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
- 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

CYBRARY

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!

CYBRARY

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

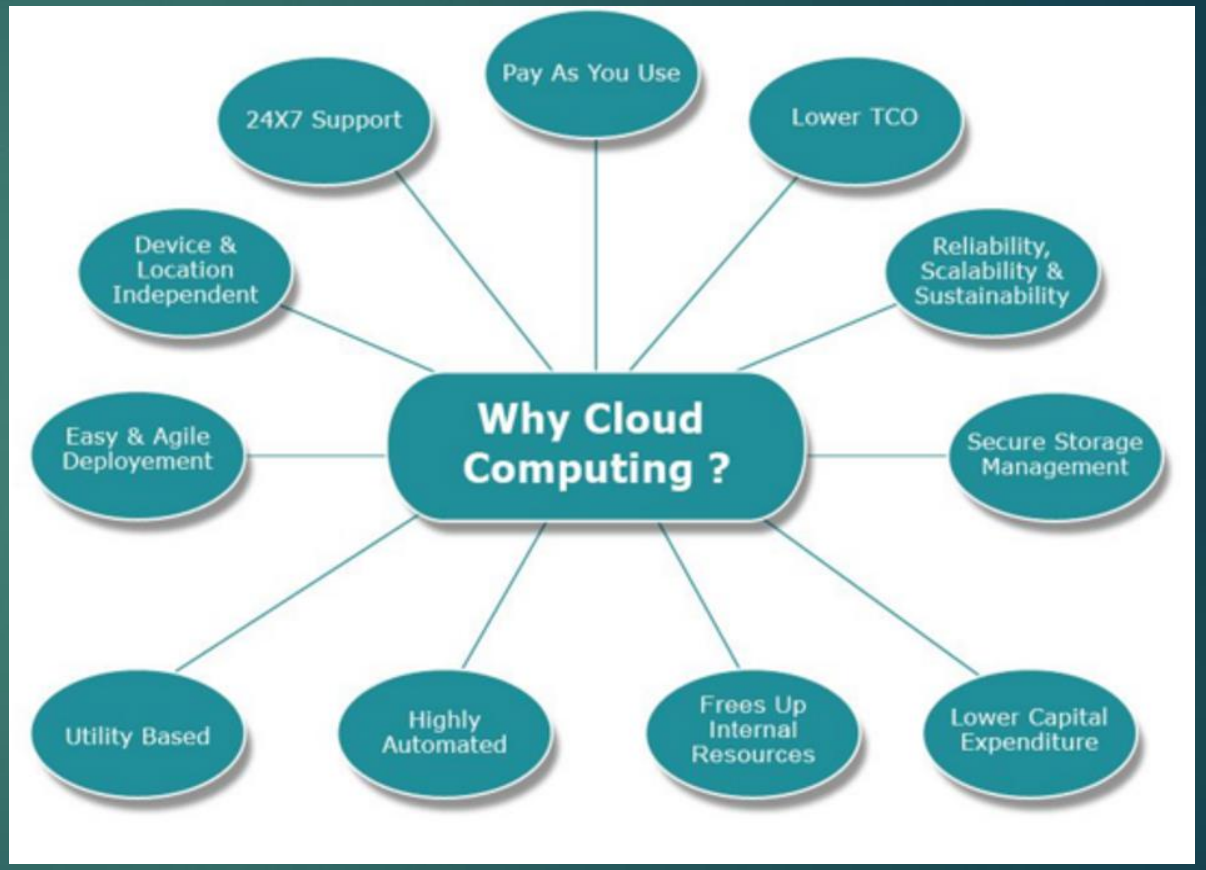
CLOUD COMPUTING NIST SP 800-145

- "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

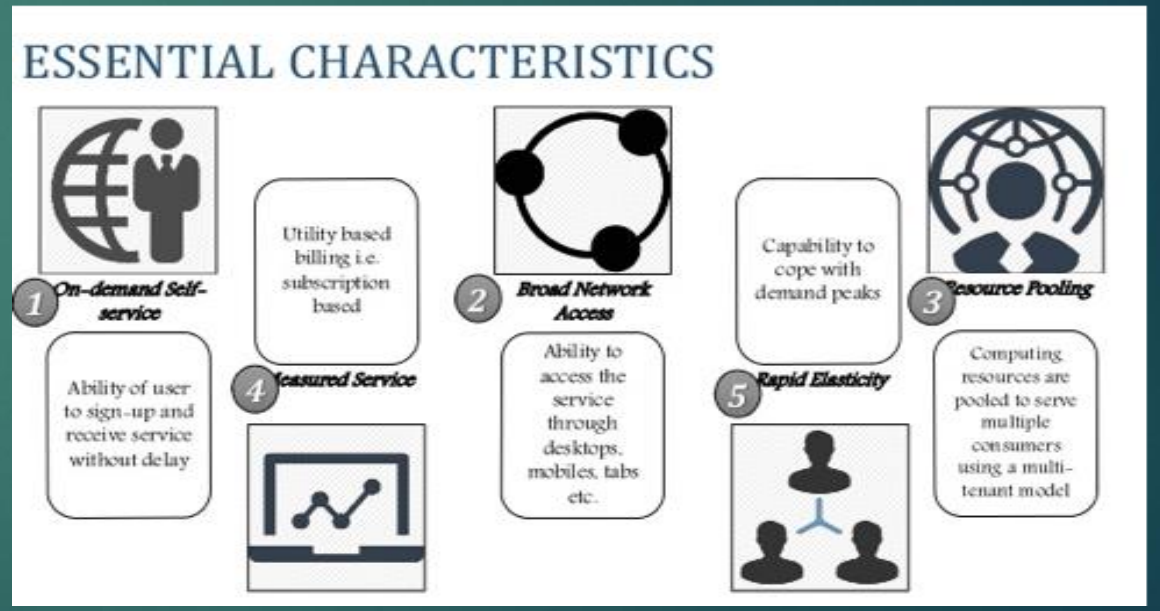


5 Characteristics of Cloud Computing

- 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

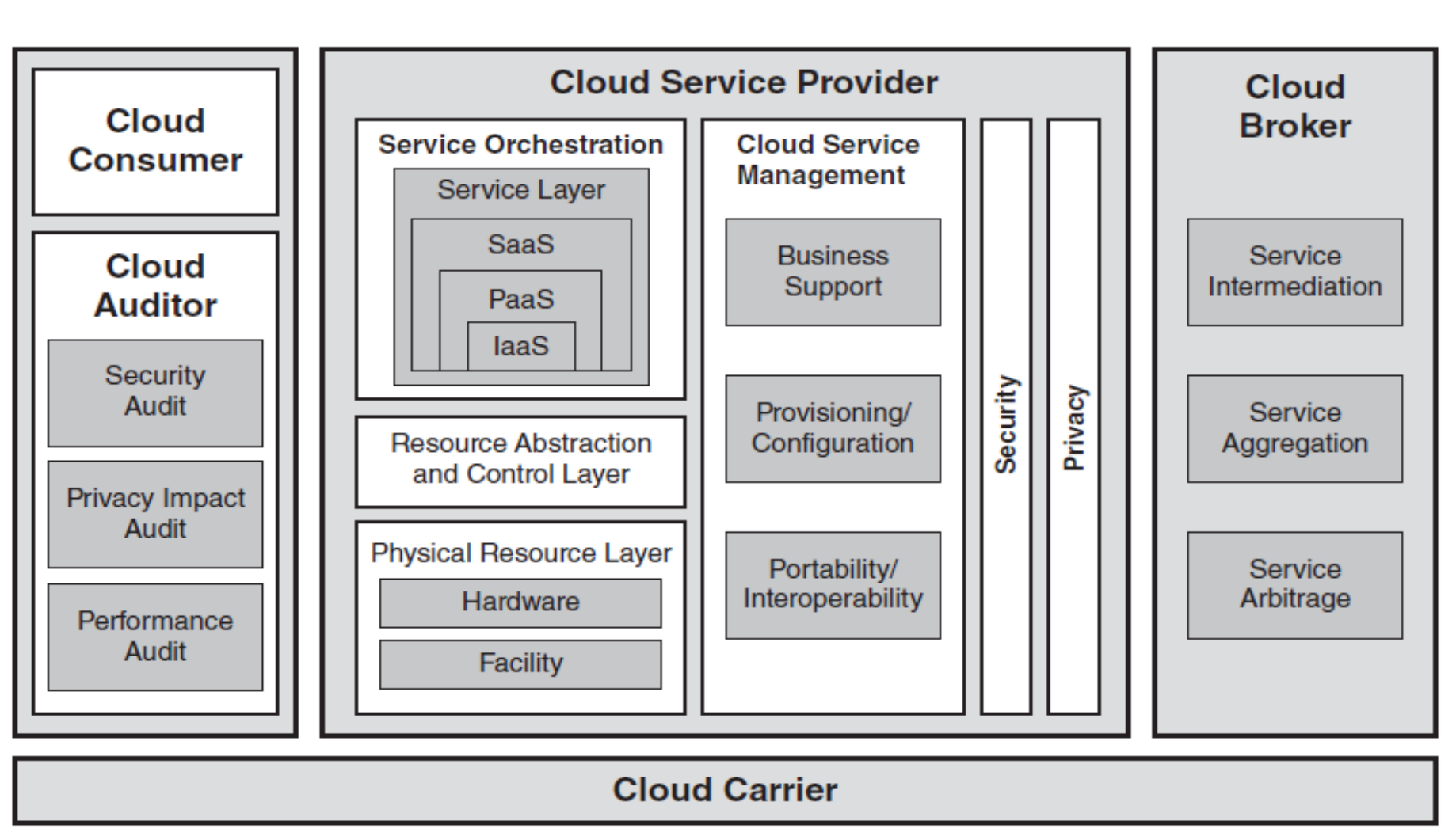


NIST's 5 Cloud Actors

- **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

