



Welcome to CCSP (Certified Cloud Security Professional)

Kelly Handerhan, Instructor



Welcome!

- Your Instructor, Kelly Handerhan
- KellyH@CyberTrain.IT
- Over twenty years experience in Information Systems, Information Assurance, and Cybersecurity
- CCSP, CISSP, CASP, Security+, PMP, CRISC, CISM
- One of the original instructors for Cybrary.it
- Owner and lead technical instructor and instructional designer for www.CyberTrain.IT





Before we get started.....

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



Domain 0

Course Introduction and Exam Specifics

Pre-Assessment Quiz

1. What type of solutions enable enterprises or individuals to store their data and computer files on the Internet using a storage service provider rather than storing the data locally on a physical disk, such as a hard drive or tape backup?
 - A. Online backups
 - B. Cloud backup solutions
 - C. Removable hard drives
 - D. Masking

2. When using an Infrastructure as a Service (IaaS) solution, what is the key benefit for the customer?
 - A. Scalability
 - B. Metered service
 - C. Energy and cooling efficiencies
 - D. Transfer of ownership cost

3. focuses on security and encryption to prevent unauthorized copying and limitations on distribution to only those who pay.
 - A. Digital rights management (DRM)
 - B. Enterprise digital rights management
 - C. Bit splitting
 - D. Degaussing

4. Which of the following represents the correct set of four cloud deployment models?
 - A. Public, Private, Joint and Community
 - B. Public, Private, Hybrid, and Community
 - C. Public, Internet, Hybrid, and Community
 - D. External, Private, Hybrid, and Community

5. What is a special mathematical code that allows encryption hardware/software to encode and then decipher an encrypted message called?
 - A. PKI
 - B. Encryption key
 - C. Public key
 - D. Masking

6. Which of the following lists the correct six components of the STRIDE threat model?
 - A. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege
 - B. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Social Engineering Elasticity

C. Spoofing, Tampering, Repudiation, Information Disclosure, Distributed Denial of Service, and Elevation of Privilege

D. Spoofing, Tampering, Nonrepudiation, Information Disclosure, Denial of Service, and Elevation of Privilege

7. What is the term for the assurance that a specific author actually created and sent a specific

item to a specific recipient, and that the message was successfully received?

A. PKI

B. DLP

C. Nonrepudiation

D. Bit splitting

8. What is the correct term for the process of deliberately destroying the encryption keys used

to encrypt data?

A. Poor key management

B. PKI

C. Obfuscation

D. Crypto-shredding

9. In a federated environment, who is the relying party, and what do they do?

A. The relying party is the service provider and they would consume the tokens generated by the identity provider.

B. The relying party is the service provider and they would consume the tokens generated by the customer.

C. The relying party is the customer and they would consume the tokens generated by the identity provider.

D. The relying party is the identity provider and they would consume the tokens generated by the service provider.

10. What is the process of replacing sensitive data with unique identification symbols that retain all the essential information about the data without compromising its security?

A. Randomization

B. Elasticity

C. Obfuscation

D. Tokenization

11. Which of the following data storage types are associated or used with Platform as a Service (PaaS)?

A. Databases and Big Data

B. SaaS application

C. Tabular

D. Raw and block

12. What is the term used for software technology that encapsulates application software from

the underlying operating system on which it is executed?

- A. Hypervisor**
- B. Application virtualization**
- C. VMWare**
- D. SaaS**

13. Which of the following represents the legislation enacted to protect shareholders and the

public from enterprise accounting errors and fraudulent practices?

- A. PCI**
- B. Gramm-Leach-Bliley Act (GLBA)**
- C. Sarbanes-Oxley Act (SOX)**
- D. HIPAA**

14. What is a device called that can safely store and manage encryption keys and is used in servers, data transmission, and log files?

- A. Private key**
- B. Hardware security module (HSM)**
- C. Public key**
- D. Trusted Operating System Module (TOS)**

15. What is a type of cloud infrastructure that is provisioned for open use by the general public

and is owned, managed, and operated by a business, academic, or government organization and exists on the premises of the cloud provider called?

- A. Private cloud**
- B. Public cloud**
- C. Hybrid cloud**
- D. Personal cloud**

16. When using transparent encryption of a database, where does the encryption engine reside?

- A. Within the database application itself**
- B. At the application using the database**
- C. On the instances attached to the volume**
- D. In a key management system**

17. What is a type of assessment called that employs a set of methods, principles, or rules for

assessing risk based on non-numerical categories or levels?

- A. Quantitative assessment**
- B. Qualitative assessment**
- C. Hybrid assessment**
- D. SOC 2**

18. What best describes the Cloud Security Alliance Cloud Controls Matrix?

- A. A set of regulatory requirements for cloud service providers**
- B. A set of software development life cycle requirements for cloud service providers**
- C. A security controls framework that provides mapping/cross relationships with the main industry-accepted security standards, regulations, and controls frameworks such as the ISO 27001/27002, ISACA's COBIT, and PCI-DSS**
- D. An inventory of cloud security controls that are arranged into separate security domains**

19. When a conflict of laws occurs, determines the jurisdiction in which the dispute will be heard.

- A. Tort law**
- B. Doctrine of Proper Law**
- C. Common law**
- D. Criminal law**

20. Which one of the following is the *most* important security consideration when selecting a new computer facility?

- A. Local law enforcement response times**
- B. Location adjacent to competitor's facilities**
- C. Aircraft flight paths**
- D. Utility infrastructure**

21. Which of the following is *always* safe to use in the disposal of electronic records within a cloud environment?

- A. Physical destruction**
- B. Overwriting**
- C. Encryption**
- D. Degaussing**

22. Which of the following describes a SYN flood attack?

- A. Rapid transmission of Internet Relay Chat (IRC) messages**
- B. Creating a high number of partially open TCP connections**
- C. Disabling the Domain Name Service (DNS) server**
- D. Excessive list linking of users and files**

23. Which of the following is an example of a form of cloud storage that applies to storing an

individual's mobile device data in the cloud and providing the individual with access to the data from anywhere?

- A. Raw storage
- B. Flash storage
- C. Obfuscation archiving
- D. Mobile cloud storage

24. Which of the following terms best describes a distributed model where software applications

are hosted by a vendor or cloud service provider and made available to customers over network resources?

- A. Infrastructure as a Service (IaaS)
- B. Public cloud
- C. Software as a Service (SaaS)
- D. Private cloud

25. Which of the following is a federal law enacted in the United States to control the way that

financial institutions deal with private information of individuals?

- A. PCI
- B. ISO/IEC
- C. Gramm-Leach-Bliley Act (GLBA)
- D. Consumer Protection Act

26. The typical function of Secure Sockets Layer (SSL) in securing Wireless Application Protocol

(WAP) is to protect transmissions that exist:

- A. Between the WAP gateway and the wireless endpoint device
- B. Between the web server and the WAP gateway
- C. From the web server to the wireless endpoint device
- D. Between the wireless device and the base station

27. What is an accounting report on controls at a service organization that replaces older SAS70 type reports?

- A. SOC 1
- B. SSAE16
- C. GAAP
- D. SOC 2

28. What is a company that purchases hosting services from a cloud server hosting or cloud computing provider who then resells to its own customers?

- A. Cloud broker
- B. Cloud computing reseller
- C. Cloud proxy

D. VAR

29. What is a type of computing comparable to grid computing that relies on sharing computing

resources rather than having local servers or personal devices to handle applications?

A. Server hosting

B. Legacy computing

C. Cloud computing

D. Intranet

30. What is a set of technologies designed to analyze application source code and binaries for

coding and design conditions that are indicative of security and vulnerabilities?

A. Dynamic application security testing (DAST)

B. Static application security testing (SAST)

C. Secure coding

D. OWASP

Answers to Pre-Assessment Quiz

- 1.** B. Cloud backup solutions enable enterprises to store their data and computer files on the Internet using a storage service rather than storing data locally on a hard disk or tape backup. This has the added benefit of providing access to data should the primary business location be damaged in some way that prevents accessing or restoring data locally due to damaged infrastructure or equipment. Online backups and removable hard drives are other options but do not by default supply the customer with ubiquitous access. Masking is a technology used to partially conceal sensitive data.
- 2.** D. The primary benefit to the customer of using Infrastructure as a Service (IaaS) is the transfer of cost of ownership. In a cloud environment, the customer uses and is billed only for what they use as opposed to the full cost of implementation, saving them a significant amount in terms of cost of ownership. While scalability, metered service, and energy and cooling efficiencies are a part of the benefit of a cloud computing environment, they are not the primary benefit or business driver behind IaaS adoption.
- 3.** A. Digital rights management (DRM) was designed to focus on security and encryption as a means of preventing unauthorized copying and limitations on distribution of content to only those authorized (purchasers). Enterprise digital rights management, also known as information rights management (IRM), is a subset of DRM and typically refers to businesses to business securing of information rights. Bit splitting is a method of hiding information across multiple geographical boundaries, and degaussing is a method of deleting data permanently from magnetic media.
- 4.** B. The only correct answer for this is Public, Private, Hybrid, and Community. Joint, Internet, and External are not cloud models.
- 5.** B. An encryption key is just that: a key used to encrypt and decrypt information. It is mathematical code that supports either hardware- or software-based encryption used to encode or decode information.
- 6.** A. The letters in STRIDE threat model represent **S**poofing of identity, **T**ampering with data, **R**epudiation, **I**nformation disclosure, **D**enial of service, and **E**levation of privilege. The other options are simply mixed up or incorrect versions of the same.
- 7.** C. Nonrepudiation means that a specific author or user cannot refute or repudiate that he or she created and/or sent a message and the receiver of the data or message cannot deny they received it.
- 8.** D. The act of crypto-shredding means destroying the key that was initially used to encrypt the data, thereby making it forever unrecoverable.
- 9.** A. The identity provider would hold all of the identities and generate a token for known users. The relying party (RP) would be the service provider and would consume the tokens. All other answers are incorrect.
- 10.** D. Replacing sensitive data with unique identification symbols is known as tokenization, a simple and only somewhat effective way of hiding or concealing sensitive data with the
- xxx** Answers to Assessment Test

replacement of unique identification symbols. It is not considered as strong as encryption but can be effective in keeping prying eyes off of sensitive information. While randomization

and obfuscation are also means of concealing information, they are done quite differently.

11. A. PaaS uses databases and Big Data storage types.

12. B. Application virtualization encapsulates application software from the underlying operating system on which it is executed.

13. C. The Sarbanes-Oxley Act (SOX) was enacted in response to the 2000 accounting scandal

that caused the bankruptcy of Enron. At that time, top executives laid the claim that they were unaware of the accounting practices that led to the company's demise. SOX not only forces executives to oversee all accounting practices, but holds them accountable should such activity occur again.

14. B. A hardware security module is a device that can safely store and manage encryption keys. These can be used in servers, workstations, and so on. Once common type is called the Trusted Platform Module (TPM) and can be found on enterprise workstations and laptops. There is no such term as a trusted operating system, and public and private keys are terms used with PKI.

15. B. This is the very definition of public cloud computing.

16. A. In transparent encryption, the encryption key for a database is stored in the boot record of the database itself.

17. B. A qualitative assessment is a set of methods or rules for assessing risk based on nonmathematical or categories or levels. One that uses those mathematical categories or levels is called a quantitative assessment. There is no such thing as a hybrid assessment, and an SOC 2 is an accounting report regarding control effectiveness.

18. C. The CCM cross-references many industry standards, laws, and guidelines.

19. B. The Doctrine of Proper Law is used when a dispute occurs over which jurisdiction will

hear a case. Tort law refers to civil liability suits. Common law refers to laws regarding marriage, and criminal law refers to violations of state or federal criminal code.

20. D. Of the answers given, option D is the most important. It is vital that any datacenter facility be close to sound facility resources such as power, water, and connectivity.

21. C. Encryption can always be used in a cloud environment, but physical destruction, overwriting,

and degaussing may not be available due to access and physical separation factors.

22. B. A SYN flood is where a TCP connection attempt is made and then cut short just prior to

completion, thereby leaving a server waiting for a response. If enough of these connection attempts are made, a "flood" occurs, causing the end unit to consume resources to the point that either services and/or the system itself become unavailable for use. The other options have no connection with a flood of any kind.

Answers to Assessment Test **xxxii**

23. D. Mobile cloud storage is defined as a form of cloud storage that applies to storing an individual's

mobile device data in the cloud and providing the individual with access to the data from anywhere.

24. C. This is the definition of the Software as a Service (SaaS) service model. Public and private

are cloud deployment models, and Infrastructure as a Service (IaaS) does not provide applications of any type.

25. C. The Gramm-Leach-Bliley Act targets U.S. financial institutions and requires them to deal specifically with protecting account holders' private information. PCI refers to credit card processing requirements, ISO/IEC is a standards organization, and the Consumer Protection

Act, while providing oversight for the protection of consumer private information, is limited in scope.

26. C. The purpose of SSL is to encrypt the communication channel between two end points. In this example, it is the end user and the server.

27. A. The correct answer is the SOC 1 report, which is designed to assess the controls primarily

revolving around financial reporting, formerly found in the SAS 70. The SOC 2 is a report that provides information related to one or more of the AICPA five security principles.

28. B. The cloud computing reseller purchases hosting services and then resells them.

29. C. Cloud computing is built on the model of grid computing whereby resources can be pooled and shared rather than having local devices do all the compute and storage functions.

30. B. Static application security testing (SAST) differs from dynamic application security testing (DAST) in that it looks at source code and binaries to see if it can detect problems before the code is loaded into memory and run.



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



Exam Requirements

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 of experience in one of the six (6) domains of the CCSP examination. Earning the [CISSP 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](#).

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

- Submit the [examination fee](#)
- Understand the experience requirements discussed above 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 prequalification questions regarding [criminal history and related background](#)



Exam Specifics

CCSP Exam Information

Length of exam	4 hours
Number of questions	125
Question format	Multiple choice
Passing grade	700 out of 1000 points
Exam Language	English
Testing center	<u>Pearson Vue Testing Center</u>



Domain 1

Architectural Concepts and Design Requirements



Remember the CISSP...

- Many answers are similar, or would work. Answer the most inclusive answer that is still correct.
- Think “End Game”
- Think long term solution
- All decisions start with risk management. Risk management starts with Determining the value for your assets.
- “Most” “Best” “Least”
- “Security Transcends Technology”
- Know your facts
- Layered Defense



Domain 1 Overview

Architectural Concepts and Design Requirements

- Drivers for Cloud Computing
- Frameworks for Cloud Computing
- Characteristics of Cloud Computing
- Service Models
- Deployment Models
- Roles
- Secure Design Principles
- Secure Lifecycle principles
- Certification



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

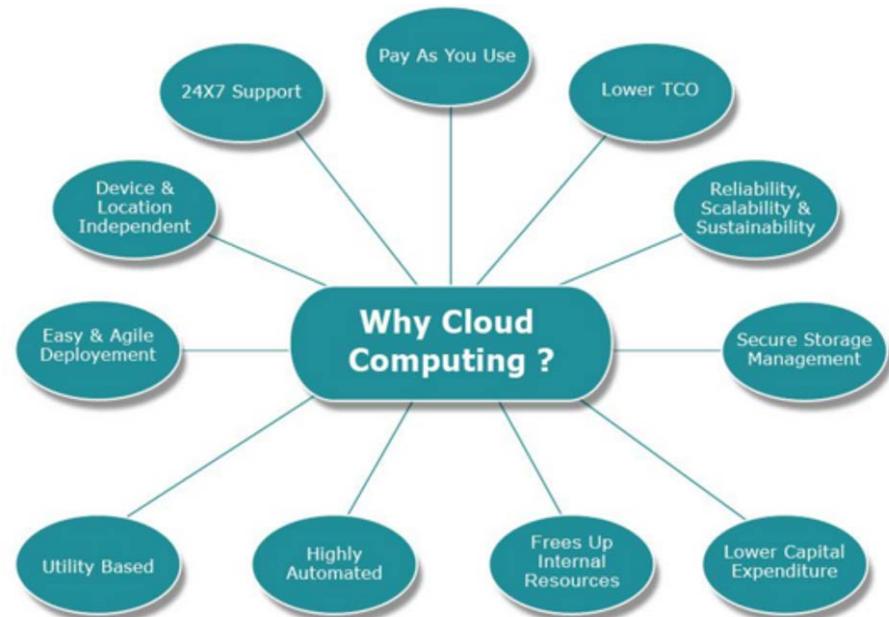
- “Cloud computing is a model for enabling ubiquitous, convenient on-demand network access to a shared pool of configurable computing resources (e.g., networks, server, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider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

--NIST Definition of Cloud Computing



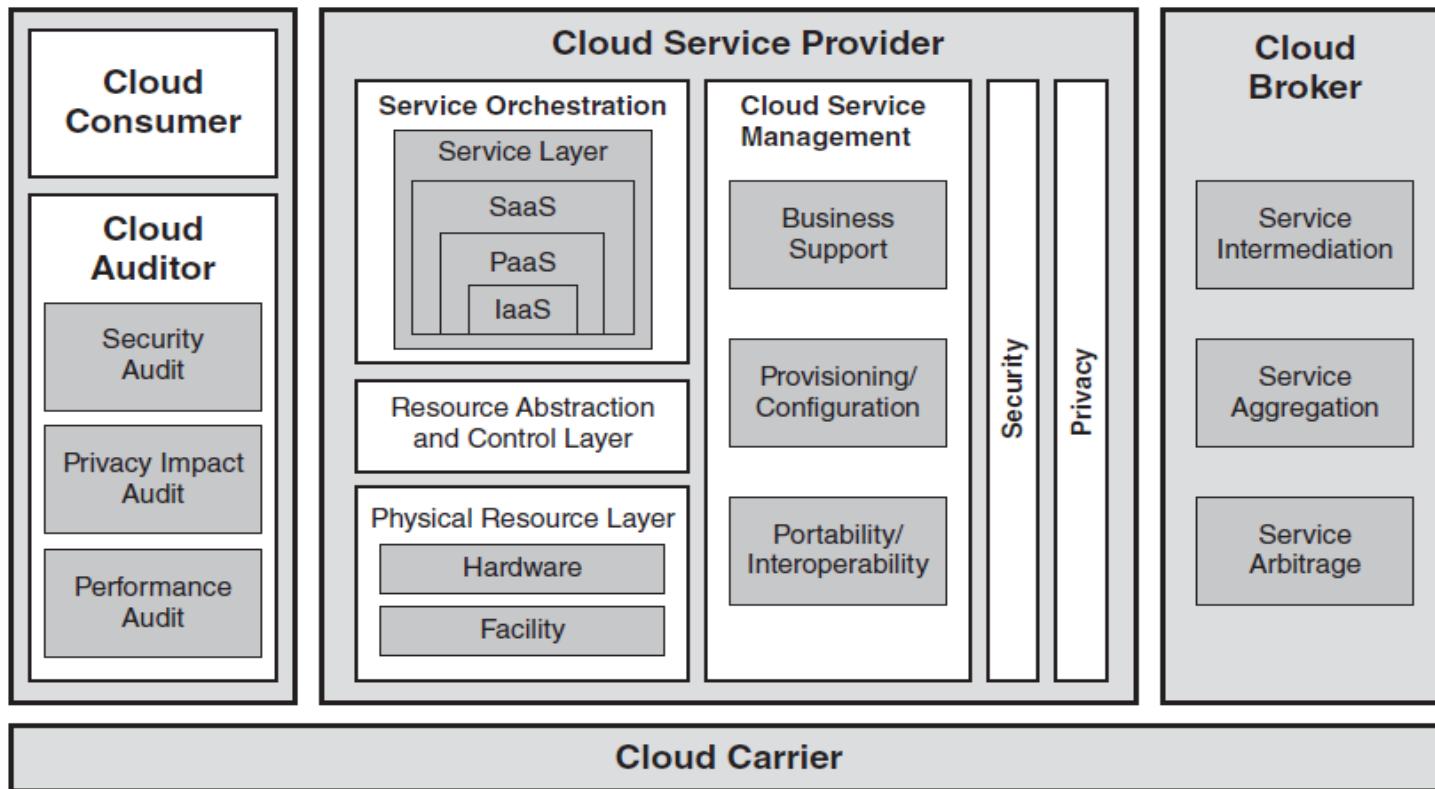
Cloud Drivers

- Scalability
- Mobility
- Elasticity
- Cost-Savings
- Risk Transference/Reduction
- Reduced Infrastructure
- Less Overhead
- Pay as you go
- Shifting Capital Expenditure to Operational Expenditure
 - Allows company to match capacity to need, as well as pay as they go (monthly) for only the services that they use





Cloud Computing





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)



Security Risks

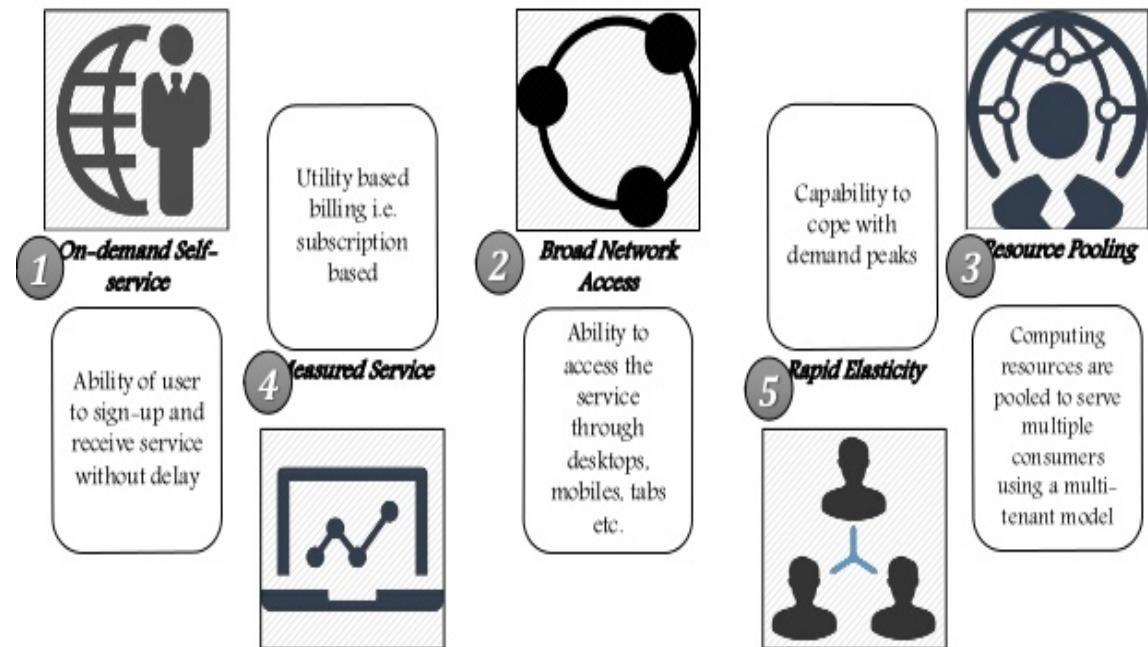
- Distributed
 - Laws vary from jurisdiction to jurisdiction
- Multitenant
 - Shared physical resources make incident response, forensics, destruction, etc difficult
- Responsibility cannot be transferred
 - Customer is still legally liable for protection of the resource—DATA OWNER MAINTAINS RESPONSIBLE IN ALL CLOUD MODELS
- Privacy
 - The degree of privacy enforcement must be specified in SLA
- CSA may have higher requirements than the enterprise



NIST's 5 Key Requirements of Cloud Computing

- On-demand self-service
- Broad network Access
- Resource pooling
- Rapid elasticity
- Measured Service

ESSENTIAL CHARACTERISTICS



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

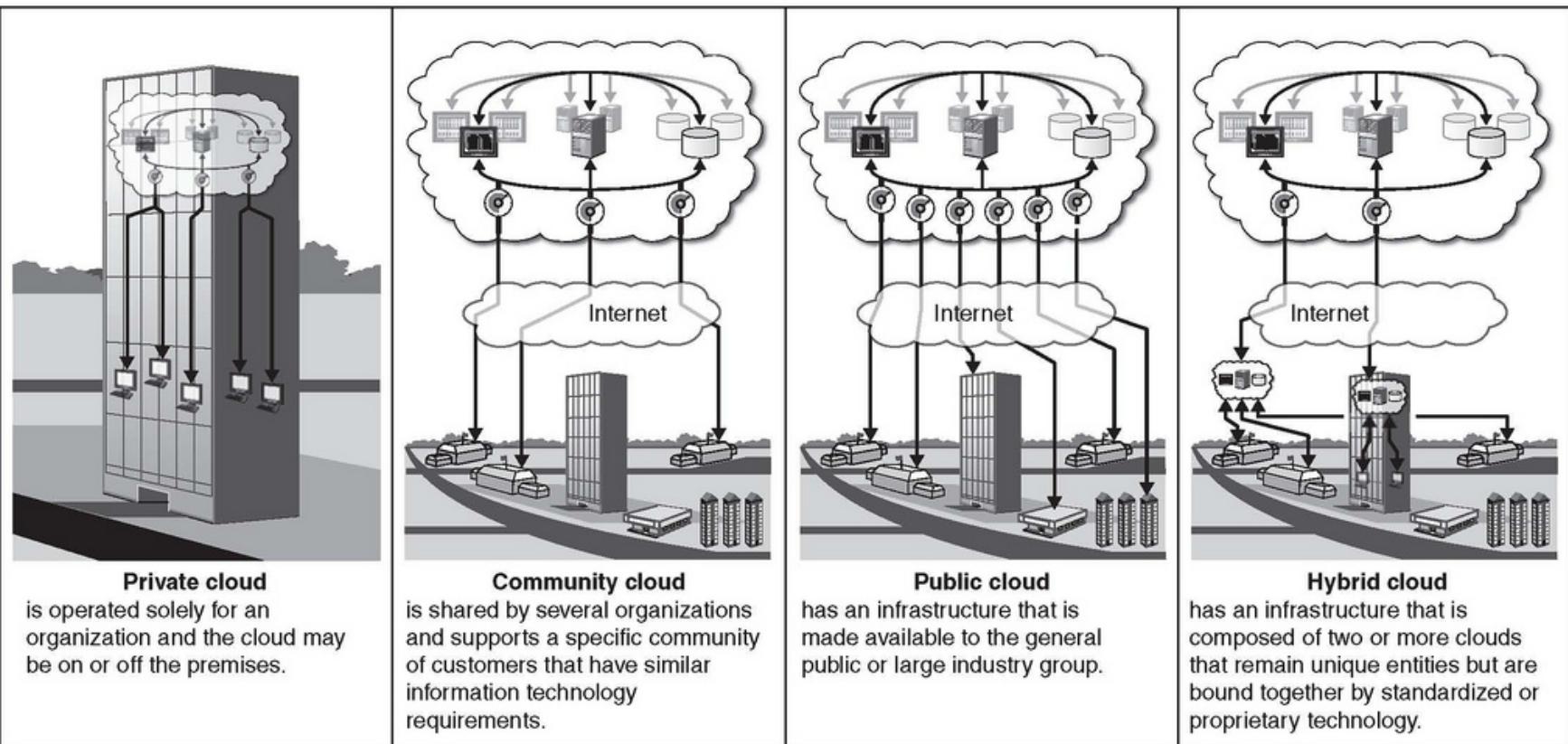


Deployment Models

- Public
- Private
- Hybrid
- Community



Deployment Models



Source: GAO analysis of NIST data.



Cloud Service Models

SaaS

PaaS

IaaS



Software



Monitoring
Content



Communication
Finance



Platform

Object Storage
Identity



Infrastructure



Cloud computing



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 Delivery

- Can be delivered either as
 - Hosted Application Management (AM): The provider hosts commercially available software for customers and delivers it over the web
 - Software on Demand: The cloud provider gives customers network-based access to a single copy of an application created specifically for SaaS distribution





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



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.



- Server scripting environment
- Management system database
- Server software
- Technical support
- Storage
- Network Access
- Design and development tools
- Hosting



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.



