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. |

Answers 1c 2e 3b 4a 5d

Question 2

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

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

Answer B

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

The correct answer is: c People

When looking to secure the key assets of any organization, three primary components are essential people, processes, and technology. People tend to present the single largest challenge to security due to the possibility of a disgruntled, rogue, or simply careless employee or contractor exposing sensitive data either by accident or on purpose.

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.

Answer

Answer C Type 2 security: Because Type 2 hypervisors are OS based, they are more attractive to attackers, given that there are far more vulnerabilities associated with the OS as well as other applications that reside within the OS layer. A lack of standardization on the OS and other layers can open up additional opportunities and exposures that might make the hypervisor susceptible to attack and compromise.

Question 5

Cloud Computing Top Threats include:

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

The correct answer is: B Data Loss, Account or Service Traffic Hijacking and Malicious Insiders  
  
Answer

Nine critical threats to cloud security (ranked in order of severity):

* Data Breaches disclosure of sensitive information to a party
* Data Loss loss of information, deletion, overwriting, corruption or integrity related to the information stored, processed, or transmitted within cloud environment
* Account or Service Traffic Hijacking attackers are able to monitor or eavesdrop on communications, capture relevant credentials, access and alter account and user provides, etc.
* Insecure Interfaces and Application Programming Interfaces (APIs) third parties, organizations, customers, etc., adding on to the provider s cloud computing resources causing it to become insecure.
* Denial of Service preventing legitimate users from accessing a resource or service; does not always require large volumes of traffic to be successful such as asymmetric application-level payload attacks.
* Malicious Insiders people tend to present the single largest security challenge due to becoming rogue, disgruntled, or careless, exposing sensitive data by accident or on purpose
* Abuse of Cloud Services
* Insufficient Due Diligence
* Shared Technology Vulnerability Issues

Question 6

1. Critical cloud business continuity success elements include all, except:
2. Understanding interdependencies and supply chain risks.
3. Regularly auditing continuity capabilities and identifying on/off premise backup sites.
4. Treating all assets and services as equal and prioritizing restoration.
5. Understanding CSP and customer responsibilities.

The correct answer is: C Treating all assets and services as equal and prioritizing restoration  
  
From the perspective of the cloud customer, business continuity elements include the relevant security pillars of availability, integrity, and confidentiality. The availability of the relevant resources and services is often the key requirement, along with the uptime and ability to access these on demand.   
Failure to ensure this results in significant impacts, including loss of earnings, loss of opportunities, and loss of confidence for the customer and provider.  
  
Two critical success factors for business continuity when utilizing cloud-based services are as follows:

1. Understanding CSP and customer responsibilities;
   * Customer responsibilities
   * CSP responsibilities
   * Understanding any interdependencies or third parties (supply chain risks)
   * Order of restoration (priority)
   * Appropriate frameworks and certifications held by the facility, services, and processes
   * Right to audit and make regular assessments of continuity capabilities
   * Communications of any issues or limited services
2. Identification of need for backups to be held onsite or offsite or with another CSP. Regularly auditing continuity capabilities and identifying on/off premise backup sites.
   * Penalties and compensation for loss of service
   * RTOs and RPOs
   * Loss of integrity or confidentiality
   * Points of contact and escalation processes
   * Failover to maintain compliance
   * Changes being communicated in a timely manner
   * Clearly defined responsibilities
   * Where usage of third parties is required per the agreed-upon SLA

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

The correct answer is: Denial of Service

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.

The correct answer is: C Bolt-on components are bad because they increase complexity and decrease security.  
  
Regardless of productivity, the increased complexity that is introduced through bolt-on components is always a security risk.  
Bolt-on components may attempt to build extra security into an API, but the added complexity usually decreases 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.

The correct answer is: B Due Diligence is the act of investigating and understanding the risk 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.  
  
  
Due Diligence = Do Detect  
Due Care = Do Correct  
  
Due Diligence is following Standards, Best Practices, Consensus of expert in order to identify potential threats what could affect you.  
  
Due care is what action your are going to take once the threats have been identified and how are you going to bring the threat level down to an acceptable level and maintain it at that level.  
  
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.

The correct answer is: A Level 7 is the highest level, indicating the most rigorous testing.  
  
The goal of CC certification is to ensure customers that the products they are buying have been evaluated and that a vendor-neutral third party has verified the vendor’s claims.  
  
To submit a product for evaluation, follow these steps:

* The vendor must complete a Security Target (ST) description that provides an overview of the product‚„¢s security features.
* A certified laboratory then tests the product to evaluate how well it meets the specifications defined in the protection profile.
* A successful evaluation leads to an official certification of the product.

The Evaluation Assurance Level (EAL1 through EAL7) of an IT product or system is a numerical grade assigned following the completion of a [Common Criteria](https://en.wikipedia.org/wiki/Common_Criteria%20) security evaluation, an [international standard](https://en.wikipedia.org/wiki/International_standard%20) in effect since 1999. The increasing assurance levels reflect added assurance requirements that must be met to achieve Common Criteria certification. The intent of the higher levels is to provide higher confidence that the system's principal security features are reliably implemented. The EAL level does not measure the security of the system itself, it simply states at what level the system was tested.

To achieve a particular EAL, the computer system must meet specific *assurance requirements*. Most of these requirements involve design documentation, design analysis, functional testing, or penetration testing. The higher EALs involve more detailed documentation, analysis, and testing than the lower ones. Achieving a higher EAL certification generally costs more money and takes more time than achieving a lower one. The EAL number assigned to a certified system indicates that the system completed all requirements for that level.

1. [Assurance levels](https://en.wikipedia.org/wiki/Evaluation_Assurance_Level#Assurance_levels%20)
   1. [1.1 EAL1: Functionally Tested](https://en.wikipedia.org/wiki/Evaluation_Assurance_Level#EAL1:_Functionally_Tested%20)
   2. [1.2 EAL2: Structurally Tested](https://en.wikipedia.org/wiki/Evaluation_Assurance_Level#EAL2:_Structurally_Tested%20)
   3. [1.3 EAL3: Methodically Tested and Checked](https://en.wikipedia.org/wiki/Evaluation_Assurance_Level#EAL3:_Methodically_Tested_and_Checked%20)
   4. [1.4 EAL4: Methodically Designed, Tested and Reviewed](https://en.wikipedia.org/wiki/Evaluation_Assurance_Level#EAL4:_Methodically_Designed.2C_Tested_and_Reviewed%20)
   5. [1.5 EAL5: Semiformally Designed and Tested](https://en.wikipedia.org/wiki/Evaluation_Assurance_Level#EAL5:_Semiformally_Designed_and_Tested%20)
   6. [1.6 EAL6: Semiformally Verified Design and Tested](https://en.wikipedia.org/wiki/Evaluation_Assurance_Level#EAL6:_Semiformally_Verified_Design_and_Tested%20)
   7. [1.7 EAL7: Formally Verified Design and Tested](https://en.wikipedia.org/wiki/Evaluation_Assurance_Level#EAL7:_Formally_Verified_Design_and_Tested%20)

NOTES:   
The higher the level number the more thorough the testing would be. EAL7 would be the most thorough testing that could be performed under Common Criteria.  
  
The second point you must pay close attention is the use of the word:  "FORMAL".   You will see the same word for the highest level of testing done under TCSEC as well.  At the "A" level rating of TCSEC FORMAL methods would be used as well. 

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

The correct answer is: C Community  
  
The cloud deployment model you choose also affects the breakdown of responsibilities of the cloud-based assets. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, or compliance considerations). It may be managed by the organizations or by a third party and may be located on premise or off premise.  
  
The three cloud models available are **public**, **private**, **community**, and **hybrid** (a mix of two of the three cloud models used at the same time).  
  
A community cloud deployment model provides cloud-based assets to two or more organizations. Maintenance responsibilities are shared based on who is hosting the assets and the service models.  
  
**TIP:**  
  
You must be familiar with each of the cloud deployment model and who is managing it, who is the owner, where is it located, and who has access. See graphic below from the [Cloud Security Alliance guide Version 3.0.](https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf%20)

The following answers are incorrect:  
  
A public cloud model includes assets available for any consumers to rent or lease and is hosted by an external CSP. Service level agreements can be effective at ensuring the CSP provides the cloud-based services at a level acceptable to the organization. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.  
  
The private cloud deployment model includes cloud-based assets for a single organization. Organizations can create and host private clouds using their own resources. If so, the organization is responsible for all maintenance. However, an organization can also rent resources from a third party and split maintenance requirements based on the service model (SaaS, PaaS, or IaaS). The cloud infrastructure is operated solely for a single organization. It may be managed by theorganization or by a third party and may be located on premise or off premise.  
  
Hybrid models include a combination of two or more clouds. Similar to a community cloud model, maintenance responsibilities are shared based on who is hosting the assets and the service models in use. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).  
  