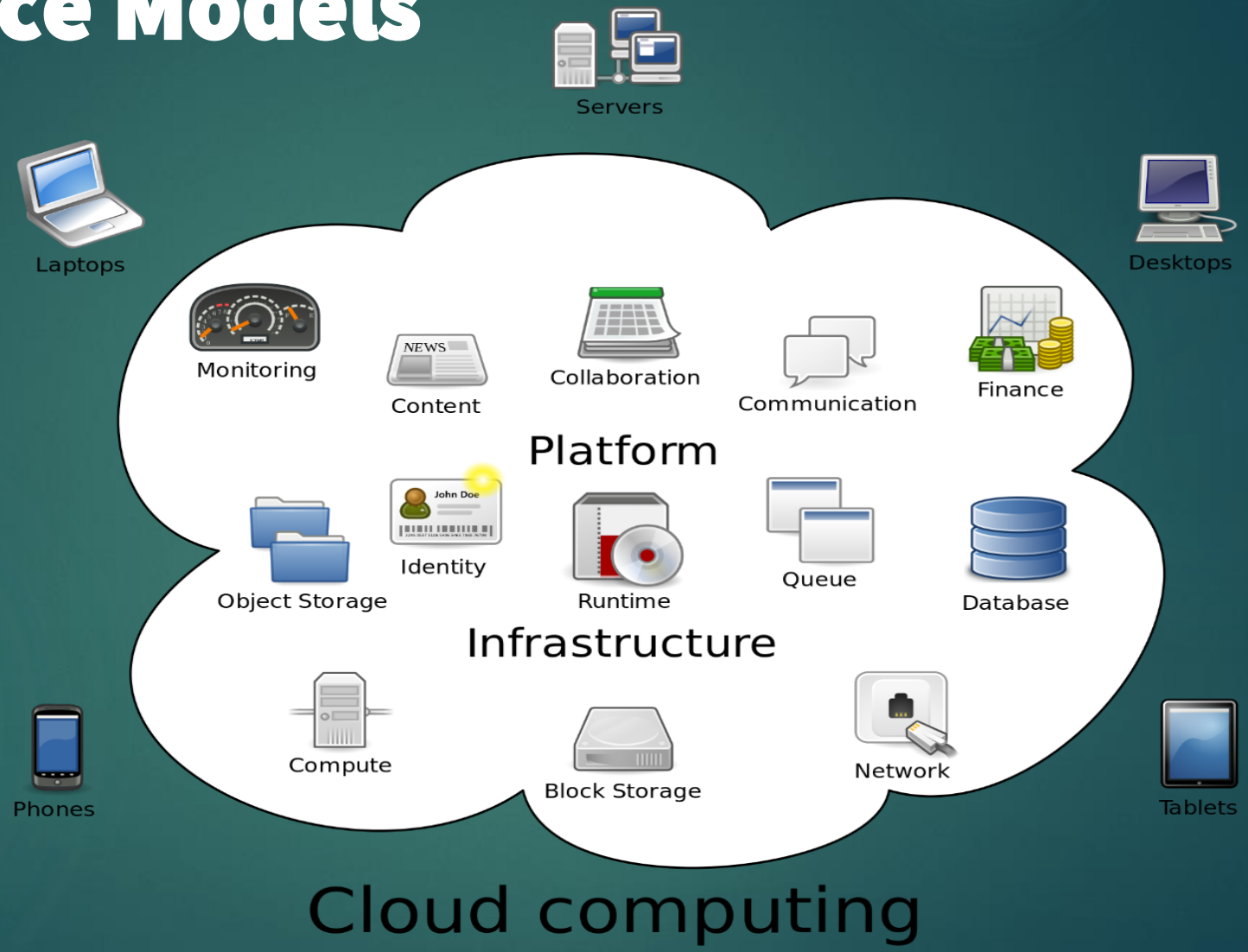
Pizza as a Service

Traditional On-Premises Deployment	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
Kitchen	Kitchen	DLLs	Kitchen
Oven	Oven	Tools	Oven
Gas	Gas	Runtime Environment	Gas
Pizza Dough	Pizza Dough	Database	Pizza Dough
Toppings	Toppings	Toppings	Toppings
Cook the Pizza	Cook the Pizza	Cook the Pizza	Cook the Pizza
Made In-House	Kitchen-as-a-Service	Create An App so users can order pizza	Pizza-as-a-Service

CYBRARY

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

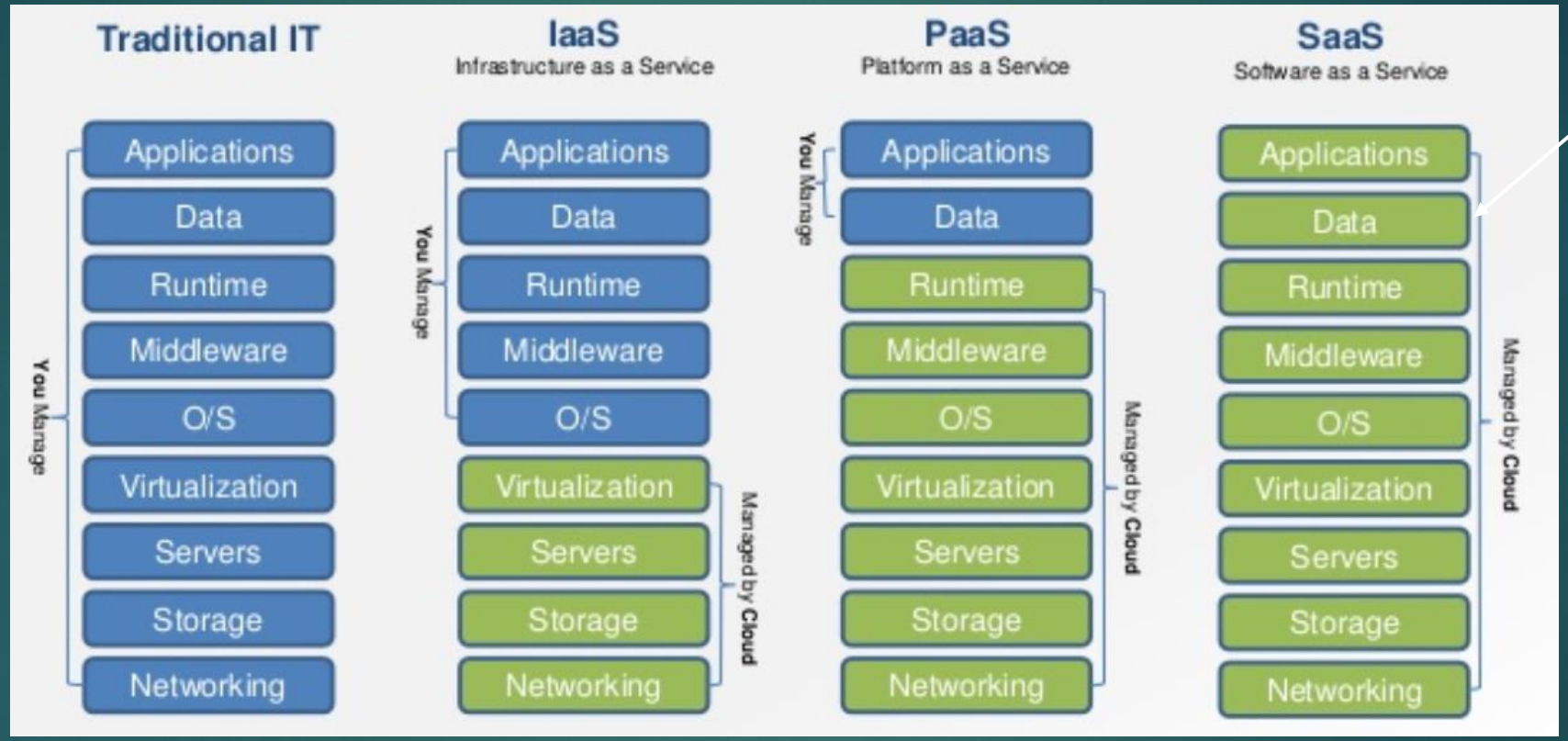
IaaS Offers:

- 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)

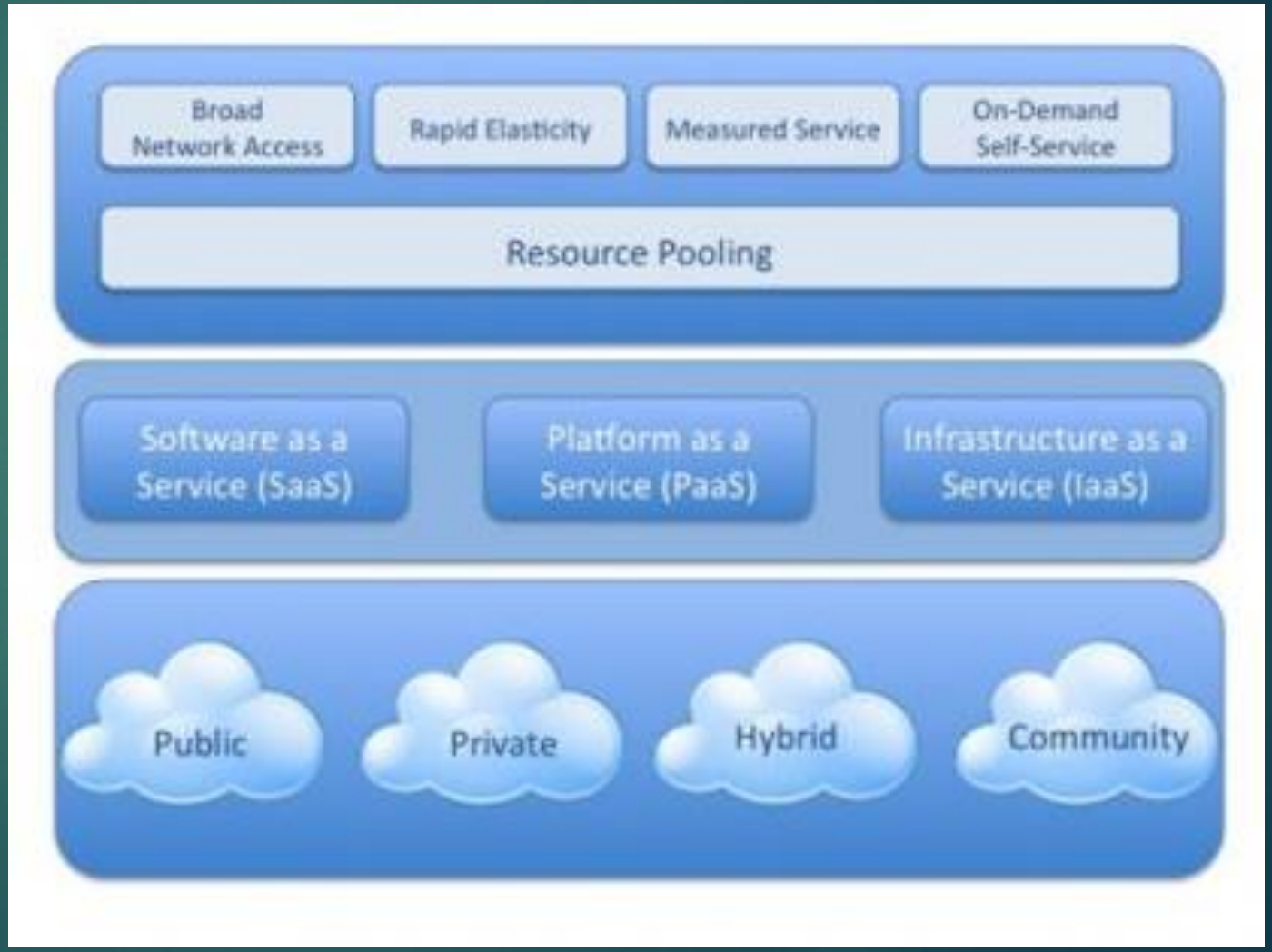
Management Responsibility



Even though data is *managed* by the CSP, data will always be the *responsibility of the owner*

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 alway 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

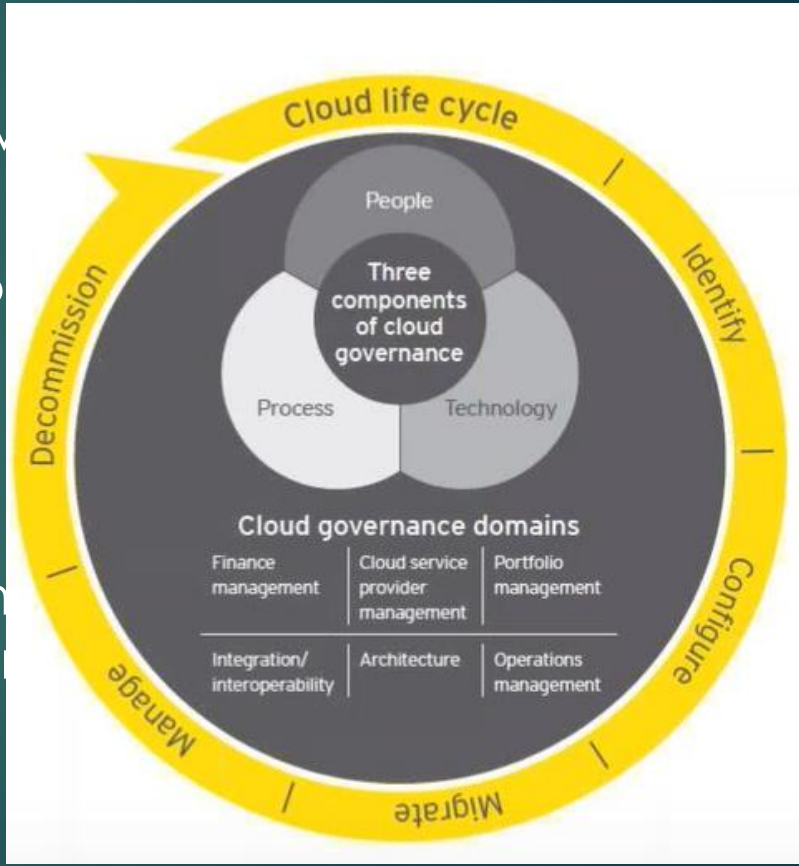
- Resiliency describes the ability to continue operating in the event of a disruption.
- Disruption could be caused by power outage, equipment failure, natural disaster, etc.
- Multiple layers of redundancy and fault tolerance must be in place
- Typically CSPs are capable of providing greater redundancy that 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 v performance
- Often an extension of existing organizational or traditio 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 gover