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

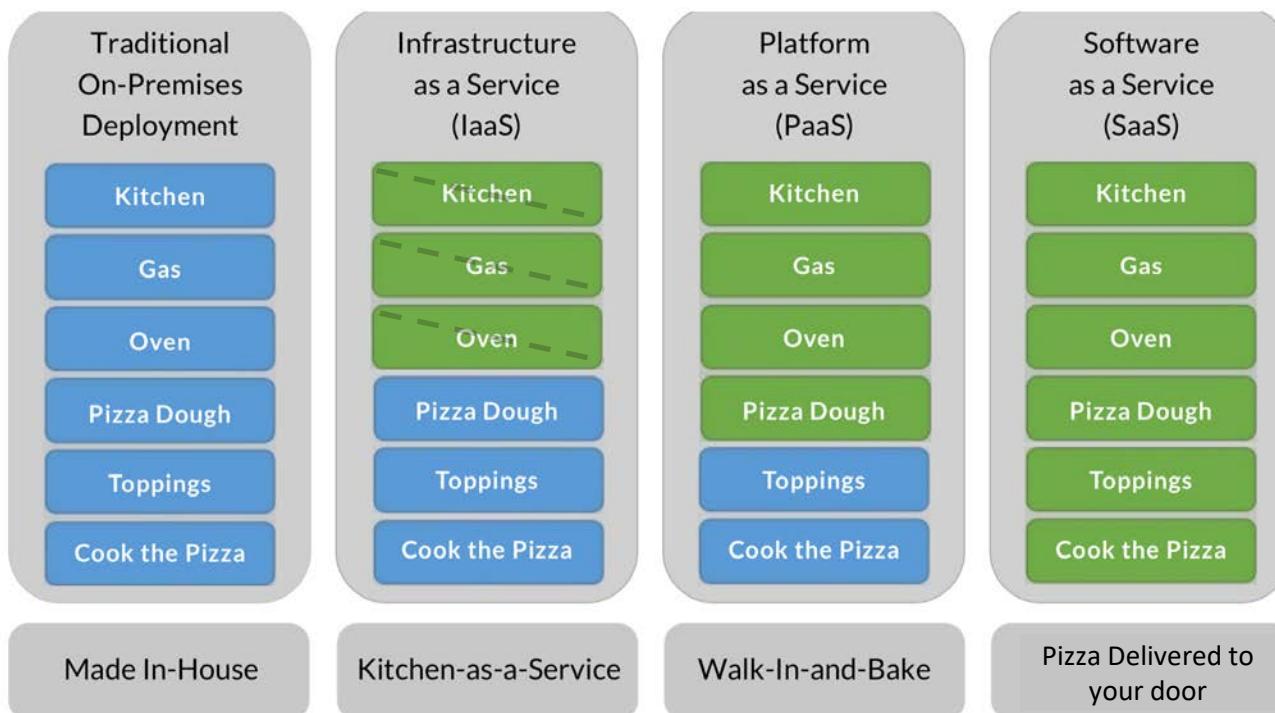


IaaS Offers:

- 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

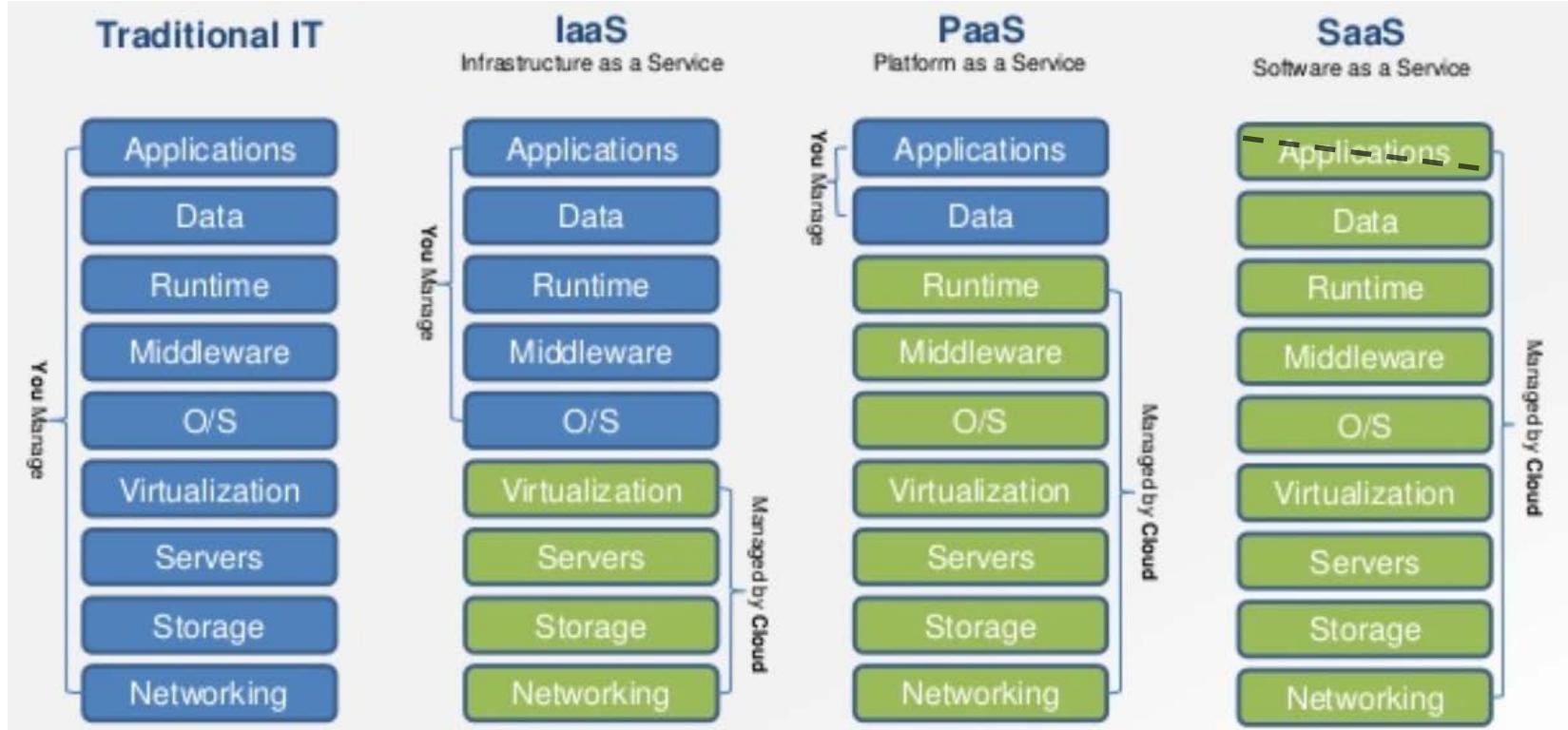


Pizza as a Service 2.0





Management Responsibility



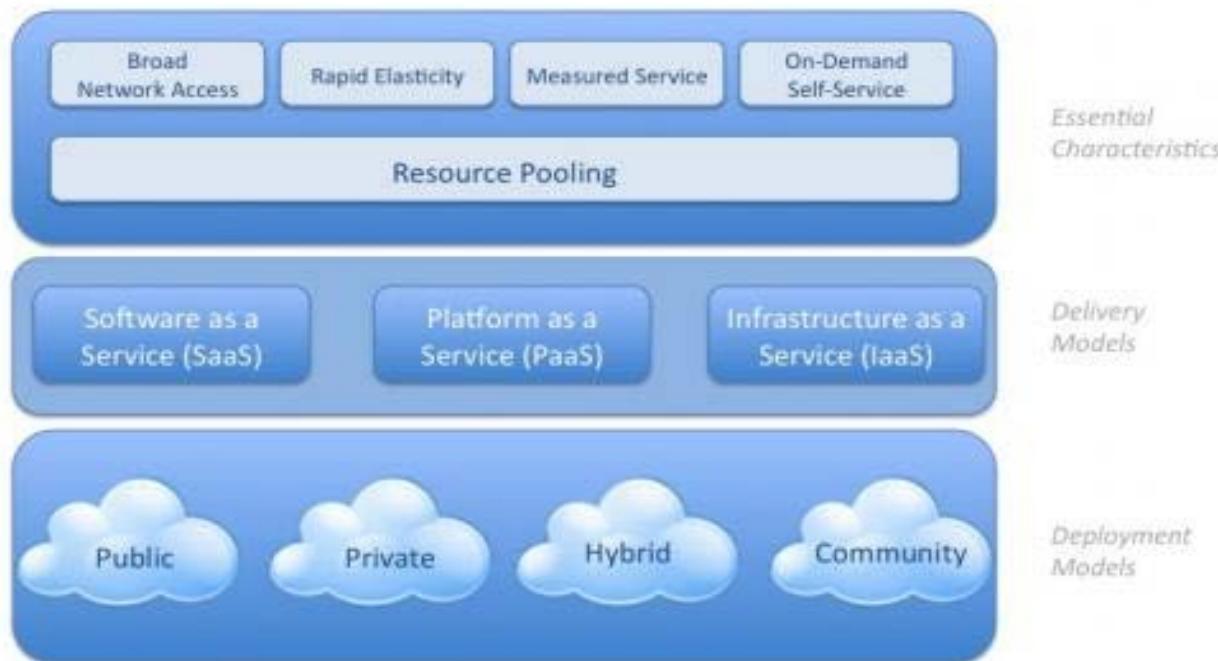


Type	Consumer	Service Provided	Service Level Coverage	Customization
SaaS	End user	APPLICATION	Application uptime	Minimal to no customization
			Application performance	Capabilities dictated by market or provider
PaaS	Application owner	DATABASE	Environment availability	High degree of application level customization available within constraints of the service offered
		Runtime environment for application code	Environment performance	Many applications will need to be rewritten
		Cloud storage	No application coverage	
		Other Cloud services such as integration		
IaaS	Application owner or IT provides OS	OPERATING ENVIRONMENT	Virtual server availability	Minimal constraints on applications installed on Standardized virtual OS builds
	Middleware and application support	Virtual server	Time to provision	
		Cloud storage	No platform or application coverage	
		Network services		



The Big Picture

Visual Model Of NIST Working Definition Of Cloud Computing
<http://www.csric.nist.gov/groups/SNS/cloud-computing/index.html>





NIST-SP 500-291, NIST 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

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



Interoperability

- Standards-driven
- 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 laws or directives
- 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
 - Confidentiality: Prevents unauthorized disclosure



Resiliency

- 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 may streamline the process of oversight and facilitate governance



Service Level Agreements

- Availability (e.g. 99.99% during work days, 99.9% for nights/weekends)
- 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)
- 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



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



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



Cloud Security Concepts

- Network Security and Perimeter
- Cryptography
- Access Control
- Data and Media Sanitization
- Virtualization Security
- Common Threats
- Security in Relation to Cloud Categories



Network Security

- Physical and Environmental Security for facility and network devices
 - Controls must enforce the CIA
 - Temperature between 64 and 72 degrees F
 - Humidity between 45-55 percent
 - Hot and cold aisles
 - Monitoring
- Technical network security controls
 - Link
 - Protocol
 - Application layer services
- Network Perimeter
 - Often considered the demarcation point, though those lines are becoming less clear or even non-existent



Cryptography

- State of Data Protection
 - Data at Rest
 - Data In Use
 - Data in Transit
- Key Management
 - Public/Private Key
 - Hashes
 - Digital Signatures
- Destruction of Data
 - Crypto-shredding



Data States

- 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



Key Management

- An essential element of key management is that the encryption key should never be stored on the same volume as the encrypted material
- Though data is stored in the cloud best practices dictate key management be handled by the client
 - 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.
 - Key Escrow



Access Control

- Regulating a Subject's ability to interact with an object
- Identity and Access Management
 - Includes the people, processes and systems that are used to manage access to enterprise resources
 - Identity of an entity is verified
 - Correct level of access is granted based on asset, services and protected resources being accessed



Phases of IAM

- Provisioning and de-provisioning of accounts
- Centralized directory services
- Privileged user management
- Authentication and access management

***IAM will be discussed in later chapters in more depth



Provisioning and De-provisioning

The goal of provisioning is to standardize, streamline, and create an efficient account creation process, while creating a consistent, measurable, traceable and auditable framework for providing access to end users.

De-Provisioning is the process whereby a user account is disabled when the user no longer requires access to the cloud-based services and resources. Includes users leaving the organization, as well as changing roles or functions or department



Centralized Directory services

- Most common protocol is LDAP, which stores, processes and facilitates a structured repository of information stored, coupled with unique identifiers and locations
- LDAP Is the communications protocol used to interact with Active Directory



Privileged User Management

- Focuses on process and ongoing requirements to manage the lifecycle of user accounts with the highest privileges
- These accounts carry the highest risk and impact
- Should include the ability to: track usage, authentication successes and failures, authorization times/dates, log successful and failed events, enforce password management and contain sufficient levels of auditing and reporting



Authorization and Access Management

- Regulates what a subject can do to an object
- Users require authorization and access management to access required/appropriate resources
- Should be functional, operational and trusted
- Should be based on sound security principles such as separation of duties, privilege management, password management, etc



Data Migration/Removal

- When leaving or migrating from a cloud provider, considerations must be made for export/import of data in standards-based formats
- “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
- How is media sanitized after removal?
- Degaussing/physical destruction is rarely an option.
- Overwriting is frequently used.
- Cryptoshredding: encrypting data and destroying the key



Matching



Virtualization Security

- Virtualization allows logical isolation on multi-tenant servers
- May also allow attackers to target relevant components and functions to gain unauthorized access to data/systems/resources]
- Relies upon the security of the Hypervisor



Hypervisor

- Allows multiple OS to share a single hardware host, with the *appearance* of each host having exclusive use of resources
- Type I Hypervisor running directly on the hardware with VM resources provided by the hypervisor. “Also referred to as “bare metal.” VMware ESXI, Citrix XenServer. Hardware based
- Type II Hypervisor runs on a host OS to provide virtualization services. VMware workstation, and MS VirtualPC. Software-based.



Hypervisor security

- Type I hypervisors significantly reduce the attack surface. Hypervisor vendors have control over relevant software that comprises and forms the hypervisor package, reducing the likelihood of malicious code being introduced at the hypervisor foundation
- Type II hypervisors have greater vulnerability since they are OS based. Numerous vulnerabilities exist within various OS opening up additional opportunities.



Common Threats

- “Notorious 9”
 - 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



Security for Different Cloud Categories

- 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)
- PaaS requires addressing 4 main issues
 - System/Resource isolation
 - User-level permissions
 - User Access Management
 - Protection against malware
- SaaS Involves 3 main issues
 - Data Segregation
 - Data Access and Policies
 - Web Application Security



Business Continuity and Disaster Recovery Planning

- Continuity Management is the process in which risks and threats to the ongoing availability of services, business functions and the organization are actively reviewed and managed at set intervals.
- Disaster recovery focuses on restoration of most critical business functions in the event of large impact events
- Must address C-I-A triad



Restoration Plan

- Due Diligence requires review of plans of the Cloud Service Provider and SLAs in relation to:
 - RPO
 - RTO
 - Compensation for loss
 - Definitions of Criticality of specific services
 - Points of contact and escalation



Critical Success Factors for Business Continuity in the Cloud

- Clearly state and ensure that the SLA addresses which components of BCP/DRP are covered and to what degree
 - Penalties/Compensation
 - RTO/RPO
 - Loss of integrity or confidentiality
 - Escalation Process/Points of contact
 - Ensure failover locations provide the same degree (or higher) of security
 - Clearly defined responsibilities for ownership of data, custodianship, and 3rd parties and supply chains provide the same degree (or higher) of security
- Ensure Understanding of Responsibilities Customer vs. CSP
 - Order of restoration (priorities)
 - Frameworks/Certifications held by facility
 - Right to audit/regular assessments of continuity
 - Communication of issues
 - On-site/Offsite backups



SLAs in Relation to Disaster Recovery

- No single points of failure
- Migration to alternate location/provider should be possible within agreed upon RTO
- Which components will be supported by the alternate CSP in the event of a failover
- Automated controls should be available to allow integrity verification
- If data backups are included, configuration options should be available for desired coverage, frequency, and recovery point restoration operations should be
- Continuous monitoring of relevant control points



Cost-Benefit Analysis

- The key driver for the adoption of cloud computing
- Resource pooling
- Shift from CapEx to OpEx
- Time and efficiencies
- No depreciation of resources
- Savings of utilities costs
- Software Licensing and maintenance costs
- Thin Clients
- Pay per usage
- Reduced TCO



Standards-based Approaches

- ISO 27001 looks to certify that the **ISMS** can address relevant risks and elements that is appropriate based on risks. **Best known and widely accepted**
- ISO 27002 is the **framework for best practice**
- SOC Service Organization Control
 - SOC I Controls at a service organization relevant to user entities internal control over financial reporting.
 - SOC II Controls at a service organization relevant to security, availability, processing integrity confidentiality, or privacy. Provides evaluation of technical controls
 - SOC III Service Organization Control defines a comprehensive approach to auditing and assesses the provider's controls and their effectiveness. CAN BE MADE PUBLICLY AVAILABLE
- 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. Common Criteria (ISO 15408)
 - Defines 7 levels of evaluation assurance, with 7 indicating the most rigorous testing
- FIPS 140 addresses uses of encryption and cryptography
- PCI-DSS, HIPPA and other regulations



Domain 1 Architectural Concepts and Design Requirements Review

- Why the Cloud? Definitions and Roles
- Cloud Service Categories (SaaS, Paas, Iaas)
- Deployment Models (Public, Private, Hybrid)
- Key Principles of Enterprise Architecture
- Network Security and Perimeter
- Identity and Access Management
- Media Sanitization
- Virtualization Security
- Threats
- Business Continuity

Review Questions CHAPTER 1

1. Which of the following is *not* a common cloud service model?
 - A. Software as a Service
 - B. Programming as a Service
 - C. Infrastructure as a Service
 - D. Platform as a Service
 2. All of these technologies have made cloud service viable except:
 - A. Virtualization
 - B. Widely available broadband
 - C. Cryptographic connectivity
 - D. Smart hubs
 3. Cloud vendors are held to contractual obligations with specified metrics by:
 - A. SLAs
 - B. Regulations
 - C. Law
 - D. Discipline
 4. drive security decisions.
 - A. Customer service responses
 - B. Surveys
 - C. Business requirements
 - D. Public opinion
 5. If a cloud customer cannot get access to the cloud provider, this affects what portion of the CIA triad?
 - A. Integrity
 - B. Authentication
 - C. Confidentiality
 - D. Availability
 6. Cloud Access Security Brokers (CASBs) might offer all the following services EXCEPT:
 - A. Single sign-on
 - B. BC/DR/COOP
 - C. IAM
 - D. Key escrow
- Review Questions 21**
7. Encryption can be used in various aspects of cloud computing, including all of these except:
 - A. Storage
 - B. Remote access
 - C. Secure sessions

D. Magnetic swipe cards

8. All of these are reasons an organization may want to consider cloud migration except:

- A. Reduced personnel costs**
- B. Elimination of risks**
- C. Reduced operational expenses**
- D. Increased efficiency**

9. The generally accepted definition of cloud computing includes all of the following characteristics except:

- A. On-demand services**
- B. Negating the need for backups**
- C. Resource pooling**
- D. Measured or metered service**

10. All of the following can result in vendor lock-in except:

- A. Unfavorable contract**
- B. Statutory compliance**
- C. Proprietary data formats**
- D. Insufficient bandwidth**

11. The risk that a cloud provider might go out of business and the cloud customer might not be able to recover data is known as:

- A. Vendor closure**
- B. Vendor lock-out**
- C. Vendor lock-in**
- D. Vending route**

12. All of these are features of cloud computing except:

- A. Broad network access**
- B. Reversed charging configuration**
- C. Rapid scaling**
- D. On-demand self-service**

13. When a cloud customer uploads PII to a cloud provider, who becomes ultimately responsible for the security of that PII?

- A. Cloud provider**
- B. Regulators**
- C. Cloud customer**
- D. The individuals who are the subjects of the PII**

14. We use which of the following to determine the critical paths, processes, and assets of an organization?

- A. Business requirements**
- B. BIA**
- C. RMF**
- D. CIA triad**

15. The cloud deployment model that features organizational ownership of the hardware and infrastructure, and usage only by members of that organization, is known as:

- A. Private**

- B.** Public
- C.** Hybrid
- D.** Motive

16. The cloud deployment model that features ownership by a cloud provider, with services offered to anyone who wants to subscribe, is known as:

- A.** Private
- B.** Public
- C.** Hybrid
- D.** Latent

17. The cloud deployment model that features joint ownership of assets among an affinity group is known as:

- A.** Private
- B.** Public
- C.** Hybrid
- D.** Community

18. If a cloud customer wants a secure, isolated sandbox in order to conduct software development

and testing, which cloud service model would probably be best?

- A.** IaaS
- B.** PaaS
- C.** SaaS
- D.** Hybrid

19. If a cloud customer wants a fully-operational environment with very little maintenance or administration necessary, which cloud service model would probably be best?

- A.** IaaS
- B.** PaaS
- C.** SaaS
- D.** Hybrid

20. If a cloud customer wants a bare-bones environment in which to replicate their own enterprise

for BC/DR purposes, which cloud service model would probably be best?

- A.** IaaS
- B.** PaaS
- C.** SaaS
- D.** Hybrid

Chapter 1: Architectural Concepts

- 1.** B. Programming as a Service is not a common offering; the others are ubiquitous throughout the industry.
 - 2.** D. Virtualization allows scalable resource allocation; broadband connections allow users to have remote access from anywhere; cryptographic connections allow for secure remote access. Smart hubs aren't widely used in cloud offerings.
 - 3.** A. Service-level agreements (SLAs) specify objective measures that define what the cloud provider will deliver to the customer.
 - 4.** C. Security is usually not a profit center, and is therefore beholden to business drivers; the purpose of security is to support the business.
 - 5.** D. Lack of access is an availability issue.
 - 6.** B. CASBs don't usually offer BC/DR/COOP services; that's something offered by cloud providers.
 - 7.** D. The data on magnetic swipe cards isn't usually encrypted.
 - 8.** B. Risks, in general, can be reduced but never eliminated; cloud service, specifically, does not eliminate risk to the cloud customer, because the customer retains a great deal of risk after migration.
 - 9.** B. Backups are still just as important as ever, regardless of where your primary data and backups are stored.
 - 10.** B. There are no written laws that require a cloud customer to remain with a certain cloud provider.
 - 11.** B. This is the definition of vendor lock-out.
 - 12.** B. This is a nonsense term used as a red herring.
 - 13.** C. Under current law, the data owner is responsible for any breaches that result in unauthorized disclosure of PII; this includes breaches caused by contracted parties and outsources services. The data owner is the cloud customer.
 - 14.** B. The business impact analysis is designed to ascertain the value of the organization's assets, and learn the critical paths and processes.
 - 15.** A. This is the definition of a private cloud model.
 - 16.** B. This is the definition of a public cloud model.
 - 17.** D. This is the definition of a community cloud model.
 - 18.** B. PaaS allows the cloud customer to install any kind of software, including software to be tested, on an architecture that includes any desired OSs.
- Chapter 2: Design Requirements **311**
- 19.** C. SaaS is the most comprehensive cloud offering, requiring little input and administration on the part of the cloud customer.
 - 20.** A. IaaS offers what is basically a hot/warm DR site, with hardware, connectivity, and utilities, allowing the customer to build out any kind of software configuration (including choosing OSs).



Domain 2

Cloud Data Security



Domain 2 Cloud data security

- Data Lifecycle Security
- Storage Architectures
- Database Security
- Data Loss Prevention (DLP)
- Data Encryption
- Key Management



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.



- 1.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.
- 2.Store:** Storing is the act committing the digital data to some sort of storage repository, and typically occurs nearly simultaneously with creation.
- 3.Use:** Data is viewed, processed, or otherwise used in some sort of activity.
- 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 (e.g., cryptoshredding)

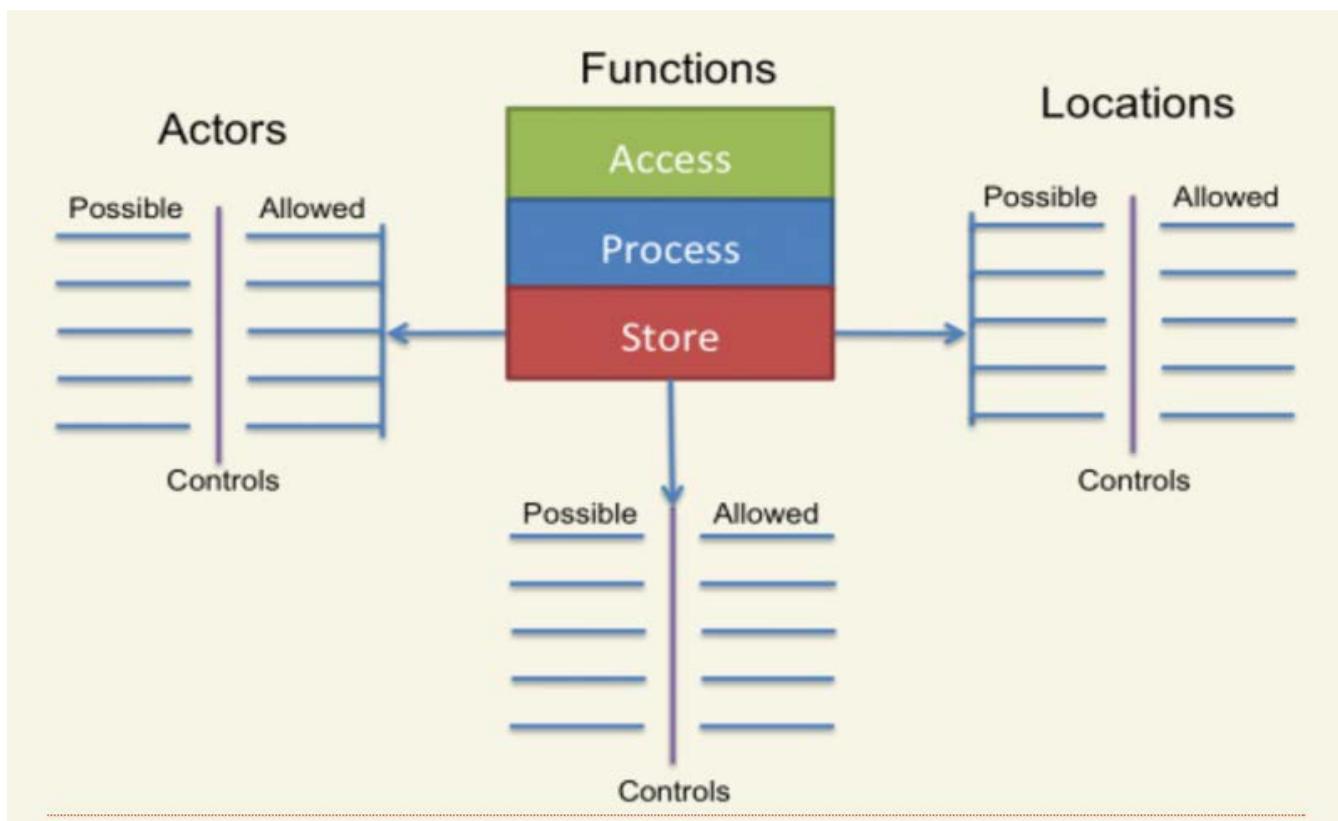


Location and Access

- Though the data lifecycle model does not specify requirements for location and access, these two factors are essential in planning the implementation of security controls
- Location? Where is the data stored/processed/transmitted
 - Jurisdiction
 - Audit
 - Threat landscape
 - What actors have access to the data
 - Does data move between locations and how?
- Access
 - Who has access to the data
 - What controls are in place
 - What devices can be used to access data

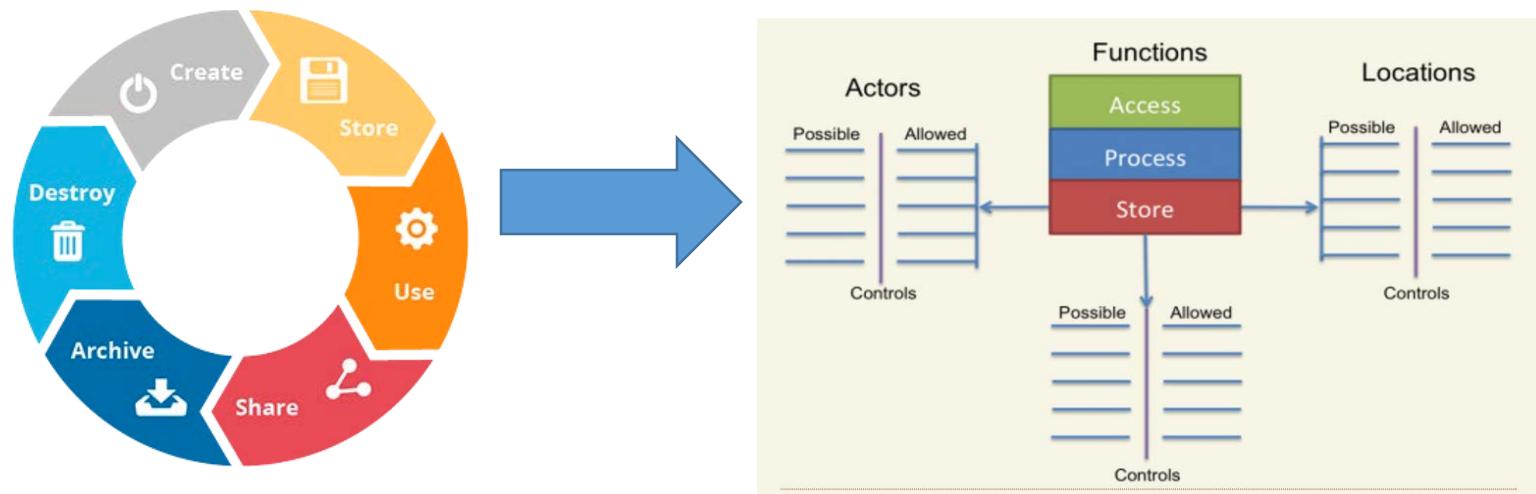


Functions, Actors, and Controls





Tying it Together



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.



Cloud Storage

- Each Cloud Service model will use specific types of storage and storage services
 - IaaS
 - PaaS
 - SaaS



Storage Architectures: IaaS

- Volume storage (block storage) Includes volumes/data stores attached to IaaS instances, usually a virtual hard drive. Should provide redundancy
- Object storage: Example: Dropbox. Used for write-once, read many; not suitable for applications like databases
 - Replication is not complete until all versions have been synchronized, which may take time
- Because of varying laws and regulations, customers should always know where their physical data is stored and is stored in compliance with their needs—LOCATION is primary concern in relation to regulations



Data Storage: PaaS

- PaaS utilizes the following data storage types:
 - 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



Threats to Data Storage

- Unauthorized usage/access
 - Strong Authentication
 - Encryption
 - Obfuscation, anonymization, tokenization, and masking
 - Organizational policies & layered Defense
- Liability due to noncompliance
 - Due care and due diligence
 - SLAs
- Dos and DDoS
 - Redundancy
 - Data Dispersion
- Corruption, modification, destruction of data
 - Hashes/Digitally signed files
- Data leakage and breaches
 - DLP
- Theft or accidental media loss
 - TPM
- Malware attack
 - Anti-malware
- Improper treatment or sanitization of data at end of lifecycle



Data Security in the Cloud

- Protecting Data moving to and within the cloud
 - SSL/TLS/IPSec
- Protecting Data in the Cloud
 - Encryption
- Detection of Data Migration to the Cloud
 - DAM, FAM, DLP
- Data Dispersion: Data is replicated in multiple physical locations across your cloud. Is used for higher availability
- Data Fragmentation involves splitting a data set into smaller fragments (or shards), and distributing them across a large number of machines.



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



Encryption Architecture

- 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

- Storage-level encryption
 - Full drive encryption—Storage level encryption can be used in addition to either volume storage encryption or object storage encryption
 - Encryption engine is located on the storage management level, with the keys managed by the CSP.
- Volume storage encryption
 - Rather than encrypting the entire drive, a customer may choose to encrypt only the necessary volume
- 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



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 in the private cloud.



Data Discovery

- Provides a way to make sense of big data—the sheer volume and diversity of data makes this challenging for the old means of static reporting
- We need flexible, near real-time analytics
- Analysis techniques
 - Metadata
 - Labels
 - Content
- Security Challenges
 - Location: Data dispersed across multiple locations and environments becomes difficult to secure
 - Access controls must be balanced between security and providing necessary access
 - Preservation requirements of information should be clearly documented



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 Classification

- Categorizes data based on its value and drives the controls that are put in place to secure it.
- Classification should enable information to be protected in alignment with the company's policy
- Within the cloud, the CSP should
 - Ensure proper security controls are in place so that whenever data is created or modified by anyone, they are forced to classify or update the data as part of the creation/modification process
 - Implement Controls (could be administrative, preventive or compensating)
 - Make metadata available, as it could be used as a means of determining classification
 - Protect data according to its classification at rest and in transit
 - Should support the reclassification process.



