# 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 | 1. 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 |
| 1. Metered Access | 1. Consumer can unilaterally provision computing capabilities as needed automatically |
| 1. On-demand self-service | 1. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms |
| 1. Resource Pooling | 1. Capabilities can be provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. |
| 1. Rapid elasticity | 1. 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?

1. Hybrid
2. Private
3. Public
4. Community

QUESTION 3

Which of the following pose the greatest challenge to security?

1. Process
2. Technology
3. People
4. 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?

1. Type 1 hypervisor runs directly on the guest OSs and reduces the likelihood of malicious software.
2. Type 2 hypervisor runs on host OSs and are more attractive to attackers.
3. Type 2 hypervisor runs directly on the guest OSs and reduces the likelihood of malicious software.
4. Type 1 hypervisor is also called bare metal hypervisors.

QUESTION 5

Cloud Computing Top Threats include:

1. Denial of Service, Data Remanence and Data Loss
2. Data Loss, Account or Service Traffic Hijacking and Malicious Insiders
3. Abuse of Cloud Services, Sufficient Due Diligence and Data Breaches
4. Secure Interfaces and Application Programming Interfaces (APIs)

QUESTION 6

Critical cloud business continuity success elements include all, except:

* 1. Understanding interdependencies and supply chain risks.
  2. Regularly auditing continuity capabilities and identifying on/off premise backup sites.
  3. Treating all assets and services as equal and prioritizing restoration.
  4. 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?

1. Denial of Service
2. Abuse of Cloud Service
3. Traffic Hijacking
4. Malicious Insider

QUESTION 8

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

1. Bolt-on components are good because they build extra security into an existing API.
2. Bolt-on components are good because they increase productivity.
3. Bolt-on components are bad because they increase complexity and decrease security.
4. 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:

1. Due Care is the methodology required for certifying a site as "cloud ready", and Due Diligence is the process of accreditation of a site.
2. 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 protectng the company, its assets, and its people from threats.
3. 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 protectng the company, its assets, and its people from threats.
4. 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 are known as the Common Criteria and have 7 Evaluation Assurance Levels. Which level indicates the highest testing evaluation?

1. Level 7 is the highest level, indicating the most rigorous testing.
2. Each level is separate and is not graded on a scale of lowest to highest.
3. Level 1 is the highest level, indicating the most rigorous testing.
4. 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?

1. Public
2. Hybrid
3. Community
4. Private

QUESTION 12

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

1. Common Criteria
2. PCI DSS
3. ISO 17799
4. 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?

1. PCI DSS
2. SOC I / SOC II / SOC III
3. ISO 27001
4. 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?

1. SOC I, Type I
2. SOC III
3. SOC I, Type II
4. SOC II

QUESTION 15

How is security best accomplished at the SaaS level?

1. Security is provided through traditional firewalls.
2. Security must be provided by the cloud consumer.
3. Security is negotiated as part of the Service Level Agreement.
4. Through collaboration.

QUESTION 16

Which of the following is NOT a characteristic of IaaS?

1. Resilience
2. Flexibility
3. 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?

1. Jericho/Open Group
2. ITIL
3. SABSA
4. TOGAF

QUESTION 18

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

1. ColTRANE
2. TOGAF
3. Jericho/Open Group
4. 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?

1. Auditability
2. SLA
3. Regulatory Compliance
4. Portability

QUESTION 20

Which of the following is a true statement?

1. Deployment of a cloud solution is always a technology decision.
2. Organizational goals that require technology, especially cloud technology are best met when technology is considered at the forefront.
3. The choice to deploy a cloud solution is primarily a technical decision.
4. 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?

1. Privacy must be outlined in the Service Level Agreement with the cloud provider.
2. Privacy is achieved through the security provided by the cloud provider.
3. Privacy is best achieved through regulatory compliance.
4. 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?

1. The focus of an organization to produce information about actions of the users.
2. The requirement of an organization to access, report, and obtain evidence of organizational controls.
3. The requirement of an organization to define processes and procedures.
4. 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?

1. The perimeter transforms into a series of highly dynamic "micro borders" for some cloud providers.
2. There is no clear perimeter in cloud networks.
3. The Board member is correct in stating that the perimeter is clearly the demarcation point.
4. 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?