  
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

The correct answer is: B PCI DSS  
  
Visa, MasterCard, and American Express established PCI DSS24 as a security standard to which all organizations or merchants that accept, transmit, or store cardholder data, regardless of size or number of transactions, must comply. PCI DSS was established following a number of significant credit card breaches. It is a comprehensive and intensive security standard that lists both technical and nontechnical requirements based on the number of credit card transactions for the applicable entities.  
  
Maintaining payment security is required for all entities that store, process or transmit cardholder data. Guidance for maintaining payment security is provided in PCI security standards. These set the technical and operational requirements for organizations accepting or processing payment transactions, and for software developers and manufacturers of applications and devices used in those transactions.

A model framework for security, the PCI Data Security Standard integrates best practices forged from the years of experience of security experts around the world.

*The standard works for some of the world’s largest corporations. And it can work for you.*

* Buy and use only approved [PIN entry devices](https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices) at your points-of-sale.
* Buy and use only [validated payment software](https://www.pcisecuritystandards.org/assessors_and_solutions/payment_applications) at your POS or website shopping cart.
* Do not store *any* sensitive cardholder data in computers or on paper.
* Use a firewall on your network and PCs.
* Make sure your wireless router is password-protected and uses encryption.
* Use strong passwords. Be sure to change default passwords on hardware and software ‚€œ most are unsafe.
* Regularly check PIN entry devices and PCs to make sure no one has installed rogue software or ‚“skimming‚ devices.
* Teach your employees about security and protecting cardholder data.
* Follow the [PCI Data Security Standard](https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss).

The following answers are incorrect:  
  
[NIST 800-53](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)  NIST Special Publication 800-53, Revision 4, represents the most comprehensive update to the security controls catalog since its inception in 2005.  The publication was developed by NIST, the Department of Defense, the Intelligence Community, and the Committee on National Security Systems as part of the Joint Task Force, an interagency partnership formed in 2009. This update was motivated principally by the expanding threat space‚€characterized by the increasing sophistication of cyber attacks and the operations tempo of adversaries (i.e., the frequency of such attacks, the professionalism of the attackers, and the persistence of targeting by attackers).  
  
[Common Criteria](https://www.commoncriteriaportal.org/cc/)  The CC permits comparability between the results of independent security evaluations. The CC does so by providing a common set of requirements for the security functionality of IT products and for assurance measures applied  
to these IT products during a security evaluation. These IT products may be implemented in hardware, firmware or software.  
  
The evaluation process establishes a level of confidence that the security functionality of these IT products and the assurance measures applied to these IT products meet these requirements. The evaluation results may help consumers to determine whether these IT products fulfil their security needs.  
  
The CC is useful as a guide for the development, evaluation and/or procurement of IT products with security functionality.  
  
The CC is intentionally flexible, enabling a range of evaluation methods to be applied to a range of security properties of a range of IT products. Therefore users of the standard are cautioned to exercise care that this flexibility is not misused. For example, using the CC in conjunction with unsuitable evaluation methods, irrelevant security properties, or inappropriate IT products, may result in meaningless evaluation results.  
  
[ISO 17799](http://www.iso.org/iso/catalogue_detail?csnumber=39612)  ISO/IEC 17799:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 17799:2005 contains best practices of control objectives and controls in the following areas of information security management:

* security policy;
* organization of information security;
* asset management;
* human resources security;
* physical and environmental security;
* communications and operations management;
* access control;
* information systems acquisition, development and maintenance;
* information security incident management;
* business continuity management;
* compliance.

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

The correct answer is: C ISO 27001  
  
All of the choices presented are frameworks which are in use for various implementations but the only one that was developed by the British Standards Institute was the ISO 27001 framework.  
  
If it cannot be measured, it cannot be managed. This is a statement that any auditor and security professional should abide by regardless of his focus. How can someone have confidence, awareness, and assurances that he and the CSP are taking the correct steps to ensure that data is secured properly? Frameworks and standards hold the key here.  
  
ISO/IEC 27001 is the international standard for information security management. By implementing the standard, organizations can identify security risks and put controls in place to manage or eliminate them, gain stakeholder and customer trust that their confidential data is protected, and help achieve preferred supplier status helping to win new business.  
  
  
The following answers are incorrect:  
  
[NIST 800-53](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf%20%20) The National Institute of Standard and Technologies (NIST) is an agency of the U.S. government that makes measurements and sets standards as needed for industry or government programs. The primary goal and objective of the 800-5323 standard is to ensure that appropriate security requirements and security controls are applied to all U.S. federal government information and information management systems. The standard requires that risk be assessed and the determination made whether additional controls are needed to protect organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation.  
  
[SOC I / SOC II / SOC III](https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/ServiceOrganization%20%20'sManagement.aspx%20%20) The Statement on Auditing Standards 70 (SAS 70) was replaced by Service Organization Control (SOC) Type 1 and Type 2 reports in 2011 following changes and a more comprehensive approach to auditing being demanded by customers and clients alike. For years, SAS 70 was seen as the de facto standard for data center customers to obtain independent assurance that their data center service provider had effective internal controls in place for managing the design, implementation, and execution of customer information.  
  
[PCI DSS](https://www.pcisecuritystandards.org/pci_security/%20%20) Visa, MasterCard, and American Express established PCI DSS24 as a security standard to which all organizations or merchants that accept, transmit, or store cardholder data, regardless of size or number of transactions, must comply. PCI DSS was established following a number of significant credit card breaches. It is a comprehensive and intensive security standard that lists both technical and nontechnical requirements based on the number of credit card transactions for the applicable entities.

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

The correct answer is: D SOC II  
  
All of the other answers are legitimate SOC Reports, but only the SOC II report addresses what is known as the "Trust Services Principles", which include Security, Availability, Processing integrity, Confidentiality, and Privacy.  
  
SOC 2 reporting was specifically designed for IT-managed service providers and cloud computing. The report specifically addresses any number of the five so-called Trust Services principles, which follow:  
  
Security: The system is protected against unauthorized access, both physical and logical.  
  
Availability: The system is available for operation and use as committed or agreed.  
  
Processing Integrity: System processing is complete, accurate, timely, and authorized.  
  
Confidentiality: Information designated as confidential is protected as committed or agreed.  
  
Privacy: Personal information is collected, used, retained, disclosed, and disposed of in conformity with the provides privacy policy.  
  
As a general guideline:  
  
SOC I: Those interested in financial statements.  
SOC II: Information technology personnel will be interested.  
SOC III: Used to illustrate conformity, compliance, and security efforts to current or potential subscribers and customers of cloud services.  
  
  
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.

The correct answer is: C Security is negotiated as part of the Service Level Agreement.  
  
When working with an external service, be sure to review any SLA (service-level agreements) to ensure security is a prescribed component of the contracted services. This could include customization of service-level requirements for your specific needs.  
  
Service levels, security, governance, compliance, and liability expectations of the service and provider are contractually stipulated, managed to, and enforced, when a service level agreement (SLA s), is offered to the consumer.  
  
There are two types of SLA s, negotiable and non negotiable.  
  
In the absence of an SLA, the consumer administers all aspects of the cloud under its control.  
  
When a non negotiable SLA is offered, the provider administers those portions stipulated in the agreement.  
  
In the case of PaaS or IaaS, it is usually the responsibility of the consumer 's system administrators to effectively manage the residual services specified in the SLA, with some offset expected by the provider for securing the underlying platform and infrastructure components to ensure basic service availability and security.  
  
[NIST Draft Publication SP 800-146 says](http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf%20%20%20%20):  
A subscriber s terms of service for a cloud are determined by a legally binding agreement between the two parties often contained in two parts: (1) a service agreement, and (2) a Service Level Agreement (SLA). Generally, the service agreement is a legal document specifying the rules of the legal contract between a subscriber and provider, and the SLA is a shorter document stating the technical performance promises made by a provider including remedies for performance failures. For simplicity, this NIST publication and most publications refers to the combination of these two documents as an SLA.  
  
The self-service aspect of clouds implies that a subscriber either (1) accepts a provider s pricing and SLA, or (2) finds a provider with more acceptable terms, potential subscribers anticipating heavy use of cloud resources may be able to negotiate more favorable terms. For the typical subscriber, however, a cloud s pricing policy and SLA are nonnegotiable.  
  
Published SLAs between subscribers and providers can typically be terminated at any time by either party, either for cause such as a subscriber s violation of a cloud s acceptable use policies, or for failure of a subscriber to pay in a timely manner.  
  
Further, an agreement can be terminated for no reason at all. Subscribers should analyze provider termination and data retention policies.  
  
Provider promises, including explicit statements regarding limitations, are codified in their SLAs. A provider s SLA has three basic parts:  
(1) a collection of promises made to subscribers,  
(2) a collection of promises explicitly not made to subscribers, i.e., limitations, and  
(3) a set of obligations that subscribers must accept.  
  
Negotiated SLA  
If the terms of the default SLA do not address all subscriber needs, the subscriber should discuss modifications of the SLA with the provider prior to use.  
  