Data Privacy terms

- 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.)
- Personal data: information relating to an identified or identifiable natural person—biometrics, health data, etc
- Processing: Operations performed on personal data—collection, recording, organization, storage, etc.
- Controller: Person, public authority, agency that determines the purposes and means of processing to be in compliance with laws and regulations
- Processor: One who processes data on behalf of the controller
- **The customer is the controller of the data and is **RESPONSIBLE** to all the legal duties addressed in the Privacy and Data Protection (P&DP) applicable laws. The service provider supplies the means and the platform, and is considered to be the processor.



CSA Cloud Controls Matrix (CCM)

- The CSA CCM provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance organized by domain.
- Designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a provider
- It provides mapping to the industry-accepted security standards such as ISO 27001/27002, COBIT, PCI-DSS



Domains of the CCM

- Audit Assurance and Compliance
- Application and Interface Security
- Business Continuity Management & Operational Resilience
- Change Control & Configuration Management
- Datacenter Security
- Data Security & Information Lifecycle Management
- Encryption & Key Management
- Governance and Risk Management
- Human Resources
- Identity & Access Management
- Interoperability & Portability
- Infrastructure & Virtualization Security
- Mobile Security
- Security Incident Management, E-Discovery, & Cloud Forensics
- Threat and Vulnerability Management
- Supply Chain Management, Transparency, and Accountability



Management Controls For Privacy and Data Protection

- Separation of Duties
- Training
- Authentication and Authorization procedures
- Vulnerability Assessments
- Backup and Recovery processes
- Logging
- Data-retention control
- Secure disposal



Data rights management

- DRM or IRM (Information Rights Management) adds an extra layer of access controls on top of the data object or document and provides granularity flowing down to printing, saving, copying and other options
- Useful for protecting sensitive organization content and intellectual property
- ACLs are embedded into the file, it is agnostic to the location of data. IRM will travel with the file (persistent)
- Dynamic policy control allows the owner to define and change user permissions and recall or expire content even after distribution



IRM Cloud Challenges

- IRM requires that all users with access should have matching encryption keys. This requires a strong and comprehensive identity structure
- Each user will need to be provisioned with an access policy and keys
- Access can be identity based or role based (RBAC)
- Identity can be implemented with a single director location or across federated trust
- End users will likely have to install a local IRM agent for key storage or authenticating and retrieval of protected information
- Can be challenging with disparate systems and document readers



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



Auditability

- In order to be able to perform effective audits and investigations The CSP should provide an audit log with as much information as is relevant
- When: Time and date of logs and events
- Where: Application identifier, application address (cluster/host or IP Address)
- Who: Human or machine
- What: Type of event, severity of event and description



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 pre-defined 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



Chain of Custody

- Chain of Custody is the preservation and protection of evidence from the time it is collected until the time it is presented in court.
- Documentation should exist for the collection, possession, condition, location, transfer, access to and any analysis performed on an item from acquisition through eventual final disposition
- Chain of Custody provision should be included in the service contract and ensure that the cloud provider will comply with requests



Domain 2 Cloud Data Security Review

- Storage Architectures
- Data Lifecycle Security
- Database Security
- Data Loss Prevention (DLP)
- Data Encryption
- Key Management

Review Questions CHAPTER 2

1. Gathering business requirements can aid the organization in determining all of this information about organizational assets, except:

- A.** Full inventory
- B.** Usefulness
- C.** Value
- D.** Criticality

2. The BIA can be used to provide information about all the following, except:

- A.** Risk analysis
- B.** Secure acquisition
- C.** BC/DR planning
- D.** Selection of security controls

3. In which cloud service model is the customer required to maintain the OS?

- A.** CaaS
- B.** SaaS
- C.** PaaS
- D.** IaaS

4. In which cloud service model is the customer required to maintain and update only the applications?

- A.** CaaS
- B.** SaaS
- C.** PaaS
- D.** IaaS

5. In which cloud service model is the customer only responsible for the data?

- A.** CaaS
- B.** SaaS
- C.** PaaS
- D.** IaaS

6. The cloud customer and provider negotiate their respective responsibilities and rights regarding

the capabilities and data of the cloud service. Where is the eventual agreement codified?

- A.** RMF
- B.** Contract
- C.** MOU
- D.** BIA

7. In attempting to provide a layered defense, the security practitioner should convince senior

management to include security controls of which type?

- A.** Technological

- B.** Physical
- C.** Administrative
- D.** All of the above

8. Which of the following is considered an administrative control?

- A.** Access control process
- B.** Keystroke logging
- C.** Door locks
- D.** Biometric authentication

9. Which of the following is considered a technological control?

- A.** Firewall software
- B.** Fireproof safe
- C.** Fire extinguisher
- D.** Firing personnel

10. Which of the following is considered a physical control?

- A.** Carpets
- B.** Ceilings
- C.** Doors
- D.** Fences

11. In a cloud environment, encryption should be used for all the following, except:

- A.** Long-term storage of data
- B.** Near-term storage of virtualized images
- C.** Secure sessions/VPN
- D.** Profile formatting

12. The process of hardening a device should include all the following, except:

- A.** Improve default accounts
- B.** Close unused ports
- C.** Delete unnecessary services
- D.** Strictly control administrator access

13. The process of hardening a device should include which of the following?

- A.** Encrypting the OS
- B.** Updating and patching the system
- C.** Using video cameras
- D.** Performing thorough personnel background checks

14. What is an experimental technology that is intended to create the possibility of processing encrypted data without having to decrypt it first?

- A.** Homomorphic
- B.** Polyinstantiation
- C.** Quantum-state
- D.** Gastronomic

15. Risk appetite for an organization is determined by which of the following?

- A.** Appetite evaluation
- B.** Senior management
- C.** Legislative mandates
- D.** Contractual agreement

16. What is the risk left over after controls and countermeasures are put in place?

- A.** Null
- B.** High
- C.** Residual
- D.** Pertinent

17. All the following are ways of addressing risk, except:

- A.** Acceptance
- B.** Reversal
- C.** Mitigation
- D.** Transfer

18. To protect data on user devices in a BYOD environment, the organization should consider

requiring all the following, except:

- A.** DLP agents
- B.** Local encryption
- C.** Multifactor authentication
- D.** Two-person integrity

19. Devices in the cloud datacenter should be secure against attack. All the following are means

of hardening devices, except:

- A.** Using a strong password policy
- B.** Removing default passwords
- C.** Strictly limiting physical access
- D.** Removing all admin accounts

20. Which of the following best describes risk?

- A.** Preventable
- B.** Everlasting
- C.** The likelihood that a threat will exploit a vulnerability
- D.** Transient

Chapter 2: Design Requirements

1. B. When we gather information about business requirements, we need to do a complete inventory, receive accurate valuation of assets (usually from the owners of those assets), and

assess criticality; this collection of information does not tell us, objectively, how useful an asset is, however.

2. B. The business impact analysis gathers asset valuation information that is beneficial for risk analysis and selection of security controls (it helps avoid putting the ten-dollar lock on the five-dollar bicycle), and criticality information that helps in BC/DR planning by letting the organization understand which systems, data, and personnel are necessary to continuously

maintain. However, it does not aid secure acquisition efforts, since the assets examined by the BIA have already been acquired.

3. D. In IaaS, the service is bare metal, and the customer has to install the OS and the software;

the customer then is responsible for maintaining that OS. In the other models, the provider installs and maintains the OS.

4. C. In PaaS, the provider supplies the hardware, connectivity, and OS; the customer installs

and maintains applications. In IaaS, the customer must also install the OS, and in SaaS, the provider supplies and maintains the applications.

5. B. SaaS is the model in which the customer supplies only the data; in the other models, the

customer also supplies the OS, the application, or both.

6. B. The contract codifies the rights and responsibilities of the parties involved upon completion

of negotiation. The RMF aids in risk analysis and design of the environment. An MOU is shared between parties for a number of possible reasons. The BIA aids in risk assessment,

DC/BR efforts, and selection of security controls.

7. D. Layered defense calls for a diverse approach to security.

8. A. A process is an administrative control; sometimes, the process includes elements of other

types of controls (in this case, the access control mechanism might be a technical control, or it might be a physical control), but the process itself is administrative. Keystroke logging is a technical control (or an attack, if done for malicious purposes, and not for auditing); door locks are a physical control; and biometric authentication is a technological control. This is a tricky question.

9. A. A firewall is a technological control. The safe and extinguisher are physical controls, and firing someone is an administrative control.

10. D. Fences are physical controls; carpets and ceilings are architectural features, and a door

is not necessarily a control: the lock on the door would be a physical security control. Although you might think of a door as a potential answer, the best answer is the fence; the exam will have questions where more than one answer is correct, and the answer that will score you points is the one that is *most* correct.

11. D. All of these activities should incorporate encryption, except for profile formatting, which is a made-up term.

12. A. We don't want to improve default accounts—we want to remove them. All the other options are steps we take to harden devices.

13. B. Updating and patching the system helps harden the system. Encrypting the OS is a distractor.

That would make the OS/machine impossible to use. Video cameras are a security control, but not one used to harden a device. Background checks are good for vetting personnel, but not for hardening devices.

14. A. Homomorphic encryption hopes to achieve that goal; the other options are terms that

have almost nothing to do with encryption.

15. B. Senior management decides the risk appetite of the organization.

16. C. This is the definition of the term.

17. B. Reversal is not a method for handling risk.

18. D. Although all the other options are ways to harden a mobile device, two-person integrity

is a concept that has nothing to do with the topic, and, if implemented, would require everyone in your organization to walk around in pairs while using their mobile devices.

19. D. Although the rest of the options are good tactics for securing devices, we can't remove

all admin accounts; the device will need to be administered at some point, and that account needs to be there.

20. C. Option C is the definition of risk—and risk is never preventable: it can be obviated, attenuated, reduced, and minimized, but never completely prevented. A risk may be everlasting

or transient, indicating that risk itself is not limited to being either.



Domain 3

Cloud Platform and Infrastructure Security



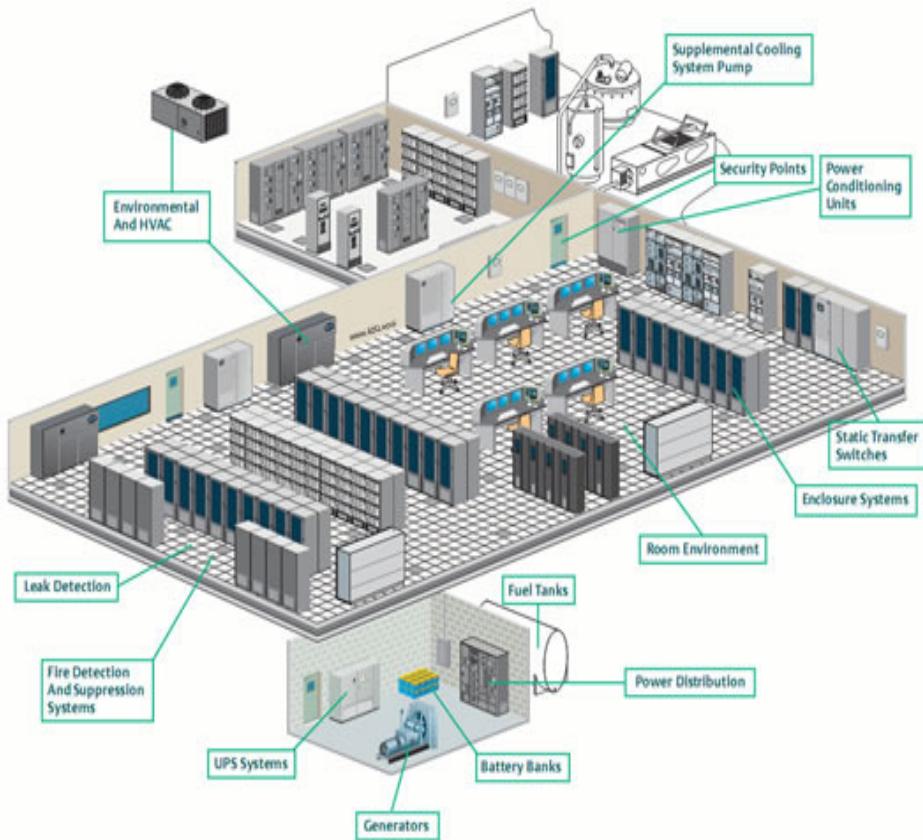
Domain 3 Cloud Platform and Infrastructure Security

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



Physical Environment of the Cloud Infrastructure

- 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.
- **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 (SDNs)

The SDN Architecture is:

DIRECTLY PROGRAMMABLE

Network control is directly programmable because it is decoupled from forwarding functions.

AGILE

Abstracting control from forwarding lets administrators dynamically adjust network-wide traffic flow to meet changing needs.

CENTRALLY MANAGED

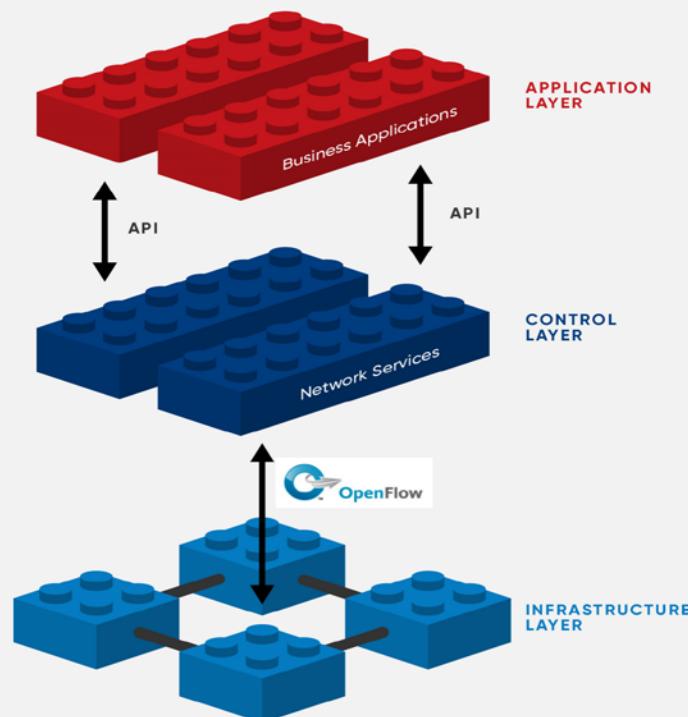
Network intelligence is (logically) centralized in software-based SDN controllers that maintain a global view of the network, which appears to applications and policy engines as a single, logical switch.

PROGRAMMATICALLY CONFIGURED

SDN lets network managers configure, manage, secure, and optimize network resources very quickly via dynamic, automated SDN programs, which they can write themselves because the programs do not depend on proprietary software.

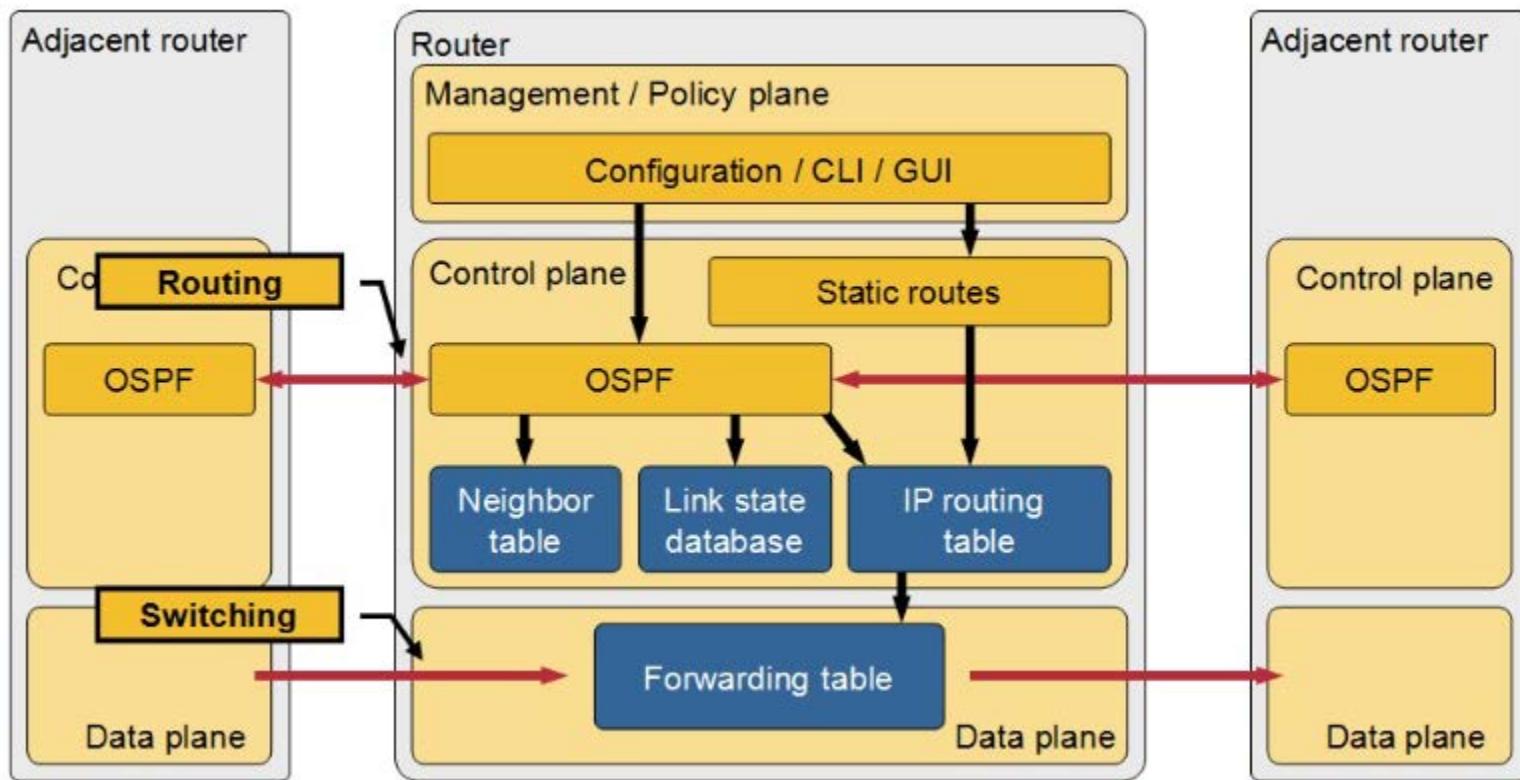
OPEN STANDARDS-BASED AND VENDOR-NEUTRAL

When implemented through open standards, SDN simplifies network design and operation because instructions are provided by SDN controllers instead of multiple, vendor-specific devices and protocols.





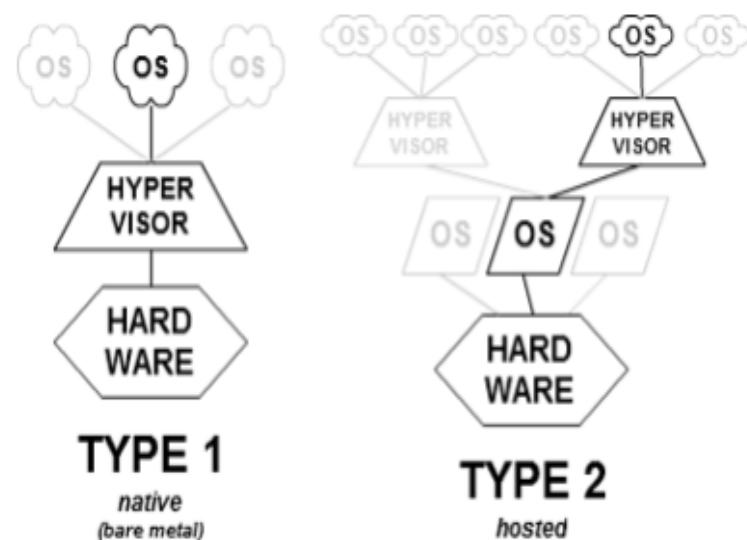
Management, Control and Data Plane





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, MS Hyper-V
- **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.)
- 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.
- 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 mitigate the risks associated with operational complexity.
- Hyperjacking:
 - Installing a rogue hypervisor that can take complete control of a host through the use of a VM based rootkit that attacks the original hypervisor, inserting a modified rogue hypervisor in its place



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
- Data Comingling:
 - 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.
- 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.



Object Storage

- Cloud Provider can provide a storage structure to customers called Object Storage
- Files and metadata can be stored
- Accessible to web-interfaces or APIs
- Uses a flat organization of containers (Amazon S3 calls them buckets)
- Uses unique IDs called keys to locate
- Can disperse data across many object storage servers
- **Consistency is a potential problem, as changes must be propagated to all servers before assurance of the latest version.



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
- 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



Legal

- 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
 - Can be CSP or customer responsibility (or shared)
 - Facility, HW, OS, software, vendor, customer, remote, should all be considered



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
- Secure erasure
- Snapshots for redundancy and investigations

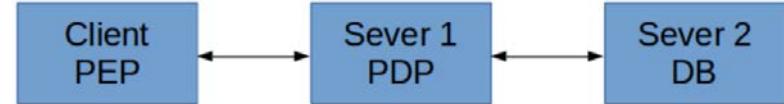


IAAA in The Cloud Infrastructure

- 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.
- 2. 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
- 3. 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

- 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

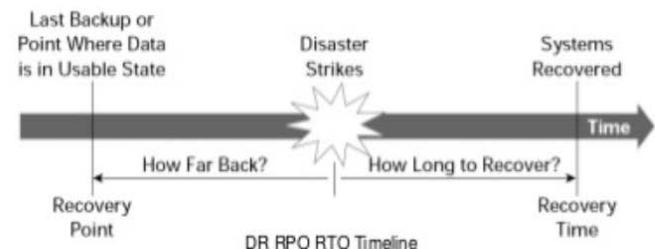
- On-premises, cloud as BCDR
 - Infrastructure is on premises, whereas the CSP provides alternate capabilities. This has traditionally been most common
 - Concerns: Different environment in the cloud. For instance, may need to convert workload on physical systems to virtual machines
- Cloud service consumer, 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?
- 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

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 grossly adversely affecting the business due to lost business transactions data



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



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
- 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
- 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 recover.
- 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 Recover and Business Continuity

Review Questions FOR CHAPTER 3

You can find the answers in Appendix A.

- 1.** All of these are methods of data discovery, except:
 - A.** Content-based
 - B.** User-based
 - C.** Label-based
 - D.** Metadata-based
- 2.** Data labels could include all the following, except:
 - A.** Date data was created
 - B.** Data owner
 - C.** Data value
 - D.** Data of scheduled destruction
- 3.** Data labels could include all the following, except:
 - A.** Source
 - B.** Delivery vendor
 - C.** Handling restrictions
 - D.** Jurisdiction
- 4.** Data labels could include all the following, except:
 - A.** Confidentiality level
 - B.** Distribution limitations
 - C.** Access restrictions
 - D.** Multifactor authentication
- 5.** All the following are data analytics modes, except:
 - A.** Real-time analytics
 - B.** Datamining
 - C.** Agile business intelligence
 - D.** Refractory iterations
- 6.** In the cloud motif, the data owner is usually:
 - A.** In another jurisdiction
 - B.** The cloud customer
 - C.** The cloud provider
 - D.** The cloud access security broker
- 7.** In the cloud motif, the data processor is usually:
 - A.** The party that assigns access rights
 - B.** The cloud customer
 - C.** The cloud provider
 - D.** The cloud access security broker
- 8.** Every security program and process should have which of the following?
 - A.** Foundational policy
 - B.** Severe penalties
 - C.** Multifactor authentication
 - D.** Homomorphic encryption

9. All policies within the organization should include a section that includes all of the following, except:

- A.** Policy maintenance
- B.** Policy review
- C.** Policy enforcement
- D.** Policy adjudication

10. The most pragmatic option for data disposal in the cloud is which of the following?

- A.** Melting
- B.** Cryptoshredding
- C.** Cold fusion
- D.** Overwriting

11. What is the intellectual property protection for the tangible expression of a creative idea?

- A.** Copyright
- B.** Patent
- C.** Trademark
- D.** Trade secret

12. What is the intellectual property protection for a useful manufacturing innovation?

- A.** Copyright
- B.** Patent
- C.** Trademark
- D.** Trade secret

13. What is the intellectual property protection for a very valuable set of sales leads?

- A.** Copyright
- B.** Patent
- C.** Trademark
- D.** Trade secret

14. What is the intellectual property protection for a confidential recipe for muffins?

- A.** Copyright
- B.** Patent
- C.** Trademark
- D.** Trade secret

15. What is the intellectual property protection for the logo of a new video game?

- A.** Copyright
- B.** Patent
- C.** Trademark
- D.** Trade secret

16. What is the aspect of the DMCA that has often been abused and places the burden of proof on the accused?

- A.** Online service provider exemption
- B.** Decryption program prohibition
- C.** Takedown notice
- D.** Puppet plasticity

17. What is the federal agency that accepts applications for new patents?

- A.** USDA
- B.** USPTO
- C.** OSHA
- D.** SEC

18. DRM tools use a variety of methods for enforcement of intellectual property rights.

These include all the following, except:

- A.** Support-based licensing
- B.** Local agent enforcement
- C.** Dip switch validity
- D.** Media-present checks

19. All of the following regions have at least one country with an overarching, federal privacy

law protecting personal data of its citizens, except:

- A.** Asia
- B.** Europe
- C.** South America
- D.** The United States

20. DRM solutions should generally include all the following functions, except:

- A.** Persistency
- B.** Automatic self-destruct
- C.** Automatic expiration
- D.** Dynamic policy control

Chapter 3: Data Classification

1. B. All the others are valid methods of data discovery; user-based is a red herring with no meaning.

2. C. All the others might be included in data labels, but we don't usually include data value, since it is prone to change frequently, and because it might not be information we want to disclose to anyone who does not have need to know.

3. B. All the others might be included in data labels, but we don't include delivery vendor, which is nonsense in context.

Chapter 3: Data Classification 313

4. D. All the others might be included in data labels, but multifactor authentication is a procedure used for access control, not a label.

5. D. All the others are data analytics methods, but "refractory iterations" is a nonsense term thrown in as a red herring.

6. B. The data owner is usually considered the cloud customer in a cloud configuration; the data in question is the customer's information, being processed in the cloud. The cloud provider

is only leasing services and hardware to the customer. The cloud access security broker (CASB) only handles access control on behalf of the cloud customer, and is not in direct contact with the production data.

7. C. In legal terms, when "data processor" is defined, it refers to anyone who stores, handles, moves, or manipulates data on behalf of the data owner or controller. In the cloud computing

realm, this is the cloud provider.

8. A. Policy drives all programs and functions in the organization; the organization should not conduct any operations that don't have a policy governing them. Penalties may or may not be an element of policy, and severity depends on the topic. Multifactor authentication and homomorphic encryption are red herrings here.

9. D. All the elements except adjudication need to be addressed in each policy. Adjudication is

not an element of policy.

10. B We don't have physical ownership, control, or even access to the devices holding the data,

so physical destruction, including melting, is not an option. Overwriting is a possibility, but it is complicated by the difficulty of locating all the sectors and storage areas that might have contained our data, and by the likelihood that constant backups in the cloud increase the chance we'll miss something as it's being overwritten. Cryptoshredding is the only reasonable

alternative. Cold fusion is a red herring.

11. A. Copyrights are protected tangible expressions of creative works. The other answers listed are answers to subsequent questions.

12. B. Patents protect processes (as well as inventions, new plantlife, and decorative patterns).

The other answers listed are answers to other questions.

13. D. Confidential sales and marketing materials unique to the organization are trade secrets.

The other answers listed are answers to other questions.

14. D. Confidential recipes unique to the organization are trade secrets. The other answers listed are answers to other questions.

15. C. Logos and symbols and phrases and color schemes that describe brands are trademarks.

The other answers listed are answers to other questions.

16. C. The DMCA provision for takedown notices allows copyright holders to demand removal of suspect content from the web, and puts the burden of proof on whoever posted the material; this function has been abused by griefers and trolls and overzealous content producers. The OSP exemption providers a safe harbor provision for web hosts.

314 Appendix A ■ Answers to the Review Questions

The decryption program prohibition makes DeCSS and other similar programs illegal.

Puppet plasticity is a nonsense term used for a red herring.

17. B. The U.S. Patent and Trademark Office accepts, reviews, and approves applications for new patents. The USDA creates and enforces agriculture regulation. OSHA oversees workplace

safety regulations. The SEC regulates publicly traded corporations.

18. C. DRM solutions use all these methods except for dip switch validity, which is a nonsense term.

19. D. The United States does not have a single, overarching personal privacy law; instead, the U.S. often protects PII by industry (HIPAA, GLBA, FERPA, and so forth.). All EU member countries adhere to the Data Protection Regulation. Argentina's Personal Data Protection Act cleaves to the EU Regulation, as does Japan's Act on the Protection of Personal Information.

20. B. DRM tools should include all the functions listed except for self-destruction, which might hurt someone.



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



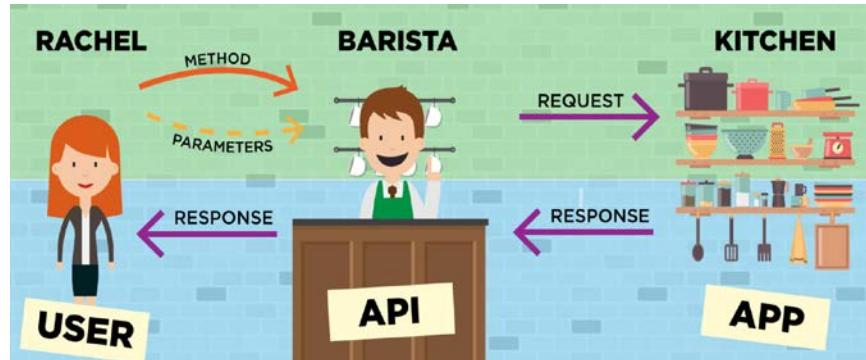
Cloud Application Architecture

- 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.



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 Grind).