1. IPSEC
2. TLS
3. KMS
4. 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?

1. Cloud Architect
2. Cloud Administrator
3. Cloud Operator
4. Cloud Storage Administrator

QUESTION 26

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

1. Remote Key Management Service
2. Segregated Key Management
3. Hybrid Key Management
4. Client Side Key Management

QUESTION 27

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

1. Rapid Elasticity
2. On-Demand Self Service
3. Measured Self-Service
4. Broad Network Access

QUESTION 28

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

1. Classifying the organizations data to determine the requirements for the cloud engagement.
2. All of the other choices are considerations.
3. Determining the best cloud formation for the business.
4. 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?

1. Centralized Key Management
2. Provisioning and De-Provisioning
3. Migration and Transference
4. 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?

1. Cloud Capability Matrix
2. STAR
3. ISO 27001
4. Cloud Security Roadmap

QUESTION 31

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

1. Lightweight Directory Access Protocol (LDAP)
2. LPIE Protocol (LPIEP)
3. Multi-Factor Authentication Protocol (MAP)
4. Privileged Identity Protocol (PIP)

QUESTION 32

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

1. A Type II Hypervisor is more secure than a Type I hypervisor.
2. A Type II Hypervisor is Bare Metal
3. A Type II Hypervisor is easier to deploy than a Type III Hypervisor
4. A Type II Hypervisor is OS-Based

QUESTION 33

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

1. Type IV hypervisors security is limited in its patch availability.
2. The limited access and strong control over the OS greatly increases the reliability and robustness of Type I hypervisors.
3. The operating system-based hypervisor is standardized, making it less vulnerable.
4. 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?

1. No, because shell access to the VM could result in configuration changes that could impact multiple tenants.
2. Yes, because a tenant needs full access to the server in order to make necessary changes to the configuration of the VMs.
3. No, because there is no way to monitor shell access to a VM server.
4. Yes, because shell access is a core comonent 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.

1. This is false because simply powering off a VM does not stop the processes from running, leading to VM sprawl
2. This is false because simply powering off a VM still leaves the image files susceptible to malware infections and missed patching
3. This is true, because simply powering off a VM renders it inaccessible to the system on which it resides
4. 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?

1. 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.
2. A single point of access to a VM environment is a security threat because it creates strict network topologies, which are counter-productive.
3. A single point of access to a VM environment is security threat due to its decreased complexity, which decreases a defense-in-depth approach.
4. 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.

1. This is a good design because it prevents SQL injection attacks.
2. This is a bad design because it creates the threat of Insecure Direct Object References.
3. This is a good design because it is efficient and operationally expedient.
4. 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?

1. Process
2. Access
3. Destroy
4. 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?

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

QUESTION 40

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

1. Appreciation of IT technologies
2. Reducing maintenance and configuration time
3. Pay per use
4. 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:

1. Had effective board oversight
2. Consistently practiced due diligence and due care
3. Had a current BIA and RA
4. Had an effective cloud backup solution

QUESTION 42

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

1. 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.
2. 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.
3. 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.
4. 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 use 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.

1. IaaS
2. Private Cloud
3. PaaS
4. SaaS

QUESTION 44

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

1. All models have the same integration level
2. PaaS
3. SaaS
4. IaaS

QUESTION 45

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

1. Software as a Service (SaaS)
2. Infrastructure as a Service (IaaS)
3. PaaS
4. Security as a Service (SecaaS)

QUESTION 46

Which of the following is true of a private cloud?

1. It may be internal or external to an organization.
2. It is always managed by a broker.
3. It must be internal to an organization.
4. 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?

1. Insecure Direct Object References
2. Security Reconfiguration
3. Cross-Site Request Forgery
4. 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?

1. Low Orbit Ion Cannon Attack
2. Denial of Service
3. Traffic Hijacking
4. Cruzr attack

QUESTION 49

The definition of cloud portability is?

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

QUESTION 50

Which of the following is a not a SSO technology?