TIP: It should be clear in all cases that one can assign/transfer responsibility but not necessarily accountability.  
  
  
Question 16

Which of the following is NOT a characteristic of IaaS?

1. Resilience
2. Flexibility
3. Capacity Pools
4. Scale

The correct answer is: B Flexibility  
  
Flexibility is a characteristic of PaaS.  
  
IaaS is the area where the traditional data center hardware resides. IaaS is characterized by:

* Converged Networks and IT Capacity Pools,
* The ability to Scale,
* Self-service, and
* On-demand capacity, and High availability and resilience.

PaaS, on the other hand, is where developers achieve flexibility through the ability to use plugins and environments to quickly meet customer needs.  
  
Another closely related term is elasticity which is where a user s environment is managed based on resource utilization.

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

The correct answer is: ITIL  
  
ITIL is the Information Technology Infrastructure Library. An easy way to remember the characteristics of ITIL is that the L stands for Library, and a Library is where documents reside.

ITIL, an acronym for Information Technology Infrastructure Library, is a set of practices for [IT Service Management](https://en.wikipedia.org/wiki/IT_Service_Management%20) (ITSM) that focuses on aligning IT services with the needs of business. In its current form (known as ITIL 2011 edition), ITIL is published as a series of five core volumes, each of which covers a different ITSM lifecycle stage. Although ITIL underpins [ISO/IEC 20000](https://en.wikipedia.org/wiki/ISO/IEC_20000%20) (previously BS15000), the International Service Management Standard for IT service management, there are some differences between the ISO 20000 standard and the ITIL framework.

ITIL describes processes, procedures, tasks, and checklists which are not organization-specific, but can be applied by an organization for establishing integration with the organization's strategy, delivering value, and maintaining a minimum level of competency. It allows the organization to establish a baseline from which it can plan, implement, and measure. It is used to demonstrate compliance and to measure improvement.

The following answers are incorrect: All of the other answers are incorrect.  
  
TOGAF is the de facto global standard for Enterprise Architecture. [The Open Group Architecture Forum](http://www.opengroup.org/getinvolved/forums/architecture%20), comprised of more than 200 enterprises, develops and maintains the TOGAF standard and publishes successive versions at regular intervals. See [Downloading TOGAF 9.](http://www.opengroup.org/togaf/downloads%20)

The TOGAF framework enables organizations to effectively address critical business needs by:

* Ensuring that everyone speaks the same language
* Avoiding lock-in to proprietary solutions by standardizing on open methods for Enterprise Architecture
* Saving time and money, and utilize resources more effectively
* Achieving demonstrable ROI

Jericho/Open Group now part of the Open Group Security Forum. The Jericho Forum Cloud Cube Model can be found at the URL in the reference section below. It is downloadable in PDF format.

SABSA is a proven methodology for developing business-driven, risk and opportunity focused Security Architectures at both enterprise and solutions level that traceably support business objectives. It is also widely used for Information Assurance Architectures, Risk Management Frameworks, and to align and seamlessly integrate security and risk management into IT Architecture methods and frameworks.

SABSA is comprised of a series of integrated frameworks, models, methods and processes, used independently or as an holistic integrated enterprise solution, including:

* Business Requirements Engineering Framework (known as Attributes Profiling)
* Risk and Opportunity Management Framework
* Policy Architecture Framework
* Security Services-Oriented Architecture Framework
* Governance Framework
* Security Domain Framework
* Through-life Security Service Management & Performance Management Framework

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
5. The correct answer is: Jericho/Open Group  
     
   The Jericho/Open Group explores considerations of whether cloud computing is appropriate for all organizations. It developed a cube model that examines different cloud architecture, know as Cloud Formations.  
     
   The Jericho Forum s objectives related to cloud computing are distinctive: enabling secure collaboration in the appropriate cloud formations best suited to the business needs.  
     
   With this in mind, the aim of this paper is to:

* point out that not everything is best implemented in clouds; it may be best to operate some business functions using a traditional non-cloud approach
* explain the different cloud formationsthat the Jericho Forum has identified
* describe key characteristics, benefits and risks of each cloud formation
* provide a framework for exploring in more detail the natureof different cloud formations and the issues that need answering to make them safe and secure places to work in.

For more information about the Jericho Cube Model https://collaboration.opengroup.org/jericho/cloud\_cube\_model\_v1.0.pdf

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

The correct answer is: A Auditability  
  
Similar to standard audit trails and systems logging, systems auditing and reporting are offered as a standard feature by many of the cloud providers. Auditability within the cloud architecture fouses on actions and activities of users and systems.  
  
The following answers are incorrect:   
  
SLA Service Level Agreements (SLAs) in the Cloud. There have been many articles written on the topic, but still there is confusion about the importance of SLAs. Most people require a blueprint for architects and contractors to start building a new home and similarly would expect a new car to come with a warranty. An SLA serves as both the blueprint and warranty for cloud computing.

Regulatory Compliance is an organization's adherence to laws, regulations, guidelines and specifications relevant to its business. Violations of regulatory [compliance](http://searchdatamanagement.techtarget.com/definition/compliance%20%20%20%20%20) regulations often result in legal punishment, including federal fines.

Examples of regulatory compliance laws and regulations include the [Dodd-Frank Act](http://searchfinancialsecurity.techtarget.com/definition/Dodd-Frank-Act%20%20%20%20%20%20), Payment Card Industry Data Security Standard ([PCI DSS](http://searchfinancialsecurity.techtarget.com/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard%20%20%20%20%20%20)) , Health Insurance Portability and Accountability Act ([HIPAA](http://searchdatamanagement.techtarget.com/definition/HIPAA%20%20%20%20%20%20)), the Federal Information Security Management Act ([FISMA](http://searchsecurity.techtarget.com/definition/Federal-Information-Security-Management-Act%20%20%20%20%20%20)) and the Sarbanes-Oxley Act ([SOX](http://searchcio.techtarget.com/definition/Sarbanes-Oxley-Act%20%20%20%20%20%20)).

As the number of rules has increased since the turn of the century, regulatory compliance has become more prominent in a variety of organizations. The trend has even led to the creation of corporate, chief and regulatory compliance officer positions to hire employees whose sole focus is to make sure the organization conforms to stringent, complex legal mandates.

Portability Consumers of cloud services may seek cloud portability so that they can migrate services to a new provider in response to a price increase or a breached service-level agreement. Other customers may seek cloud portability capabilities to fulfill a business need, such as moving cloud-based resources to another provider that is geographically closer to the consumers of the cloud service.

Cloud portability requires interoperability among cloud providers, which means that one cloud provider must be able to replicate the application environment that the previous cloud provider had established for the service.

The [IEEE](http://whatis.techtarget.com/definition/IEEE-Institute-of-Electrical-and-Electronics-Engineers%20%20%20%20%20%20) has formed a working group to develop a set of interoperability standards -- the IEEE P2301 Draft Guide for Cloud Portability and Interoperability Profiles. Several vendors and providers have formed the open source [OpenStack](http://whatis.techtarget.com/definition/OpenStack%20%20%20%20%20%20) initiative, which is developing a cloud operating system that would provide some of the interoperability required for cloud portability. Individual vendors have also formed partnerships to create technology for cloud 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.

The correct answer is: D Funding and technology decisions for movement to the cloud should be made with the business direction at the core.  
  
This question is a trap for many overly technical thinkers.  
  
It should always be understood that business direction must lead any decisions about the type of technology to use.  
  
Another point to keep in mind is that the non-vendor specific exams, such as the CCSP are always geared more towards management of the business over the technical aspects of the business.

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.

The correct answer is: A Privacy must be outlined in the Service Level Agreement with the cloud provider.  
  
Due to the disparate geographic locations of cloud data, privacy must be outlined and understood as part of the Service Level Agreement. It is neither built into any cloud computing model or part of the essential elements which comprise cloud computing. Security of the data is not related to privacy.

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.

The correct answer is: The requirement of an organization to adhere to relevant laws, guidelines and specifications relevant to its business.  
  
While all of the answers are related to how governance is achieved (through auditing and defined processes), regulatory compliance is directly associated with following laws and guidelines.  
  
Regulatory compliance is an organization's adherence to laws, regulations, guidelines and specifications relevant to its business. Violations of regulatory compliance regulations often result in legal punishment, including federal fines.

Examples of regulatory compliance laws and regulations include the [Dodd-Frank Act](http://searchfinancialsecurity.techtarget.com/definition/Dodd-Frank-Act%20), Payment Card Industry Data Security Standard ([PCI DSS](http://searchfinancialsecurity.techtarget.com/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard%20)) , Health Insurance Portability and Accountability Act ([HIPAA](http://searchdatamanagement.techtarget.com/definition/HIPAA%20)), the Federal Information Security Management Act ([FISMA](http://searchsecurity.techtarget.com/definition/Federal-Information-Security-Management-Act%20)) and the Sarbanes-Oxley Act ([SOX](http://searchcio.techtarget.com/definition/Sarbanes-Oxley-Act%20)).