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

- Some of the characteristics of SOAP include the following:
- 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

	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
Security Governance, Risk, and Compliance (GRC)			
Data Security			
Application Security			
Platform Security			
Infrastructure Security			
Physical Security			

Enterprise Responsibility

Shared Responsibility

CSP Responsibility

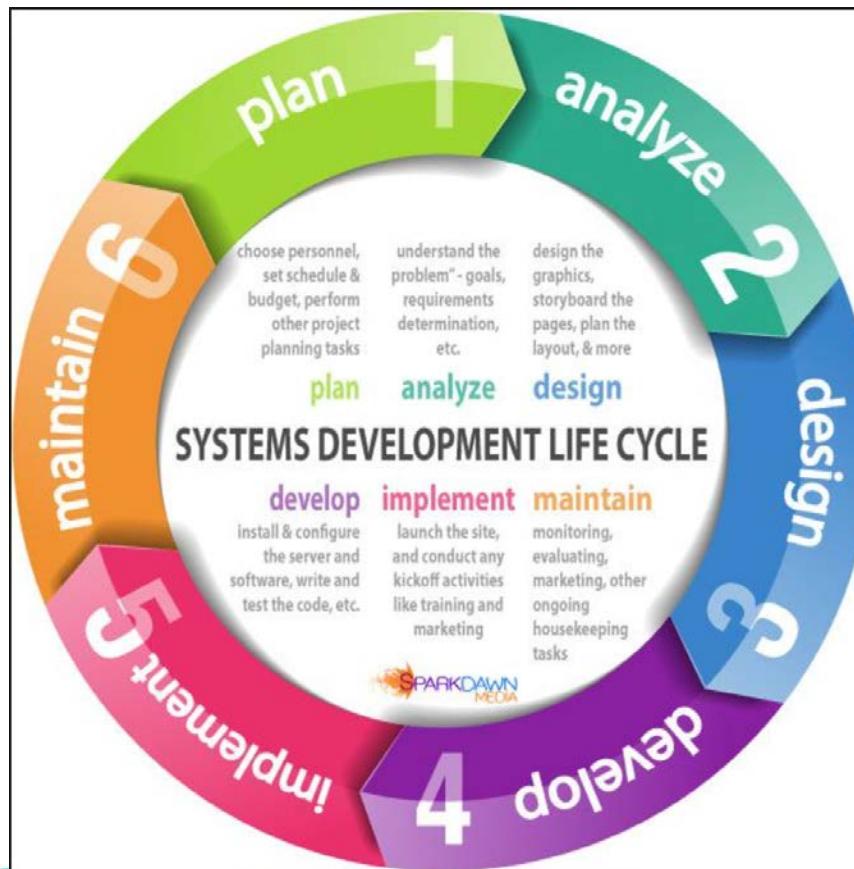


THE SDLC (Software Development Life-Cycle) for the Cloud

- 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

https://www.owasp.org/index.php/About_OWASP

OWASP Top 10 Application Security Risks – 2017

**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.



Identity and Access Management

- IAAA
 - Identity
 - Authentication
 - Authorization
 - Accounting



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.



Identity and Access Management

Provisioning Identities

SCIM

Authentication



Authorization





Identity

A typical environment



Firewall



Active Directory



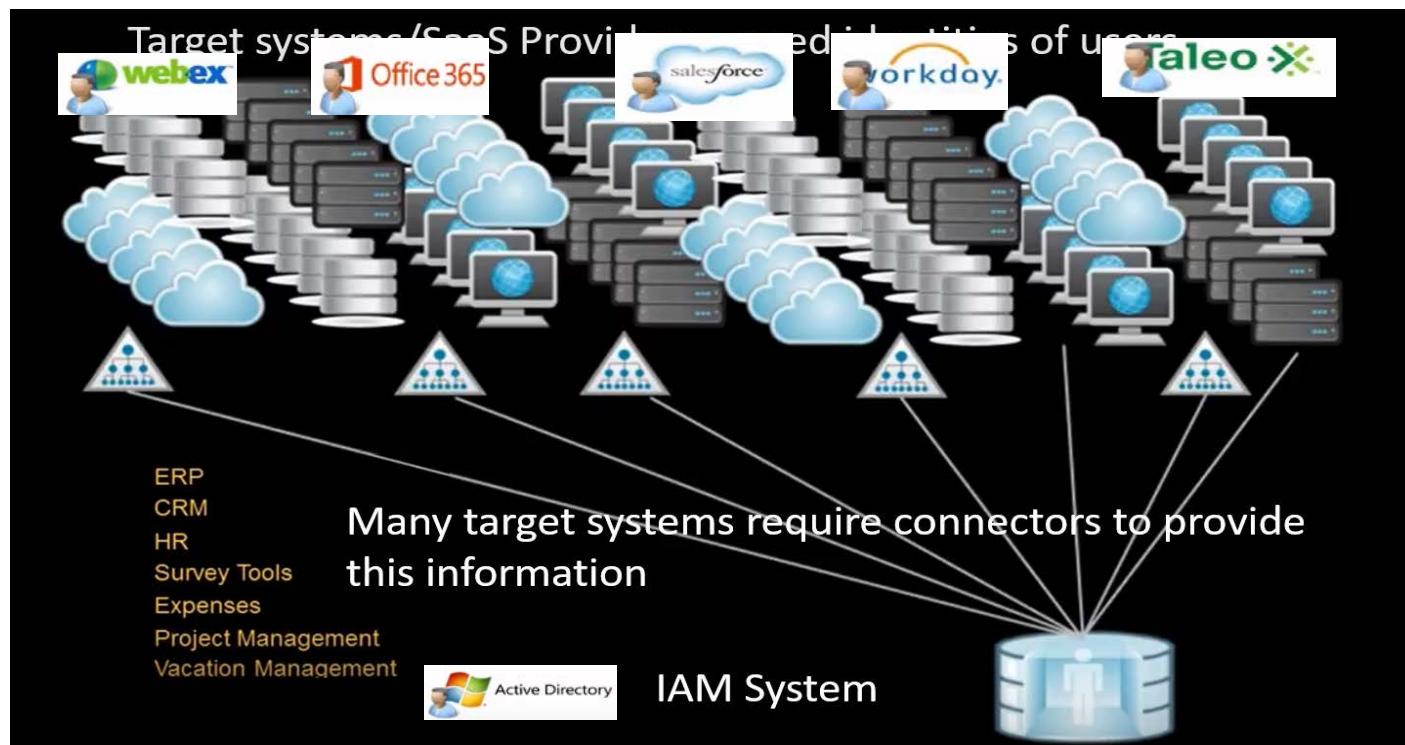


Traditional Identity Management

- Manual hand-entry
 - Error prone and slow
- Bulk upload
 - High latency – often a one-time operation
- Custom APIs and connectors
 - High cost to develop against
 - Proprietary to each service provider
- SAML Just-in-Time Provisioning
 - No pre-provisioning
 - No deprovisioning

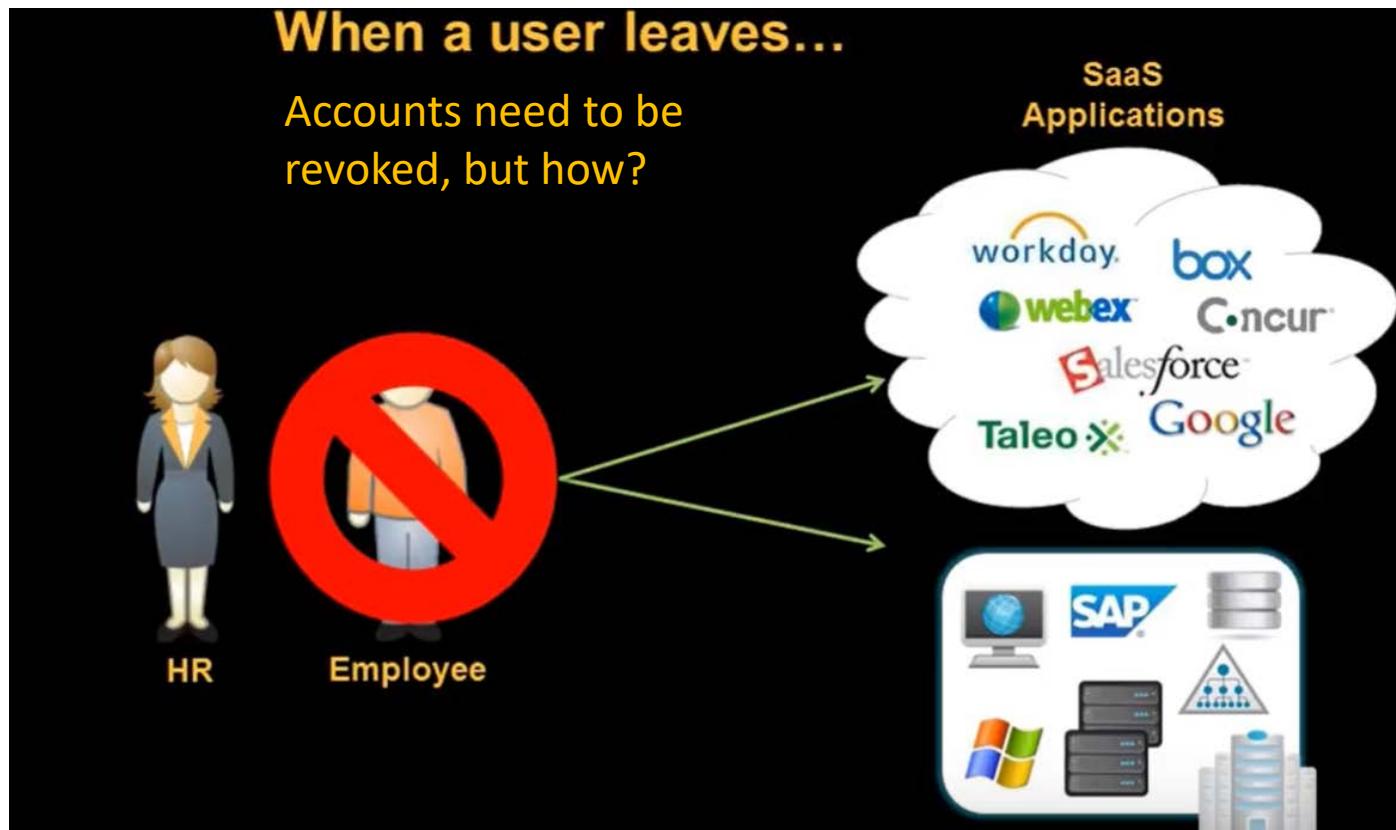


Identity Management Provisioning with Custom APIs





Deprovisioning



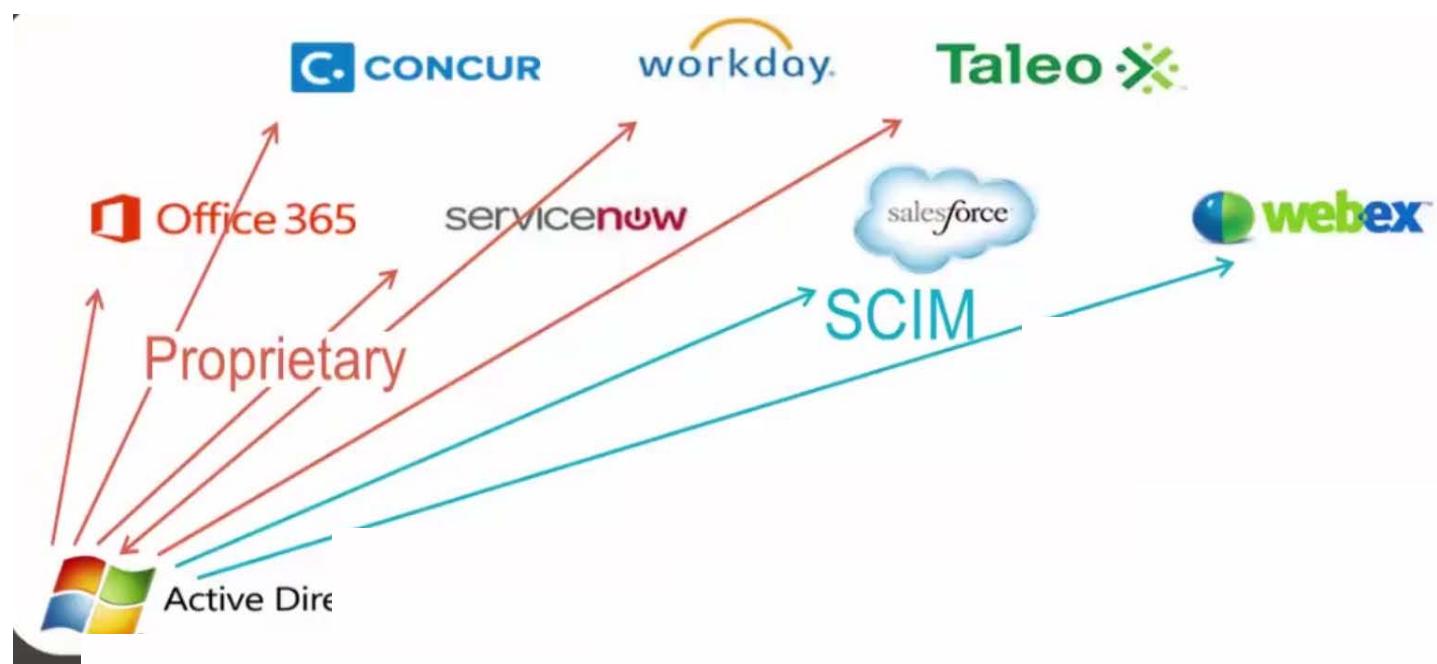


Instead....

As a company on-boards and off-boards employees, they are added and removed from the company's electronic employee directory. As long as the service provider supports the SCIM standard, SCIM Could then be used to automatically add/delete (or, provision/de-provision) accounts for those users in external systems such as Google Apps for Work, Office 365, or Salesforce.com. Then, a new user account would exist in the external systems for each new employee, and the user accounts for former employees would be removed from those systems

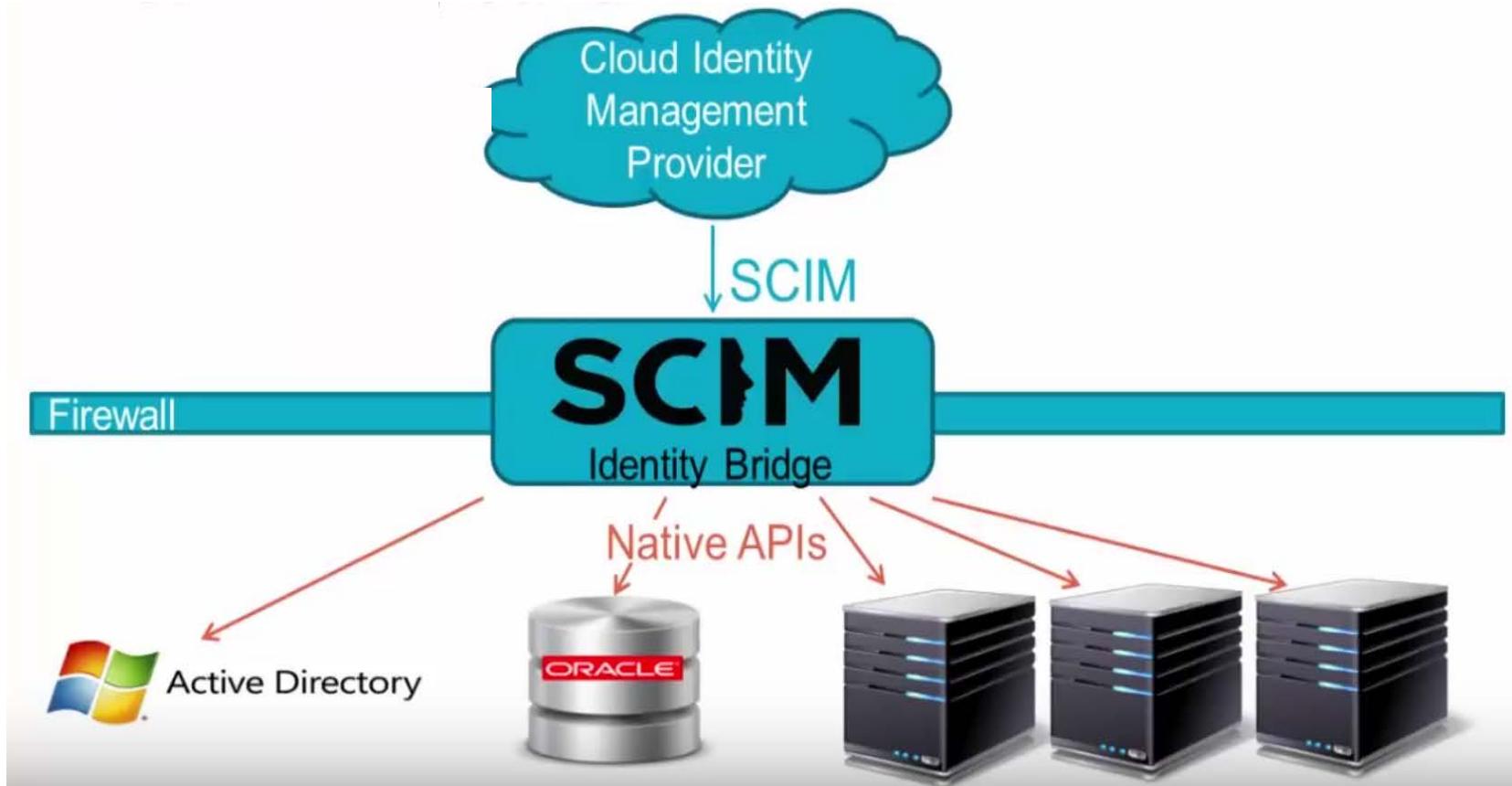


Proprietary and SCIM





Cloud Bridge





Authentication

- Relevant Standards/Protocols

- 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
- SAML: XML-based framework designed to communicate user authentication, entitlement and attribute information to other entities
- OpenID Connect: based on OAuth 2.0 allowing developers authenticate their users across web sites and apps without having to own and manage password files. Allows information from an Identity provider to be used.

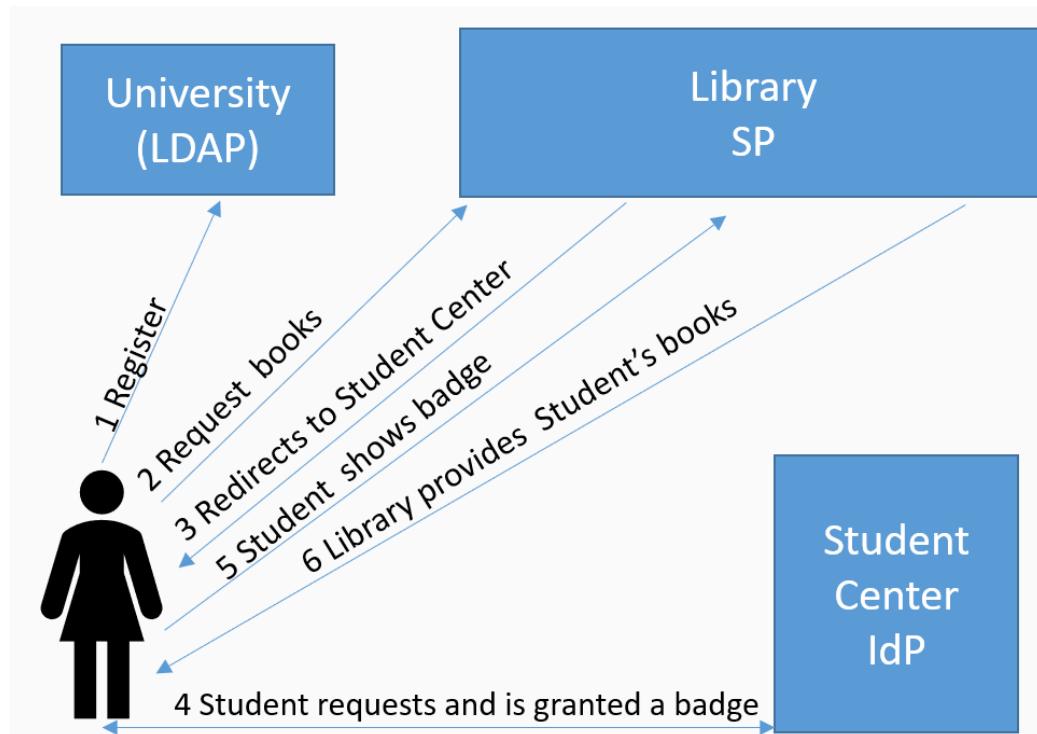


SAML (Security Assertion Markup Language)

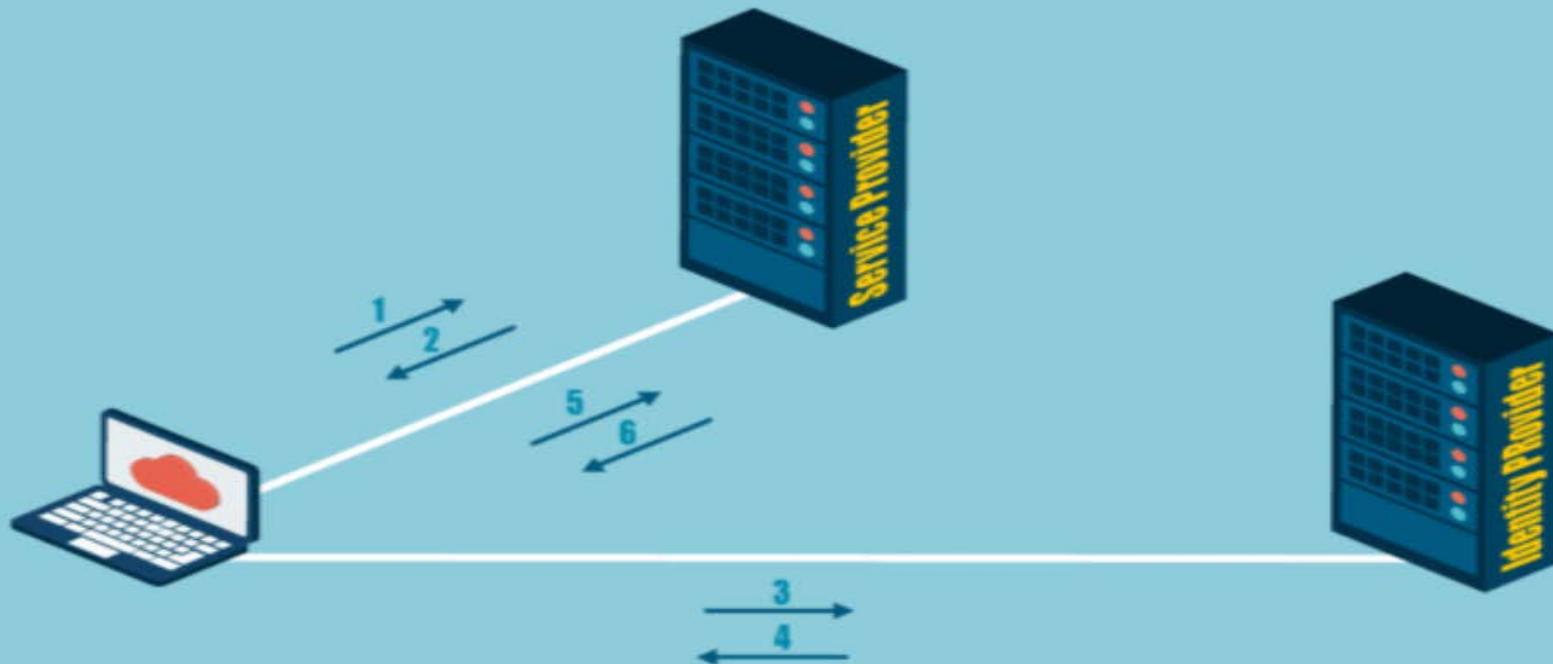
- For SSO with web applications, SAML works using set of browser redirects and message exchanges.
 1. User tries to access web application, the application redirects user to identity provider.
 2. User authenticates himself
 3. Identity provider issues a claims token and redirects user back to the application.
 4. Application then validates the token (trust needs to be established out of band between application and IdP), authorizes user access by asserting claims, and allows user to access protected resources.
 5. The token is then stored in the session cookie of user browser, ensuring the process doesn't have to be repeated for every access request



SAML Assertions



1. Student Registers at School
2. Student goes to library to receive his books
3. Library directs student to the student center to pick up his Student ID badge
4. Student Center has access to the same database as the university, so they verify the identity of the student and give him his student id badge
5. Student Provides the library his Student ID Number and badge and requests his books.
6. Library accepts the school ID as proof of authenticity and provides student his books



SAML v2.0 Process Flow

- 1 User attempts to access a hosted corporate application
- 2 *Service provider generates and sends SAML request to the user*
- 3 User is redirected to the *identity provider* together with the SAML request
- 4 *Identity provider authenticates user, parses SAML request and generates encoded SAML response which is sent to the user's browser*
- 5 User's browser sends SAML response to *service provider*
- 6 *Service provider verifies the user's SAML response and grants application access*

Software SECURED



OpenID Connect

- Open standard for authentication, promoted by the non-profit OpenID Foundation
- As of March 2016, there are over a billion OpenID-enabled accounts on the internet, and organizations such as Google, WordPress, Yahoo, and PayPal use OpenId to authenticate users
- A *user* must obtain an OpenID account through an OpenID *identity provider* (for example, Google). The user will then use that account to sign into any website (the *relying party*) that accepts OpenID authentication
- OpenID standard provides a framework for the communication that must take place between the identity provider and the relying party.

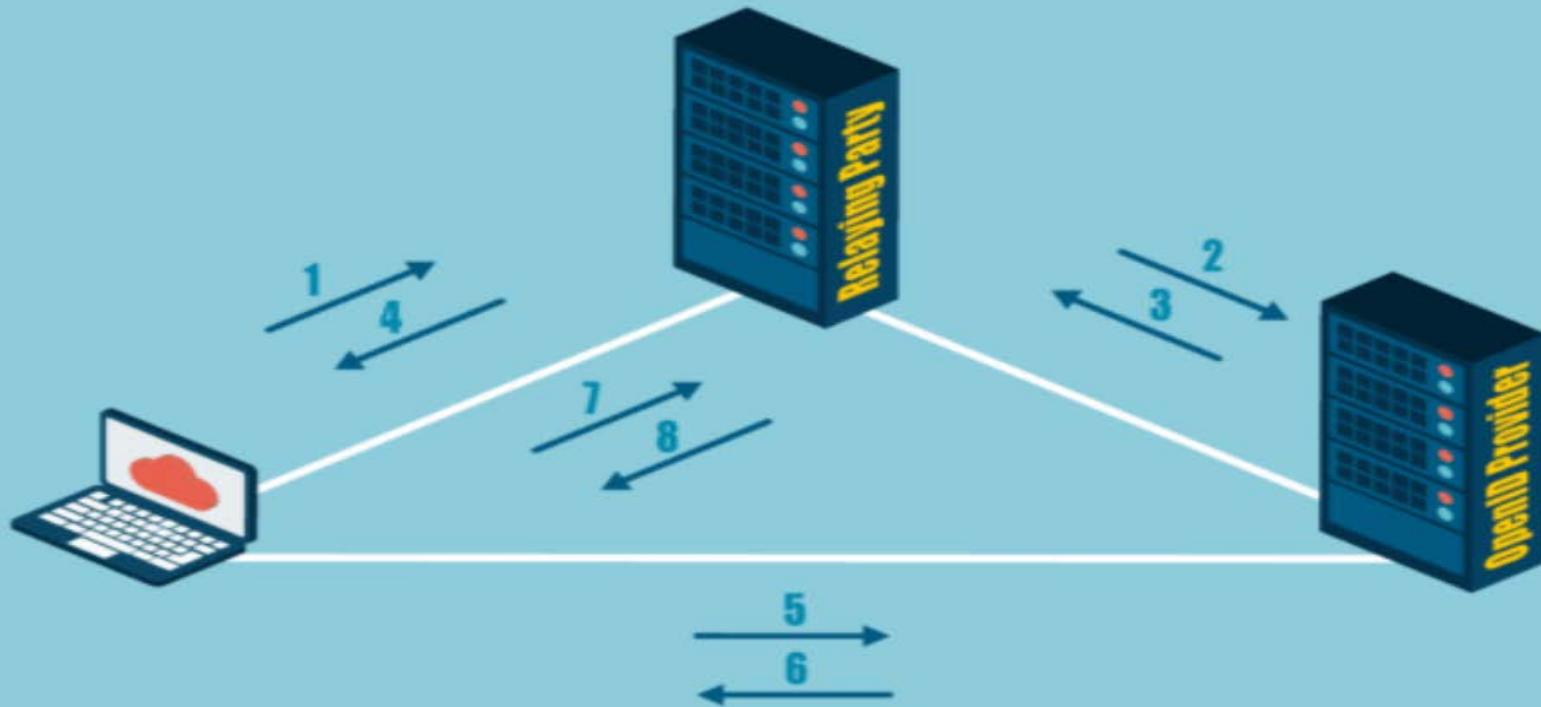


OpenID Connect



Alice is a Canadian citizen who wants to visit the US.

- At the border, the US asks for proof of identity (her passport).
- Because the US government trusts the Canadian government to accurately provide identification for its citizens, the US accepts Alice's Canadian passport as reliable proof of her identity
- Alice is allowed entry into the US, In this example, Alice is the end user, the **US is the (RP) Relying party**, and **Canada is the (OP) OpenID Provider**.



OpenID Connect Process Flow

- 1 User provides their OpenID URL (<https://jane.openidprovider.com>)
- 2 Relaying party discovers via XPS and initiates association with OpenID provider
- 3 OpenID provider generates key and association then returns key and association to relaying party
- 4 Relaying partner forwards key and association to the user
- 5 User is redirected to OpenID provider with authentication request
- 6 OpenID validates requests redirecting the user to relaying party with signed assertion
- 7 User presents signed assertion to relaying party
- 8 Relaying party validates assertion and creates session



Authorization: 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





Managing the IAAA in the Cloud through Federations

- Relevant Standards/Protocols

- 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
- SAML: XML-based framework designed to communicate user authentication, entitlement and attribute information to other entities
- 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.
- 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



WS-Federation vs. SAML

- Purpose for both WS-Fed and SAML is similar, however WS-Fed is considered faster, SAML more secure
- Decouple the applications (relying party / service provider) from identity provider.
- This decoupling allows multiple applications to use a single identity provider with a predefined protocol, and not care about the implementation
- For web applications, this works via a set of browser redirects and message exchanges.
 1. User accesses web app,
 2. the application redirects user to identity provider.
 3. User authenticates himself,
 4. identity provider issues a claims token and redirects user back to the application
 5. Application then validates the token (trust needs to be established out of band between application and IdP) then authorizes user access by asserting claims, and allows user to access protected resources.
 6. The token is then stored in the session cookie of user browser, ensuring the process doesn't have to be repeated for every access request.