1. SAML
2. SCIM
3. XACML
4. OpenID Connect

QUESTION 51

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

1. Cloud owner
2. Cloud auditor
3. Cloud director
4. 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?

1. 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.
2. Resource pooling allows for dynamic adjustment to shared resources, but is only available in a private cloud.
3. 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.
4. Resource pooling provides dedicated resources to cloud tenants.

QUESTION 53

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

1. Customer controls services deployed within the cloud, storage, deployed applications, and operating systems (including licensing)
2. Cloud provider is responsible for the operating system and hosting environment including libraries, service and tools
3. Cloud provier supplies a full cloud platform and software application to the customer
4. 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?

1. Hybrid complexity
2. Strict segmentation
3. Resource pools
4. 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?

1. Resource pooling provides dedicated resources to the cloud tenants
2. Resource pooling is only used in private cloud
3. Resource pooling provides shared services with cloud computing
4. 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?

1. Access to event and diagnostic data is dependent on the development team.
2. The SaaS platform typically has the least amount of control and access to event and diagnostic data.
3. The PaaS platform typically has the least amount of control and access to event and diagnostic data.
4. 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?

1. No, it does not make sense to modify old rules. Only new rules should be added to address new threats.
2. No, it does not make sense to modify old rules, as that can run contrary to company policy.
3. Yes, it makes sense to modify old rules to reduce false positives.
4. 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?

1. Crypto-Shredding
2. Degaussing
3. Physical destruction
4. Overwriting

QUESTION 4

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

1. Data Encryption Procedures
2. Data Monitoring procedures
3. Backup and DR options
4. Data Format and Media Types

QUESTION 5

Which of the following is an example of Unstructured Data?

1. Text and Multimedia content
2. Relational Database content
3. IAM information
4. 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

1. The PLA provides a clear and effective way to communicate the level of personal data protection provided by a service provider.
2. The PLA provides guidelines for compensatory damages for non-compliance with data protection legislation.
3. The PLA works as a tool to assess the level of a service provider's compliance with data protection legislative requirements and leading practices.
4. 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?

1. The goal of the PLA is to fulfill the Privacy and Data Protection laws applicable to the controller.
2. The goal of the PLA is to fulfill the Privacy and Data Protection laws applicable to the processor.
3. The goal of the PLA is to fulfill the Privacy and Data Protection laws applicable to the Data Loss Protection Manager.
4. 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?

1. Data may only be classified if it is going to be shared.
2. The preferred time to classify content is during the creation phase.
3. The preferred time to classify content should be during consideration of the storage of the data.
4. 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?

1. Storage
2. Obsfuscation
3. Encryption
4. Classification

QUESTION 10

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

1. Not all data should be shared and not all sharing should present a threat.
2. Data should only be shared if it is also archived.
3. Data should only be shared according to a need-to-know model of data security.
4. 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?

1. Data in Use is most vulnerable
2. Archived Data is most vulnerable
3. Data is most vulnerable during the destruction process
4. 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?

1. PaaS utilizes Volume and Object Data storage.
2. PaaS utilizes Structured and Unstructered Data storage.
3. PaaS utilizes Raw and Ephemeral Data storage.
4. 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?

1. This statement is false because the data can be downloaded to a portable device that could become lost or stolen.
2. This statement is true because data dispersion protects data loss.
3. This statement is false because the data is stored on local discs in the possession of the cloud user.
4. 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?

1. 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.
2. 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.
3. 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.
4. 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?

1. Tokenized masking is the technology that chunks a data object into the segments
2. Erasure coding is the technology that chunks a data object into the segments
3. Encryption algorithmic dispersion is the technology that chunks a data object into the segments
4. 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?

1. The majority of cloud-based DLP is focused at the Discovery and Classification level.
2. The majority of cloud-based DLP is focused at the Anonymization level.
3. The majority of cloud-based DLP is focused at the Data in Motion level.
4. 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?

1. 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.
2. In a "Data in Motion" topology, the DLP monitoring engine shoud be deployed in an unstructured database.
3. In a "Data in Motion" topology, the DLP monitoring engine shoud be deployed at the endpoint, where the data is processed.
4. 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?

1. Separation of duties has no impact on key management.
2. Separation of duties shifts the responsibility to the Board of Directors.
3. Separation of duties requires that a manager approves the action in order to proceed with the key management function.
4. 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?

