2016: Provides guidelines on evaluating the information security performance and the effectiveness of an information security management system. Establishes:
 - Monitoring and measurement of information security performance
 - Monitoring and measurement of the effectiveness of an ISMS
 - Analysis and evaluation of the results of monitoring and measurement
- ISO 27005: Provides guidelines for Information Security Risk Management for organizations following ISO 27001 Framework

Privacy in the US

Privacy in the United States

- The data collected by many organizations aren't regulated
- There are no federal privacy laws in the US, though there are regulations geared towards specific industries.
- Individual states may have additional privacy regulations as well.
- However, many companies can use, share, or sell any data they collect about you without notifying you that they're doing so.
- No national law standardizes when (or if) a company must notify you if your data is breached or exposed to unauthorized parties.
- If a company shares your data, including sensitive information such as your health or location, with third parties (like data brokers), those third parties can further sell it or share it without notifying you.

Laws vs. Regulations

How are laws and regulations similar?

- Laws and regulations are similar in that they both try to specify and organize what that authorizing body feels is appropriate behavior. In this sense, we can think of laws and regulations as rules that are established by the federal, state, or local government or their appropriating agency. Often, Regulations are written to implement the specifics of a particular law. (e.g. licensing laws and licensing regulations; Mental Health Parity laws, and their regulations)
- Laws and regulations, under statute, have to hold public hearings open to anyone interested in testifying for public comment before making decisions about adopting, changing or eliminating a law or regulation.
- Laws and regulations are also enforced to the full authority of the law. If you were to violate a law or regulation, there may be penalties up to or including imprisonment or fines.

How are laws and regulations different?

- Laws go through the bill process before becoming established as a law. A bill has to be written, sponsored by a legislator, debated and passed through both the House of Representatives and the Senate after various committee and budget hearings before going to the Executive to be signed into law. A regulation is created by a governmental agency, often to actually implement a given law, and does not have to go through the bill process described above. With regulations, an agency holds a public hearing and after that hearing makes a decision on either adopting, changing or rejecting the regulation.
- Laws are also rules that govern everyone equally, while regulations only effect those who deal directly with the agency who is enforcing them. In other words, a law can govern the action of both the DEP and the FBI, but the DEP cannot write regulations that would be enforceable to the FBI.

Important US Laws and Regulations

| Name | Purpose | Administrators Enforcers | |
|--|--|--------------------------|---|
| The Electronic Communication Privacy Act (ECPA) | Enhance laws restricting the government from putting wire taps on phone calls, updating them to include electronic communication in the form of data. | * | * |
| The Stored Communications Act (SCA, Title II of the Electronic Communications Privacy Act) | Restrict government from forcing ISPs to disclose customer data the ISP might possess. | * | * |
| Graham-Leach-Bliley Act (GLBA) | Allow banks to merge with and own insurance companies. Included in the law were stipulations that customer account information be kept secure and private, and that customers be allowed to opt out of any information-sharing arrangements the bank or insurer might engage in. | FDIC, FFIEC | FDIC and DFI |
| Sarbanes-Oxley Act (SOX) | Increase transparency into publicly traded corporations' financial activities. Includes provisions for securing data and expressly names the traits of confidentiality, integrity, and availability. | SEC | SEC |
| Health Insurance Portability and Accountability Act (HIPAA) | Protect patient records and data, known as electronic protected health information (ePHI). | DHHS | OCR |
| Family Educational Rights and Privacy Act (FERPA) | Prevent academic institutions from sharing student data with anyone other than parents of students (up to age 18) or the students (after age 18). | Department of Education | Department of Education (Family Policy Compliance Office) |
| The Digital Millennium Copyright Act (DMCA) | Update copyright provisions to protect owned data in an Internet-enabled world. Makes cracking of access controls on copyrighted media a crime, and enables copyright holders to require any site on the Internet to remove content that may belong to the copyright holder. | ** | ** |

FISMA

- Highlights the importance of information security to the economic and national security interests of the United States
- FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

FEDRAMP

The [Federal Risk and Authorization Management Program \(FedRAMP\)](#) is a government-wide program that provides a standardized approach to security **assessment, authorization, and continuous monitoring** for cloud products and services. FedRAMP empowers agencies to use modern cloud technologies, with emphasis on security and protection of federal information, and helps accelerate the adoption of secure, cloud solutions.