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

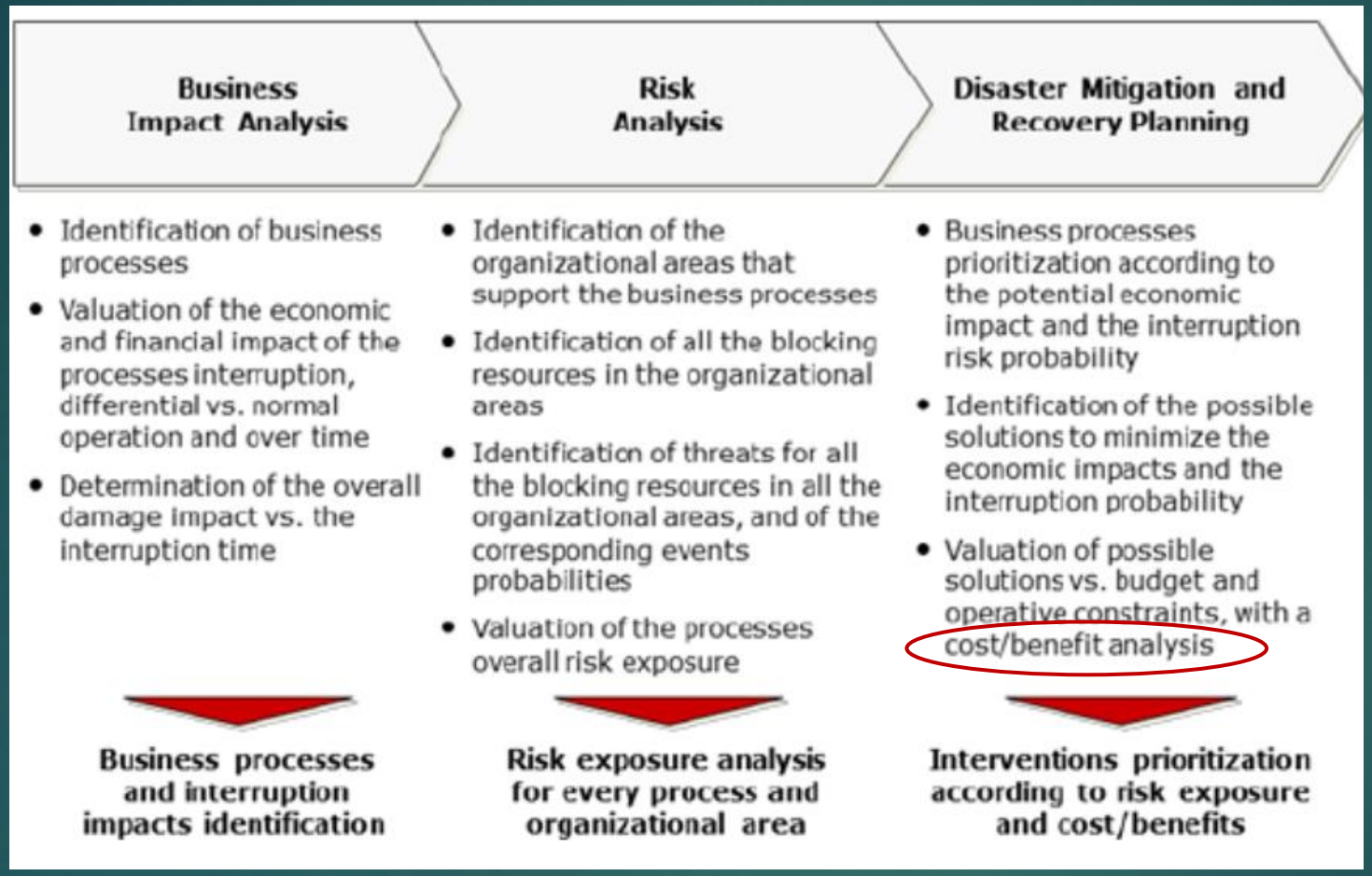
Valuation of Assets

- 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



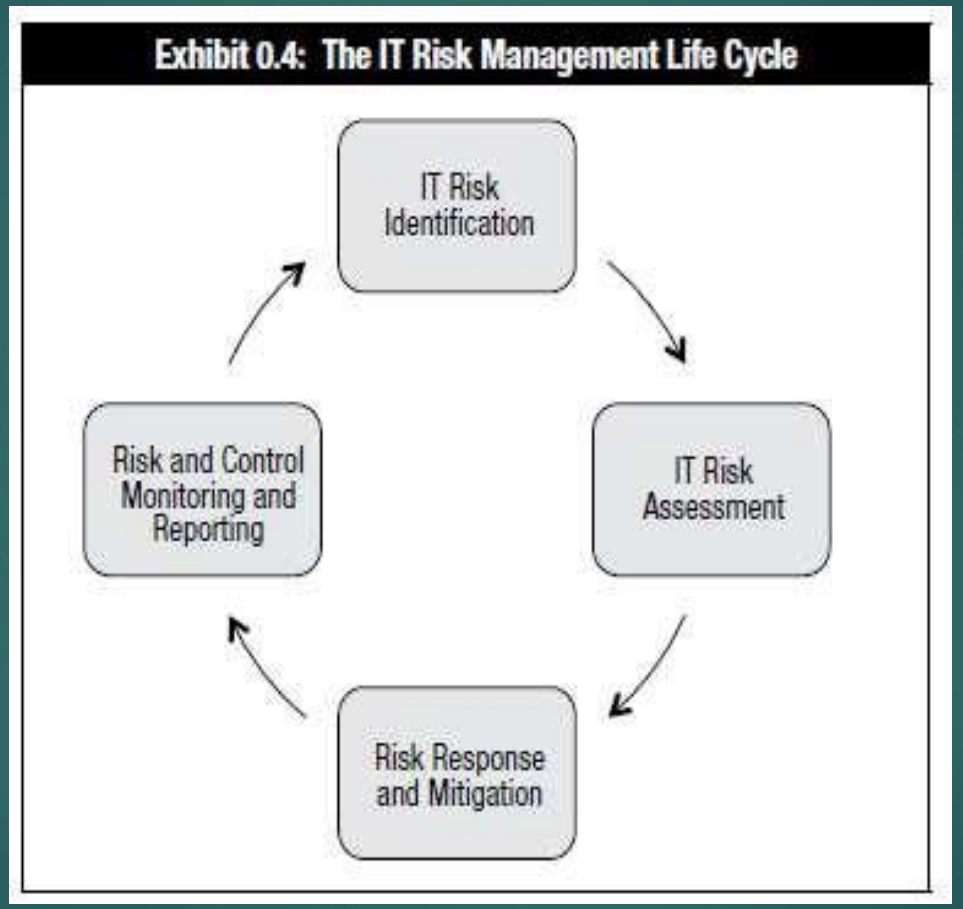
Risk Definitions

- **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

Risk Identification		Qualitative Rating				Quantitative Rating	Risk Response			
Risk Description	Risk Category	Probability	Impact	Risk Score	Risk Ranking	EMV (Expected Monetary Value)	Risk Response	Trigger (KRI--Key Risk Indicator)	Risk Owner	Status
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					