1. LUN Checks.
2. Metadata.
3. Indexed Sequential Access.
4. Dashboards.

QUESTION 20

Which of the following Data Discovery techniques uses pattern matching?

1. Labels.
2. Simple DBs.
3. Locations.
4. Content analysis.

QUESTION 21

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

1. The controller is defined as the person or authority that controls the the data subject.
2. The controller is defined as a natural or legal person, public authority, agency, or any other body that processes personal data.
3. 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.
4. 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?

1. 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.
2. 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.
3. All liabilities are assigned to the Controller role, and its country of establishmentmainly determines the applicable Privacy and Data Protection law and jurisdiction.
4. 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?

1. Governance, Risk & Compliance is an Enterprise Responsibility across all cloud service models.
2. Governance, Risk & Compliance is a Shared Responsibility across all cloud service models.
3. Governance, Risk & Compliance is an Enterprise Responsibility in the SaaS service model, and and Enterprise responsibility in the PaaS service model.
4. 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?

1. At the client.
2. In the Application
3. Within the database.
4. At the instance

QUESTION 25

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

1. Infrastructure as a Service (IaaS)
2. Software as a Service (SaaS)
3. Security as a Service (SecaaS)
4. 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 retrival procedures. A cloud data retention policy should contain which of the following components?

1. Data Owner
2. Legislation, regulation, and standards requirements.
3. Access Control List
4. 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?

1. 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.
2. Because an IRM contains ACLs and is embedded into the original file, IRM is agnostic to the location of the data.
3. Because an IRM contains ACLs and is embedded into the original file, IRM can only be used for documents.
4. 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?

1. Policy enforcement
2. Corporate governance
3. Audit control
4. Enterprise risk management

QUESTION 2

What statement is most accurate about cloud object storage?

1. Object storage features are never used for storing operating system images.
2. Object storage features offer increased, real-time data consistency, making them perfect for frequently changing data.
3. 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.
4. 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?

1. You should suggest a battery backup unit to prevent power failures.
2. You should suggest that the single fuel tank is a single point of failure and the design should include a redundant fuel tank.
3. You should suggest a larger fuel tank to accommodate longer power failures.
4. 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?

1. 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.
2. 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.
3. 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.
4. 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 whch of the following cloud risks?

1. Control conflict.
2. Software related risks.
3. Resource exhaustion.
4. 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?

1. Law enforcement activity, such as the siezure of a hard drive, has the potential to create a problem due to the storage locations of the data on the disk.
2. Law enforcement activity, such as the seizure of a physical hard drive, has the potential to violate regulatory requirements of data handling and storage.
3. 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.
4. 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 a 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?

1. Physical Security is a shared responsibility in an IaaS platform, and Platform Security is a shared responsibility in a PaaS platform.
2. Application Security is a shared responsibility in a PaaS platform, and Data Security is a shared responsibility in a SaaS platform
3. Infrastructure Security is a shared responsibility in an IaaS platform, and Application Security is a shared responsibility in a SaaS platform.
4. Platform Security is a shared responsibility in both the PaaS and SaaS platforms.‚

QUESTION 8

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

1. Testability should be considered during the budget phase of the BCDR plan.
2. Testability should be considered during the performance phase of the BCDR plan.
3. Testability should be considered during the scope phase of the BCDR plan.
4. 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?

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

QUESTION 10

What are the main components of SAML?

1. Assertions, Protocol, and Binding
2. Assertions, Protocol, and Authentication
3. Assertions, Protocol, and Authorization
4. Authentication, Attribute and Authorization

QUESTION 11

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

1. Tabletop Exercise / Structured Walk-Through Test specifically requires all operational and support personnel.
2. Test Plan Review specifically requires all operational and support personnel.
3. Walk-Through Drill / Simulation Test specifically requires all operational and support personnel.
4. Functional Drill/ Parallel Test specifically requires all operational and support personnel.
5. 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 recomends that the snapshots be stored on a secure server with access available only to the cloud administrative teams. Is this a good idea?

1. 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 vritualized snapshot image.
2. 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.
3. 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.
4. 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?