FedRAMP consists of two primary entities: the Joint Authorization Board (JAB) and the Program Management Office (PMO). Members of the JAB include the chief information officers (CIOs) from the Department of Defense, Department of Homeland Security, and General Services Administration. The JAB serves as the primary governance and decision-making body for FedRAMP.

Intellectual Property

Intellectual Property

- Intellectual Property Law
 - Protecting products of the mind
 - Company must take steps to protect resources covered by these laws
these laws or these laws may not protect them
- Main international organization run by the UN is the World Intellectual Property Organization (WIPO)
- Licensing is the most prevalent violation, followed by plagiarism, piracy and corporate espionage



Copyright

- Copyright

- Copyright protections lasts for the lifetime of the author plus 70 years or years or 75 years for corporations
- Work does not need to be registered or published to be protected
- Protects expression of ideas rather than the ideas themselves
- Author to control how work is distributed, reproduced, used
- Protects the expression of the resource instead of the resource itself

- Two Limitations on Copyright:

- First sale
- Fair Use



Trademark

- Protect word, name, symbol, sound, shape, color or combination used to identify product to distinguish from others
- Protect from someone stealing another company's "look and feel"
- Corporate brands and operating system logos
- Trademark Law Treaty Implementation Act protects trademarks internationally

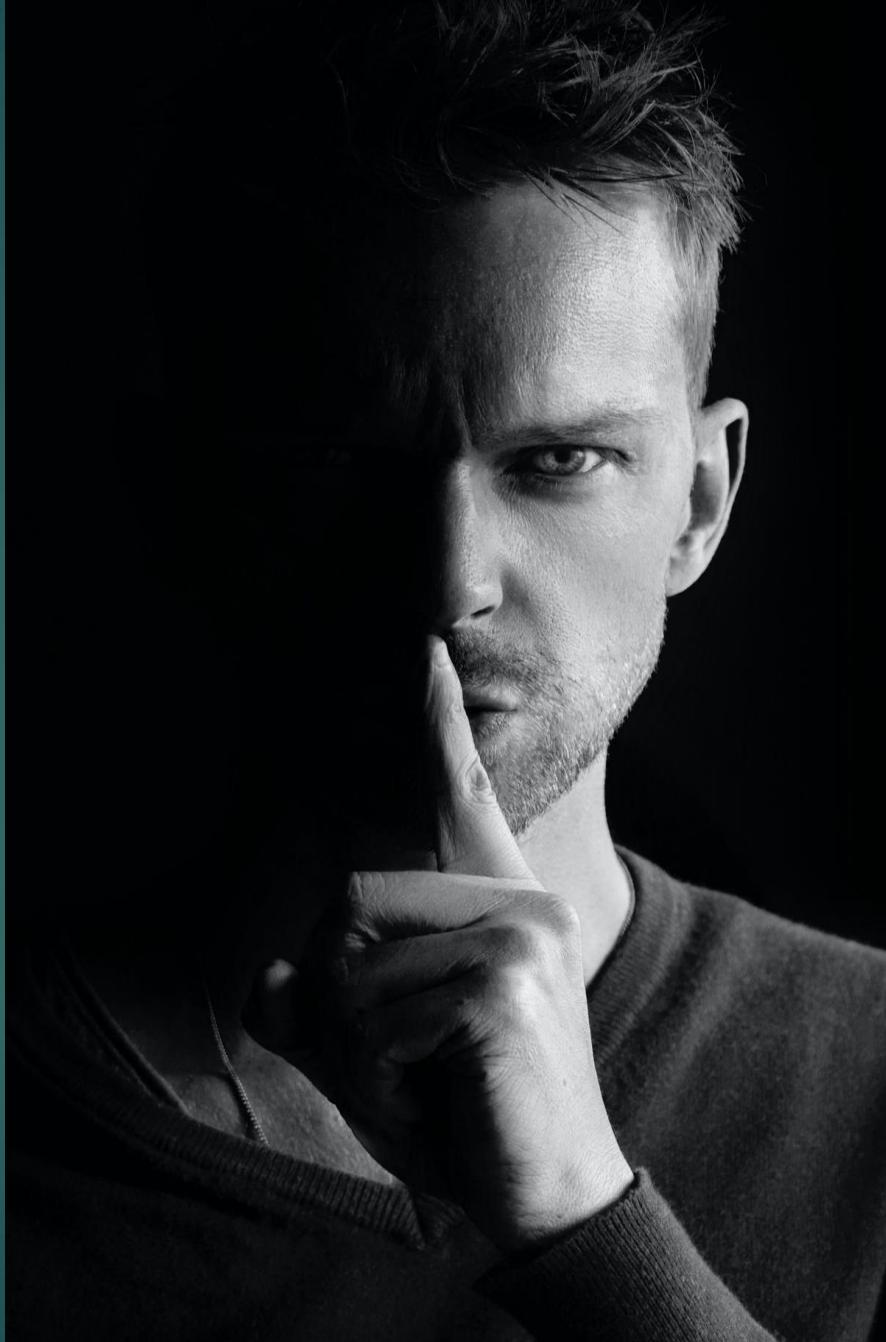


Patent

- Valid for 20 years
- Protection for those who have legal ownership of an invention
- Invention must be novel and non-obvious
- Owner has exclusive control of invention for 20 years
 - Cryptographic algorithm
- Published to stimulate other inventions
- No organization enforces patents. It is up to the owner to pursue the patent rights through the legal system

Trade Secret

- Resource must provide competitive value
- Must be reasonably protected from unauthorized use or disclosure
- Proprietary to a company and important for survival
- Must be genuine and not obvious



International Law and Standards

GDPR

1. Personal Data Redefined

GDPR changes the definition of personal data, reflecting changes in technology. Browser history, purchase history, and other related activity will no longer be acceptable under the GDPR unless the individual in question has explicitly consented

2. Individual Rights

Opt-in and Consent

Right to Access

Right to be Forgotten

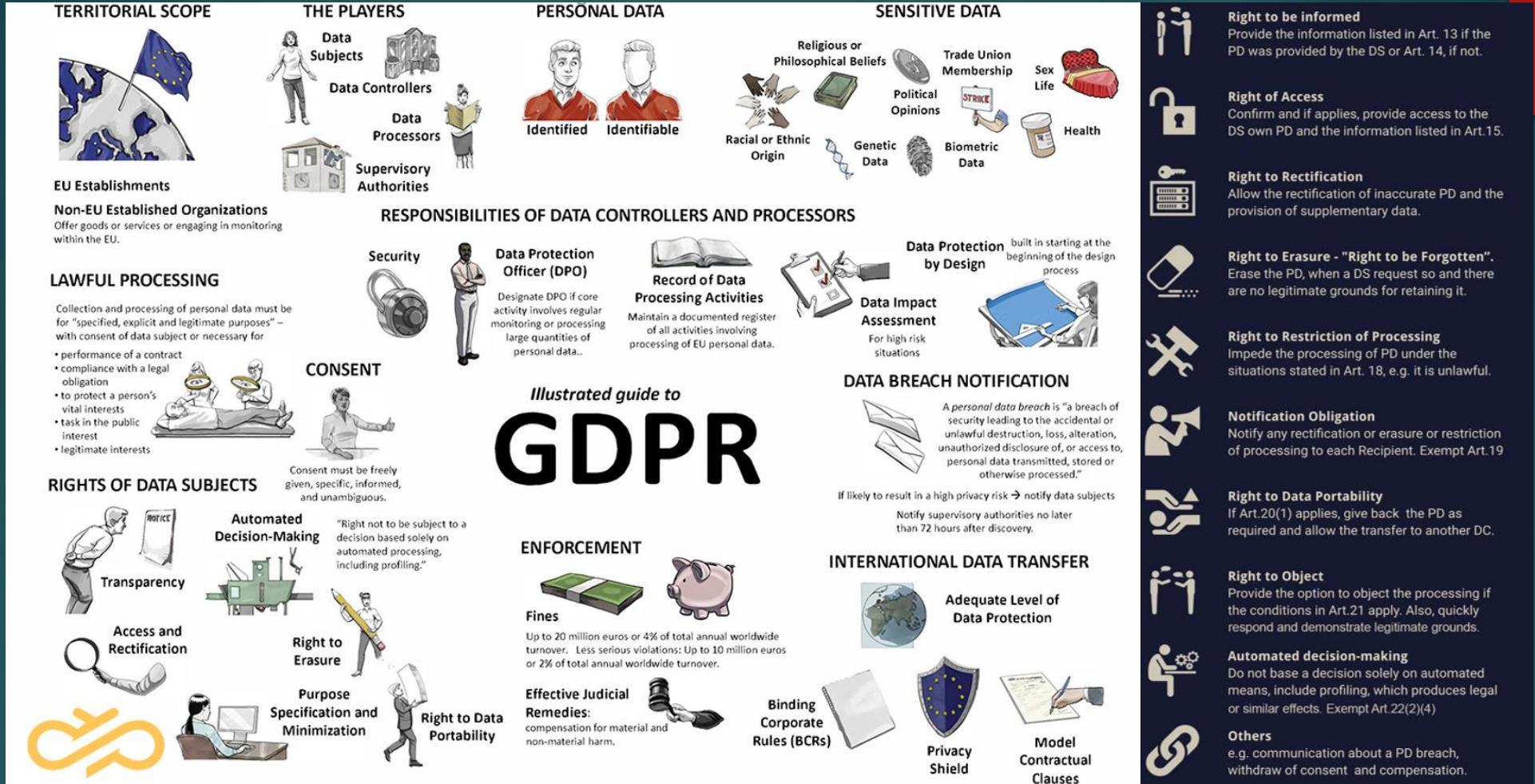
3. Data Controllers vs. Data Processors: Both data controllers and processors will be jointly responsible for complying with the new rules, meaning if an organization outsources data entry or analysis to a third party or processes data on behalf of another organization, both parties are required to abide by the GDPR and are liable for violations.