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

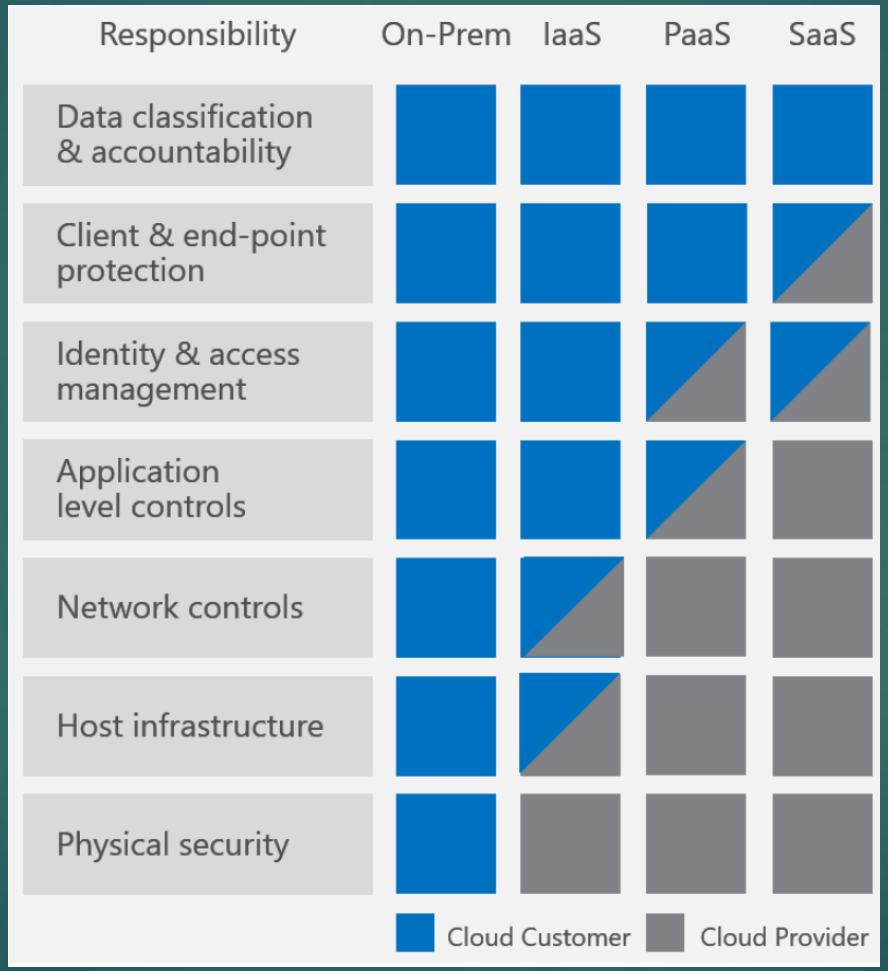
Boundaries: PaaS

- 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

Boundaries: SaaS

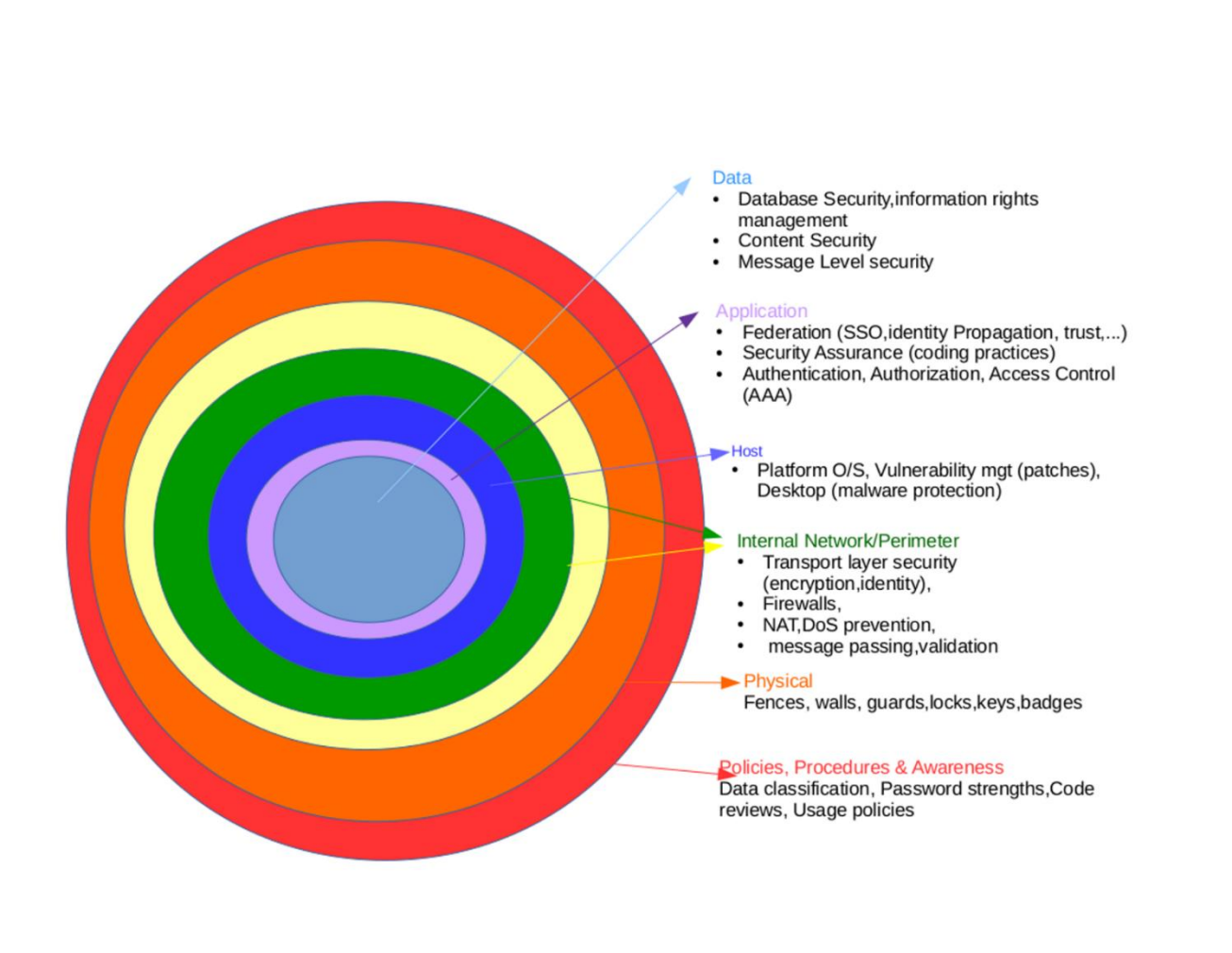
- CSP is responsible for:
  - Most elements of the environment
- Customer is responsible for
  - Identity and Access Management
  - Data

Boundary Summary



Defense in Depth

Defense in Depth



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

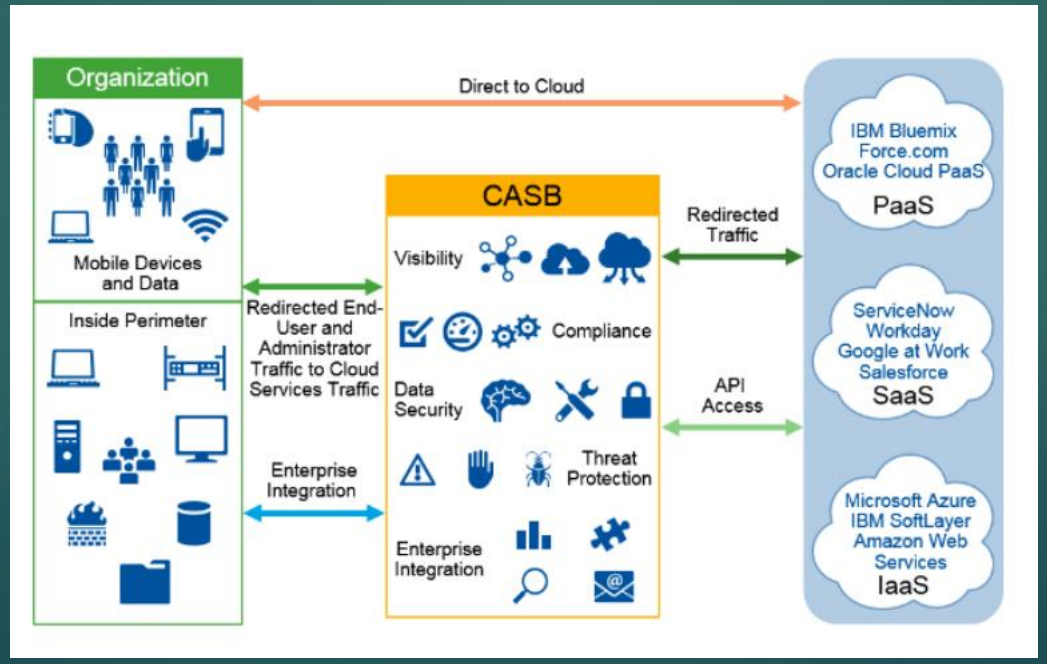
***Applies to virtual systems also

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

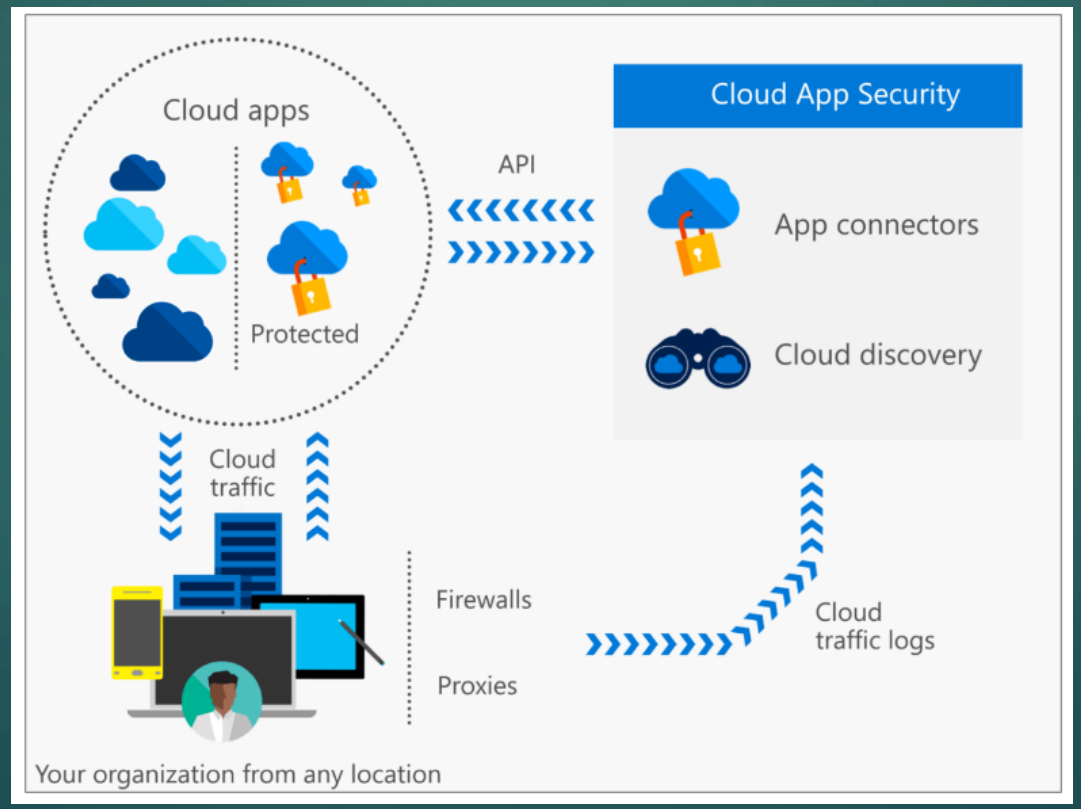
CASB (Cloud Access Security Brokers)

- 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

- 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 Lifecycle Security
- Data Inventory and Discovery
- 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 the means and the platform, and is considered to be the processor.