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



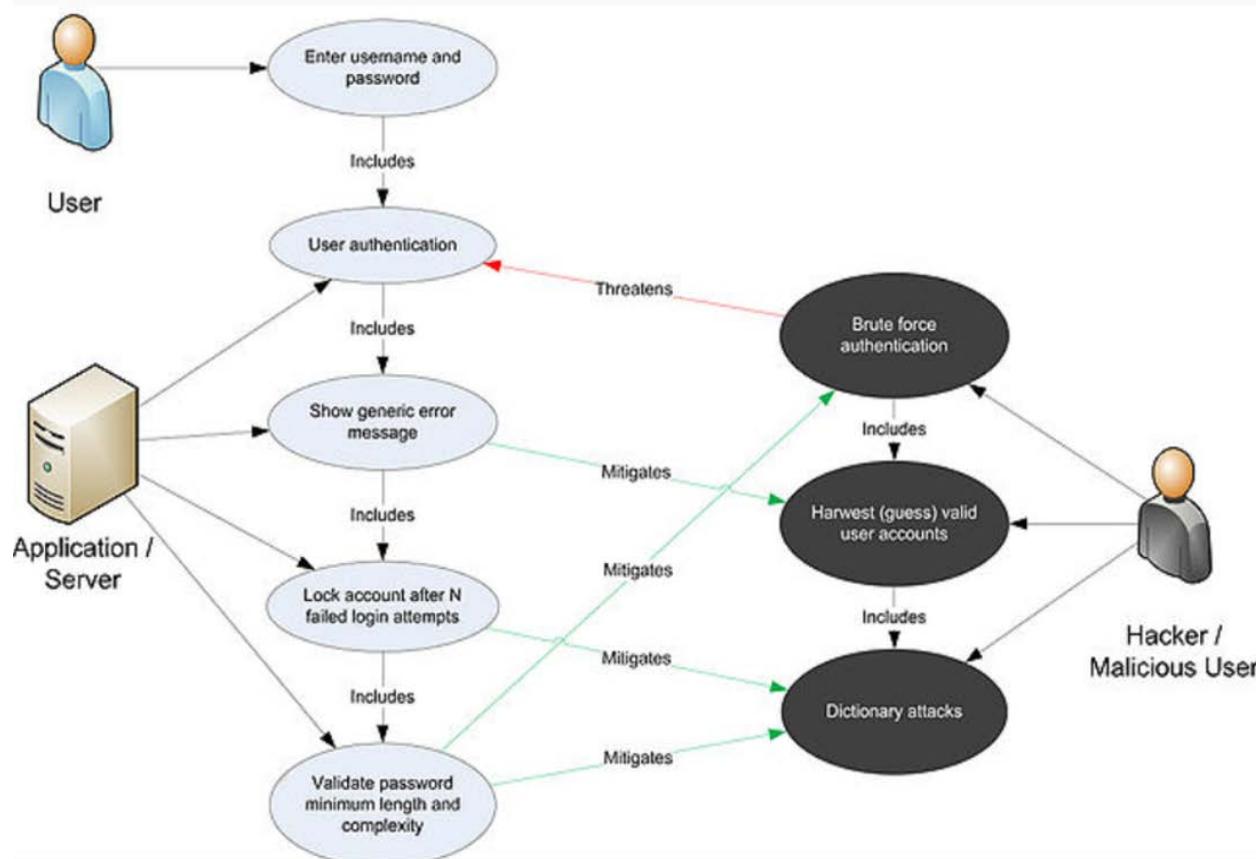


Threat Modeling

- 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 lifecycle
- 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 4 Cloud Application Security

Review Questions

1. Which of the following best represents the definition of REST?

- A. Built on protocol standards
- B. Lightweight and scalable
- C. Relies heavily on XML
- D. Only supports XML output

2. Which of the following is not one of the SDLC phases?

- A. Define
- B. Reject
- C. Design
- D. Test

3. Which of the following is *not* a component of the STRIDE model?

- A. Spoofing
- B. Repudiation
- C. Information disclosure
- D. External pen testing

4. Which of the following best describes SAST?

- A. A set of technologies that analyze application source code, and bit code for coding and design problems that would indicate a security problem or vulnerability
- B. A set of technologies that analyze application bit code, and binaries for coding and design problems that would indicate a security problem or vulnerability
- C. A set of technologies that analyze application source code, byte code, and binaries for coding and design problems that would indicate a security problem or vulnerability
- D. A set of technologies that analyze application source code for coding and design problems that would indicate a security problem or vulnerability

5. Which of the following best describes data masking?

- A. A method where the last few numbers in a dataset are not obscured. These are often used for authentication.
- B. A method for creating similar but inauthentic datasets used for software testing and user training.
- C. A method used to protect prying eyes from data such as social security numbers and credit card data.
- D. Data masking involves stripping out all similar digits in a string of numbers so as to obscure the original number.

- 6.** Which of the following best describes a sandbox?
- A.** An isolated space where transactions are protected from malicious software
 - B.** A space where you can safely execute malicious code to see what it does
 - C.** An isolated space where untested code and experimentation can safely occur separate from the production environment
 - D.** An isolated space where untested code and experimentation can safely occur within the production environment
- 7.** Identity and access management (IAM) is a security discipline that ensures which of the following?
- A.** That all users are properly authorized
 - B.** That the right individual gets access to the right resources at the right time for the right reasons
 - C.** That all users are properly authenticated
 - D.** That unauthorized users will get access to the right resources at the right time for the right reasons
- 8.** In a federated identity arrangement using a trusted third-party model, who is the identity provider and who is the relying party?
- A.** A contracted third party/the various member organizations of the federation
 - B.** The users of the various organizations within the federation/a CASB
 - C.** Each member organization/a trusted third party
 - D.** Each member organization/each member organization
- 9.** Which of the following best describes the Organizational Normative Framework (ONF)?
- A.** A container for components of an application's security, best practices, catalogued and leveraged by the organization
 - B.** A framework of containers for all components of application security, best practices, catalogued and leveraged by the organization
 - C.** A set of application security, and best practices, catalogued and leveraged by the organization
 - D.** A framework of containers for some of the components of application security, best practices, catalogued and leveraged by the organization
- 10.** APIs are defined as which of the following?
- A.** A set of protocols, and tools for building software applications to access a web-based software application or tool
 - B.** A set of standards for building software applications to access a web-based software application or tool
 - C.** A set of routines, standards, protocols, and tools for building software applications to access a web-based software application or tool
 - D.** A set of routines and tools for building software applications to access web-based Software applications

11. The application normative framework is best described as which of the following?

- A.** A stand-alone framework for storing security practices for the ONF
- B.** A subset of the ONF
- C.** A superset of the ONF
- D.** The complete ONF

12. Which of the following best describes SAML?

- A.** A standard for developing secure application management logistics
- B.** A standard for exchanging authentication and authorization data between security domains
- C.** A standard for exchanging usernames and passwords across devices
- D.** A standard used for directory synchronization

13. Which of the following best describes the purpose and scope of ISO/IEC 27034-1?

- A.** Describes international privacy standards for cloud computing
- B.** Provides an overview of application security that introduces definitive concepts, principles, and processes involved in application security
- C.** Serves as a newer replacement for NIST 800-53 r4
- D.** Provides an overview of network and infrastructure security designed to secure cloud Applications

14. Which of the following best describes data masking?

- A.** Data masking is used in place of encryption for better performance.
- B.** Data masking is used to hide PII.
- C.** Data masking is used to create a similar, inauthentic dataset used for training and Software testing.
- D.** Data masking is used in place of production data.

15. Database activity monitoring (DAM) can be:

- A.** Host-based or network-based
- B.** Server-based or client-based
- C.** Used in the place of encryption
- D.** Used in place of data masking

16. Web application firewalls (WAFs) are designed primarily to protect applications from Common attacks like:

- A.** Syn floods
- B.** Ransomware
- C.** XSS and SQL injection
- D.** Password cracking

17. Multifactor authentication consists of at least two items. Which of the following best represents this concept?

- A.** A complex password and a secret code
- B.** Complex passwords and an HSM
- C.** A hardware token and a magnetic strip card
- D.** Something you know and something you have

18. SOAP is a protocol specification providing for the exchange of structured information or data in web services. Which of the following is *not* true of SOAP?

- A.** Standards-based
- B.** Reliant on XML
- C.** Extremely fast
- D.** Works over numerous protocols

19. Dynamic application security testing (DAST) is best described as which of the following?

- A.** Test performed on an application or software product while it is using real data in production
- B.** Test performed on an application or software product while it is being executed in memory in an operating system.
- C.** Test performed on an application or software product while being consumed by cloud customers
- D.** Masking

20. Sandboxing provides which of the following?

- A.** A test environment that isolates untrusted code changes for testing in a production environment
- B.** A test environment that isolates untrusted code changes for testing in a nonproduction environment
- C.** A testing environment where new and experimental code can be tested in a production environment
- D.** A testing environment that prevents isolated code from running in a nonproduction Environment

Chapter 4: Cloud Application Security Answers

- 1.** B. The other answers all list aspects of SOAP.
- 2.** B. The other answers are all possible stages used in software development.
- 3.** D. The other answers all include aspects of the STRIDE model.
- 4.** C. All the possible answers are good, and are, in fact, correct. C, however, is the most complete and therefore the best answer.
- 5.** B. Again, all of these answers are actually correct, but B is the best answer, because it is the most general, includes the others, and is therefore the optimum choice. This is a good example of the type of question that can appear on the actual exam.
- 6.** C. Options A and B are also correct, but C is more general and incorporates them both. D is incorrect, because sandboxing does not take place in the production environment.
- 7.** B. Options A and C are also correct, but included in B, making B the best choice. D is incorrect, because we don't want unauthorized users gaining access.
- 8.** A. In a trusted third-party model of federation, each member organization outsources the review and approval task to a third party they all trust. This makes the third party the identifier
(it issues and manages identities for all users in all organizations in the federation), and the various member organizations are the relying parties (the resource providers that share resources based on approval from the third party).
- 9.** B. Option A is incorrect, because it refers to a specific applications security elements, meaning it is about an ANF, not the ONF. C is true, but not as complete as B, making B the better choice. D suggests that the framework contains only "some" of the components, which is why B (which describes "all" components) is better.
- 10.** C. All the answers are true, but C is the most complete.
- 11.** B. Remember, there is a one-to-many ratio of ONF to ANF; each organization has one ONF and many ANFs (one for each application in the organization). Therefore, the ANF is a subset of the ONF.
- 12.** B. Option C is also true, but not as comprehensive as B. A and D are simply not true.
- 13.** B. Option B is a description of the standard; the others are not.
- 14.** C. Options B and D are also correct, but not as comprehensive as C, making C the best choice. A is not correct; we don't want to encrypt data if we're using the data for testing or display purposes, the common uses of masked data.
- 15.** A. We don't use DAM in place of encryption or masking; DAM augments these options without replacing them. We don't usually think of the database interaction as client-server, so A is the best answer.
- 16.** C. WAFs detect how the application interacts with the environment, so they are optimal for detecting and refuting things like SQL injection and XSS. Password cracking, syn floods, and ransomware usually aren't taking place in the same way as injection and XSS, and they are better addressed with controls at the router and through the use of HIDS, NIDS, and antimalware tools.
- 17.** D. Option D is the best, most general, and most accurate answer.
- 18.** C. The other answers are true of SOAP.

19. B. We do the testing prior to deployment, so A and C are incorrect. D is simply a distractor.

20. A. Options B and C are incorrect, because a sandbox is not in the production environment.

D is incorrect in that sandboxing does not prevent code from running.



Domain 5

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



Logical Design

- Multi-Tenancy
- Cloud Management Plane
- Virtualization Technology
- Other logical Design Considerations
- 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 Tier 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
- 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

- 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
- 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)
 - Isolated data channels
 - Tamper warning labels
 - Housing intrusion detection
 - Fixed firmware
 - Tamper-proof circuit board
 - Safe buffer design
 - Selective USB access
 - Push-button control



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 applications 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

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

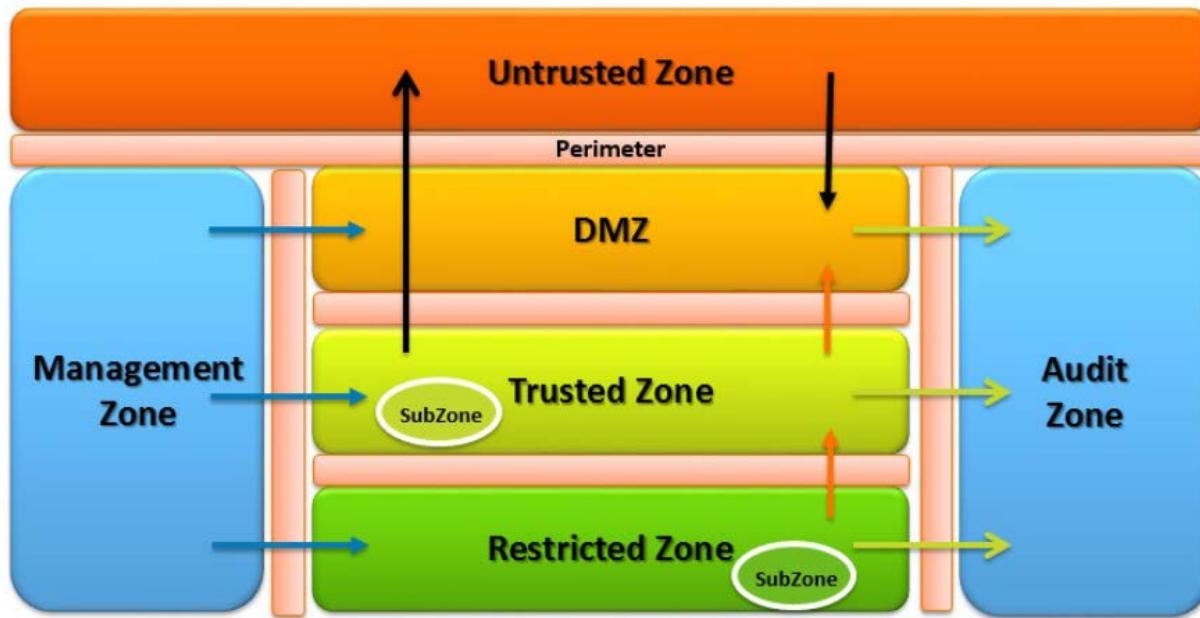
Containment:

- Control communications and resources on both inbound and outbound requests
- Set a default deny policy on all inter-segment connections





Zone Architecture

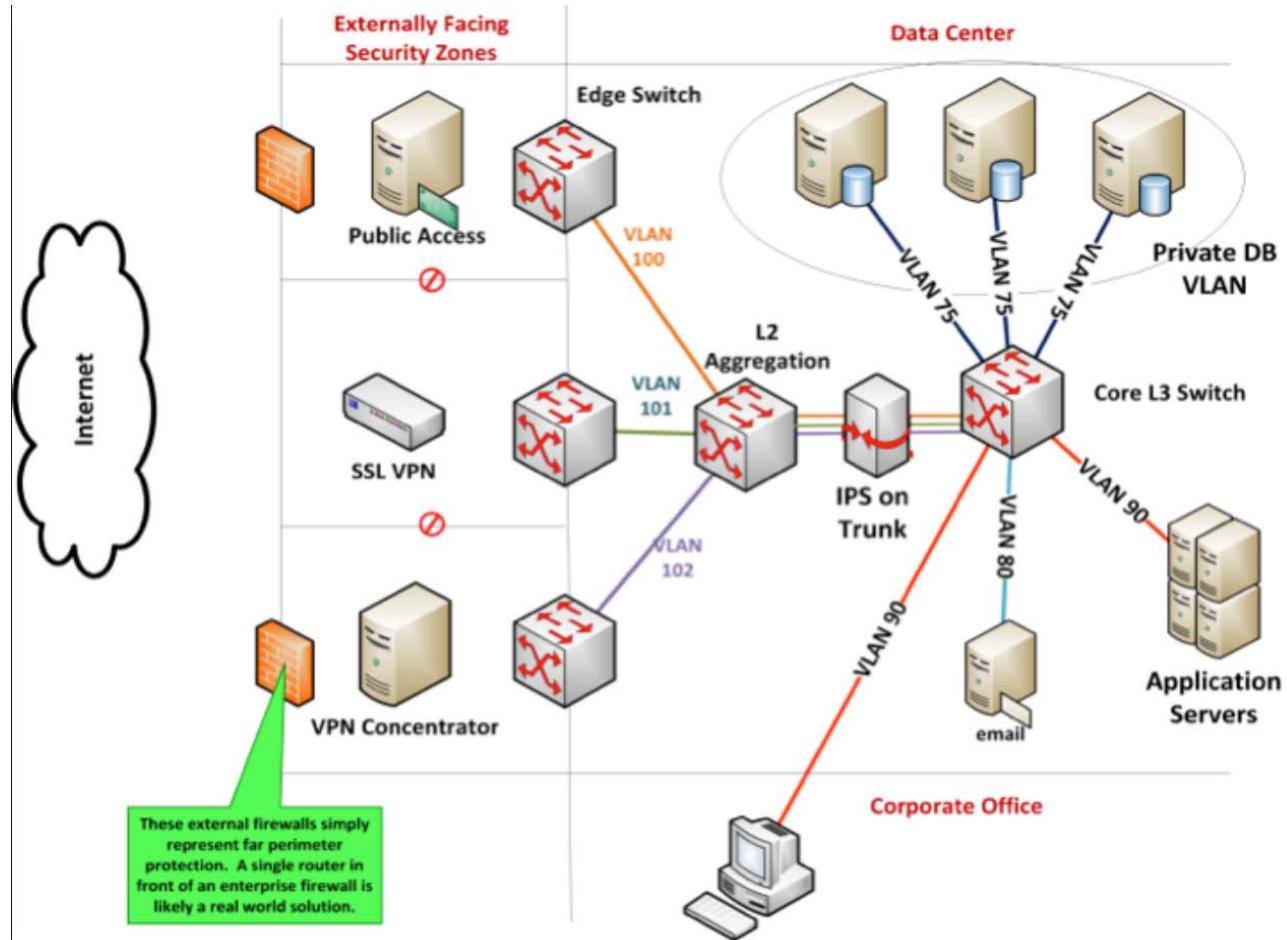


- **Untrusted Zone –**
 - External Systems (not owned by organization)
 - Internet, Public data classification
- **Semi-Trusted (DMZ) –**
 - Externally-Exposed systems
 - Public data classification
 - 3rd Party Exposed systems
 - Business Partner systems
- **Trusted Zone –**
 - Internally-Exposed systems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





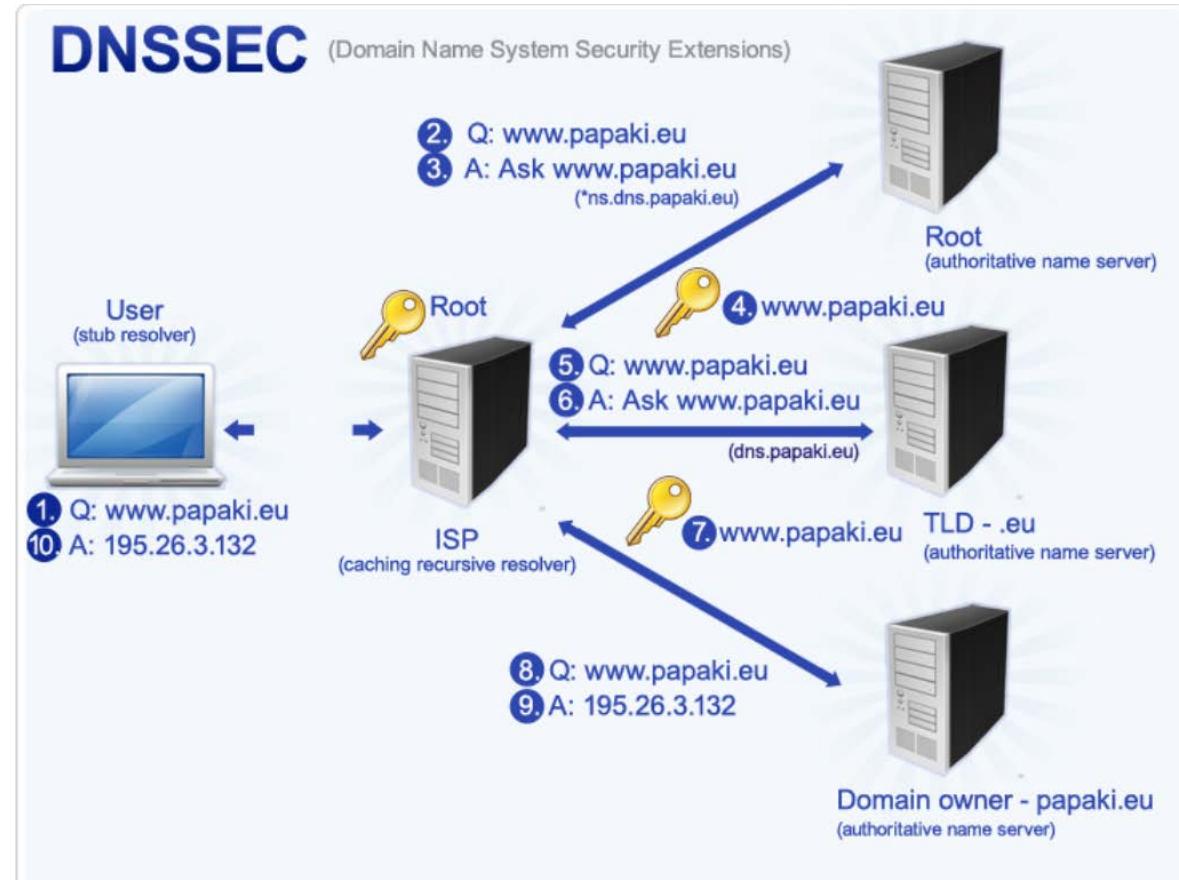
Secure network configuration: DNS

- DNS servers are desirable targets

- Footprinting
- Denial-of-Service Attack
- Data modification
- Redirection
- Spoofing



- 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**.





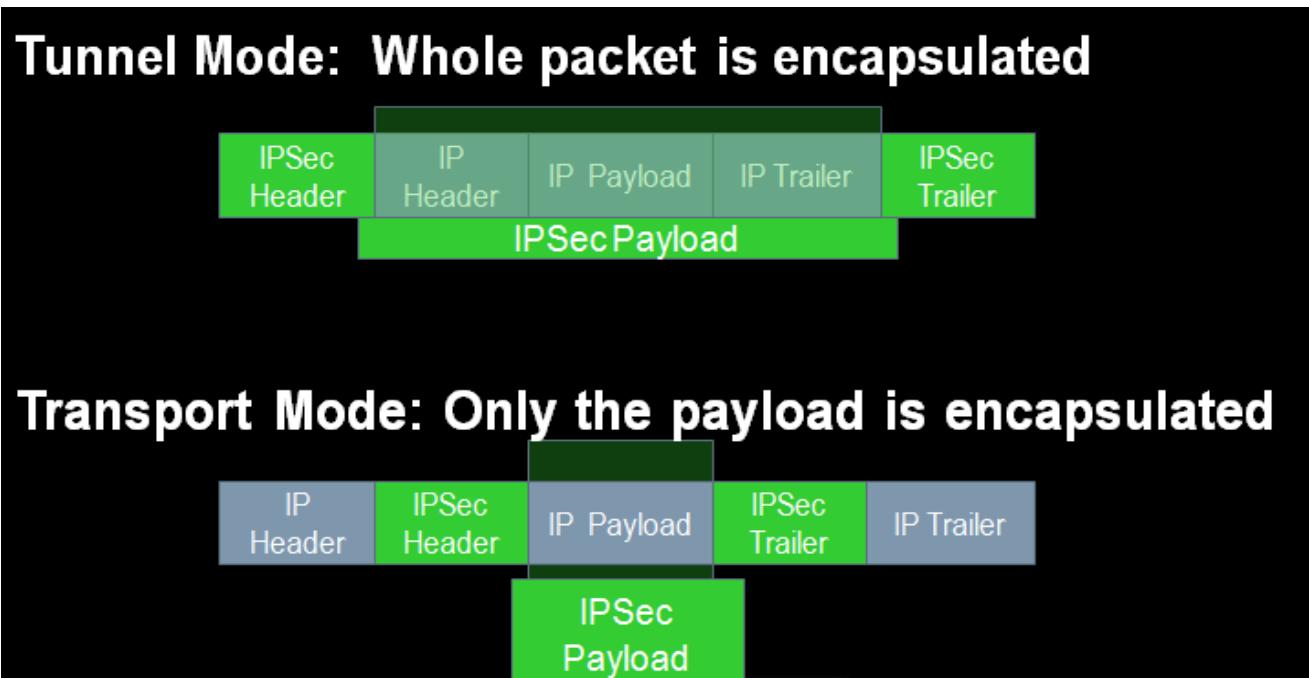
Secure network configuration

- 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.



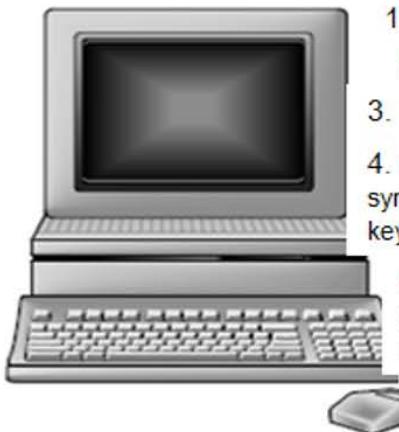


IPSec Sub-protocols

- ❑ **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



Client

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 transmits this encrypted session key across the network
5. Server is able to use its private key to decrypt the session key. Now both the 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



Server



Server threats

- Mistake – programming bug in OS or software
 - Intentional vs. unintentional actors
 - Local vs. remote
-
- Asset management, system baselines, automation technologies, change management, exception reporting system, and vendor specific configuration guidance



Clustered hosts

- Resource Sharing
 - Reservations – minimum availability of resources
 - Limits – maximum availability of resources
 - Shares – provisioning through prioritization (% based)
- Distributed Resource Scheduling (DRS)/ Compute Resource Scheduling
 - Highly available resources
 - Workload balance
 - Manage/scale without disruption



Dynamic operation

- Dynamic allocation of resources
- Elasticity: degree to which a system can adapt to workload changes by provisioning and deprovisioning resources automatically such that at each point in time the available resources match the current demand as much as possible
 - “adapt” to workload changes--flexibility
 - Customer can request, receive and later release resources
 - “Overprovisioning” costs
 - Flexible and scalable



Storage clusters

- Clustered Storage Architectures
 - Tight Coupling: Physical backplane allows high performance interconnections
 - Loose Coupling: Cost-effective growth; performance, I/O and storage within same node; scales with capacity
- Storage Cluster Goals
 - Required service levels (SLA)
 - Separate customer data in multi-tenancy
 - Confidentiality/ Integrity/ Availability



Maintenance mode

- A configuration mode utilized when updating or configuring different components of the cloud environment.
- Vendor specific guidelines for entering, operating in and exiting maintenance mode
- should be documented in SLA
- While in maintenance mode, customer access is blocked and alerts are disabled. Logging is still enabled
- Hosted VMs and data should be migrated prior to entering maintenance mode if they require availability through the maintenance period
- Often used to patch/update systems and mitigate issues



Physical infrastructure

- Flexible and efficient
- Faster deployment of resources
- Higher application service levels
- Less administrative overhead
- Lower infrastructure, energy and facility costs
- Increased security



Physical infrastructure (cont.)

- Servers
- Virtualization
- Storage
- Network
- Management
- Security
- Backup and Recovery
- Infrastructure Systems



Access control for remote access

- “Private” cloud
- “Community” cloud
- “Public” cloud
- “Hybrid” cloud
- Scope (General, On-site private, outsourced private, On-site community, outsourced community, Public)



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



Backup and restoration

- Inclusion of configuration data for hosts
- Control
 - Access – Who and what
- Visibility
 - Monitor status of data and programs



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
 - PatternMatching
 - 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)



Management plan

- Maintenance
 - Scheduling
 - Notification
 - Adequate Resources
- Orchestration
 - Automation
 - Configuration, coordination, and management
 - SLA requirements of provider



Building a Logical infrastructure

- Logical Design
- Physical Design
- Secure Configuration (Hardware Specific)
 - Storage Controller Configuration
- Networking Models
 - Traditional Networking Model
 - Converged Networking Model



Running a logical infrastructure

- Building a Secure Configuration
 - VLANs
 - TLS
 - DNS
 - IPSec
- OS Hardening via App Baseline
- Baseline Configuration by Platform
 - Windows/ Linux/ VMware



Running a logical infrastructure (Cont.)

- Availability of a Guest OS
 - High Availability
 - Line recovery
 - Automatic migration
 - Fault Tolerance
 - Component, storage, server w/ built-in fault tolerance
 - Software based implementation for OS



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



Network security controls

- Defense in Depth
- VLANs
- Access Controls
- IPSec and TLS
- IDS/IPS Deployment
- Firewalls
- Honeypots/nets
- Separation of flow
- Zoning and masking
- vCNS/ NSX



Network security controls (cont.)

- Log Capture and Analysis
 - Centralization and off-site storage
- Management Plan Implementation
 - Due diligence and research
- Compliance – Regulations and Controls
 - Current awareness vs. cloud requirements



IT Service Management (ITSM)

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



Operations management

- Information Security
- Configuration
- Change
- Incident Response
- Release and Deployment
- Service Level
- Availability
- Capacity
- Business Continuity
- Continual Service Improvement



Operations management (cont.)

- Information Security Management
 - Policy
 - Organization
 - Assets
 - Human Resources
 - Physical and Environmental
 - Communications
 - Access Control
 - Acquisition, development and maintenance
 - Responsibility



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



Operations management

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



Operations management (cont.)