4. Information Governance and Security

Privacy: Data Regulation: GDPR requires that organizations consider compliance with the regulation from the inception of systems and processes—that is, that they implement “privacy by design.”

Security: Impact Assessments: Requires organization to conduct vulnerability assessments and penetration Testing

5. Data Breach Notification and Penalties: The GDPR requires organizations to report data breaches to the individuals whose data was compromised and to their supervisory authority within 72 hours.



OECD (Organization for Economic Cooperation and Development)

- The Organization for Economic Co-operation and Development (OECD) is a unique forum where the governments of 37 democracies with market-based economies collaborate to develop policy standards to promote sustainable economic growth.
- First set of accepted international privacy principles
- Focus on global need to enhance privacy through risk management approach
- Includes
 - National privacy strategies
 - Privacy management programs
 - Data security breach notification

Australian Privacy Act of 1988

- Transparency in the handling of personal information
- Rules on collecting information from solicitation
- Correctness and integrity of collected data

PIPEDA

- The Personal Information Protection and Electronic Documents Act is a Canadian law relating to data privacy. It governs how private sector organizations collect, use and disclose personal information in the course of commercial business

APEC

- Asia Pacific Economic Cooperation Privacy Framework
- Promotes consistent approach to information privacy to ensure the free flow of information
- Regional standard to address privacy as it relates to:
 - Privacy as an international issue
 - Electronic trading environments
 - Cross-border Data flow

eDiscovery



E-discovery

- E-Discovery refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case.
- Can be carried out online or offline—cloud computing will require online discovery
- Challenges
 - US Federal Rules of Civil Procedure require a party to litigation is expected to preserve and produce electronically stored information in its “Possession, custody, or control.” Who has control/custody?

E-discovery

- eDiscovery Investigations
 - SaaS-based eDiscovery
 - eDiscovery software vendor hosts their application on their own networks and delivers it to customers via the Internet. Customers use the application for various eDiscovery tasks such as analysis or review. Often perform tasks such as collection, preservation or review
 - Hosted eDiscovery (provider)
 - The customer collects relevant data in response to an eDiscovery matter, processes it, and sends it via the Internet to their hosting provider. The provider stores customer data on their site or in a co-location facility, and runs various levels of eDiscovery on the data .
 - Third-party eDiscovery: Cloud Customer may hire a third party with expertise with ediscovery in the cloud

Chain of Custody

- Chain of Custody **must** be well documented from point of evidence identification and collection forward
 - A history of how the evidence was
 - Collected
 - Analyzed
 - Transported
 - Preserved
 - Necessary because digital evidence can be manipulated so easily
 - Three forensic hashes are required to guarantee evidence on drive(s) was not modified:
 - Drive should be write-protected and hashed
 - Bit level copy should be taken of drive. Copy should be hashed
 - Examination and analysis should be conducted on the copy (in a write-protected system. Afterwards this copy should be hashed