As the number of rules has increased since the turn of the century, regulatory compliance has become more prominent in a variety of organizations. The trend has even led to the creation of corporate, chief and regulatory [compliance officer](http://searchcio.techtarget.com/definition/CCO%20) positions to hire employees whose sole focus is to make sure the organization conforms to stringent, complex legal mandates.

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.

The correct answer is: The classic definition of a network perimeter takes on different meanings under different guises and deployment models.  
  
This is a scenario based question in which all the answers are correct, however, only one serves as the best answer.  
  
In this case, Richie is tasked with speaking to the Board of Directors, and he is also in the delicate position of pointing out that one member of the board has an incorrect assumption about cloud environments.  
  
The best way to approach this is to introduce the general concept of the varied perimeters offered by the cloud.  
  
It should always be remembered that the non-vendor specific exams, such as the CCSP are always geared more towards management of the business over the technical aspects of the business, and the ability to speak to board members is an important facet of a business approach.  
  
There is no relevance to which type of corporation Richie is addressing. The definitions of cloud perimeter does not change based on the industry. Each industry will need to choose the best cloud deployment based on what is best for their particular business.  
  
Question 24

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

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

The correct answer is: C KMS  
  
KMS is the acronym for Key Management service. It is a vital component of a cryptographic solution, but it is not a protocol.  
  
This question is a negative question. Which means the answer that is NOT a protocol is the correct choices.  
  
All of the other choices presented are protocol used to protect data in transit.  
  
TLS Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).  
  
SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.   
  
IPSec or IP Security is an Internet Engineering Task Force (IETF) standard suite of protocols that provides data authentication, integrity, and confidentiality as data is transferred between communication points across IP networks. IPSec provides data security at the IP packet level. A packet is a data bundle that is organized for transmission across a network, and it includes a header and payload (the data in the packet). IPSec emerged as a viable network security standard because enterprises wanted to ensure that data could be securely transmitted over the Internet. IPSec protects against possible security exposures by protecting data while in transit.  
  
  
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

The correct answer is: A Cloud Architect  
  
Cloud Roles

Cloud computing has created new requirements for how applications are built, managed and supported by cloud infrastructure. Additionally, teams now have to take responsibility for ensuring proper billing and maintenance.

Cloud Administrator (and Cloud Operator)

This is a top-level role, with responsibility for overseeing the organization‚„¢s overall cloud implementation. A cloud administrator is typically tasked with setting up, monitoring and maintaining the cloud architecture, and along the way is bound to interact often with system, cloud storage and network administrators.  
  
The cloud operator is essentially a junior cloud administrator who oversees to day-to-day operations.

Cloud Application Architect

Cloud application architects shape software for deployment on specific clouds. They typically adapt or port applications for compatibility. Moreover, this role bridges the gap between end users and back-end systems. Architects need both the system administrator experience to tune operating systems and the rapport with end users to make sure that applications exhibit consistently high performance and usability throughout their life cycles.

Cloud Architect

Title notwithstanding, the cloud architect does a very different job from the cloud application architect. Essentially, cloud architects determine whether private clouds align with the goals of their respective organizations. To this end, these architects design the platform and evaluate technologies and vendors to find the right fit.

Cloud Data Architect

Another architect role, this one primarily deals with the management of cloud-stored data. Cloud data architects deal with the wide variety of storage types and associated service-level agreements, ensuring that storage is used appropriately and optimally.

Cloud Service Manager

Similar to cloud data architects, cloud service managers work with SLAs. They may design rules, policies and SLA pricing models, while also keeping SLAs current so that they align with organizational priorities.

Cloud Storage Administrator

Cloud storage administrators create SLAs for different users and map bandwidth, capacity and reliability of storage services to user groups. They monitor the integrity of SLAs and may work with other administrators in the organization.

Cloud Developer

Cloud developers create software for infrastructure, on clients such as the euca2ools suite or system components like Eucalyptus Cloud Controller. They may work with the cloud administrator during debugging.

Cloud User

Not a technical role per se, but a term denoting anyone who has accessed to compute resources such images and instances within a cloud environment. Cloud users may be granted system administrator privileges for the instances that they initiate.

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

The correct answer is: D Client Side Key Management  
This decentralized approach puts the customer in complete control of encryption/decryption keys.  
  
As shown in the graphic below from the Cloud Security Alliance Encryption Implementation Guidance, almost all processing and control is done on the customer side. The cloud provider does not hold keys, has minimal knowledge of users, cannot decrypt customer data, and facilitates the storage of encrypted data. The KMS is provided and run by the cloud provider,  
but the KMS resides on customer s premise and the keys are generated and held by the customer.  
  
This type of solution can be used by cloud storage and SaaS providers,

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

The correct answer is: Rapid Elasticity  
  
Rapid Elasticity is the equivalent of the scalability of traditional cloud computing.  
  
Seamless and quick Scale-out as well as scale-in are two characteristics of Rapid Elasticity.  
  
Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand.  
To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.  
  
The following are Essentials characteristics of the cloud. There are 4 in total with Elasticity mentioned above:  
  
On-Demand Self Service A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider. Broad network access.  
  
Measured Self-Service Cloud systems automatically control and optimize resource use by leveraging a metering 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.  
  
Broad Network Access Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).  
  
Resource pooling The provider s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of  
abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.  
  
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.

The correct answer is: B All of the other choices are considerations.  
  
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

The correct answer is: Provisioning and De-Provisioning  
  
This is a question that is designed to confuse you when answering any *other* questions about Identity and Access Management. Only one of the answers is a key component of IAM.  
  
Some test takers may flag this question because they may think that it correctly lists the 4 key components, and they may answer subsequent Identity and Access management questions based on these false choices.  
  
Some of those later questions may also include these incorrect choices.  
  
Be careful of misleading choices in these types of questions.

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

Answer is B

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)

The correct answer is: Lightweight Directory Access Protocol (LDAP)  
  
The Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.  
  
[Directory services](https://en.wikipedia.org/wiki/Directory_services%20) play an important role in developing intranet and Internet applications by allowing the sharing of information about users, systems, networks, services, and applications throughout the network.  
  
As examples, directory services may provide any organized set of records, often with a hierarchical structure, such as a corporate email directory. Similarly, a telephone directory is a list of subscribers with an address and a phone number.  
  
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

The correct answer is:  D Type II Hypervisor is OS-based  
  
The primary software component in virtualization is a hypervisor. The hypervisor manages the VMs, virtual data storage, and virtual network components. As an additional layer of software on the physical server, it represents an additional attack surface. If an attacker is able to compromise a physical host, the attacker can potentially access all of the virtual systems hosted on the physical server. Administrators often take extra care to ensure virtual hosts are hardened.  
  
There are only 2 Hypervisor types:

* Type I, which runs directly on the hardware with VM resources provided by the hypervisor, Type 1 hypervisors run directly on the system hardware. They are often referred to as a "native " or "bare metal " or "embedded " hypervisors in vendor literature. Type I hypervisor are known to be more secure. and
* Type II, which runs on a host operating system. Type 2 hypervisors run on a host operating system. When the virtualization movement first began to take off, Type 2 hypervisors were [most popular](http://searchvmware.techtarget.com/answer/How-does-a-Type-2-hypervisor-compare-to-a-Type-1-hypervisor%20%20%20%20%20%20). Administrators could buy the software and install it on a server they already had.

In Summary, Type I = Hardware, Type II = Operating System  
  
TIP:  
This question intentionally offers a misleading answer by mentioning a hypervisor type that does not exist (Type III). Beware of these misleading choices that could subsequently cause you to incorrectly answer other related questions on the exam later on.  
  
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.

The correct answer is: B The limited access and strong control over the OS greatly increases the reliability and robustness of Type I hypervisors.  
  
The operating-system based hypervisor is a Type II hypervisor, which is more vulnerable due to the lack of standardization on the OS and other layers.  
  
A great web site you should visit is the [Search Virtualization web site](http://searchservervirtualization.techtarget.com/feature/Whats-the-difference-between-Type-1-and-Type-2-hypervisors%20%20%20). Here is what they say about this topic:  
  
In virtualization, the hypervisor (also called a virtual machine monitor) is the low-level program that allows multiple operating systems to run concurrently on a single host computer. Hypervisors use a thin layer of code in software or firmware to allocate resources in real-time. You can think of the [hypervisor](http://searchservervirtualization.techtarget.com/definition/hypervisor%20%20%20) as the traffic cop that controls I/O and memory management.

There are [two types of hypervisors](http://searchservervirtualization.techtarget.com/answer/Virtual-security-tactics-for-Type-1-and-Type-2-hypervisors%20%20%20): Type 1 and Type 2.

Type 1 hypervisors run directly on the system hardware. They are often referred to as a "native " or "bare metal " or "embedded " hypervisors in vendor literature.

Type 2 hypervisors run on a host operating system. When the virtualization movement first began to take off, Type 2 hypervisors were most popular. Administrators could buy the software and install it on a server they already had.