- Incident Management
 - Event: A change in state
 - Incident: a collection of events which have an impact on a system
 - Purpose of Incident Response—minimize the impact to the business
 - Objectives
 - Incident Management Plan
 - Incident Management Teams
 - Classification: Impact * Urgency = Priority
 - Process



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

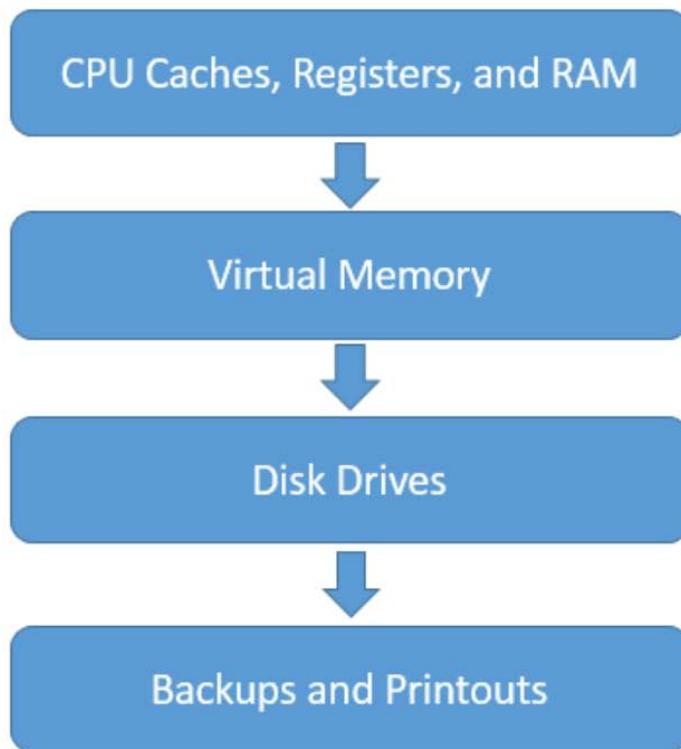


The Process of Digital Forensics

- 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
- Exam—Data
- Analysis—Information
- Reporting
- Lessons Learned



Volatility



Swap File





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



Risk Management

- Processes of identifying, analyzing, assessing, mitigating, or transferring risk.
- The main goal is to mitigate risk until the residual risk falls within acceptable levels of tolerance
- “Umbrella” term that includes all risk-related actions



Risk Definitions

- Asset: Anything of Value to the company
- Vulnerability: A weakness; the absence of a safeguard
- 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 probability of a threat materializing
- Controls: Physical, Administrative, and Technical Protections
 - Safeguards
 - Countermeasure
- Total Risk: The risk that exists before any control is implemented
- Residual Risk: Leftover risk after applying a control
- Secondary Risk: When one risk response triggers another risk event



Risk Management Steps

- Risk Assessment
 - Identify and Valuate Assets
 - Identify Threats and Vulnerabilities
- Risk Analysis
 - Qualitative vs. Quantitative
- Risk Mitigation/Response
 - Reduce
 - Accept
 - Transfer
 - Avoid
 - Reject
- Ongoing Controls Evaluation

Information Asset	Existing Controls	Vulnerability	Threat	Likelihood of Threat	Impact (Confidentiality, Integrity, Availability)	Risk Level	Risk Treatment Control	Likelihood of Threat	Impact (Confidentiality, Integrity, Availability)	iRisk Level After Treatment
Information, system, person, process or facility	Description of current controls that protect the asset.	Opportunities to compromise the asset if controls are not present or are weak.	What action or event could cause a negative impact to this asset in consideration of the vulnerability?	"How often do we expect this threat to create an impact?" Not Foreseeable = 1 Foreseeable = 2 Low = 3 Medium = 4 High = 5 (See scoring guidance)"	"What would be the impact to the mission if this threat occurs?" Negligible = 1 Low = 2 Medium = 3 High = 4 Severe = 5 (See scoring guidance)"	"Low = 1 - 6 Medium = 8-10 High = 12 - 16 Severe = 20 - 25 Risk = Impact x Likelihood Acceptable Level Below 8.0"	What control will we apply to address this risk? (See comment for guidance on likelihood levels)"	"Not Foreseeable = 1 Foreseeable = 2 Low = 3 Medium = 4 High = 5 (See scoring guidance)"	"Very Low = 1 Low = 2 Medium = 3 High = 4 Severe = 5 (See comment for guidance on impact levels)"	"Low = 1 - 6 Medium = 8-10 High = 12 - 16 Severe = 20 - 25 Risk = Impact x Likelihood Acceptable Level Below 8.0"
Access rights	Passwords are required to access Windows end-user systems	Local administrator accounts on end-user machines use the same administrator password.	This configuration allows pass-the-hash attacks which provide people or malware access to any other similarly configured system on the local area network. A breach to any machine can leak any information in the enterprise.	Low	Medium	9.00	Salt administrator passwords with machine names so the hashed versions of the passwords cannot be used to access other systems.	Not Foreseeable	Very Low	1.00
In-House Developed applications	Programmers create applications that satisfy stated business requirements	Applications are developed without adherence to standard security practices (see OWASP), such as input filtering, session protection, encryption storage or proper configuration.	Applications that provide access to PII are internally developed and are demonstrated as being highly susceptible to attack. A breach of all stored PII could occur through applications.	Medium	Severe	20.00	Install a Web Application Firewall (WAF) immediately. Create a plan to recode all applications over the next three years to make them more resilient against attack, following OWASP and other standards.	Foreseeable	Medium	6.00
VPN access	User laptops store unique soft tokens that are paired with soft token at the VPN router. Users can access the VPN using laptops with those registered soft tokens and a user name and password	Client requires that we provide hard tokens to allow access to systems, as stated in their contracts and audit tests.	If a laptop is stolen and a user name and password is known, then access to the VPN and protected client data will occur, creating a breach and likely loss of the contract.	Foreseeable	Medium	6.00	Deploy 250 hard tokens to users, and a process for managing tokens for the 6-month rotated assignment of the hard tokens.	Foreseeable	Medium	6.00



Risk Analysis

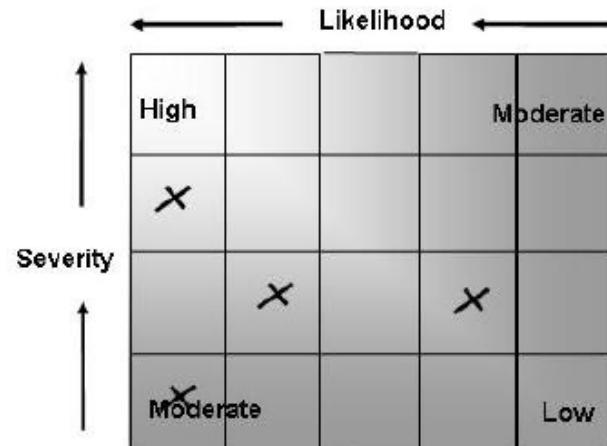
- Qualitative
 - Subjective analysis to help prioritize probability and impact of risk events.
 - May use Delphi Technique
- Quantitative:
 - Using objective, empirical data , often seeking to provide a dollar value to a particular risk event.
 - Much more sophisticated in nature, a quantitative analysis if much more difficult and requires a special skill set
 - Business decisions are made on a quantitative analysis
 - Can't exist on its own. Quantitative analysis depends on qualitative information



Qualitative Analysis

- Subjective in Nature
- Uses words like “high” “medium” “low” to describe likelihood and severity (or probability and impact) of a threat exposing a vulnerability
- Delphi technique is often used to solicit objective opinions

**Inherent (Initial) Risk
(before controls)**



Exposure areas:
Information Integrity Loss
Disclosure
Availability Loss



Quantitative Analysis

- More experience required than with Qualitative
- Involves calculations to determine a dollar value associated with each risk event
- Business Decisions are made on this type of analysis
- Goal is to the dollar value of a risk and use that amount to determine what the best control is for a particular asset
- Necessary for a cost/benefit analysis



Quantitative Analysis Formulas and Terms

- (AV) Asset Value: Dollar figure that represents what the asset is worth to the organization
- (EF) Exposure Factor: The percentage of loss that is expected to result in the manifestation of a particular risk event.
- (SLE) Single Loss Expectancy: Dollar figure that represents the cost of a single occurrence of a threat instance
- (ARO) Annual Rate of Occurrence: How often the threat is expected to materialize
- (ALE) Annual Loss Expectancy: Cost per year as a result of the threat
- (TCO) Total Cost of Ownership is the total cost of implementing a safeguard. Often in addition to initial costs, there are ongoing maintenance fees as well.
- (ROI) Return on Investment: Amount of money saved by implementation of a safeguard. Sometimes referred to as the value of the safeguard/control.



Quantitative Analysis Formulas

- $SLE = AV * EF$
- $ALE = SLE * ARO$

$TCO = \text{Initial Cost of Control} + \text{Yearly fees}$

Return on Investment:

ALE (before implementing control)
– ALE (after implementing control)
– cost of control
= ROI (Value of Control)



Risk Mitigation

- Quantitative Analysis leads to the proper risk Mitigation strategy.
- Reduce
- Accept
- Transfer
- Avoidance
- Rejection



Managing risk (logical & physical)

- Adverse Impacts
- Likelihood of Occurrence
- Loss of confidentiality, integrity or availability
- Impact to operations (mission, function, image or reputation), organizational assets, individuals and other organizations



Risk-management process

- Framing risk
- Assessing risk
 - Conducting a Risk Assessment (Qualitative vs. Quantitative); Single Loss Expectancy (SLE), Annualized Rate of Occurrence (ARO), Annualized Loss Expectancy (ALE)
 - Identifying Vulnerabilities
 - Identifying Threats
 - Selecting Tools and Techniques
 - Likelihood Determination



Risk-management process (cont.)

- Responding to risk
 - Determination of impact
 - Determination of risk
 - Critical aspects
 - Traditional Responses
- Monitoring risk
 - Residual Risk
 - Risk Assignment
 - Countermeasure Selection
 - Implementation (Mobile App, Web 2.0, Cloud...)



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

Chapter 5 Operations Review Questions PART I

1. What is the lowest tier of datacenter redundancy, according to the Uptime Institute?

- A. 1
- B. V
- C. C
- D. 4

2. What is the amount of fuel that should be on hand to power generators for backup datacenter

power, in all tiers, according to the Uptime Institute?

- A. 1
- B. 1,000 gallons
- C. 12 hours
- D. As much as needed to ensure all systems may be gracefully shut down and data securely stored

3. Which of the following is *not* one of the three types of training?

- A. Integral
- B. Initial
- C. Recurring
- D. Refresher

4. Which of the following is part of the STRIDE model?

- A. Repudiation
- B. Redundancy
- C. Resiliency
- D. Rijndael

5. Which of the following is *not* part of the STRIDE model?

- A. Spoofing
- B. Tampering
- C. Resiliency
- D. Information disclosure

6. Which of the following is *not* a feature of SAST?

- A. Source code review
- B. Team-building efforts
- C. "White-box" testing
- D. Highly skilled, often expensive outside consultants

7. Which of the following is *not* a feature of DAST?

- A. Testing in runtime
- B. User teams performing executable testing
- C. "Black-box" testing
- D. Binary inspection

8. Which of the following is *not* a feature of a secure KVM component?

- A. Keystroke logging
- B. Sealed exterior case
- C. Welded chipsets

- D.** Push-button selectors
- 9.** What type of redundancy can we expect to find in a datacenter of any tier?
- A.** All operational components
 - B.** All infrastructure
 - C.** Emergency egress
 - D.** Full power capabilities
- 10.** What should be the primary focus of datacenter redundancy and contingency planning?
- A.** Critical path/operations
 - B.** Health and human safety
 - C.** Infrastructure supporting the production environment
 - D.** Power and HVAC
- 11.** Which of the following techniques for ensuring cloud datacenter storage resiliency uses parity bits and disk striping?
- A.** Cloud-bursting
 - B.** RAID
 - C.** Data dispersion
 - D.** SAN
- 12.** Which resiliency technique attenuates the possible loss of functional capabilities during contingency operations?
- A.** Cross-training
 - B.** Metered usage
 - C.** Proper placement of HVAC temperature measurements tools
 - D.** Raised floors
- 13.** Which of the following has *not* been attributed as the cause of lost capabilities due to DoS?
- A.** Hackers
 - B.** Construction equipment
 - C.** Changing regulatory motif
 - D.** Squirrels
- 14.** Which of the following aids in the ability to demonstrate due diligence efforts?
- A.** Redundant power lines
 - B.** HVAC placement
 - C.** Security training documentation
 - D.** Bollards
- 15.** What is often a major challenge to getting both redundant power and communications utility connections?
- A.** Expense
 - B.** Carrying medium
 - C.** Personnel deployment
 - D.** Location of many datacenters
- 16.** Which of the following is *not* an aspect of physical security that ought to be considered in

the planning and design of a cloud datacenter facility?

- A. Perimeter
- B. Vehicular approach/traffic
- C. Fire suppression
- D. Elevation of dropped ceilings

17. The Brewer-Nash security model is also known as which of the following?

- A. MAC
- B. The Chinese Wall model
- C. Preventive measures
- D. RBAC

18. Which kind of hypervisor would malicious actors prefer to attack, ostensibly because it offers a greater attack surface?

- A. Cat IV
- B. Type II
- C. Bare metal
- D. Converged

19. Which of the following techniques for ensuring cloud datacenter storage resiliency uses encrypted chunks of data?

- A. Cloud-bursting
- B. RAID
- C. Data dispersion
- D. SAN

20. Security training should *not* be:

- A. Documented
- B. Internal
- C. A means to foster a non-adversarial relationship between the security office and operations personnel
- D. Boring

Review Questions Chapter 5 Operations PART II

1. Which form of BC/DR testing has the most impact on operations?

- A. Tabletop
- B. Dry run
- C. Full test
- D. Structured test

2. Which form of BC/DR testing has the least impact on operations?

- A. Tabletop
- B. Dry run
- C. Full test
- D. Structured test

3. Which characteristic of liquid propane increases its desirability as a fuel for backup generators?

- A. Burn rate
- B. Price
- C. Does not spoil
- D. Flavor

4. How often should the CMB meet?

- A. Whenever regulations dictate
- B. Often enough to address organizational needs and attenuate frustration with delay
- C. Every week
- D. Annually

5. Adhering to ASHRAE standards for humidity can reduce the possibility of .

- A. Breach
- B. Static discharge
- C. Theft
- D. Inversion

6. A UPS should have enough power to last how long?

- A. 12 hours
- B. 10 minutes
- C. One day
- D. Long enough for graceful shutdown

236 Chapter 9 ■ Operations Management

7. A generator transfer switch should bring backup power online within what time frame?

- A. 10 seconds
- B. Before the recovery point objective is reached
- C. Before the UPS duration is exceeded
- D. Three days

8. Which characteristic of automated patching makes it attractive?

- A. Cost
- B. Speed
- C. Noise reduction
- D. Capability to recognize problems quickly

9. Which tool can reduce confusion and misunderstanding during a BC/DR response?

- A. Flashlight
- B. Controls matrix
- C. Checklist
- D. Call tree

10. When deciding whether to apply specific updates, it is best to follow , in order to demonstrate due care.

- A. Regulations
- B. Vendor guidance
- C. Internal policy
- D. Competitors' actions

- 11.** The CMB should include representations from all of the following offices except:
- A. Regulators
 - B. IT department
 - C. Security office
 - D. Management
- 12.** For performance purposes, OS monitoring should include all of the following except:
- A. Disk space
 - B. Disk I/O usage
 - C. CPU usage
 - D. Print spooling
- 13.** Maintenance mode requires all of these actions except:
- A. Remove all active production instances
 - B. Initiate enhanced security controls
 - C. Prevent new logins
 - D. Ensure logging continues
- 14.** What is one of the reasons a baseline might be changed?
- A. Numerous change requests
 - B. Power fluctuation
 - C. To reduce redundancy
 - D. Natural disaster
- 15.** In addition to battery backup, a UPS can offer which capability?
- A. Communication redundancy
 - B. Line conditioning
 - C. Breach alert
 - D. Confidentiality
- 16.** Deviations from the baseline should be investigated and .
- A. Documented
 - B. Enforced
 - C. Revealed
 - D. Encouraged
- 17.** The baseline should cover which of the following?
- A. As many systems throughout the organization as possible
 - B. Data breach alerting and reporting
 - C. A process for version control
 - D. All regulatory compliance requirements
- 18.** A localized incident or disaster can be addressed in a cost-effective manner by using which of the following?
- A. UPS
 - B. Generators
 - C. Joint operating agreements
 - D. Strict adherence to applicable regulations
- 19.** Generator fuel storage for a cloud datacenter should last for how long, at a minimum?
- A. 10 minutes

- B.** Three days
 - C.** Indefinitely
 - D.** 12 hours
- 20.** The BC/DR kit should include all of the following except:
- A.** Flashlight
 - B.** Documentation equipment
 - C.** Hard drives
 - D.** Annotated asset inventory

Answers Chapter 5 Operations Review Questions PART I

- 1.** A. There are four tiers of the Uptime Institute's datacenter redundancy rating system, with 1 being the lowest and 4 the highest.
- 2.** C. The other answers are distractors.
- 3.** A. The three common types of security training are initial, recurring, and refresher.
- 4.** A. Repudiation is an element of the STRIDE model; the rest of the answers are not.
- 5.** C. Resiliency is not an element of the STRIDE model; all the rest of the answers are.
- 6.** B. Team-building has nothing to do with SAST; all the rest of the answers are characteristics of SAST.
- 7.** D. Binary inspection has nothing to do with DAST, and it is not really a term that means anything in our industry (although it could be interpreted as a type of code review, more related to SAST); all the rest of the answers are characteristics of DAST.
- 8.** A. Keystroke logging is not a characteristic of secure KVM design; in fact, secure KVM components should attenuate the potential for keystroke logging. All the rest of the answers are characteristics of secure KVM components.
- 9.** C. Emergency egress redundancy is the only aspect of datacenters that can be expected to be found in datacenters of any tier; the rest of the answers list characteristics that can be found only in specific tiers.
- 10.** B. Regardless of the tier level or purpose of any datacenter, design focus for security should always consider health and human safety paramount.
- 11.** B. Parity bits and disk striping are characteristic of RAID implementations. Cloud-bursting is a feature of scalable cloud hosting. Data dispersion uses parity bits, but not disk striping; instead, it uses data chunks and encryption. SAN is a data storage technique, but not focused on resiliency.
- 12.** A. Cross-training offers attenuation of lost contingency capabilities by ensuring personnel will be able to perform essential tasks, even if they are not primarily assigned to those positions in a full-time capacity. Metered usage is a benefit for cloud customers associated with ensuring value for payment, but not resiliency. Proper placement of HVAC temperature measurement and raised floors both aid in optimizing component performance but are not practically associated with resiliency. This is a difficult question, and it could be read in ways that would suggest other correct answers.
- 13.** C. Changing regulations should not result in lack of availability. All the other answers have caused DoS outages.

14. C. Security training documentation can be used to show that personnel have received adequate, pertinent training to a suitable level, which demonstrates due diligence—that is, effort in furtherance of due care. All the other answers are beneficial to the resiliency and durability of the datacenter, but they are not methods for demonstrating due diligence. This is a difficult question, and it could be read in ways that would suggest other correct answers.

15. D. The location of many datacenters—rurally situated, distant from metropolitan areas—may create challenges for finding multiple power utility providers and ISPs, as those areas just aren't usually served by multiple vendors. Expense is not usually a concern; economies of scale make costs acceptable as part of the pricing structure. Personnel deployment doesn't usually affect access to either type of connection. The carrying medium has nothing to do with challenges for finding multiple providers and is not even a common industry term.

16. D. The height of dropped ceilings is not a security concern, except in action movies. The rest of the answers are all aspects of physical security that should be taken into account when planning and designing a datacenter.

17. B. The Brewer-Nash model is also known as the Chinese Wall model.

18. B. Type II hypervisors run via the OS on the host machine; this makes them attractive to attackers, as both the machine and the OS offer potential attack vectors. Cat IV and converged

are not terms associated with hypervisors. Bare-metal hypervisors (Type I) are less preferable to attackers, as they offer less attack surface.

19. C. Data dispersion uses parity bits, data chunks, and encryption. Parity bits and disk striping

are characteristic of RAID implementations. Cloud-bursting is a feature of scalable cloud hosting. SAN is a data storage technique but not focused on resiliency.

20. D. Security training should not be boring; you want attendees to be enthused so that they

pay attention, which enhances recall of the material, elevating security for the organization. All the other answers are characteristics of good security training.

Answers Chapter 5 Operations Review Questions PART II

1. C. The full test will involve every asset in the organization, including all personnel. The others will have lesser impact, except for D, which is a red herring.

2. A. The tabletop testing involves only essential personnel and none of the production assets.

The others will have greater impact, except for D, which is a red herring.

3. C. Liquid propane does not spoil, which obviates necessity for continually refreshing and restocking it and might make it more cost-effective. The burn rate has nothing to do with its suitability, unless it has some direct bearing on the particular generator the datacenter owner has chosen. The various relative prices of fuel fluctuate. Flavor is a distractor in this question and means nothing.

4. B. Frustrated employees and managers can increase risk to the organization by implementing

their own, unapproved modifications to the environment. The particular interval changes from organization to organization.

5. B. A datacenter with less than optimum humidity can have a higher static electricity discharge

rate. Humidity has no bearing on breaches or theft, and inversion is a nonsense term used as a distractor.

6. D. The UPS is intended to last only long enough to save production data currently being processed. The exact quantity of time will depend on many variables and will differ from one datacenter to the next.

7. C. Generator power should be online before battery backups fail. The specific amount of time will vary between datacenters.

8. B. Automated patching is much faster and more efficient than manual patching. It is, however,

not necessarily any less expensive than manual patching. Manual patching is overseen by administrators, who will recognize problems faster than automated tools. Noise reduction

is not a factor in patch management at all.

9. C. Checklists serve as a reliable guide for BC/DR activity and should be straightforward enough to use that someone not already an expert or trained in BC/DR response could ostensibly accomplish the necessary tasks. Flashlights and call trees are certainly useful during BC/DR actions, but not for the purpose of reducing confusion and misunderstanding.

Control matrices are not useful during BC/DR actions.

10. B. A datacenter that doesn't follow vendor guidance might be seen as failing to provide due

care. Regulations, internal policy, and the actions of competitors might all inform the decision

to perform an update and patch, but these are not necessarily directly bearing on due care. This

is a difficult, nuanced question, and all the answers are good, but option B is the best.

11. A. Regulators are not involved in an organization's CMB; all the rest are.

12. D. Print spooling is not a metric for system performance; all the rest are.

13. B. While the other answers are all steps in moving from normal operations to maintenance

mode, we do not necessarily initiate any enhanced security controls.

14. A. If the CMB is receiving numerous change requests to the point where the amount of requests would drop by modifying the baseline, then that is a good reason to change the baseline. None of the other reasons should involve the baseline at all.

15. B. A UPS can provide line conditioning, adjusting power so that it is optimized for the devices it serves and smoothing any power fluctuations; it does not offer any of the other listed functions.

Chapter 10: Legal and Compliance Part 1 **323**

16. A. All deviations from the baseline should be documented, including details of the investigation

and outcome. We do not enforce or encourage deviations. Presumably, we would already be aware of the deviation, so “revealing” is not a reasonable answer.

17. A. The more systems that be included in the baseline, the more cost-effective and scalable

the baseline is. The baseline does not deal with breaches or version control; those are the provinces of the security office and CMB, respectively. Regulatory compliance might (and usually will) go beyond the baseline and involve systems, processes, and personnel that are not subject to the baseline.

18. C. Joint operating agreements can provide nearby relocation sites so that a disruption limited to

the organization’s own facility and campus can be addressed at a different facility and campus.

UPS and generators are not limited to serving needs for localized causes. Regulations do not

promote cost savings and are not often the immediate concern during BC/DR activities.

19. D. The Uptime Institute dictates 12 hours of generator fuel for all cloud datacenter tiers.

20. C. While hard drives may be useful in the kit (for instance, if they store BC/DR data such as inventory lists, baselines, and patches), they are not necessarily required. All the other items should be included.



LEGAL AND COMPLIANCE

Domain 6



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



International legal conflicts

- Local law vs. global technology offerings
- Trans-border disputes
- Data breach application
- 2011 – Cloudflare/ LulzSec
- 2014 – Microsoft/ eMail



Legislative concepts

- International Law
- State Law
- Copyright/Piracy
- Enforceable Government Request
- Intellectual Property
- Privacy
- Doctrine
- Criminal
- Tort
- Restatement Conflict



Frameworks and guidelines

- Organization for Economic Cooperation and Development (OECD) – Privacy and Security
- Asia Pacific Economic Cooperation (APEC) Privacy Framework
- EU Data Protection Directive
- General Data Protection Regulation
- ePrivacy Directive
- HIPAA, GLBA and others



Common legal requirements

- US Federal Law
- States Laws
- Standards
- International and Regional Regulations
- Contractual Obligations
- Restrictions of Cross-border Transfers



Legal controls and Cloud providers

- Third party dynamic – PROVIDER
- Understanding of legal application to each party
 - Collect, store, process & destroy
- Safe Harbor, HIPAA, PCI
- Specific positions – CEO/CIO, BoD
- Contractual clauses for customer and provider
- Accountability



E-discovery

- Challenges
- Considerations and Responsibilities
- Reducing Risk
- eDiscovery Investigations
 - SaaS-based eDiscovery
 - Hosted eDiscovery (provider)
 - Third-party eDiscovery



Cloud forensics and Iso/iec 27050-1

- Involvement of service providers
- Importance of communication
- ISO/IEC standards for best practices
 - 27037:2012
 - 27041:2014-01
 - 27042:2014-01
 - 27043
 - 27050-1



Personal information

- Contractual vs. Regulated Personally Identifiable Information (PII)
 - Contractual PII
 - Scope, subcontractors, removal/deletion of data, security controls, location, return/restitution, audit rights
 - Regulated PII
 - Mandatory breach reporting



Personal information (cont.)

- Country Specific Legislation and Regulations
 - European Union
 - EU Data Protection Directive (also known as Directive 95/46/EC) is a regulation adopted by the European Union to protect the privacy and protection of all personal data collected for or about citizens of the EU, especially as it relates to processing, using or exchanging such data
 - Asia-Pacific Economic Cooperation Council (APEC)
 - A framework recognizing the importance of the development of effective privacy protections that avoid barriers to information flows, ensure continued trade, and economic Growth
 - Canada
 - The Personal Information Protection and Electronic Documents Act (PIPEDA) conforms to the EU Data Directive and Privacy Regulation.
 - US
 - Requires users to “opt-out” consent with exceptions for sensitive information for health care and other
 - COPPA (Children’s Online Privacy Protection Rule) imposes certain requirements on operators of websites or online services directed to children under 13 years of age



Personal information (cont.)

- United States
 - Safe Harbor
 - Safe Harbor Alternative
 - EU View on US Privacy
 - HIPAA – 1996
 - GLBA
 - Stored Communication Act
 - Sarbanes-Oxley Act (SOX)



Personal information (cont.)

- Australia and New Zealand
 - APPS (Cross-border disclosure)
 - APP11.1
- Russia
- Switzerland
 - Third party data processing
 - Transferring Abroad
 - Data Security



Auditing in the cloud

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



Auditing in the cloud (cont.)

- Impact of Requirement Programs
- Assuring Challenges of Cloud & Virtualization
- Information Gathering
- Audit Scope
 - Statements
 - Restrictions
 - Gap Analysis



Auditing in the cloud (cont.)

- Cloud Auditing Goals
- Audit Planning
 - Define Objectives
 - Define Scope
 - Conduct Audit
 - Refine Process/ Lessons Learned



Standard privacy (iso/iec 27018)

- Consent
- Control
- Transparency
- Communications
- Independent annual audits



Generally accepted privacy principles (gapp)

- AICPA standard
 - 74 detailed principles
 - 10 privacy principles groups
 - Define, document, communicate, assign
 - Provide notice
 - Describe choices
 - Collection... etc.



Internal Information Security Management Systems (ISMS)

- Value of an ISMS
 - Structure, measured and ongoing security
 - “top-down” sponsorship and endorsement
- ISO 27001:2013 Domains – A.5 through A.18
 - “established guidelines and general principles...”
- Repeatability and Standardization
 - Policies, practices and controls
 - Standardizing and measuring
 - Reliance and dependencies on third parties



Implementing policies

- Organizational Policies
- Functional Policies
- Cloud Computing Policies
 - Password
 - Remote Access
 - Encryption
 - Third-party
 - Segregation of Duties
 - Incident Management
 - Backup and Recovery



Relevant stakeholders

- Stakeholder Identification Challenges
 - Defining architecture, objectivity, engagement, cost identification, extending risk management
- Governance Challenges
 - Audits, regulatory and legal compliance, reporting, updating and documenting
- Communication Coordination
 - IT, Security, Vendors Compliance, Audit, Risk, Legal... etc.
- Specialized Compliance Requirements for Regulated Industries



Distributed IT models

- Communications/ Clear Understanding
- Coordination/Management of Activities
- Governance of Processes/Activities
- Coordination
- Security Reporting



Cloud and Enterprise Risk Management

- Risk Profile
- Risk Appetite
- Data Owner/Controller vs. Data Custodian/Processor
- Service Level Agreement
 - Components – Guarantees, Penalties, Exclusions, Suspension, Liability, Data Protection, Disaster Recovery, Recommendations



Cloud and ERM

- Ensuring Quality of Service (QoS)
 - Availability
 - Outage Duration
 - MTBF
 - Capacity Metrics
 - Performance Metrics
 - Reliability Metrics
 - Storage Device Metrics
 - Server Metrics
 - Instance Startup Metrics
 - Response Time Metrics
 - MTTSo Metrics
 - MTTR Metric
 - Scalability Metrics



Risk mitigation

- Risk Management Metrics
 - Risk Scorecard – minimal, low moderate, high, maximum (critical)
- Risk Frameworks
 - ISO 31000:2009, ISO 27001:2013
 - European Network and Information Security Agency (ENISA)
 - National Institute of Standards and Technology (NIST)
 - SP 800-146



Outsourcing and contract design

- Personnel, roles, functions and business processes
- Scope
- Reasons, rationale, requirements, business drivers & potential impacts
- Responsibility to coordinate, communicate and interpret challenges



Business requirements

- Evaluate needs and requirements
- Cloud strategy development
- “In scope” suitability
- Documentation of “exceptions, restrictions, or potential risks...”
- Regulatory and compliance requirements
- BCP/DRP availability



Vendor management

- Understanding Risk Exposure
- Accountability of Compliance
- Common Criteria Assurance Framework
 - ISO/IEC 15408-1:2009
- CSA Security, Trust and Assurance Registry (STAR) – 2011
 - Level 1 – Self Assessment
 - Level 2 – Attestation
 - Level 3 – Ongoing Monitoring



Ccsl and ccsm

- CCS – TUV Rhineland
- CSA – OCF Levels 1, 2, & 3
- EuroCloud
- ISO/IEC 27001
- PCI-DSS
- LEET
- AICPA – SOC Levels 1, 2, & 3



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



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

Review Questions Chapter 6 Legal and Compliance

1. Which is the lowest level of the CSA STAR program?
 - A. Continuous monitoring
 - B. Self-assessment
 - C. Hybridization
 - D. Attestation
2. Which of the following is a valid risk management metric?
 - A. KPI
 - B. KRI
 - C. SLA
 - D. SOC
3. Which of the following frameworks focuses specifically on design implementation and management?
 - A. ISO 31000:2009
 - B. HIPAA
 - C. ISO 27017
 - D. NIST 800-92
4. Which of the following frameworks identifies the top 8 security risks based on likelihood and impact?
 - A. NIST 800-53
 - B. ISO 27000
 - C. ENISA
 - D. COBIT
5. The CSA STAR program consists of three levels. Which of the following is not one of those levels?
 - A. Self-assessment
 - B. Third-party assessment-based certification
 - C. SOC 2 audit certification
 - D. Continuous monitoring-based certification
6. Which ISO standard refers to addressing security risks in a supply chain?
 - A. ISO 27001
 - B. ISO/IEC 28000:2007
 - C. ISO 18799
 - D. ISO 31000:2009
7. Which of the following is *not* a risk management framework?
 - A. NIST SP 800-37
 - B. European Union Agency for Network and Information Security (ENISA)
 - C. Key risk indicators (KRI)
 - D. ISO 31000:2009
8. Which of the following best define risk?