Cloud Forensic Challenges

- Steps and responsibilities of digital forensics vary between the service and deployment models.
 - Can rarely get physical access to evidence in the Public Cloud
 - IaaS, VM image can be acquired
 - SaaS the CSP should have/provide secure access to the application log
 - Roles and levels of access should be documented in the SLA
- Regular backups/shapshots of previous images
- Configuring auditing
- Centralization of logs
- Hash audit logs
- Data retention policies

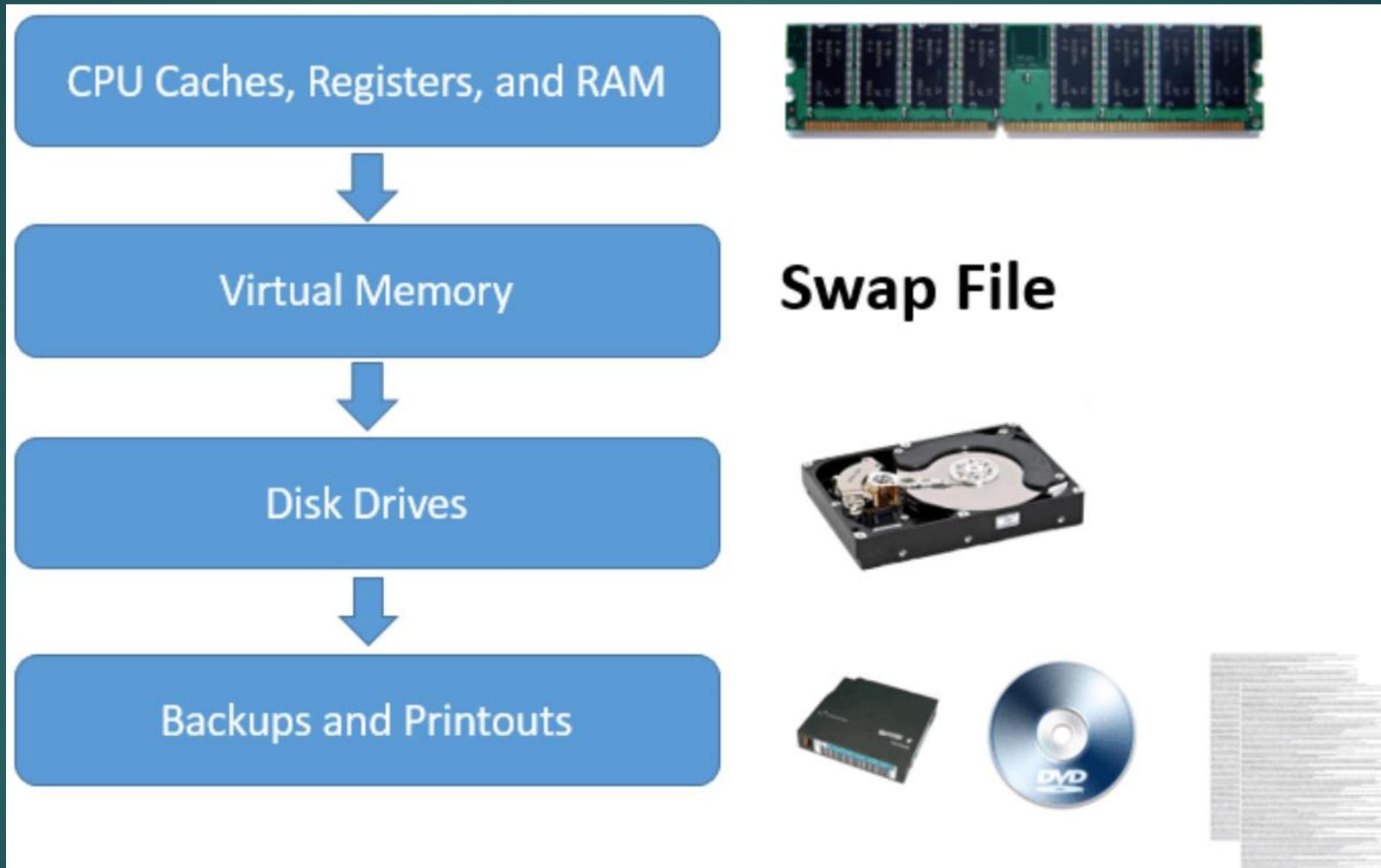
Forensics Readiness

- Steps and responsibilities of digital forensics vary between the service and deployment models.
 - Can rarely get physical access to evidence in the Public Cloud
 - IaaS, VM image can be acquired
 - SaaS the CSP should have/provide secure access to the application log
 - Roles and levels of access should be documented in the SLA
- Regular backups/shapshots of previous images
- Configuring auditing
- Centralization of logs
- Hash audit logs
- Data retention policies