Type 1 hypervisors are gaining popularity because building the hypervisor into the firmware is proving to be more efficient. According to IBM, Type 1 hypervisors provide higher performance, availability, and security than Type 2 hypervisors. (IBM recommends that Type 2 hypervisors be used mainly on client systems where efficiency is less critical or on systems where support for a broad range of I/O devices is important and can be provided by the host operating system.)

Exam Tip:  
There is no such thing as a Type IV hypervisor. This question intentionally offers a misleading answer by mentioning a hypervisor type that does not exist (Type IV). Beware of these misleading choices that could subsequently cause you to incorrectly answer other related questions on the exam.  
  
  
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.

The correct answer is: A No, because shell access to the VM could result in configuration changes that could impact multiple tenants.  
  
PaaS tenants should not have shell access to the servers running their instances (even when virtualized).  
  
The rationale behind this is to limit the chance and likelihood of configuration or system changes affecting multiple tenants.  
  
Where possible, administration facilities should be restricted to siloed containers to reduce this risk. Careful consideration should be given before access is provided to the underlying infrastructure hosting a PaaS instance.  
  
In enterprises, this may have less to do with malicious behavior and more to do with efficient cost control; it takes time and effort to undo tenant-related fixes to their environment.

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

The correct answer is: This is false, because simply powering off a VM still leaves the image files susceptible to malware infections and missed patching.  
  
- A powered off VM is a file and like all files, it is susceptible to malware infections. Another problem with a powered off VM is that it may be turned on at a later time and may have missed a critical security patch, making it vulnerable to attacks that exploit the unpatched system.  
  
- VM sprawl is a concern when working in a virtual environment but it is irrelevant to the question that was asked. Sprawl occurs when you lose control of the amount of content on your image store.  
  
Cloud servers contain tens of VMs. These VMs may be active or offline and, regardless of state, are susceptible to attacks. Active VMs are vulnerable to all traditional attacks that can affect physical servers. Once a VM is compromised, VMs on the same physical server can attack each other because they share the same hardware and software resources, including memory, device drivers, storage, and hypervisor software.

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.

The correct answer is: 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.  
  
Hosts have a limited number of access points (NICs) available to all VMs. This represents a critical security vulnerability: compromising these access points opens the door to compromise the VMs, the hypervisor, or the virtual switch.  
  
The Cloud Security Alliance Common Controls Matrix (CCM) provides a good go-to guide for specific risks for SaaS, PaaS, and IaaS.  You can get a copy at the URL below:  
  
<https://cloudsecurityalliance.org/group/cloud-controls-matrix/>

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).

The correct answer is: B This is a bad design because it creates the threat of Insecure Direct Object References.  
  
Insecure Direct Object references occur when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key.  Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.  
  
In this case, an attacker could anticipate that the March earnings report will be posted with the name "Earnings\_2016\_3 ".  
  
A change to the URL (known as URL tampering) could reveal this report. If the report is posted before the official earnings statement is released to the public, an attacker can gain valuable market information.  
  
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

The correct answer is: Access  
  
Access is the only action that maps to all of the areas of the Data security LifeCycle model.  
  
The six areas of the Secure Data Lifecycle seen below are: Create, Store, Use, Share, Archive and Destroy.  
  
The functions that can be imposed on the data are: Access, Process, Store.  
  
The lifecycle includes six phases from creation to destruction. Although it is shown as a linear progression, once created, data can bounce between phases without restriction, and may not pass through all stages (for example, not all data is eventually destroyed  
  
1.Create. Creation is the generation of new digital content, or the alteration/updating/modifying 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, not including modification.  
  
4. Share. Information is made accessible to others, such as between users, to customers, and to 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).

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

The correct answer is:  D CC is an international evaluation framework.  
  
The CC is updated periodically. Distinctly, the CC has two key components:  
  
Protection profiles: Define a standard set of security requirements for a specific type of product, such as a firewall, IDS, or unified threat management (UTM).  
  
The evaluation assurance levels (EALs): Define how thoroughly the product is tested. EALs are rated using a sliding scale from 1‚€œ 7, with 1 being the lowest-level evaluation and 7 being the highest.  
  
The higher the level of evaluation, the more quality assurance (QA) tests the product would have undergone.  
  
NOTE:  Undergoing more tests does not necessarily mean the product is more secure.  
  
The seven EALs are as follows:   
  
EAL1: Functionally tested  
EAL2: Structurally tested  
EAL3: Methodically tested and checked  
EAL4: Methodically designed, tested, and reviewed  
EAL5: Semiformally designed and tested  
EAL6: Semiformally verified design and tested  
EAL7: Formally verified design and tested

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

The correct answer is: A Appreciation of IT technologies.  
  
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

The correct answer is: B Consistently practiced due diligence and due care  
  
Due diligence is the act of investigating and understanding the risks a company faces.  
  
Due care is the development and implementation of policies and procedures to aid in protecting the company, its assets, and its people from those threats.  
  
Had the U of ABC practiced due care and due diligence, it would have had a current BIA, RA, business continuity plan, etc.;  
  
They would have understood and documented the University's and CSP s responsibilities prior to signing SLAs, contracts, etc., and would have better understood cloud services, performance, resiliency, options, etc.  
  
Furthermore, practicing due diligence and due care would have helped to address and lessen the ill effects of its inadequate board and employee turnover issues.

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.

The correct answer is:  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.  
  
According to ‚“The NIST Definition of Cloud Computing,‚ in SaaS, ‚“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 networks, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.‚

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

The correct answer is: D SaaS

Software as a Service (SaaS). The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure2. 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 userspecific application configuration settings.

The following answers are incorrect:

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).

IaaS

Private Cloud

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).

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

IaaS

Private Cloud

PaaS

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).

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.3 The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting

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

The correct answer is: C SaaS  
  
Understanding the relationships and dependencies between cloud computing models is critical to understanding cloud computing security risks.  
  
IaaS is the foundation of all cloud services, with PaaS building upon IaaS, and SaaS in turn building upon PaaS as described in the Cloud Reference Model diagram. In this way, just as capabilities are inherited, so are information security issues and risk. It is important to note that commercial cloud providers may not neatly fit into the layered service models. Nevertheless, the reference model is important for relating real world services to an architectural framework and understanding that the resources and services require security analysis.  
  
It should therefore be clear that there are significant trade offs to each model in terms of integrated features, complexity versus openness (extensibility), and security. Generally, SaaS provides the most integrated functionality built directly into the offering, with the least consumer extensibility, and a relatively high level of integrated security (at least the provider bears a responsibility for security).  
  
SaaS in turn is built upon the underlying IaaS and PaaS stacks and provides a self contained operating environment that is used to deliver the entire user experience, including the content, its presentation, the application(s), and management capabilities.  
  
TIP:  
The key takeaway for security architecture is that the lower down the stack the cloud service provider stops, the more security capabilities and management consumers are responsible for implementing and managing themselves.  
  
IaaS IaaS includes the entire infrastructure resource stack from the facilities to the hardware platforms that reside in them. It incorporates the  
capability to abstract resources (or not), as well as deliver physical and logical connectivity to those resources. Ultimately, IaaS provides a set of  
API s, which allows management and other forms of interaction with the infrastructure by consumers.  
  
PaaS PaaS sits on top of IaaS and adds an additional layer of integration with application development frameworks, middleware capabilities, and functions such as database, messaging, and queuing. These services allow developers to build applications on the platform with programming languages and tools that are supported by the stack.

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)

The correct answer is: A Software as a Service (SaaS)

Software as a Service (SaaS). The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure2. 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.

 The following answers are incorrect:

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).

Infrastructure as a Service (IaaS)

PaaS

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).

Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.3 The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Infrastructure as a Service (IaaS)

PaaS

Security as a Service (SecaaS)

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).

Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.3 The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Cloud Computing represents one of the most significant shifts in information technology the industry has experienced. Reaching the point where computing functions as a utility has great potential, promising expansive innovations. One such innovation is the centralization of security resources. The security industry has recognized the benefits of a standardized security framework for both the providers and consumers. In the context of a cloud service level agreement between providers and consumers, a standardized security framework takes the form of a document that specifies which security services are provided how and where. With the maturation of security offerings based on standard frameworks, cloud consumers have recognized the need to centralize computing resources for providers and consumers. One of the milestones of the maturity of cloud as a platform for business operations is the adoption of Security as a Service (SecaaS) on a global scale and the recognition of how security can be enhanced. The worldwide implementation of security as an outsourced commodity will eventually minimize the disparate variances and security voids.

SecaaS is looking at Enterprise security from the cloud – this is what differentiates it from most of the other work / research on cloud security. Predominantly cloud security discussions have focused on how to migrate to the Cloud and how to ensure Confidentiality, Integrity, Availability and Location are maintained when using the Cloud. SecaaS looks from the other side to secure systems and data in the cloud as well as hybrid and traditional enterprise networks via cloud-based services. These systems may be in the cloud or more traditionally hosted within the customer’s premises. An example of this might be

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.