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

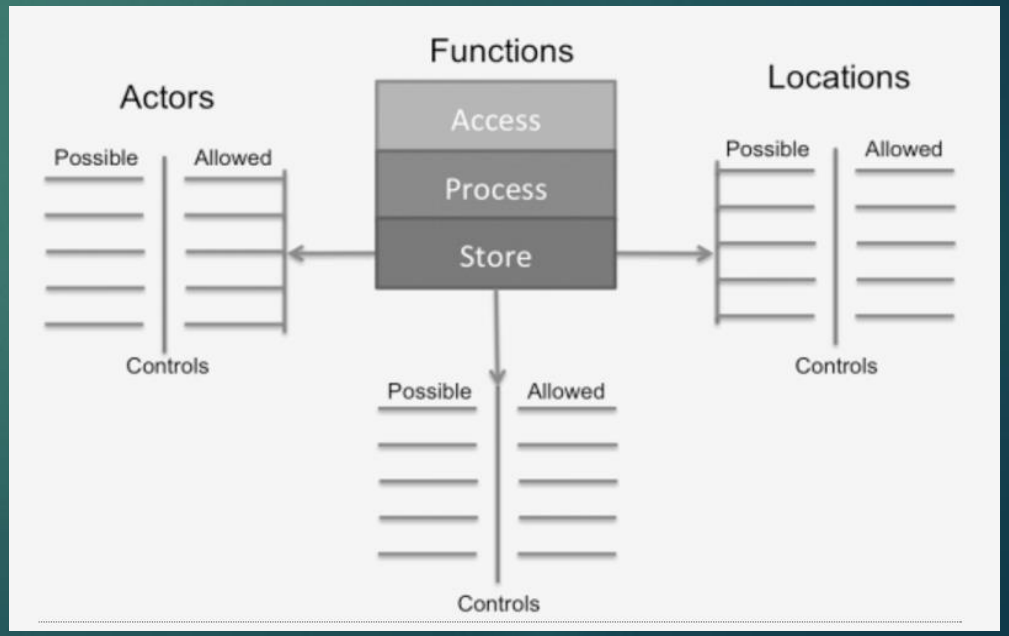
- Archival period is determined by policy
- Often policy is the result of external drivers such as legal requirements
- Certain Industries require data be retained for a certain time period
- At the end of the archival period, data should be destroyed across all locations in a manner consistent with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

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 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…	• 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…	• affect critical business decisions? • affect health and safety? • have a monetary impact? • have a reputational impact? • have a legal/regulatory impact?
Availability—Would nonavailability…	• have a reputational impact? • affect health and safety? • have a monetary impact? • have a legal/regulatory impact?

Source: https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2017/volume-5/doing-more-with-less_joa_eng_0917

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

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

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.
  - H*igh-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.

FIPS 200

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

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

NIST 800-53

CNTL NO.	CONTROL NAME *Control Enhancement Name*	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*					

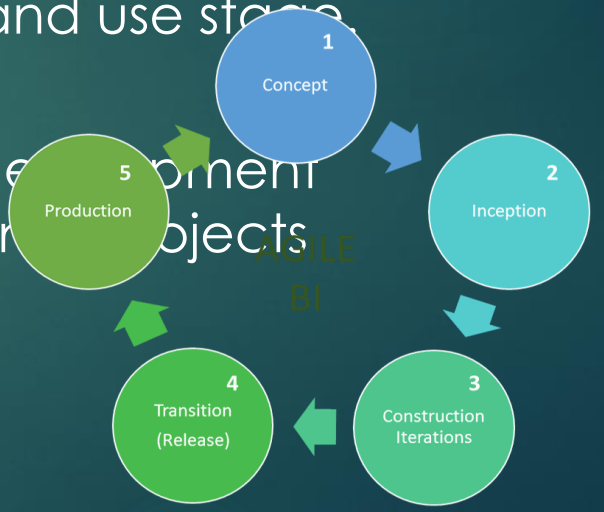
Data Discovery/Analytics

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 Analytics

- **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 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

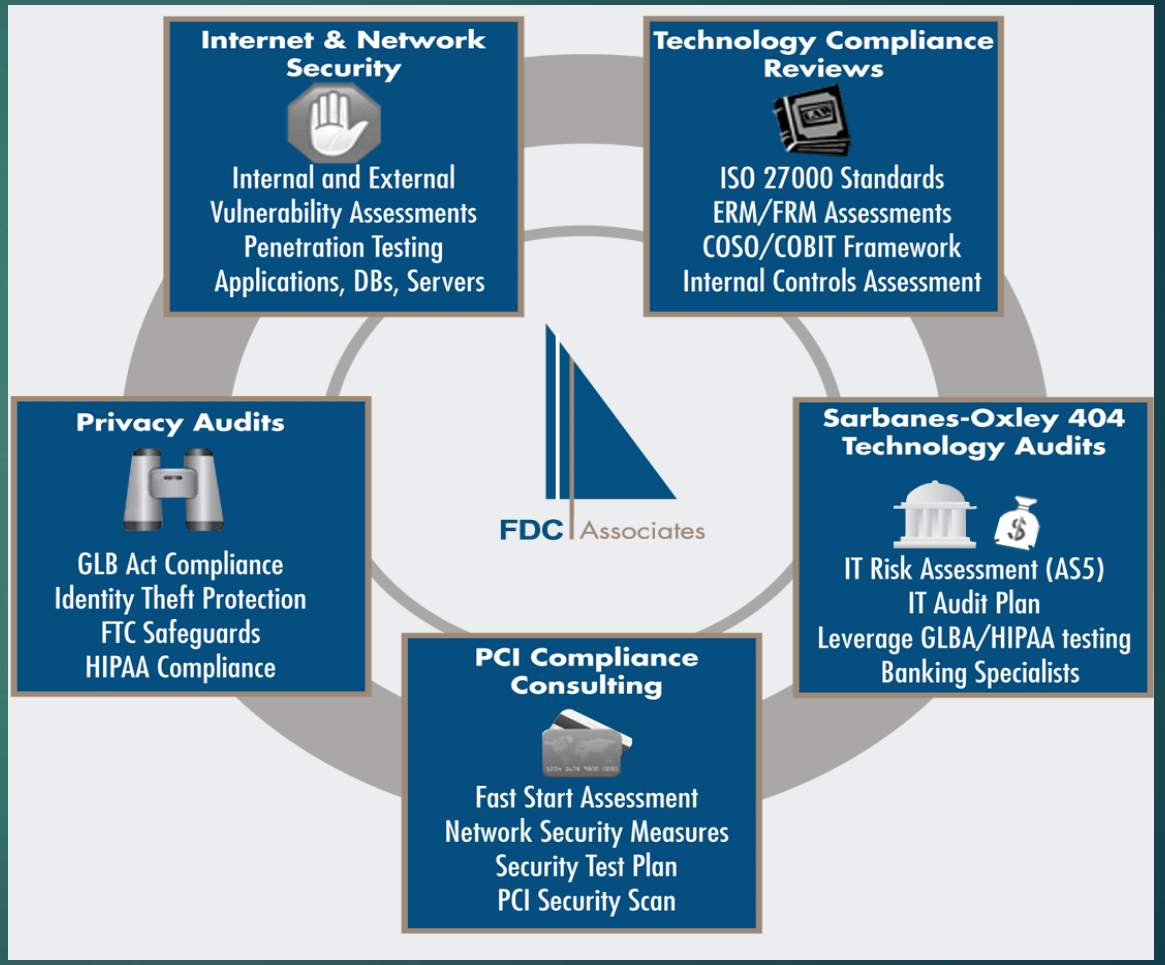
- Data retention: Established protocol for keeping information for operational or regulatory compliance needs.
- Cloud considerations:
  - Legal, regulatory and standards requirements must be well-documented and agreed upon
  - Data mapping should map all relevant data in order to understand formats, 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 productions 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