- A. Threat coupled with a breach
- B. Vulnerability coupled with an attack
- C. Threat coupled with a threat actor
- D. Threat coupled with a vulnerability

9. Which of the following is not a part of the ENISA Top 8 Security Risks of cloud computing?

- A. Vendor lock-in
- B. Isolation failure
- C. Insecure or incomplete data deletion
- D. Availability

10. Which of the following is a risk management option that halts a business function?

- A. Mitigation
- B. Acceptance
- C. Transference
- D. Avoidance

11. Which of the following best describes a cloud carrier?

- A. A person or entity responsible for making a cloud service available to consumers
- B. The intermediary who provides connectivity and transport of cloud services between cloud providers and cloud consumers
- C. The person or entity responsible for keeping cloud services running for customers
- D. The person or entity responsible for transporting data across the Internet

12. Which of the following methods of addressing risk is most associated with insurance?

- A. Transference
- B. Avoidance
- C. Acceptance
- D. Mitigation

13. Which of the following components are part of what a CCSP should review when looking at contracting with a cloud service provider?

- A. The physical layout of the datacenter
- B. Background checks for the provider's personnel
- C. Use of subcontractors
- D. Redundant uplink grafts

14. A data custodian is responsible for which of the following?

- A. The safe custody, transport, storage of the data, and implementation of business rules
- B. Logging access and alerts
- C. Data content
- D. Data context

15. Which of the following is *not* a way to manage risk?

- A. Enveloping
- B. Mitigating
- C. Accepting

D. Transferring

16. Which of the following is not a risk management framework?

- A. Hex GBL**
- B. COBIT**
- C. NIST SP 800-37**
- D. ISO 31000:2009**

17. Which of the following is not appropriate to include in an SLA?

- A. The number of user accounts allowed during a specified period**
- B. Which personnel are responsible and authorized among both the provider and the customer**
- C. The amount of data allowed to be transmitted and received between the cloud provider and customer**
- D. The time allowed to migrate from normal operations to contingency operations**

18. What is the Cloud Security Alliance Cloud Controls Matrix (CCM)?

- A. An inventory of cloud service security controls that are arranged into separate security domains**
- B. An inventory of cloud services security controls that are arranged into a hierarchy of security domains**
- C. A set of regulatory requirements for cloud service providers**
- D. A set of software development life cycle requirements for cloud service providers**

19. Which of the following is not one of the types of controls?

- A. Transitional**
- B. Administrative**
- C. Technical**
- D. Physical**

20. Which of the following is not an example of an essential internal stakeholder?

- A. IT analyst**
- B. IT director**
- C. CFO**
- D. HR director**

Answers Chapter 6: Legal and Compliance

- 1.** B. The lowest level is Level 1, which is self-assessment, Level 2 is an external third-party attestation, and Level 3 is a continuous-monitoring program. Hybridization does not exist as part of the CSA STAR program.
- 2.** B. KRI stands for key risk indicator. KRIs are the red flags if you will in the world of risk management. When these change, they indicate something is amiss and should be looked at quickly to determine if the change is minor or indicative of something important.
- 3.** A. ISO 31000:2009 specifically focuses on design implementation and management. HIPAA refers to health care regulations, NIST 800-92 is about log management, and ISO 27017 is about cloud specific security controls.
- 4.** C. ENISA specifically identifies the top 8 security risks based on likelihood and impact.
- 5.** C. The SOC 2 report is not a part of the CSA Star program. It is a totally different audit reporting standard developed by the AICPA.
- 6.** B. ISO /IEC 28000-2007 applies to security controls in supply chains. The others are cloud computing standards by have little to do with supply chain management.
- 7.** C. Key risk indicators are useful, but they are not a framework. ISO 31000:2009 is an international standard that focuses on designing, implementing, and reviewing risk management processes and practices. NIST SP 800-37 is the Guide for Implementing the Risk Management Framework (RMF), a methodology for handling all organizational risk in a holistic, comprehensive, and continual manner. European Union Agency for Network and Information Security (ENISA) identifies 35 types of risks organizations should consider but goes further by identifying the top eight security risks based on likelihood and impact.
- 8.** D. The best definition of risk is that of a threat coupled with a vulnerability.
- 9.** D. The ENISA Top 8 Security Risks of Cloud Computing does not include availability, even though it is certainly a risk that could be realized.
- 10.** D. Avoidance halts the business process, mitigation entails using controls to reduce risk, acceptance involves taking on the risk, and transference usually involves insurance.
- 11.** B. A cloud carrier is the intermediary who provides connectivity and transport of cloud services between cloud providers and cloud customers.
- 12.** A. Avoidance halts the business process, mitigation entails using controls to reduce risk, acceptance involves taking on the risk, and transference usually involves insurance.
- 13.** C. The use of subcontractors can add risk to the supply chain and should be considered; trusting the provider's management of their vendors and suppliers (including subcontractors) is important to trusting the provider. Conversely, the customer is not likely to be allowed to review the physical design of the datacenter (or, indeed, even know the exact location of the datacenter) or the personnel security specifics for the provider's staff. "Redundant uplink grafts" is a nonsense term used as a distractor.
- 14.** A. A data custodian is responsible for the safe custody, transport, and storage of data, and the implementation of business roles.

15. A. Enveloping is a nonsense term, unrelated to risk management. The rest are not.

16. A. Hex GBL is a reference to a computer part in Terry Pratchett's fictional Discworld universe.

The rest are not.

17. B. Roles and responsibilities should be included in the contract, not the SLA; a good method to determine whether something might belong in the SLA at all is figuring out whether a numerical value is associated with it—in this case, the element involves names and offices (roles), not numerical values, so it's immediately recognizable as something that isn't appropriate for the SLA. Options A and C are explicitly defined by exact numbers and are just the sort of aspects that belong in the SLA. Option D, the amount of time allowed to transition between normal and contingency operations, is also an explicit numerical value, but it is not a recurring event, regularly anticipated during each period of performance (or shouldn't be, anyway; if your cloud provider is fluctuating between normal and

contingency ops every performance period, you should probably find a new provider), so this is something that can be defined once in the contract, and if the provider fails to perform in the (hopefully rare) event it needs to be evaluated, then the provider is in breach, and there should be remedies available other than the SLA. This is not an easy question, and understanding

the nuances can be difficult.

18. A. The CSA CCM is an inventory of cloud service security controls that are arranged into separate security domains, not a hierarchy.

19. A. Transitional is not a term we associate with types of controls; the rest are.

20. A. An IT analyst is generally not high enough of a position to be able to provide quality information to other stakeholders. However, the IT director would be in such a positon, as would the others.



End of Lecture...Now What?

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

FINAL REVIEW

PLEASE FIND ANSWERS AND EXPLANATIONS AT

<http://tinyurl.com/KellysCCSP>

Architectural Concepts and Design Requirements

QUESTION 1

This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Please match the characteristics below with their descriptions

Characteristic	Description
1. Broad Network Access	a. The provider's computing resources are combined to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand
2. Metered Access	b. Consumer can unilaterally provision computing capabilities as needed automatically
3. On-demand self-service	c. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms
4. Resource Pooling	d. Capabilities can be provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand.
5. Rapid elasticity	e. Cloud systems automatically control and optimize resource use by leveraging capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and

	reported, providing transparency for both the provider and consumer of the utilized service.
--	--

QUESTION 2

What type of cloud deployment model is best for highly sensitive or proprietary information?

- a) Hybrid
- b) Private
- c) Public
- d) Community

QUESTION 3

Which of the following pose the greatest challenge to security?

- a) Process
- b) Technology
- c) People
- d) None of the other choices presented

QUESTION 4

The hypervisor allows multiple OSs to share a single hardware host. Which statement pertaining to the hypervisor is FALSE?

- a) Type 1 hypervisor runs directly on the guest OSs and reduces the likelihood of malicious software.
- b) Type 2 hypervisor runs on host OSs and are more attractive to attackers.
- c) Type 2 hypervisor runs directly on the guest OSs and reduces the likelihood of malicious software.
- d) Type 1 hypervisor is also called bare metal hypervisors.

QUESTION 5

Cloud Computing Top Threats include:

- a) Denial of Service, Data Remanence and Data Loss
- b) Data Loss, Account or Service Traffic Hijacking and Malicious Insiders
- c) Abuse of Cloud Services, Sufficient Due Diligence and Data Breaches
- d) Secure Interfaces and Application Programming Interfaces (APIs)

QUESTION 6

Critical cloud business continuity success elements include all, except:

- a. Understanding interdependencies and supply chain risks.
- b. Regularly auditing continuity capabilities and identifying on/off premise backup sites.
- c. Treating all assets and services as equal and prioritizing restoration.
- d. Understanding CSP and customer responsibilities.

QUESTION 7

A system design that does not create a single point of failure is the best defense against which of the following common threats?

- a) Denial of Service
- b) Abuse of Cloud Service
- c) Traffic Hijacking
- d) Malicious Insider

QUESTION 8

Which of the following is true of "bolt-on" components to cloud APIs?

- a) Bolt-on components are good because they build extra security into an existing API.
- b) Bolt-on components are good because they increase productivity.
- c) Bolt-on components are bad because they increase complexity and decrease security.
- d) Bolt-on components are bad because they decrease the complexity of cloud security.

QUESTION 9

It is incumbent on the cloud professional to ensure that both Due Care and Due Diligence are exercised in the drive to the cloud. Due Diligence and Due Care are defined as:

- a) Due Care is the methodology required for certifying a site as "cloud ready", and Due Diligence is the process of accreditation of a site.
- b) Due Diligence is the act of investigating and understanding the risks a company faces, and Due Care is the development and implementation of policies and procedures to aid in protecting the company, its assets, and its people from threats.
- c) Due Care is the act of investigating and understanding the risks a company faces, and Due Diligence is the development and implementation of policies and procedures to aid in protecting the company, its assets, and its people from threats.
- d) Due Diligence is the development of remediation of risks to people, processes and technology, and Due Care is the act of citing risks in an implementation process in an organization.

QUESTION 10

The Trusted Computer System Evaluation Criteria (TCSEC) are guidelines known as the Common Criteria and have 7 Evaluation Assurance Levels. Which level indicates the highest testing evaluation?

- a) Level 7 is the highest level, indicating the most rigorous testing.
- b) Each level is separate and is not graded on a scale of lowest to highest.
- c) Level 1 is the highest level, indicating the most rigorous testing.
- d) Level 4 is the highest, as it is in the exact middle of one and seven.

QUESTION 11

Which cloud deployment model is best described as an infrastructure shared by organizations that have similar mission, security requirements, concerns, and compliance considerations?

- a) Public
- b) Hybrid
- c) Community
- d) Private

QUESTION 12

This standard, consisting of 12 domains and over 200 controls was established as a result of significant credit card breaches.

- a) Common Criteria
- b) PCI DSS
- c) ISO 17799
- d) NIST 800-53

QUESTION 13

This framework, which is considered to be the most widely known and accepted information security standard, was originally developed and created by the British Standards Institute under the name of BS 7799. It is now known as which of the following?

- a) PCI DSS
- b) SOC I / SOC II / SOC III
- c) ISO 27001
- d) NIST 800-53

QUESTION 14

Service Organization Control (SOC) reports are broken into 3 types. Which type is of most interest to a technical audience due to its Trust Services Principles?

- a) SOC I, Type I
- b) SOC III
- c) SOC I, Type II
- d) SOC II

QUESTION 15

How is security best accomplished at the SaaS level?

- a) Security is provided through traditional firewalls.
- b) Security must be provided by the cloud consumer.
- c) Security is negotiated as part of the Service Level Agreement.
- d) Through collaboration.

QUESTION 16

Which of the following is NOT a characteristic of IaaS?

- a) Resilience
- b) Flexibility
- c) Capacity Pools

QUESTION 17

Which of the following consists of a library of documents that are used in implementing a framework for IT Service management?

- a) Jericho/Open Group
- b) ITIL
- c) SABSA
- d) TOGAF

QUESTION 18

Which of the following architectures uses a cube model to create a framework for exploring different cloud formations?

- a) ColTRANE
- b) TOGAF
- c) Jericho/Open Group
- d) NIST

QUESTION 19

Which of the following terms best describes the ability for cloud consumers to access evidence, actions, controls and process that were performed by a specified user?

- a) Auditability
- b) SLA
- c) Regulatory Compliance
- d) Portability

QUESTION 20

Which of the following is a true statement?

- a) Deployment of a cloud solution is always a technology decision.
- b) Organizational goals that require technology, especially cloud technology are best met when technology is considered at the forefront.
- c) The choice to deploy a cloud solution is primarily a technical decision.
- d) Funding and technology decisions for movement to the cloud should be made with the business direction at the core.

QUESTION 21

Privacy in the cloud is most often achieved through which of the following?

- a) Privacy must be outlined in the Service Level Agreement with the cloud provider.
- b) Privacy is achieved through the security provided by the cloud provider.
- c) Privacy is best achieved through regulatory compliance.
- d) Privacy is one of the essential elements of cloud computing and need not be addressed as it is part of resource pooling.

QUESTION 22

Regulatory compliance is most closely aligned with which of the following?

- a) The focus of an organization to produce information about actions of the users.
- b) The requirement of an organization to access, report, and obtain evidence of organizational controls.
- c) The requirement of an organization to define processes and procedures.
- d) The requirement of an organization to adhere to relevant laws, guidelines and specifications relevant to its business.

QUESTION 23

Richie has been asked to speak with the Board of Directors at a law firm about cloud deployments.

One of the board members has told the board that the cloud is the best business decision for them due to the clear perimeter offered between the cloud provider and the cloud customers. What is the best advice that Richie can give to the Board members?

- a) The perimeter transforms into a series of highly dynamic "micro borders" for some cloud providers.
- b) There is no clear perimeter in cloud networks.
- c) The Board member is correct in stating that the perimeter is clearly the demarcation point.
- d) The classic definition of a network perimeter takes on different meanings under different guises and deployment models.

QUESTION 24

Which of the following protocols is NOT used to protect data in transit?

- a) IPSEC
- b) TLS
- c) KMS
- d) SSL

QUESTION 25

Which of the following roles is most likely responsible for reviewing how data is protected in transit as well as the design and assessment of encryption algorithms for use within cloud environments?

- a) Cloud Architect
- b) Cloud Administrator
- c) Cloud Operator
- d) Cloud Storage Administrator

QUESTION 26

Which of the following approaches is typically used for SaaS environments and cloud deployments?

- a) Remote Key Management Service
- b) Segregated Key Management
- c) Hybrid Key Management
- d) Client Side Key Management

QUESTION 27

Which of the following essential characteristics of the cloud most closely resembles the scalability of traditional computing?

- a) Rapid Elasticity
- b) On-Demand Self Service
- c) Measured Self-Service

- d) Broad Network Access

QUESTION 28

What is a key activity for any organization considering moving to the cloud?

- a) Classifying the organizations data to determine the requirements for the cloud engagement.
- b) All of the other choices are considerations.
- c) Determining the best cloud formation for the business.
- d) Understanding if the cloud is the correct choice for the business of the organization.

QUESTION 29

The primary goal is to standardize, streamline, and create an efficient account creation and management process, while creating a consistent, measurable, traceable, and auditable framework providing access to end users. What are we referring to?

- a) Centralized Key Management
- b) Provisioning and De-Provisioning
- c) Migration and Transference
- d) Multi-Factor Authentication and Resource Access

QUESTION 30

Which of the following is the name of the free, publicly accessible registry where cloud service providers can publish their CSA-related assessments?

- a) Cloud Capability Matrix
- b) STAR
- c) ISO 27001
- d) Cloud Security Roadmap

QUESTION 31

Which of the following is the primary protocol in relation to Centralized Directory Services?

- a) Lightweight Directory Access Protocol (LDAP)
- b) LPIE Protocol (LPIEP)
- c) Multi-Factor Authentication Protocol (MAP)
- d) Privileged Identity Protocol (PIP)

QUESTION 32

What is true about a Type II (Two) Hypervisor?

- a) A Type II Hypervisor is more secure than a Type I hypervisor.
- b) A Type II Hypervisor is Bare Metal
- c) A Type II Hypervisor is easier to deploy than a Type III Hypervisor

- d) A Type II Hypervisor is OS-Based

QUESTION 33

Why is a Type I Hypervisor less vulnerable to attack than other hypervisor types?

- a) Type IV hypervisors security is limited in its patch availability.
- b) The limited access and strong control over the OS greatly increases the reliability and robustness of Type I hypervisors.
- c) The operating system-based hypervisor is standardized, making it less vulnerable.
- d) Type I hypervisors are NOT less vulnerable to attack than Type II hypervisors.

QUESTION 34

In a PaaS environment, should a tenant be given shell access to the server that runs their VM instances?

- a) No, because shell access to the VM could result in configuration changes that could impact multiple tenants.
- b) Yes, because a tenant needs full access to the server in order to make necessary changes to the configuration of the VMs.
- c) No, because there is no way to monitor shell access to a VM server.
- d) Yes, because shell access is a core component of a PaaS implementation.

QUESTION 35

A guaranteed method to protect a VM from attack is to power it off. True or False? Choose the best statement below.

- a) This is false because simply powering off a VM does not stop the processes from running, leading to VM sprawl
- b) This is false because simply powering off a VM still leaves the image files susceptible to malware infections and missed patching
- c) This is true, because simply powering off a VM renders it inaccessible to the system on which it resides
- d) This is true because simply powering off a VM makes it safe against malware infections and missed patching

QUESTION 36

Why is a single point of access to a VM environment considered a security threat?

- a) A single point of access to a VM environment is a security threat because it opens the door to a compromise of the virtual cloud infrastructure.
- b) A single point of access to a VM environment is a security threat because it creates strict network topologies, which are counter-productive.
- c) A single point of access to a VM environment is a security threat due to its decreased complexity, which decreases a defense-in-depth approach.

- d) A single point of access to a VM environment is a security threat because it creates too many physical endpoints, increasing complexity.

QUESTION 37

Nancy is designing a web site for a public company. As part of the design, she has created a web page that allow each new earnings report to be posted simply by adding an incremental number to the public URL name. The January report would be added to URL as "Earnings_2016_1 ", and the February report would be "Earnings_2016_2 ". You have been asked to evaluate this design decision. Please choose the best answers from the following choices.

- a) This is a good design because it prevents SQL injection attacks.
- b) This is a bad design because it creates the threat of Insecure Direct Object References.
- c) This is a good design because it is efficient and operationally expedient.
- d) This is a bad design because it creates the threat of a Cross-Site Request Forgery (CSRF).

QUESTION 38

According to the Data Security Lifecycle, there are a number of actions which can be taken on data. Which of these functions maps to all areas of the Data Security Lifecycle?

- a) Process
- b) Access
- c) Destroy
- d) Store

QUESTION 39

Common Criteria (CC) has two key components: Protection profiles and Evaluation Assurance Levels (EALs).

Which of the following statements concerning CC is TRUE?

- a) EALs define a standard set of security requirements for a specific type of product
- b) Protection profiles define how thoroughly a product is tested on a scale of 1-7
- c) More testing means that the product is more secure, whereas less testing means that the product is less secure
- d) CC is an international evaluation framework

QUESTION 40

Benefits of cloud computing may include all of the following except:

- a) Appreciation of IT technologies
- b) Reducing maintenance and configuration time
- c) Pay per use

- d) Pooling resources

QUESTION 41

After years of receiving negative internal and external audit report findings and now facing loss of accreditation and government funding, University of ABC (U of ABC) has decided to move to cloud computing.

The University has not conducted a Business Impact Analysis (BIA) or Risk Assessment (RA) in at least five years; and has had a high employee turnover rate over the past two years after changes in its executive staff and Board members.

Upon interviewing several vendors, senior management has decided to use the CSP that guarantees staff and student availability to computing resources. Last month, a natural disaster resulted in staff and students losing availability to computing resources. CSP was not responding to any of ABC's requests or inquiries. Furthermore, as a result of the ensuing bad publicity, student enrollment has declined. Perhaps some of these issues could have been avoided if U of ABC would have:

- a) Had effective board oversight
- b) Consistently practiced due diligence and due care
- c) Had a current BIA and RA
- d) Had an effective cloud backup solution

QUESTION 42

Which answer best describes Software as a Service (SaaS)?

- a) Consumer can provision processing, storage, networks and other fundamental operating computing resources. Consumer does not manage or control underlying infrastructure, but has control over OS storage and deployed applications and possible select network components such as firewalls.
- b) Consumer uses provider's applications and resources. The consumer does not manage or control the underlying cloud infrastructure, but has control over the deployed application.
- c) Consumer deploys cloud infrastructure that the consumer created or acquired. Consumer does not manage or control underlying infrastructure, but has control over deployed application and possible configuration settings for the application hosting environment.
- d) Consumer uses provider's applications, applications are accessible from various client devices through thin client or program interface, and the consumer manages or controls underlying infrastructure. Security lies more with consumer.

QUESTION 43

Which of the following cloud deployment models is used when the capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The

applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

- a) IaaS
- b) Private Cloud
- c) PaaS
- d) SaaS

QUESTION 44

Looking at the cloud deployment models below and integrated functionality, which one achieve the highest level of integration?

- a) All models have the same integration level
- b) PaaS
- c) SaaS
- d) IaaS

QUESTION 45

Within which cloud service model would you find and control applications settings only?

- a) Software as a Service (SaaS)
- b) Infrastructure as a Service (IaaS)
- c) PaaS
- d) Security as a Service (SecaaS)

QUESTION 46

Which of the following is true of a private cloud?

- a) It may be internal or external to an organization.
- b) It is always managed by a broker.
- c) It must be internal to an organization.
- d) It must be external to an organization.

QUESTION 47

The Open Web Application Security Project (OWASP) has produced a list of the top ten critical web application security threats that should be tested. Which of the following threats could be best mitigated by input validation?

- a) Insecure Direct Object References
- b) Security Reconfiguration
- c) Cross-Site Request Forgery
- d) Injection Flaws

QUESTION 48

A Man in The Middle attack against a cloud consumer is most closely aligned with which of the following common threats?

- a) Low Orbit Ion Cannon Attack
- b) Denial of Service
- c) Traffic Hijacking
- d) Cruzr attack

QUESTION 49

The definition of cloud portability is?

- a) The deployment of a company's cloud computing strategy
- b) The ability to move applications and related data between CSPs, or between public and private cloud environments.
- c) A company that purchases hosting services from a cloud server hosting or cloud computing provider and then resells them to its own customers.
- d) Multiple customers using the same public cloud.

QUESTION 50

Which of the following is not a SSO technology?

- a) SAML
- b) SCIM
- c) XACML
- d) OpenID Connect

QUESTION 51

Which of the following is a VALID cloud system role based on ISO/IEC 17788?

- a) Cloud owner
- b) Cloud auditor
- c) Cloud director
- d) Cloud billing partner

QUESTION 52

Resource pooling is an important concept for cloud computing. Which of the following statements about resource pooling is most correct?

- a) Resource pooling and the ability to dynamically adjust to varying customer needs is the reason cloud computing is significantly more expensive than traditional data centers.
- b) Resource pooling allows for dynamic adjustment to shared resources, but is only available in a private cloud.

- c) Resource pooling allows companies to dynamically have the resources they need when they need it rather than having to build out systems large enough to handle their maximum load.
- d) Resource pooling provides dedicated resources to cloud tenants.

QUESTION 53

Which of the following statements is correct about Infrastructure as a Service (IaaS)?

- a) Customer controls services deployed within the cloud, storage, deployed applications, and operating systems (including licensing)
- b) Cloud provider is responsible for the operating system and hosting environment including libraries, service and tools
- c) Cloud provider supplies a full cloud platform and software application to the customer
- d) Cloud provider is responsible for patching and deploying systems

QUESTION 54

The new complex and dynamic nature of VMs in the cloud has created new categories of security threats. Which of the following is one of these threats?

- a) Hybrid complexity
- b) Strict segmentation
- c) Resource pools
- d) No physical endpoints

QUESTION 55

Resource pooling is an important concept of the cloud computing. Which of the following statement about resource pooling is correct?

- a) Resource pooling provides dedicated resources to the cloud tenants
- b) Resource pooling is only used in private cloud
- c) Resource pooling provides shared services with cloud computing
- d) Resource pooling provides economies of the scale, hence significant cost saving to the cloud customers

Cloud Data Security

QUESTION 1

Which cloud platform typically has the least amount of control and access to event and diagnostic data?

- a) Access to event and diagnostic data is dependent on the development team.
- b) The SaaS platform typically has the least amount of control and access to event and diagnostic data.
- c) The PaaS platform typically has the least amount of control and access to event and diagnostic data.
- d) All cloud platforms have equal control and access to event and diagnostic data.

QUESTION 2

When working with the SIEM device it is necessary to add new rules in order to address new risks. Does it ever make sense to modify old rules?

- a) No, it does not make sense to modify old rules. Only new rules should be added to address new threats.
- b) No, it does not make sense to modify old rules, as that can run contrary to company policy.
- c) Yes, it makes sense to modify old rules to reduce false positives.
- d) Yes, it makes sense to modify old rules to secure data for proper disposal.

QUESTION 3

Which of the following is considered to be the only reasonable method of data disposal in a cloud environment?

- a) Crypto-Shredding
- b) Degaussing
- c) Physical destruction
- d) Overwriting

QUESTION 4

When formulating a data archiving policy for the cloud, which aspect of data governance is most closely associated with the proper application of security controls throughout the data lifecycle?

- a) Data Encryption Procedures

- b) Data Monitoring procedures
- c) Backup and DR options
- d) Data Format and Media Types

QUESTION 5

Which of the following is an example of Unstructured Data?

- a) Text and Multimedia content
- b) Relational Database content
- c) IAM information
- d) Raw Device Mapping

QUESTION 6

The Cloud Security Alliance (CSA) baseline outline 3 requirements for a service provider Privacy Level Agreement (PLA).

Which of the following is not defined as a PLA requirement

- a) The PLA provides a clear and effective way to communicate the level of personal data protection provided by a service provider.
- b) The PLA provides guidelines for compensatory damages for non-compliance with data protection legislation.
- c) The PLA works as a tool to assess the level of a service provider's compliance with data protection legislative requirements and leading practices.
- d) The PLA provides a way to offer contractual protection against possible financial damages due to lack of compliance.

QUESTION 7

In the context of data protection measures, the Privacy Level Agreement (PLA) plays an essential role towards an ultimate goal. What is that goal?

- a) The goal of the PLA is to fulfill the Privacy and Data Protection laws applicable to the controller.
- b) The goal of the PLA is to fulfill the Privacy and Data Protection laws applicable to the processor.
- c) The goal of the PLA is to fulfill the Privacy and Data Protection laws applicable to the Data Loss Protection Manager.
- d) The goal of the PLA is to fulfill the Privacy and Data Protection laws applicable to the cloud service provider.

QUESTION 8

According to the Data Lifecycle model, when is the preferred time to classify content according to its sensitivity and value?

- a) Data may only be classified if it is going to be shared.
- b) The preferred time to classify content is during the creation phase.
- c) The preferred time to classify content should be during consideration of the storage of the data.
- d) Data need only be classified during the archive phase of the Data Lifecycle.

QUESTION 9

Which phase of the Cloud Data Lifecycle typically occurs nearly simultaneously with data creation?

- a) Storage
- b) Obsfuscation
- c) Encryption
- d) Classification

QUESTION 10

According to the Sharing phase of the Cloud Data LifeCycle, what is a general rule of security when sharing data?

- a) Not all data should be shared and not all sharing should present a threat.
- b) Data should only be shared if it is also archived.
- c) Data should only be shared according to a need-to-know model of data security.
- d) All data should be shared and access is not a Data LifeCycle concern.

QUESTION 11

At which point in the Cloud Data LifeCycle Phases is data considered most vulnerable?

- a) Data in Use is most vulnerable
- b) Archived Data is most vulnerable
- c) Data is most vulnerable during the destruction process
- d) Data in Storage is most vulnerable

QUESTION 12

Each cloud service model uses different data storage types. Which storage type is associated with the PaaS cloud service model?

- a) PaaS utilizes Volume and Object Data storage.
- b) PaaS utilizes Structured and Unstructured Data storage.
- c) PaaS utilizes Raw and Ephemeral Data storage.
- d) PaaS utilizes Volume and, File Data storage.

QUESTION 13

The best part of cloud computing is that the risk of accidental loss of media is entirely eliminated due to the inability of a person to access the physical data center. True or False?

- a) This statement is false because the data can be downloaded to a portable device that could become lost or stolen.
- b) This statement is true because data dispersion protects data loss.
- c) This statement is false because the data is stored on local discs in the possession of the cloud user.
- d) This statement is true because the data is always encrypted.

QUESTION 14

What is the biggest challenge with the end of data use in a cloud environment, and what is a mitigating risk to that challenge?

- a) The biggest challenge to the end of data use is that encryption keys are not destroyed, making the data easily recoverable. However, key escrow mitigates this risk.
- b) The biggest challenge to the end of data use is that useful digital remnants can be located. However, physical destruction of the media mitigates this risk.
- c) The biggest challenge to the end of data use is that physical destruction of the media cannot be enforced. However, the dynamic nature of data, where data is kept in different storage locations mitigates the risk that useful digital remnants can be located.
- d) The biggest challenge to the end of data use is that data may still be accessed by unauthorized people. However, the DLP solutions protect the data from leaving the environment.

QUESTION 15

Regarding Data Dispersion, what is the underlying technology where segments of data are encrypted and dispersed across the network and makes dispersion possible?