1. In a federated identity model, authorization is typically with the relying party whereas authentication is a function of the identity provider.
2. In a federated identity model, authentication is typically with the relying party whereas authorization is a function of the identity provider.
3. Identity management is governed through resource usage.
4. 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?

1. John the Ripper and Low Orbit Ion Cannon.
2. Puppet and Chef.
3. Punch and Judy.
4. 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?

1. An API gateway.
2. Database activity monitoring (DAM).
3. A Cloud web application firewall (WAF).
4. 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?

1. 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.
2. 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.
3. Yes, the burden of avoiding data loss falls solely on the provider, since the provider has assumed full responsibility for data protection.
4. 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?

1. The ANF is used in conjunction with the ONF and is created for a specific application.
2. The ANF is a separate entity from the ONF - they have no relation to each other.
3. The ONF maintains the applicable portions of the ANF that are needed to enable a specific application to acheive a required level of security.
4. 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?

1. STRIDE.
2. Black box.
3. Threat modeling.
4. Repudiation.

QUESTION 6

What are the three subcomponents of applications?

1. Data, Technology, Processes.
2. Data, Functions, Technology.
3. People, Processes, Technology.
4. Data, Functions, Processess.

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?

1. SOAP only supports the YAML data format.
2. SOAP only supports the JSON data format.
3. SOAP only supports the XML data format.
4. SOAP only supports the XAML data format.

QUESTION 8

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

1. Release.
2. Maintenance.
3. Analysis.
4. 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".

1. Injection.
2. Cross-site request forgery.
3. Insecure direct object reference.
4. 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.

1. Indirect secure object reference.
2. Insecure direct object reference.
3. Inferential secure object deference.
4. 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?

1. The Static application security test and the Dynamic application security test play different roles - one is not better than the other.
2. A Dynamic application security test is better because it tests the HTTP and HTML interfaces of the web applications.
3. 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.
4. 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?

1. Header, Reflected and DOM-based
2. Stored, Reflected and DCOM-based
3. Stored, Reflected and DOM-based
4. 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?

1. Security Assertion Markup Language (SAML) 2.0
2. OAuth 2.0
3. WS-Federation Version 1.2
4. 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?

1. Degaussing
2. Data Vaulting
3. Cipher /U
4. Crypto-shredding

QUESTION 16

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

1. SAML
2. OpenID  Connect
3. OAuth
4. WS-Federation
5. RADIUS

## Operations

QUESTION 1

How is security best accomplished at the SaaS level?

1. Through collaboration.
2. Security must be provided by the cloud consumer.
3. Security is provided through traditional firewalls.
4. 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:

1. Hosting racks of physical infrastructure with each server in a separate "coop" to form a clear demarcation from other tenant equpment.
2. Hosting racks of physical infrastructure with each virtual switch in a separate environment to protect against "cam bus wolf-packs".
3. Hosting of racks of physical infrastructure within long rectangles with isolated power strips, thereby reducing electrical anomalies.
4. 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?

1. 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).
2. 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.
3. 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.
4. 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 accomodate more users than originally subscribed. The ability to "oversubscribe " is especially true when implementing iSCSI storage technology.  
What is your impression of this statement?

1. 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.
2. This statement made by the sales representative is accurate. ‚ One of the key benefits of cloud computing is rapid elasticity across all platform models.
3. 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.
4. 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?

1. 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.
2. There is a misperception that cloud computing removes data compliance responsibility; however, the data owner is still fully responsible for compliance.
3. 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.
4. 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?

1. Broadcast packets sent by one of the workstations can reach all the others in the VLAN.
2. All the workstations must go through a gateway in order to communicate with each other.
3. Broadcast packets sent by one of the workstations cannot reach all the others in the VLAN.
4. 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?

1. Another name for a DNSKEY is a "Trust Anchor".
2. Another name for a DNSKEY is a "DNS Signature".
3. Another name for a DNSKEY is an "Authoritative Zone".
4. 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?

1. Spoofing
2. Redirection
3. Footprinting
4. 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?

1. 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.
2. 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.
3. 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.‚
4. 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?

1. Access Control
2. Memory
3. Network
4. 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?

1. An IDS does not sit inline on the network, so it may miss some traffic.
2. An IDS is a passive system, so it does nothing proactively.
3. An IDS lacks "deep visibility" into network activity.
4. 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?