The correct answer is: A It may be internal or external to an organization.  
  
The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.  
  
The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.  
  
The private cloud deployment model includes cloud-based assets for a single organization. Organizations can create and host private clouds using their own resources. If so, the organization is responsible for all maintenance. However, an organization can also rent resources from a third party and split maintenance requirements based on the service model (SaaS, PaaS, or IaaS).

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

Answer D

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

The correct answer is: C Traffic Hijacking  
  
Hijacking is a form of Man In The Middle (MITM) attack. Even thou this is not a cloud-specific threat, it has been a constant thorn and challenge for security professionals to combat through the years.  
  
Account and Service traffic hijacking has long been targeted by attackers, using methods such as phishing, more recently smishing (SMS Phishing), spear-phishing (targeted phishing attacks), and exploitation of software and other applications vulnerabilities.  
  
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.

The correct answer is: The ability to move applications and related data between CSPs, or between public and private cloud environments.

Question 50

Which of the following is a not a SSO technology?

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

The correct answer is C

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

The correct answer is:

Cloud auditor

Cloud auditor - this is someone specifically responsible for conducting audits of cloud systems and cloud applications.  This is primarily done by an independent third party rather than by your CSP, but often paid by the customer to provide validation that the SLAs are being met

DISCUSSION:

The cloud computing roles based on ISO/IEC 11788 include:

1)  Cloud auditor - this is someone specifically responsible for conducting audits of cloud systems and cloud applications.  This is primarily done by an independent third party rather than by your CSP, but often paid by the customer to provide validation that the SLAs are being met

2)  Cloud service broker - A partner that serves as an intermediary between the cloud service customer and the cloud service provider.  An example would be someone that sells cloud space to be hosted on Amazon Web Services.

3)  Cloud service customer - the person that is utilizing services through the cloud service provider.

4)  Cloud service partner - holds a relationship with the cloud service provider OR the cloud service customer.  Their responsibility is to assist with the delivery of cloud services.

5)  Cloud service provider - offers cloud services to cloud customers - such as Amazon Web Services, Microsoft, or Google

6)  Cloud service user - someone who interacts with the services being offered by the cloud services customer.   For example, a subscriber to Netflix would be a cloud service user.

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.

The correct answer is: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.

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.

Source: https://www.techopedia.com/definition/29545/resource-pooling

The idea behind resource pooling is that through modern scalable systems involved in cloud computing and software as a service (SaaS), providers can create a sense of infinite or immediately available resources by controlling resource adjustments at a meta level. This allows customers to change their levels of service at will without being subject to any of the limitations of physical or virtual resources.  
  
The kinds of services that can apply to a resource pooling strategy include data storage services, processing services and bandwidth provided services. Other related terms include rapid elasticity, which also involves the dynamic provisioning of services, and on-demand self-service, where customers could change their levels of service without actually contacting a service provider. All of this automated service provisioning is a lot like other kinds of business process automation, which replaced more traditional, labor-intensive strategies with new innovations that rely on increasingly powerful virtual networks and data handling resources. In these cases, the goal is to separate the client experience from the actual administration of assets, so that the process of delivery is opaque and the services seem to be automatically and infinitely available.

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

The correct answer is:

Customer controls services deployed within the cloud, storage, deployed applications, and operating systems (including licensing)

For your exam, you must be familiar with the following Service Models:

Software as a Service (SaaS).

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.

Platform as a Service (PaaS).

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.

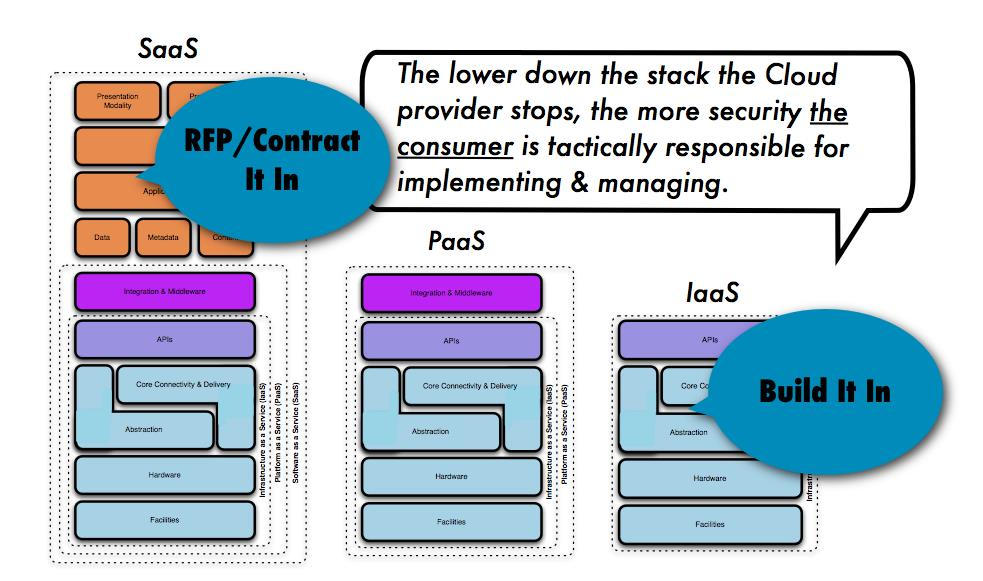
The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

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).

See graphic below from the Cloud Security Alliance (CSA) Security Guidance document:



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

The correct answer is:

No physical endpoints

Physical endpoints are traditionally used in defining managing and protecting IT assets. The absence of these physical endpoints strips away a layer of protection.

DISCUSSION:

NOTE:  ISC2 uses the term EndPoint as a synonym for Control.   If you read the question again and you replace EndPoint with Control then it makes more senses as an answer.

Loss of Physical Control Again, distributed ownership means not only a decrease in expenses but a decreased amount of control as well. Lack of physical control equates to a relative decrease in physical security.  
  
These new categories of security threats are a result of the new, complex, and dynamic nature of the cloud virtual infrastructure, see the list below:  
  
Multitenancy: By design, different users within a cloud share the same applications and the physical hardware to run their VMs. As a result, information leakage, as well as an increase in the attack surface and the risk of VM-to-VM or VM-to-hypervisor compromise, can occur.  
  
Loss of control: Users are typically not aware of the location of their data and services, whereas the CSPs host and run VMs without being aware of their contents.  
  
Network topology: Cloud architecture is dynamic due to the fact that existing workloads change over time because of the creation and removal of VMs. In addition, the abilities of VMs to migrate from one host to another leads to the rise of undefined network topologies.  
  
Logical network segmentation: Within IaaS, the requirement for isolation alongside the hypervisor remains a key and fundamental activity to reduce external sniffing, monitoring, and interception of communications and others within the relevant segments.  
  
No physical endpoints: Due to the server and network virtualization, the number of physical endpoints (such as switches, servers, and NICs) is reduced. These physical endpoints are traditionally used in defining, managing, and protecting IT assets.  
  
Single point of access (SPOA) or SPOF: Hosts have a limited number of access points (NICs) available to all VMs. This represents a critical security vulnerability: compromising these access points opens the door to compromise the VMs, the hypervisor, or the virtual switch.

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

The correct answer is:

Resource pooling provides economies of the scale, hence significant cost saving to the cloud customers

Significant cost savings can be realized for all customers of the cloud through resource pooling and the economies of scale that it affords.  
  
DISCUSSION:

Resource pooling is an IT term used in cloud computing environments to describe a situation in which providers serve multiple clients, customers or "tenants" with provisional and scalable services. These services can be adjusted to suit each client's needs without any changes being apparent to the client or end user.

One of the most important concepts in cloud computer is resource pooling or multi-tenancy. In a cloud environment, regardless of the type of cloud offering, you always will have a mix of applications and systems that coexist within the same set of physical and virtual resources. As cloud customers add to and expand their usage within the cloud, the new resources are dynamically allocated within the cloud, and the customer has no control over (and, really, no need to know) where the actual services are deployed. This aspect of cloud can apply to any type of service deployed within the environment, including processing, memory, network utilization, and devices, as well as storage.

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.

The correct answer is: The SaaS platform typically has the least amount of control and access to event and diagnostic data.  
  
As a CCSP, you have tools at your disposal that can help you filter the large number of events that take place continuously within the cloud infrastructure, allowing you to selectively focus on those that are most relevant and important.  
  
As with most questions that address control in the cloud, SaaS offers the LEAST amount of control. Development teams may be able to help with access to event and diagnostic information, but that would occur on a PaaS platform, not the SaaS platform.  
  
In SaaS environments, you typically have minimal control of, and access to, event and diagnostic data. Most infrastructure-level logs are not visible to the CCSP, and they will be limited to high-level, application-generated logs that are located on a client endpoint. In order to maintain reasonable investigation capabilities, auditability, and traceability of data, it is recommended to specify required data access requirements in the cloud SLA or contract with the CSP.