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

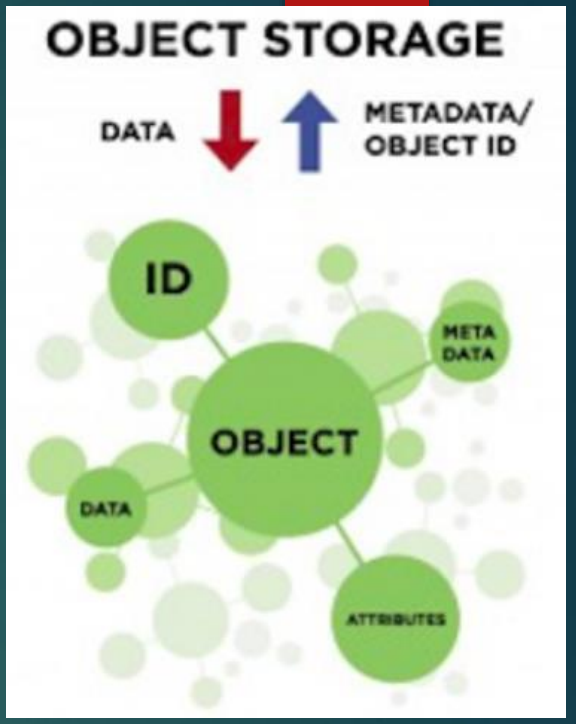
- United States
  - ITAR (International Traffic in Arms Regulation) Prohibits export of defense-related information
  - EAR (Export Administration Regulations) govern the export and re-export of items for reasons of national security, non-proliferation, foreign policy, and short supply. Covers civilian 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: IaaS—Object-Based Storage



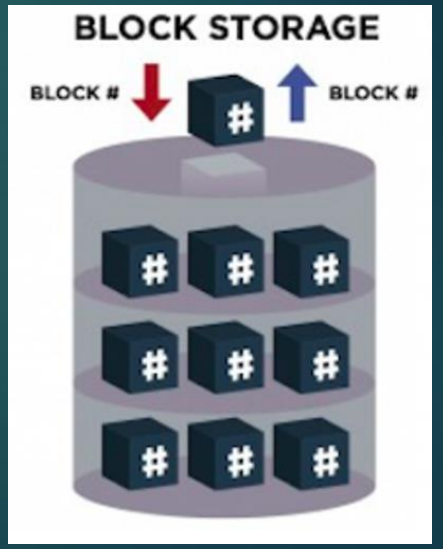
- Less common than block or file
- Objects go in "buckets" and buckets are accessed via an API
- Accessed by applications through APIs
- Relatively low performance/low-cost option
- Best for static content
- Extremely large amounts of storage available unstructured data
- **Particularly good for archival 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

Use Case for Object-Based Storage

- Storage of **unstructured data** like music, image, and video files.
- Storage for backup files, database dumps, and log files.
- Large data sets. Whether you're storing pharmaceutical or financial data, or multimedia files such as photos and videos, storage can be used as your **big data** object store.
- Archive files in place of local tape drives. Media assets such as **video footage** can be stored in object storage and archived to AWS glacier.

Storage Architectures: Block-Based

- Block storage is often configured to decouple the data from the user's environment and spread it across multiple environments that can better serve the data. And then, when data is requested, the underlying storage software reassembles the blocks of data from these environments and presents them back to the user. It is usually deployed in storage-area network (SAN) environments and must be tied to a functioning server.
- **Because block storage doesn't rely on a single path to data—like file storage does—it can be retrieved quickly**.
- Each is independent and can be partitioned so it can be accessed in a different operating system, which gives the user complete freedom to configure their data
- Downsides:
  - Block storage can be expensive.
  - Limited capability to handle metadata

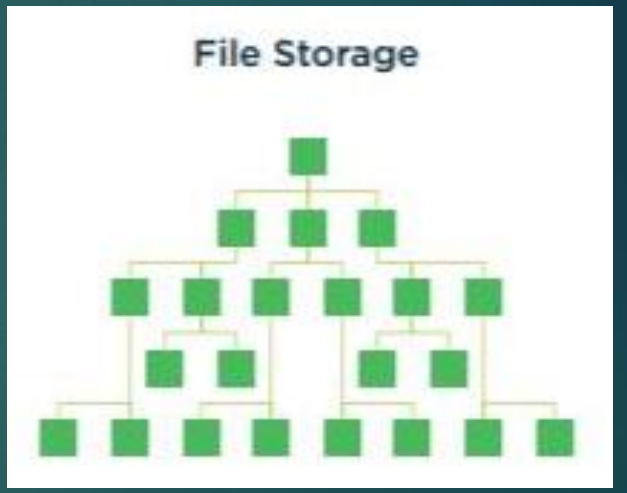


Uses for Block-Based Storage

- **Ideal for databases**, since a DB requires consistent I/O performance and low-latency connectivity.
- Use block storage for **RAID Volumes**, where you combine multiple disks organized through stripping or mirroring.
- Any application which requires **service side processing**, like Java, PHP, and .Net will require block storage.
- Running **mission-critical** applications like Oracle, SAP, Microsoft Exchange, and Microsoft SharePoint.

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: IaaS

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 or 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

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.