1. Infrastructure as a Service and Platform as a Service (IaaS and PaaS).
2. Platform as a Service and Software as a Service (PaaS and SaaS).
3. Infrastructure as a Service (IaaS).
4. 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?

1. SOX
2. NIST
3. GLBA
4. HIPAA

QUESTION 14

What is a noted benefit of SIEM systems?

1. SIEM systems are not subject to any known attacks, making them the best line of defense along with a firewall.
2. SIEM systems eliminate the need for an Intrusion Detection System (IDS).
3. SIEM systems are compliant with all regulations relating to ensuring data privacy and protection.
4. 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?

1. A Logical network design lacks the use of terms from the customer's business vocabulary.
2. A Logical network design lacks specific details such as technologies and standards while focusing on the needs at a general level.
3. A Logical network design is not part of the SDLC.
4. 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?

1. When scheduling system repair and maintenance, the CSP needs to ensure adequate resources are available to meet expected demand and SLA requirements.
2. When scheduling system repair and maintenance, a host system must be placed into maintenance mode before starting any work on it.
3. When scheduling system repair and maintenance, a host system must be powered off or moved to another host before starting any work on it.
4. 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?

1. Availability
2. Confidentiality
3. Authorization
4. Integrity

## Legal and Compliance

QUESTION 1

Components of an effective distributed information technology (IT) model generally includes all, except:

1. Communicating in a structured and standardized way.
2. Clearly assigned and identified requirements that are documented in SLAs.
3. Readily available independent security vendor reports.
4. Project management.

QUESTION 2

Concerning relevant cloud computing stakeholders within an organization, relevant stakeholders usually do not include:

1. Executive Committee and Directors.
2. Vendor Management, Compliance and Audit teams.
3. IT, Information Security, Logistics and Risk teams.
4. Legal, Finance and Operations teams.

QUESTION 3

Organizational policies are not useful in helping to reduce:

1. Retrievable data loss.
2. Financial loss.
3. Misuse and abuse of systems and resources.
4. 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?

1. Criminal, tort and privacy laws
2. International, State, and privacy laws.
3. Copyright and Intellectual property rights.
4. Unenforceable governmental request

QUESTION 5

Which of the following statements is FALSE ?

1. Tort laws hold individuals liable for costs and consequences of wrongful acts
2. Criminal laws define punishment and seek to protect the safety and well-being of the public
3. The European Union (EU) Directive 95/46/EC helps protect processing, use and exchange of personal citizen data within the European Union
4. Copyright laws protect logos and symbols

QUESTION 6

Which of the following is not included in the audit planning phase?

1. Define audit policies.
2. Refine the audit process.
3. Define audit scope and conduct audit.
4. Define audit objectives.

QUESTION 7

The focus of most cloud-based audits includes all, except:

1. Contractural requirements.
2. The ability to meet service level agreements (SLAs).
3. Technical assessments.
4. 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?

1. Disclosure to third parties, Security for privacy, Quality, Monitoring and enforcement
2. Management, Notice, Choice and consent
3. Collection, Use, Rention and disposal, Access
4. Confidentiality, Integrity, Availability

QUESTION 9

On what, must the Cloud Security Provider (CSP) and the cloud customer focus?

1. Risk
2. Confidentiality, Integrity, Availability
3. Resiliency
4. Interoperability

QUESTION 10

What statement concerning the Service Level Agreement (SLA) is false?

1. The SLA should reference compliance and best practice activities.
2. SLAs tend to be structured in favor of the customer as penalty clauses within the SLA is a form of transferring risks.
3. Customers pay for time and costs associated with making changes to existing SLAs.
4. 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) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

1. Is not encrypted.
2. Relevant to a pending or reasonably anticipated litigation or government investigation.
3. Contains credit card information, in conjunction with PCI DSS requirements.
4. 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 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

1. Data that does NOT include Personably Identifying Information of employees.
2. Data that does NOT include Personably Identifying Information of customers.
3. Data that are within its possession, custody or control.
4. 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?

1. Cloud Customer
2. Cloud Provider
3. Cloud Architect
4. Cloud Broker