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.

The correct answer is: Yes, it makes sense to modify old rules to reduce false positives.  
  
SIEM is a term for software products and services combining security information management (SIM) and security event management (SEM). SIEM technology provides real-time analysis of security alerts generated by network hardware and applications. SIEM is sold as software, appliances, or managed services and is used to log security data and generate reports for compliance purposes. The acronyms SEM, SIM, and SIEM are sometimes used interchangeably.  
  
Adding new rules: Rules are built to allow detection of new events. Rules allow for the mapping of expected values to log files and detect events. In continuous operation mode, rules have to be updated to address new risks.  
  
Reduction of false positives: The quality of the continuous operations audit logging depends on the ability to gradually reduce the number of false positives to maintain operational efficiency. This requires constant improvement of the rule set in use.

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

The correct answer is: Crypto-Shredding  
  
Crypto-shredding may be the best option for many cloud deployments, since it relies less on complete access to all physical media, which may be difficult or impossible even in completely private/internal cloud deployments.  
  
The only reasonable method of properly destroying cloud data is encrypting the data.  
  
The process of encrypting the data to dispose of it is called digital shredding or crypto-shredding.  
  
Crypto-shredding is the process of deliberately destroying the encryption keys that were used to encrypt the data originally. The data is encrypted with the keys, so the data is rendered unreadable (at least until the encryption protocol used can be broken or is capable of being brute-forced by an attacker).  
  
To perform proper crypto-shredding, consider the following:

* The data should be encrypted completely without leaving clear text remaining.
* The technique must make sure that the encryption keys are completely unrecoverable.

This can be hard to accomplish if an external CSP or other third party manages the keys.

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

The correct answer is: Data Monitoring procedures.  
  
Data governance is the process of tracking all data access and movements to make sure that all security controls are being applied properly throughout the data lifecycle.  
  
Data stored in the cloud tends to be replicated and moved. To maintain data governance, it is required that all data access and movements be tracked and logged to make sure that all security controls are being applied properly throughout the data lifecycle.  
  
  
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

The correct answer is: Text and Multimedia content  
  
**Structured data**: Information with a high degree of organization, such that inclusion in a relational database is seamless and readily searchable by simple, straightforward search engine algorithms or other search operations.  
  
**Unstructured data**: Information that does not reside in a traditional row-column database. Unstructured data files often include text and multimedia content. Examples include email messages, word processing documents, videos, photos, audio files, presentations, web pages, and many other kinds of business documents. Although these sorts of files may have an internal structure, they are still considered unstructured because the data they contain does not fit neatly in a database.

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.

The correct answer is: The PLA provides guidelines for compensatory damages for non-compliance with data protection legislation.  
  
The other three choices listed are the three baseline guidelines for a Privacy Level Agreement. This choice is not.  
  
The CSA has defined baselines for compliance with data protection legislation and leading practices with the realization of a standard format named by the Privacy Level Agreement (PLA). By means of the PLA, the service provider declares the level of personal data protection and security that it sustains for the relevant data processing.  
  
The PLA, as defined by the CSA, does the following:

* Provides a clear and effective way to communicate the level of personal data protection offered by a service provider
* Works as a tool to assess the level of a service provider s compliance with data protection legislative requirements and leading practices
* 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.

The correct answer is: The goal of the PLA is to fulfill the Privacy and Data Protection laws applicable to the controller.  
  
Generally, the ultimate responsibility lies with the controller, and even in the case of a processor's actions, remember that the processor is acting on behalf of the controller.  
  
Because the application of data-protection measures has the ultimate goal of fulfilling the P& DP laws applicable to the controller, any constraints arising from specific arrangements of a cloud service operation shall be made clear by the service provider to avoid consequences for unlawful personal data processing. For example, with regard to servers located across several countries, it would be difficult to ensure the proper application of measures such as encryption for sensitive data on all systems.  
  
  
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.

The correct answer is: The best time to classify data is during the creation phase.  
  
The creation phase is the preferred time to classify content according to its sensitivity and value to the organization.  
  
The generation or acquisition of new digital content, or the altering or updating of existing content. This phase can happen internally in the cloud or externally.  Careful classification is important because poor security controls can be implemented if content is classified incorrectly.  
  
The 6 phases of the Cloud Data LifeCycle are:

The lifecycle includes six phases from creation to destruction. *Although we show it as a linear progression, once created, data can bounce between phases without restriction, and may not pass through all stages* (for example, not all data is eventually destroyed).

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).

These high-level activities describe the major phases of a datum‚„¢s life, and in a future post we will cover security controls for each phase. But before we discuss controls we need to incorporate two additional aspects: *locations* and *access devices*.

Question 9

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

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

The correct answer is: Storage  
  
The act of committing the digital data to some sort of storage repository.  Typically occurs nearly simultaneously with creation.  
  
When storing the data, it should be protected in accordance with its classification level. Controls such as encryption, access policy, monitoring, logging, and backups should be implemented to avoid data threats. Content can be vulnerable to attackers if access control lists (ACLs) are not implemented well, files are not scanned for threats, or files are classified incorrectly.  
  
The 6 phases of the Cloud Data LifeCycle are:

The lifecycle includes six phases from creation to destruction. *Although we show it as a linear progression, once created, data can bounce between phases without restriction, and may not pass through all stages* (for example, not all data is eventually destroyed).

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).

These high-level activities describe the major phases of a datum s life, and in a future post we will cover security controls for each phase. But before we discuss controls we need to incorporate two additional aspects: *locations* and *access devices*.

Please visit the Securosis web site at the URL listed below within the reference section for a lot more info about the Cloud Data Lifecycles.  
  
The following answers are incorrect:  
  
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.

The correct answer is: Not all data should be shared, and not all sharing should present a threat.  
  
Information being made accessible to others, such as between users, to customers, and to partners. Not all data should be shared, and not all sharing should present a threat. But because data that is shared is no longer at the organization control, maintaining security can be difficult. Technologies such as DLP can be used to detect unauthorized sharing, and IRM technologies can be used to maintain control over the information.  
  
The 6 phases of the Cloud Data LifeCycle are:

The lifecycle includes six phases from creation to destruction. *Although we show it as a linear progression, once created, data can bounce between phases without restriction, and may not pass through all stages* (for example, not all data is eventually destroyed).

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).

These high-level activities describe the major phases of a datum s life, and in a future post we will cover security controls for each phase. But before we discuss controls we need to incorporate two additional aspects: *locations* and *access devices*.

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

The correct answer is: Data in Use is most vulnerable.  
  
Data being viewed, processed, or otherwise used in some sort of activity, not including modification. Data in use is most vulnerable because it might be transported into unsecure locations such as workstations, and to be processed, it must be unencrypted. Controls such as data loss prevention (DLP), information rights management (IRM), and database and file access monitors should be implemented to audit data access and prevent unauthorized access.

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.

The correct answer is: PaaS utilizes Structured and Unstructured Data storage.  
  
PaaS utilizes the following data storage types:  
  
**Structured**: Information with a high degree of organization, such that inclusion in a relational database is seamless and readily searchable by simple, straightforward search engine algorithms or other search operations.  
  
**Unstructured**: Information that does not reside in a traditional row-column database. Unstructured data files often include text and multimedia content. Examples include email messages, word processing documents, videos, photos, audio files, presentations, web pages, and many other kinds of business documents. Although these sorts of files may have an internal structure, they are still considered unstructured because the data they contain does not fit neatly in a database.

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.

The correct answer is: This statement is false because the data can be downloaded to a portable device that could become lost or stolen.  
  
It is important to be aware of the relevant data security technologies you may need to deploy or work with to ensure the Availability, Integrity, and Availability (AIC) of data in the cloud. Potential controls and solutions can include the following:  
  
**DLP**: For auditing and preventing unauthorized data exfiltration  
  
**Encryption**: For preventing unauthorized data viewing Obfuscation, anonymization, tokenization, and  
  
**Masking**: Different alternatives for protecting data without encryption

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.

The correct answer is: 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.  
  
**Improper treatment or sanitization after end of use**: End of use is challenging in cloud computing because usually we cannot enforce physical destruction of media. But the dynamic nature of data, where data is kept in different storages with multiple tenants, mitigates the risk that digital remnants can be located.  
  
  
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

The correct answer is: Erasure coding is the technology that chunks a data object into the segments.  
  
To provide high availability for data, assurance, and performance, storage applications often use the data dispersion technique. Data dispersion is similar to a RAID solution, but it is implemented differently. Storage blocks are replicated to multiple physical locations across the cloud. In a private cloud, you can set up and configure data dispersion yourself.  
  
Users of a public cloud do not have the capability to set up and configure data dispersion, although their data may benefit from the CSP using data dispersion.  
  