The Process of Digital Forensics

- Identification---Primary Responders goal is to **preserve** evidence and begin the Chain of Custody documentation
- Collection—label, record, acquire evidence, ensuring that modification does not occur
- Examination—Data
- Analysis—Information
- Reporting
- Lessons Learned

Volatility



Integrity of Evidence

- Avoid handling evidence as much as possible
- Work on copies rather than originals
- Use write protected systems to prevent modification
- Use hashes to guarantee integrity

3rd Party Governance

Vendor Management

- Common Criteria Assurance Framework
 - ISO/IEC 15408-1:2009
- CSA Security, Trust and Assurance Registry (STAR) – 2011
 - The Security, Trust and Assurance Registry (STAR) is an online registry of cloud provider security controls.
 - free, publicly accessible and searchable repository designed to help cloud customers review the security practices of participating cloud providers
 - Level 1 – Self Assessment: Cloud providers either submit a completed The Consensus Assessments Initiative Questionnaire (CAIQ), or to submit a report documenting compliance with Cloud Controls Matrix (CCM).
 - Level 2 – Attestation: CSA STAR Attestation is a collaboration between CSA and the AICPA to provide guidelines for CPAs to conduct SOC 2 engagements using criteria from the AICPA (Trust Service Principles, AT 101) and the CSA Cloud Controls Matrix. STAR Attestation provides for rigorous third party independent assessments of cloud providers.
 - Level 3 – Ongoing Monitoring: CSA STAR Continuous Monitoring enables automation of the current security practices of cloud providers. Providers publish their security practices according to CSA formatting and specifications, and customers and tool vendors can retrieve and present this information in a variety of contexts.

Contract Management

- Identify Challenges Early
 - Understand contractual requirements driving baseline
 - Understand gaps used to challenge and request changes to contracts
 - CSP leverage for audits
- Key Contract Components
 - Performance measurements, SLAs, incident response, regulatory compliance familiarity... etc.

Supply Chain Management

- Supply Chain Risk
 - Regular updates
 - Avoidance of single points of failure
 - Prioritization of contracts
- Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)
 - Guidance for provider selection – 13 domains
- The ISO 28000:2007 Supply Chain Standard
 - Plan, Do, Check, Act (PDCA) lifecycle for continuous improvement
- SCA Tools examine code for weaknesses related to open source components
 - Many applications rely upon open-source components that contain vulnerable code.
 - SCA (Software Composition Analysis) Tools are developed to examine which open-source components are part of a software package and all security professionals to protect against issues in the supply chain
 - SCA provides an organization with visibility into the third-party code that its applications rely upon and therefore provide assurance in the supply chain

Domain 6 Legal and Compliance

- Legislative Concepts
- Legal Controls and CSP
- Standard Privacy Requirements
- Internal ISMS
- ERM and the Cloud
- Business Requirements
- 3rd Party Governance
- CSA STAR
- Supply Chain Management

The 6 Domains of CCSP

CISSP Course Syllabus:

- Domain 0: Introduction and Exam Specifics
- Domain 1: Architectural Concepts and Design Requirements
- Domain 2: Cloud Data Security
- Domain 3: Cloud Platform and Infrastructure
- Domain 4: Cloud Application Security
- Domain 5: Operations
- Domain 6: Legal and Compliance

End of Lecture...Now What?

- Schedule the test
- Work on review questions; Let questions help you determine what to study
- [Tinyurl.com/KellysCCSP2023](http://tinyurl.com/KellysCCSP2023)
 - Slides
 - Notes
 - Supplementary Material
- EMAIL ME IF YOU NEED HELP Kellyh@cybertrain.it
- GO PASS THIS TEST!!!
 - And let Kelly know how you did!