- a) Tokenized masking is the technology that chunks a data object into the segments
- b) Erasure coding is the technology that chunks a data object into the segments
- c) Encryption algorithmic dispersion is the technology that chunks a data object into the segments
- d) Data blocking is the technology that chunks a data object into the segments

QUESTION 16

Data Loss Protection consists of various components. At which component are the majority of cloud-based DLP focused?

- a) The majority of cloud-based DLP is focused at the Discovery and Classification level.
- b) The majority of cloud-based DLP is focused at the Anonymization level.
- c) The majority of cloud-based DLP is focused at the Data in Motion level.
- d) The majority of cloud-based DLP is focused at the Object storage level.

QUESTION 17

An organization has asked their Cloud Security Professional how to set up a Data Loss Prevention strategy for Data in Motion. What is the most likely response to this QUESTION?

- a) In a "Data in Motion" topology, the DLP monitoring engine shoud be deployed near the organizational gateway to monitor outgoing protocols, such as HTTPS, SMTP, and FTP.
- b) In a "Data in Motion" topology, the DLP monitoring engine shoud be deployed in an unstructured database.
- c) In a "Data in Motion" topology, the DLP monitoring engine shoud be deployed at the endpoint, where the data is processed.
- d) In a "Data in Motion" topology, the DLP monitoring engine shoud be deployed where the data resides, usually on one or more subsystems.

QUESTION 18

It is advised that key management functions should be conducted separately from the cloud provider in order to enforce separation of duties. Why are separation of duties used for this protection mechanism?

- a) Separation of duties has no impact on key management.
- b) Separation of duties shifts the responsibility to the Board of Directors.
- c) Separation of duties requires that a manager approves the action in order to proceed with the key management function.
- d) Separation of duties requires forced collusion to occur if unauthorized access is attempted.

QUESTION 19

When discussing Data Discovery, there are separate approaches, including Big Data projects, Real-time analytics, and Agile business intelligence. There are also specific Data

Discovery techniques that are used for the purpose of data analysis. Which of the following is the most common analysis technique?

- a) LUN Checks.
- b) Metadata.
- c) Indexed Sequential Access.
- d) Dashboards.

QUESTION 20

Which of the following Data Discovery techniques uses pattern matching?

- a) Labels.
- b) Simple DBs.
- c) Locations.
- d) Content analysis.

QUESTION 21

Some common privacy terms include: Processing, Personal data, Processor, and Controller. What is the best definition of a Controller?

- a) The controller is defined as the person or authority that controls the the data subject.
- b) The controller is defined as a natural or legal person, public authority, agency, or any other body that processes personal data.
- c) The controller is defined as the natural or legal person, public authority, agency, or any other body that alone or jointly with others determines the purposes and means of the processing of personal data.
- d) The controller is defined as the operation that is performed upon personal data, whether or not by automatic means.

QUESTION 22

When working with Privacy and Data Protection, to what entity are all liabilities assigned?

- a) All liabilities are assigned to the Processor role, and the country of establishment does not determine the applicable Privacy and Data Protection law and jurisdiction.
- b) All liabilities are assigned to the Controller and Processor roles, due to their joint responsibility over the custodianship of the data across the countries of establishment relevant to the applicable Privacy and Data Protection law and jurisdiction.

- c) All liabilities are assigned to the Controller role, and its country of establishment mainly determines the applicable Privacy and Data Protection law and jurisdiction.
- d) Liabilities cannot be assigned to any particular role, due to varying Privacy and Data Protection laws in the countries of establishment and their jurisdictions.

QUESTION 23

Various types of security present responsibilities for cloud entirely on the cloud provider, entirely on the enterprise, or it may be shared depending on the cloud service model in use. For example, when using SaaS, Application security is a shared responsibility, whereas, platform security in the SaaS service model is strictly a Cloud Provider responsibility.

When addressing Security Governance, Risk & Compliance (GRC) Where does the responsibility lie with all service models?

- a) Governance, Risk & Compliance is an Enterprise Responsibility across all cloud service models.
- b) Governance, Risk & Compliance is a Shared Responsibility across all cloud service models.
- c) Governance, Risk & Compliance is an Enterprise Responsibility in the SaaS service model, and an Enterprise responsibility in the PaaS service model.
- d) Governance, Risk & Compliance is a legal responsibility, not a Shared, Enterprise, or Cloud provider responsibility.

QUESTION 24

In a File Level Object Storage encryption model, where is the encryption engine commonly implemented?

- a) At the client.
- b) In the Application
- c) Within the database.
- d) At the instance

QUESTION 25

In which Service offering are you most likely to see the terms "volume storage" and "object storage"?

- a) Infrastructure as a Service (IaaS)
- b) Software as a Service (SaaS)
- c) Security as a Service (SecaaS)
- d) Platform as a Service (PaaS)

The correct answer is: Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

QUESTION 26

A data retention policy in an organization should define retention periods, data formats, data security and data retrieval procedures. A cloud data retention policy should contain which of the following components?

- a) Data Owner
- b) Legislation, regulation, and standards requirements.
- c) Access Control List
- d) Data property attribute descriptions

QUESTION 27

Information Rights Management (IRM) is more than the use of standard encryption technologies to provide confidentiality for data. One such feature is the use of an Access Control List (ACL) which determines who can open a document and what they can do with it. What additional benefit does an Access Control List provide?

- a) Because an IRM contains ACLs and is embedded into the original file, IRM does not move with the file, which offers a layer of protection by obfuscating attribution.
- b) Because an IRM contains ACLs and is embedded into the original file, IRM is agnostic to the location of the data.
- c) Because an IRM contains ACLs and is embedded into the original file, IRM can only be used for documents.
- d) Because an IRM contains ACLs and is embedded into the original file, IRM strictly controls the location of a file, which prevents "file escape".

Cloud Platform and Infrastructure Security

QUESTION 1

Stakeholders in a company need to see that their interests are taken care of and that management has a structure and process to ensure that they execute the goals of the organization. Which of the following best describes the general business term that addresses this broad area in an organization?

- a) Policy enforcement
- b) Corporate governance
- c) Audit control
- d) Enterprise risk management

QUESTION 2

What statement is most accurate about cloud object storage?

- a) Object storage features are never used for storing operating system images.
- b) Object storage features offer increased, real-time data consistency, making them perfect for frequently changing data.
- c) Object storage features are typically minimal, allowing you to only store, retrieve, copy, and delete files as well as the ability to control which users can undertake these actions.
- d) Object storage features offer the most robust advantages when using granular file-level controls.

QUESTION 3

While reviewing the design of a new data center, you notice that there is only one fuel tank for the generators that would be used to power the center in the event of a power failure. What would you suggest to the management team?

- a) You should suggest a battery backup unit to prevent power failures.
- b) You should suggest that the single fuel tank is a single point of failure and the design should include a redundant fuel tank.
- c) You should suggest a larger fuel tank to accommodate longer power failures.
- d) You do not need to suggest any changes as there is nothing wrong with the data center design in its current form.

QUESTION 4

When creating a Business Continuity and Disaster Recovery (BCDR) plan, is it wise to consult or adapt Information Technology (IT) project planning and risk management methodologies?

- a) No, it is not wise to consult or adapt IT project planning and risk management methodologies as the creation and implementation of a fully tested BCDR plan has to be formed without any preconceived ideas and assumptions about the current environment.
- b) Yes, it is wise to consult or adapt IT project planning and risk management methodologies, as the creation and implementation of a fully tested BCDR plan has a great structural resemblance to any other IT implementation plan.
- c) Yes, however it is wise to consult only the IT project planning, but not the risk management methodologies since the creation and implementation of a fully tested BCDR plan only moderately resembles other IT implementation plans.
- d) No, it is not wise to consult or adapt IT project planning and risk management methodologies, as the creation and implementation of a fully tested BCDR plan should not resemble any other IT implementation plan.

QUESTION 5

A Denial of Service (DoS) attack is most closely associated with which of the following cloud risks?

- a) Control conflict.
- b) Software related risks.
- c) Resource exhaustion.
- d) Isolation control failure.

QUESTION 6

Some legal risks associated with cloud computing include Data protection, Jurisdiction, and Law enforcement activities. In what way is Law enforcement activity a greater risk than all of the other risks?

- a) Law enforcement activity, such as the seizure of a hard drive, has the potential to create a problem due to the storage locations of the data on the disk.
- b) Law enforcement activity, such as the seizure of a physical hard drive, has the potential to violate regulatory requirements of data handling and storage.
- c) Law enforcement activity, such as the seizure of a physical hard drive, has the potential to violate licensing agreements for the software contained on the disks.
- d) Law enforcement activity, such as the seizure of a physical hard drive, has the potential to expose data of multiple customers.

QUESTION 7

In a cloud environment, there are different areas of responsibility for the Enterprise and the Cloud provider. At some levels, there are responsibilities that are shared by both the Enterprise and the cloud provider. Which of the following statements is true about shared responsibilities?

- a) Physical Security is a shared responsibility in an IaaS platform, and Platform Security is a shared responsibility in a PaaS platform.
- b) Application Security is a shared responsibility in a PaaS platform, and Data Security is a shared responsibility in a SaaS platform
- c) Infrastructure Security is a shared responsibility in an IaaS platform, and Application Security is a shared responsibility in a SaaS platform.
- d) Platform Security is a shared responsibility in both the PaaS and SaaS platforms.,

QUESTION 8

At which phase of the Business Continuity / Disaster Recovery (BCDR) planning should testability be considered?

- a) Testability should be considered during the budget phase of the BCDR plan.
- b) Testability should be considered during the performance phase of the BCDR plan.
- c) Testability should be considered during the scope phase of the BCDR plan.
- d) Testability should be considered during the design phase of the BCDR plan.

QUESTION 9

Which statement about a Security Assertion Markup Language (SAML) Token is NOT true?

- a) A SAML Token is an XML structure that lists the claims about the user account.
- b) A SAML token is issued by the user's Identity Provider (IDP)
- c) A SAML token is signed with an SSL certificate so applications and organizations know to trust it
- d) SAML token is issued by the user's Service Provider

QUESTION 10

What are the main components of SAML?

- a) Assertions, Protocol, and Binding
- b) Assertions, Protocol, and Authentication
- c) Assertions, Protocol, and Authorization
- d) Authentication, Attribute and Authorization

QUESTION 11

Which Business Continuity / Disaster Recovery (BCDR) test scenario requires participation specifically from all operational and support personnel?

- a) Tabletop Exercise / Structured Walk-Through Test specifically requires all operational and support personnel.
- b) Test Plan Review specifically requires all operational and support personnel.
- c) Walk-Through Drill / Simulation Test specifically requires all operational and support personnel.
- d) Functional Drill/ Parallel Test specifically requires all operational and support personnel.
- e) The correct answer is: The Walk-Through Drill / Simulation Test specifically requires all operational and support personnel.

QUESTION 12

John is assessing an organization's cloud security practices and virtualization risks. He notices that the virtualization snapshots are stored on a server that is freely accessible to all team members in the organization. John recommends that the snapshots be stored on a secure server with access available only to the cloud administrative teams. Is this a good idea?

- a) No, this is not a good idea. Virtualized snapshot images are only useful to someone who has a working virtualization model, so there is no risk if a regular team member can access a virtualized snapshot image.
- b) No, this is not a good idea. Virtualized snapshot images are not portable, so they could not be used anywhere other than their original location, so there is no risk associated with them.
- c) Yes, this is a good idea. Virtualized images can be used for additional storage space by an unsuspecting team member, which would create data version skew.
- d) Yes, this is a good idea. Virtualized snapshot images should be protected because they contain sensitive information.

QUESTION 13

Which of the following statements about Identity Management is true?

- a) In a federated identity model, authorization is typically with the relying party whereas authentication is a function of the identity provider.
- b) In a federated identity model, authentication is typically with the relying party whereas authorization is a function of the identity provider.
- c) Identity management is governed through resource usage.
- d) Authorization and authentication are both functions of the identity provider whereas federated identity management is a function of SAML.

Cloud Application Security

QUESTION 1

From a security perspective, once an application has been implemented using the Software Development LifeCycle principles (SDLC), the application enters a secure operations phase. Proper software configuration management and versioning are essential to application security. What are two common tools that are used for configuration management?

- a) John the Ripper and Low Orbit Ion Cannon.
- b) Puppet and Chef.
- c) Punch and Judy.
- d) Summit and Peak.

QUESTION 2

Supplemental security devices add additional elements and layers to a defense-in-depth architecture.

Which of the following supplemental devices would be most effective against a Denial of Service (DoS) attack?

- a) An API gateway.
- b) Database activity monitoring (DAM).
- c) A Cloud web application firewall (WAF).
- d) An XML gateway.

QUESTION 3

The Cloud Security Alliance's Top Threats Working Group published *The Notorious Nine*, a list of the top nine cloud threats in 2013. One of the threats listed is Data Loss. Does the burden of responsibility for data loss in the cloud fall solely on the cloud provider?

- a) No, the burden of avoiding data loss does not fall solely on the provider, since the cloud customer can also cause data loss that is beyond the control of the provider.
- b) Yes, the burden of avoiding data loss falls solely on the provider, since the cloud customer cannot cause any data loss that is not recoverable by the cloud provider.
- c) Yes, the burden of avoiding data loss falls solely on the provider, since the provider has assumed full responsibility for data protection.
- d) No, the burden of avoiding data loss does not fall solely on the provider, it falls solely on the cloud customer who is the ultimate custodian of the data.

QUESTION 4

The International Standards Organization (ISO) has developed and published ISO/IEC 27034-1 which defines concepts, frameworks and processes to help organizations integrate security within their software development lifecycle.

Some of the broader concepts of ISO/IEC 27034-1 include "Organizational Normative Framework" (ONF), "Application Normative Framework" (ANF), and "Application Security Management Process" (ASMP).

How do the Application Normative Framework (ANF), and the Organizational Normative Framework (ONF) work in relation to a specific application?

- a) The ANF is used in conjunction with the ONF and is created for a specific application.
- b) The ANF is a separate entity from the ONF - they have no relation to each other.
- c) The ONF maintains the applicable portions of the ANF that are needed to enable a specific application to achieve a required level of security.
- d) The ONF shares a many-to-many relationship to the ANF, where many ONFs will be created along with many ANFs.

QUESTION 5

Once an application design is created it is important to determine any weaknesses in the application before the application is introduced to production. What is the name given to this type of testing?

- a) STRIDE.
- b) Black box.
- c) Threat modeling.
- d) Repudiation.

QUESTION 6

What are the three subcomponents of applications?

- a) Data, Technology, Processes.
- b) Data, Functions, Technology.
- c) People, Processes, Technology.
- d) Data, Functions, Processes.

QUESTION 7

The two common Application Programming interfaces (APIs) for cloud environments are Representational State Transfer (REST) and Simple Object Access Protocol (SOAP). Which data format is supported only in SOAP?

- a) SOAP only supports the YAML data format.
- b) SOAP only supports the JSON data format.
- c) SOAP only supports the XML data format.
- d) SOAP only supports the XAML data format.

QUESTION 8

Which of the following is not a stage of the Software Development Lifecycle (SDLC) methodology?

- a) Release.
- b) Maintenance.
- c) Analysis.
- d) Performance.

QUESTION 9

The most common software vulnerabilities are found in the Open Web Application Security Project (OWASP) Top 10 list.

Which of the following occurs "when untrusted data is sent to an interpreter as part of a command or query".

- a) Injection.
- b) Cross-site request forgery.
- c) Insecure direct object reference.
- d) Cross-site scripting.

QUESTION 10

The most common software vulnerabilities are found in the Open Web Application Security Project (OWASP) Top 10.

Which of the following occurs when a developer's code or URL includes information to an internal implementation object, such as a file, directory, or database key.

- a) Indirect secure object reference.
- b) Insecure direct object reference.
- c) Inferential secure object deference.
- d) Secure indirect object reference.

QUESTION 11

The Application development team has called you into a meeting to discuss an upcoming application security test. The lead developer is stating that a Static application security test is better than a Dynamic application security test. The application team leader is stating the opposite.

As the Cloud Security Professional, what is your response?

- a) The Static application security test and the Dynamic application security test play different roles - one is not better than the other.
- b) A Dynamic application security test is better because it tests the HTTP and HTML interfaces of the web applications.
- c) A Static application security test is better than a Dynamic application security test because it can be used to find XSS errors, SQL injection, buffer overflows, unhandled error conditions, and potential backdoors.
- d) Neither test is adequate to test application security. A full pen test is required.

QUESTION 12

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious payload into a legitimate website. XSS is amongst the most rampant of web application vulnerabilities and occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

Cross-site Scripting can be classified into three major categories, what are they?

- a) Header, Reflected and DOM-based
- b) Stored, Reflected and DCOM-based
- c) Stored, Reflected and DOM-based
- d) Cookie, Reflected and DOM-based

QUESTION 13

Federated identity management (FIM) provides the policies, processes, and mechanisms that manage identity and trusted access to systems across organizations.

What is the most commonly accepted standard used in the industry today?

- a) Security Assertion Markup Language (SAML) 2.0
- b) OAuth 2.0
- c) WS-Federation Version 1.2
- d) OpenID Connect

QUESTION 14

Some software development lifecycle models include an operations and disposal phase. When an application has run its course and is no longer required, it is disposed of. From a cloud perspective, it is challenging to ensure that data is properly disposed of because you have no way to physically remove the drives. Given that restriction, what is a recognized way to ensure secure disposal of data in a cloud environment?

- a) Degaussing
- b) Data Vaulting
- c) Cipher /U

d) Crypto-shredding

QUESTION 16

Which of the following is NOT a standard for Federated Identity Implementation?

- a) SAML
- b) OpenID Connect
- c) OAuth
- d) WS-Federation
- e) RADIUS

Operations

QUESTION 1

How is security best accomplished at the SaaS level?

- a) Through collaboration.
- b) Security must be provided by the cloud consumer.
- c) Security is provided through traditional firewalls.
- d) Security is negotiated as part of the Service Level Agreement.

QUESTION 2

Over the past decade, data center design has been standardized to increase efficiency of data center operations.

A method known as the "chicken coop datacenter" is geared toward which of the following efficiency goals:

- a) Hosting racks of physical infrastructure with each server in a separate "coop" to form a clear demarcation from other tenant equipment.
- b) Hosting racks of physical infrastructure with each virtual switch in a separate environment to protect against "cam bus wolf-packs".
- c) Hosting of racks of physical infrastructure within long rectangles with isolated power strips, thereby reducing electrical anomalies.
- d) Hosting of racks of physical infrastructure within long rectangles with a long side facing the prevailing wind, thereby allowing natural cooling.

QUESTION 3

When planning the cooling costs for a data center, what will the power requirements be dependent upon?

- a) The power requirements for cooling a data center depend on the costs per BTU divided by the volume displacement of coolant per square footage of the data center (measured in ergs).
- b) The power requirements for cooling a data center are reversely correlated to the amount of heat being removed measured against the temperature difference between the inside of the data center and the outside air.

- c) The power requirements for cooling a data center depend on the amount of equipment in each rack and the temperature difference between the intake and exhaust areas of the equipment.
- d) The power requirements for cooling a data center depend on the amount of heat being removed as well as the temperature difference between the inside of the data center and the outside air.

QUESTION 4

A cloud representative is describing some of the advantages of the cloud over traditional data center operations by saying that one of the advantages of the cloud is its ability to rapidly adjust to accommodate more users than originally subscribed. The ability to "oversubscribe" is especially true when implementing iSCSI storage technology. What is your impression of this statement?

- a) The statement made by the sales representative is accurate. , Oversubscription in the cloud is one of the benefits, and iSCSI allows a greater "pipe" than older technologies, so all network traffic can flow freely within the system.
- b) This statement made by the sales representative is accurate. , One of the key benefits of cloud computing is rapid elasticity across all platform models.
- c) The statement made by the sales representative is inaccurate. , It is true that the cloud offers the ability to subscribe more users as-needed, however, oversubscription of an iSCSI storage system is not advised.
- d) The statement made by the sales representative is inaccurate. , Oversubscription is not permissible on cloud platform, yet it is permissible in a traditional data center iSCSI setup.

QUESTION 5

Which of the following is a true statement when addressing the challenges of Regulatory requirements in a SaaS environment?

- a) There is a misperception that the the cloud provider is responsible for compliance; however, neither the provider or the cloud customer are responsible for compliance once the data is moved to the cloud.
- b) There is a misperception that cloud computing removes data compliance responsibility; however, the data owner is still fully responsible for compliance.
- c) There is a misperception that the data owner is completely responsible for compliance; however, it is a shared responsibility between the cloud customer and the cloud provider.
- d) There is a misperception that cloud computing does not remove data compliance responsibility; however the cloud provider assumes that responsibility once it is in possession of the data.

QUESTION 6

Which of the following is true of a VLAN configuration?

- a) Broadcast packets sent by one of the workstations can reach all the others in the VLAN.
- b) All the workstations must go through a gateway in order to communicate with each other.
- c) Broadcast packets sent by one of the workstations cannot reach all the others in the VLAN.
- d) Broadcasts sent by workstations that are not in the VLAN can reach workstations that are in the VLAN.

QUESTION 7

An effective protection against DNS attacks is achieved through the use of the DSNSEC suite of extensions. A recursive or forwarding DNS server recognizes that a zone supports DNSSEC if it has a DNSKEY for that zone. What is another name for a DNSKEY?

- a) Another name for a DNSKEY is a "Trust Anchor".
- b) Another name for a DNSKEY is a "DNS Signature".
- c) Another name for a DNSKEY is an "Authoritative Zone".
- d) Another name for a DNSKEY is a "DNSSEC qualifier".

QUESTION 8

Which threat to domain name resolution service could happen when a DNS server accepts and uses incorrect information from a host that has no authority in providing that information in the first place?

- a) Spoofing
- b) Redirection
- c) Footprinting
- d) Data Modification

QUESTION 9

Clustered storage is the use of two or more storage servers working together to increase performance, capacity, or reliability. Clustering distributes workloads to each server, manages the transfer of workloads between servers, and provides access to all files from any server regardless of the physical location of the file.

Two basic clustered storage architectures exist, known as *tightly coupled* and *loosely coupled*.

Which of the following is most accurate about these types of storage architectures?

- a) A tightly coupled cluster backplane fixes the minimum size of the cluster and delivers a high-performance interconnect between servers for load-balanced performance, however, the minimum cluster size eliminates scalability, so the cluster cannot grow. A loosely coupled cluster offers cost-effective building blocks that can start small and grow as applications demand. A loose cluster offers performance, I/O, and storage capacity within the same node. As a result, performance scales with capacity and vice versa.
- b) A tightly coupled cluster backplane fixes the maximum size of the cluster, yet it delivers a high-performance interconnect between servers for load-balanced performance and maximum scalability as the cluster grows. A loosely coupled cluster offers cost-effective building blocks, however, the cost-effectiveness reduces the desired elasticity of the solution. A loose cluster offers limited performance, reduced I/O, and limited storage capacity within the same node. As a result, performance does not scale with capacity and vice versa.
- c) A tightly coupled cluster offers an unlimited cluster size, and delivers a high-performance interconnect between servers for load-balanced performance and maximum scalability as the cluster grows. A loosely coupled cluster offers building blocks that can start small and grow as applications demand, however, these building blocks are costly in both money and performance. As a result, performance and I/O are reduced, but storage capacity is unlimited.,
- d) A tightly coupled cluster backplane fixes the maximum size of the cluster, yet it delivers a high-performance interconnect between servers for load-balanced performance and maximum scalability as the cluster grows. A loosely coupled cluster offers cost-effective building blocks that can start small and grow as applications demand. A loose cluster offers performance, I/O, and storage capacity within the same node. As a result, performance scales with capacity and vice versa.

QUESTION 10

Performance monitoring is essential for the secure and reliable operation of a cloud environment. Which of the following is not part of a performance monitoring strategy?

- a) Access Control
- b) Memory
- c) Network
- d) Disk

QUESTION 11

Network security is best achieved using a "Defense In Depth" approach which seeks to build mutually reinforcing layers of protective systems and policies to manage them. Fine-tuning these systems is vital to achieving the desired level of security. An intrusion detection system (IDS) is part of a layered approach to security, but it is not without its problems. What is the primary complaint with Intrusion Detection Systems?

- a) An IDS does not sit inline on the network, so it may miss some traffic.

- b) An IDS is a passive system, so it does nothing proactively.
- c) An IDS lacks "deep visibility" into network activity.
- d) An IDS generates a large number of false positives and false negatives.

QUESTION 12

As a CCSP, it is your responsibility to ensure that proper log management takes place. The type of log data collected depends on the type of service provided. In which service model would the cloud service provider typically not collect or have access to the log data, leaving the responsibility of log management to the cloud customer?

- a) Infrastructure as a Service and Platform as a Service (IaaS and PaaS).
- b) Platform as a Service and Software as a Service (PaaS and SaaS).
- c) Infrastructure as a Service (IaaS).
- d) Software as a Service (SaaS).

QUESTION 13

When conducting a vulnerability assessment, which area of compliance testing is most suitable if your organization is storing medical records?

- a) SOX
- b) NIST
- c) GLBA
- d) HIPAA

QUESTION 14

What is a noted benefit of SIEM systems?

- a) SIEM systems are not subject to any known attacks, making them the best line of defense along with a firewall.
- b) SIEM systems eliminate the need for an Intrusion Detection System (IDS).
- c) SIEM systems are compliant with all regulations relating to ensuring data privacy and protection.
- d) SIEM systems map to and support the implementation of the Critical Controls for Effective Cyber-Defense.

QUESTION 15

What is a true statement about the logical design for a network?

- a) A Logical network design lacks the use of terms from the customer's business vocabulary.
- b) A Logical network design lacks specific details such as technologies and standards while focusing on the needs at a general level.
- c) A Logical network design is not part of the SDLC.
- d) A Logical network design uses concrete details to describe complex systems.

QUESTION 16

What is most important for the Cloud Security Professional to consider before performing system repair and maintenance?

- a) When scheduling system repair and maintenance, the CSP needs to ensure adequate resources are available to meet expected demand and SLA requirements.
- b) When scheduling system repair and maintenance, a host system must be placed into maintenance mode before starting any work on it.
- c) When scheduling system repair and maintenance, a host system must be powered off or moved to another host before starting any work on it.
- d) When scheduling system repair and maintenance, the CSP must ensure that all appropriate security protections and safeguards continue to apply to all hosts while in maintenance mode.

QUESTION 17

Business continuity management is the process of reviewing and managing risks and threats to services, business functions, and the organization. Which of the following elements is often the key business continuity requirement?

- a) Availability
- b) Confidentiality
- c) Authorization
- d) Integrity

Legal and Compliance

QUESTION 1

Components of an effective distributed information technology (IT) model generally includes all, except:

- a) Communicating in a structured and standardized way.
- b) Clearly assigned and identified requirements that are documented in SLAs.
- c) Readily available independent security vendor reports.
- d) Project management.

QUESTION 2

Concerning relevant cloud computing stakeholders within an organization, relevant stakeholders usually do not include:

- a) Executive Committee and Directors.
- b) Vendor Management, Compliance and Audit teams.
- c) IT, Information Security, Logistics and Risk teams.
- d) Legal, Finance and Operations teams.

QUESTION 3

Organizational policies are not useful in helping to reduce:

- a) Retrievable data loss.
- b) Financial loss.
- c) Misuse and abuse of systems and resources.
- d) Reputational, regulatory and legal issues.

QUESTION 4

The CCSP official study guide has a list of legislative items that might impact your cloud environments. Which of the following choices is not part of that list?

- a) Criminal, tort and privacy laws
- b) International, State, and privacy laws.
- c) Copyright and Intellectual property rights.
- d) Unenforceable governmental request

QUESTION 5

Which of the following statements is FALSE ?

- a) Tort laws hold individuals liable for costs and consequences of wrongful acts
- b) Criminal laws define punishment and seek to protect the safety and well-being of the public
- c) The European Union (EU) Directive 95/46/EC helps protect processing, use and exchange of personal citizen data within the European Union
- d) Copyright laws protect logos and symbols

QUESTION 6

Which of the following is not included in the audit planning phase?

- a) Define audit policies.
- b) Refine the audit process.
- c) Define audit scope and conduct audit.
- d) Define audit objectives.

QUESTION 7

The focus of most cloud-based audits includes all, except:

- a) Contractual requirements.
- b) The ability to meet service level agreements (SLAs).
- c) Technical assessments.
- d) Industry best practice standards and frameworks.

QUESTION 8

The 10 main privacy principles according to AICPA's Generally Accepted Privacy Principles (GAPP) include all of the statements below except one, which one is it?

- a) Disclosure to third parties, Security for privacy, Quality, Monitoring and enforcement
- b) Management, Notice, Choice and consent
- c) Collection, Use, Retention and disposal, Access
- d) Confidentiality, Integrity, Availability

QUESTION 9

On what, must the Cloud Security Provider (CSP) and the cloud customer focus?

- a) Risk
- b) Confidentiality, Integrity, Availability

- c) Resiliency
- d) Interoperability

QUESTION 10

What statement concerning the Service Level Agreement (SLA) is false?

- a) The SLA should reference compliance and best practice activities.
- b) SLAs tend to be structured in favor of the customer as penalty clauses within the SLA is a form of transferring risks.
- c) Customers pay for time and costs associated with making changes to existing SLAs.
- d) The SLA is critical in establishing secure business and operational requirements.

QUESTION 11

Complete the sentence below:

Generally speaking, in the United States, a party is obligated to undertake reasonable steps to prevent the destruction or modification of data or information in its possession, custody, or control that it knows (or reasonably should know) _____.

- a) Is not encrypted.
- b) Relevant to a pending or reasonably anticipated litigation or government investigation.
- c) Contains credit card information, in conjunction with PCI DSS requirements.
- d) Provides enough PII to jeopardize a customer's Right to Privacy.

QUESTION 12

Please complete the sentence below:

In most jurisdictions in the United States, a party's obligation to produce relevant information is limited to documents and _____.

- a) Data that does NOT include Personally Identifying Information of employees.
- b) Data that does NOT include Personally Identifying Information of customers.
- c) Data that are within its possession, custody or control.
- d) Data as listed in the Graham / Livingston Act of 2007.

QUESTION 13

Company ABC, an ISP, offers online backup services to its subscribers. The company uses a cloud provider to store the backups of its subscribers. The Cloud providers servers were hacked, and the ISP's customers data were exposed and sold on the dark web. Who can the ISP customers hold liable for the breach?

- a) Cloud Customer

- b) Cloud Provider
- c) Cloud Architect
- d) Cloud Broker