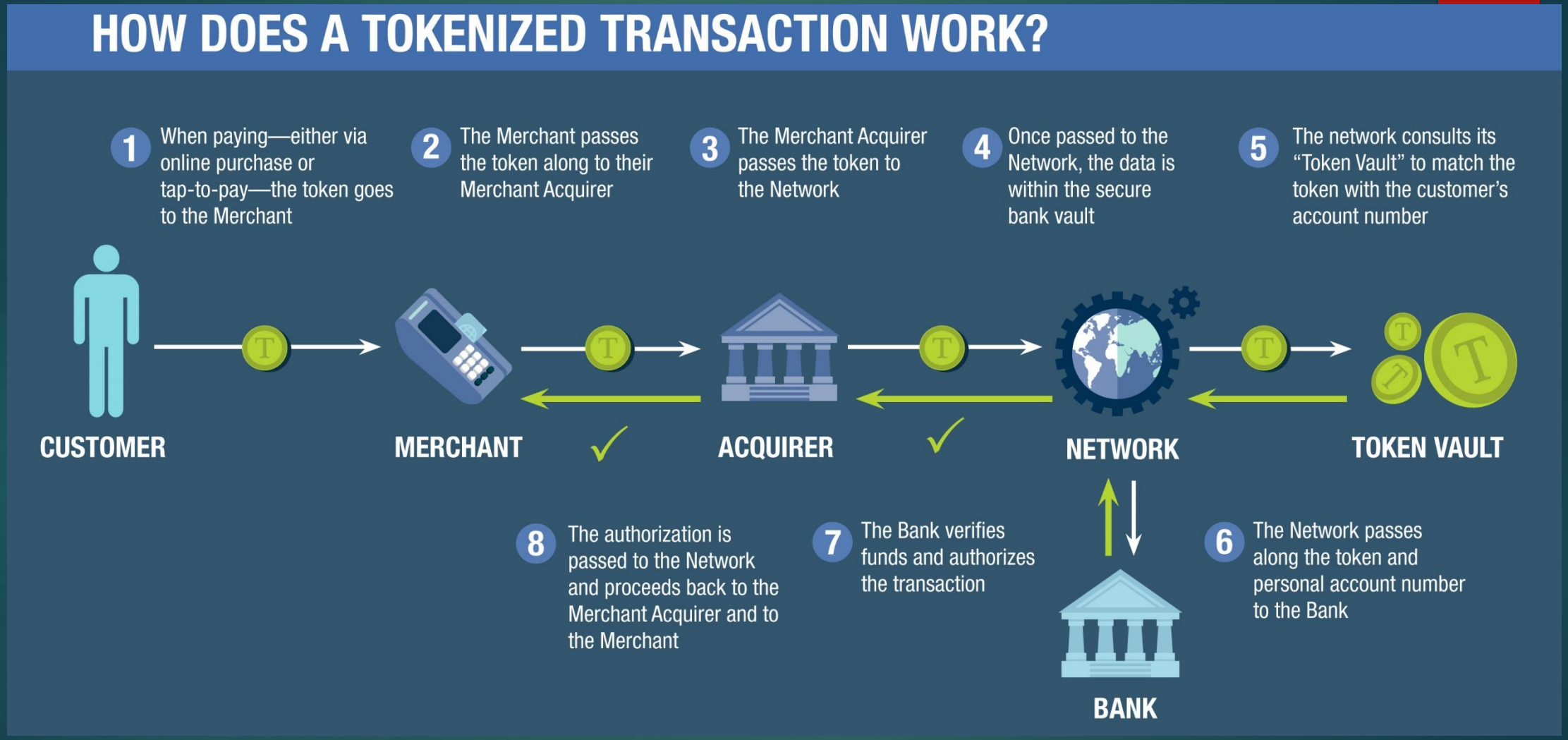
Encryption Best Practices

- 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



Monitoring: Security and Event Management

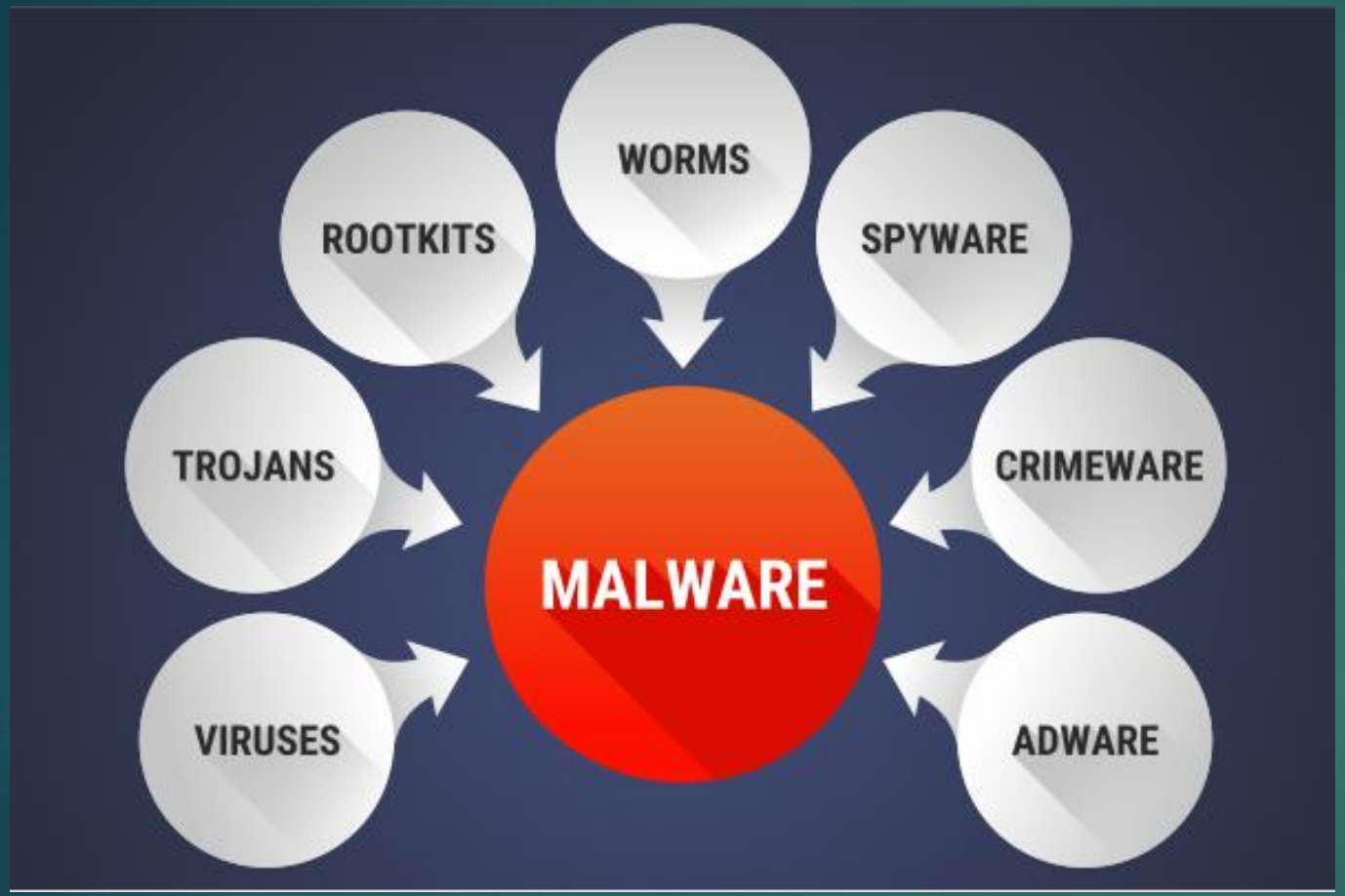
- Software and products combining security information management and event management. It provides real-time analysis of security alerts generated by network hardware and applications. SEIM Systems often provide:
  - Aggregation from many sources and correlation across common attributes
  - Alerting 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



Scan

Scans your system for any known threats, then gives you information about the found threats and removes them for you.

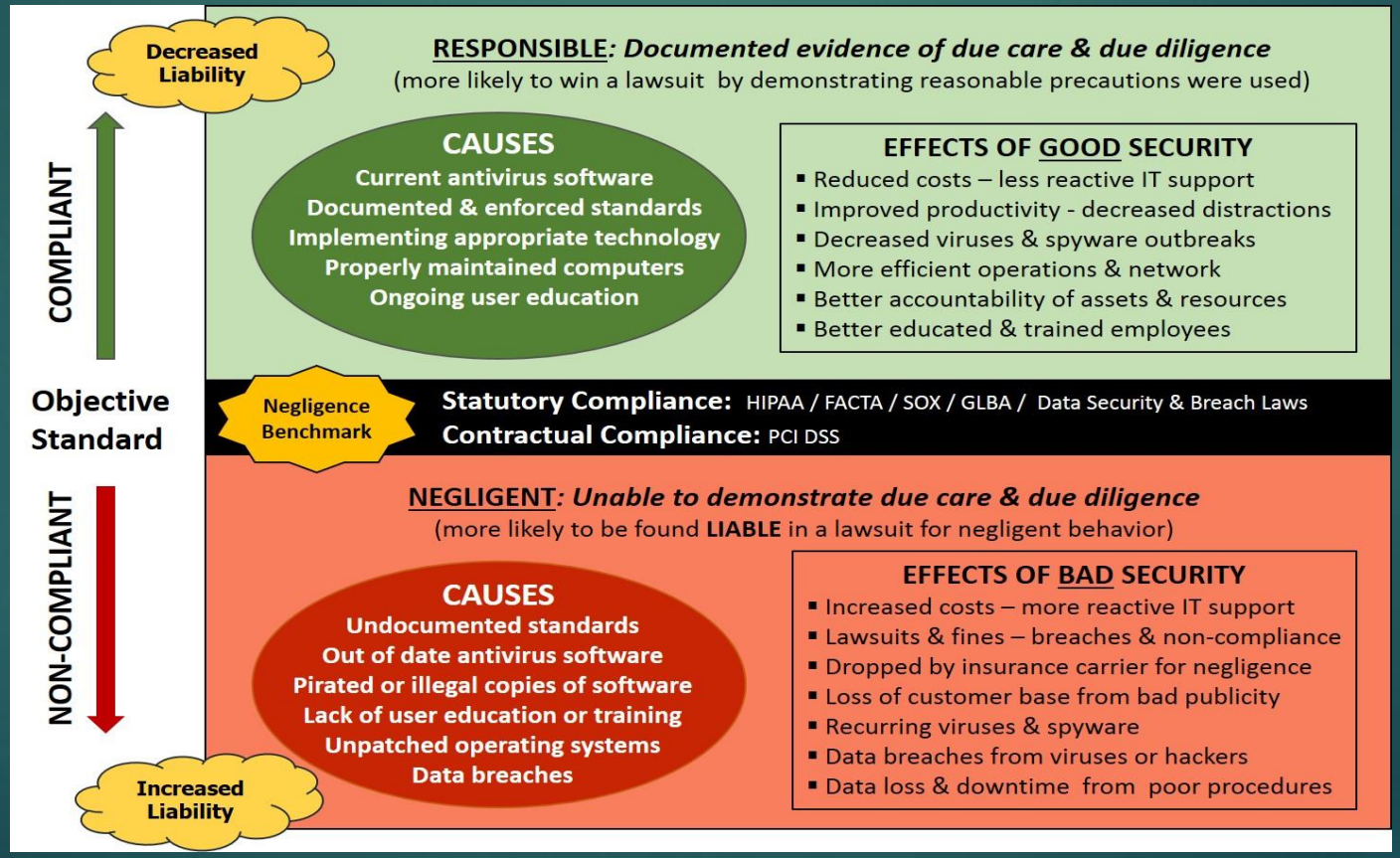
Next Steps

Additional resources if your problem has not been solved after scanning and removing anything found.

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 polices, 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"
  - Data Breaches: Disclosure
  - Data Loss: Loss of integrity or destruction
  - Account or Service Hijacking: Attacker sniffing or MITM
  - Insecure Interfaces/APIs: provided by vendors to access their networks
  - DoS or DDos
  - Malicious insiders
  - Abuse of cloud services: Inherent weakness of any internet service
  - Insufficient Due Diligence/Due Care
    - Due diligence investigating and understanding risks
    - Due care: Developing policies and procedures to address risks
  - Shared Technology Vulnerabilities: multiple tenants brings in risks