The underlying architecture of this technology involves the use of erasure coding, which chunks a data object (think of a file with self-describing metadata) into segments. Each segment is encrypted, cut into slices, and dispersed across an organization‚„¢s network to reside on different hard drives and servers. If the organization loses access to one drive, the original data can still be put back together. If the data is generally static with few rewrites, such as media files and archive logs, creating and distributing the data is a one-time cost.  If the data is dynamic, the erasure codes have to be re-created and the resulting data blocks redistributed.

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.

The correct answer is: The majority of cloud-based DLP is focused at the Discovery and Classification level.  
  
DLP, also known as data leakage prevention or data loss protection, describes the controls put in place by an organization to ensure that certain types of data (structured and unstructured) remain under organizational controls, in line with policies, standards, and procedures.  
  
Controls to protect data form the foundation of organizational security and enable the organization to meet regulatory requirements and relevant legislation (that is, EU data-protection directives, U.S. privacy act, Health Insurance Portability and Accountability Act [HIPAA], and Payment Card Industry Data Security Standard [PCI DSS]). DLP technologies and processes play important roles when building those controls. The appropriate implementation and use of DLP reduces both security and regulatory risks for the organization.  
  
DLP consists of three components:  
  
**Discovery and classification**: This is the first stage of a DLP implementation and an ongoing and recurring process. The majority of cloud-based DLP technologies are predominantly focused on this component. The discovery process usually maps data in cloud storage services and databases and enables classification based on data categories (regulated data, credit card data, public data, and more).  
  
**Monitoring**: Data usage monitoring for both ingress- and egress-based traffic flows forms the key function of DLP. Effective DLP strategies monitor the usage of data across locations and platforms while enabling administrators to define one or more usage policies. The ability to monitor data can be executed on gateways, servers, and storage as well as workstations and endpoint devices. Recently, the adoption of external services to assist with DLP ‚“as a service‚ has increased, along with many cloud-based DLP solutions. The monitoring application should be able to cover most sharing options available for users (email applications, portable media, and Internet browsing) and alert them to policy violations.  
  
**Enforcement**: Many DLP tools provide the capability to interrogate data and compare its location, use, or transmission destination against a set of policies to prevent data loss. If a policy violation is detected, specified relevant enforcement actions can automatically be performed. Enforcement options can include the ability to alert and log, block data transfers or reroute them for additional validation, or encrypt the data prior to leaving the organizational boundaries.

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.

The correct answer is: In a "Data in Motion " topology, the DLP engine should be deployed near the organizational gateway to monitor outgoing protocols, such as HTTPS, SMTP, and FTP.  
  
**DLP Architecture**  
  
DLP tool implementations typically conform to the following topologies:  
  
**Data in motion (DIM)**: Sometimes referred to as network-based or gateway DLP. In this topology, the monitoring engine is deployed near the organizational gateway to monitor outgoing protocols such as hypertext transfer protocol (HTTP), hypertext transfer protocol secure (HTTPS), simple mail transfer protocol (SMTP), and file transfer protocol (FTP). The topology can be a mixture of proxy based, bridge, network tapping, or SMTP relays. To scan encrypted HTTPS traffic, appropriate mechanisms to enable SSL interception and broker are required to be integrated into the system architecture.  
  
**Data at rest (DAR)**: Sometimes referred to as storage-based data. In this topology, the DLP engine is installed where the data is at rest, usually one or more storage subsystems, as well as file and application servers. This topology is effective for data discovery and for tracking usage but may require integration with network- or endpoint-based DLP for policy enforcement.  
  
**Data in use (DIU)**: Sometimes referred to as client or endpoint based. The DLP application is installed on a user s workstations and endpoint devices. This topology offers insights into how users use the data, with the ability to add protection that the network DLP may not be able to provide. The challenge with client-based DLP is the complexity, time, and resources to implement across all endpoint devices, often across multiple locations and significant numbers of users.  
  
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.

The correct answer is: Separation of duties requires forced collusion to occur if unauthorized access is attempted.  
  
The idea of forced collusion is that it makes a crime easier to detact if there is more than one actor participating in the crime.  
  
**Key Management Considerations**   
  
Here are some considerations when planning key management:  
  
Random number generation should be conducted as a trusted process.  
  
Throughout the lifecycle, cryptographic keys should never be transmitted in the clear; they should always remain in a trusted environment.  
  
When considering key escrow or key management ‚“as a service,‚ carefully plan to take into account all relevant laws, regulations, and jurisdictional requirements.  
  
Lack of access to the encryption keys will result in lack of access to the data. This should be considered when discussing confidentiality threats versus availability threats.  
  
**Where possible, key management functions should be conducted separately from the CSP to enforce separation of duties and force collusion to occur if unauthorized data 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.

The correct answer is: Metadata  
  
Metadata is the most common method of data alanysis.  
  
Data discovery tools differ by technique and data matching abilities. Assume you wanted to find credit card numbers. Data discovery tools for databases use a couple of methods to find and then identify information. Most use special login credentials to scan internal database structures, itemize tables and columns, and then analyze what was found.  
  
Three basic analysis methods are employed: Metadata, Labels, and Content analysis.  
  
**Metadata**: This is data that describes data. All relational databases store metadata that describes tables and column attributes. In the credit card example, you would examine column attributes to determine whether the name of the column or the size and data type resembles a credit card number. If the column is a 16-digit number or the name is something like CreditCard or CC#, then there‚„¢s a high likelihood of a match. Of course, the effectiveness of each product will vary depending on how well the analysis rules are implemented. This remains the most common analysis technique.  
  
**Labels**: This is marked by data elements being grouped with a tag that describes the data. This can be done at the time the data is created, or tags can be added over time to provide additional information and references to describe the data. In many ways, it is just like metadata but slightly less formal. Some relational database platforms provide mechanisms to create data labels, but this method is more commonly used with flat files, becoming increasingly useful as more firms move to Indexed Sequential Access Method (ISAM) or quasi-relational data storage, such as Amazon‚„¢s simpleDB, to handle fast-growing data sets. This form of discovery is similar to a Google search, with the greater the number of similar  labels, the greater likelihood of a match. Effectiveness is dependent on the use of labels. ISAM is a file management system developed at IBM that allows records to be accessed either sequentially (in the order they were entered) or randomly (with an index). Each index defines a different ordering of the records.  
  
**Content analysis**: In this form of analysis, the data itself is analyzed by employing pattern matching, hashing, statistical, lexical, or other forms of probability analysis. In the case of the credit card example, when you find a number that resembles a credit card number, a common method is to perform a Luhn check on the number itself. This is a simple numeric checksum used by credit card companies to verify if a number is valid. If the number you discover passes the Luhn check, the probability is high that you have discovered a credit card number. The Luhn formula, which is also known as the modulus 10, or mod 10 algorithm, generates and validates the accuracy of credit card numbers. Content analysis is a growing trend and one that‚„¢s being used successfully in DLP and web content analysis products.  
  
Question 20

Which of the following Data Discovery techniques uses pattern matching?

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

The correct answer is: Content analysis  
  
In this form of analysis, the data itself is analyzed by employing pattern matching, hashing, statistical, lexical, or other forms of probability analysis. In the case of the credit card example, when you find a number that resembles a credit card number, a common method is to perform a Luhn check on the number itself. This is a simple numeric checksum used by credit card companies to verify if a number is valid. If the number you discover passes the Luhn check, the probability is high that you have discovered a credit card number. The Luhn formula, which is also known as the modulus 10, or mod 10 algorithm, generates and validates the accuracy of credit card numbers. Content analysis is a growing trend and one that‚„¢s being used successfully in DLP and web content analysis products.

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.

The correct answer is: The controller is defined as the natural or legal person, public authority, agency, or any othr body that alone or jointly with others determines the puirposes and means of the processing of personal data.  
  
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. Where the purposes and means of processing are determined by national or community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or community law.  
  
The following are common privacy terms and their basic meanings:  
  
Data subject: A subject who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity (such as telephone number or IP address).  
  
Personal data: Any information relating to an identified or identifiable natural person. There are many types of personal data, such as sensitive and health data and biometric data. According to the type of personal data, the P& DP laws usually set out specific privacy and data-protection obligations (such as security measures and data subject‚„¢s consent for the processing).  
  
Processing: Operations that are performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction. Processing is undertaken for specific purposes and scopes; as a result, the P& DP laws usually set out specific privacy and data-protection obligations, such as security measures and data subject‚„¢s consent for the processing.  
  
Controller: 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. Where the purposes and means of processing are determined by national or community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or community law.  
  
Processor: A natural or legal person, public authority, agency, or any other body that processes personal data on behalf of the controller.

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 establishment mainly 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.

The correct answer is: All liabilities are assigned to the controller role, and its country of establishment mainly determines the applicable Privacy and Data Protection law and jurisdiction.  
  
The customer determines the ultimate purpose of the processing and decides on the outsourcing or the delegation of all or part of the concerned activities to external organizations. Therefore, the customer acts as a controller. In this role, the customer is responsible and subject to all the legal duties that are addressed in the P& DP laws applicable to the controller‚„¢s role. The customer may task the service provider with choosing the methods and the technical or organizational measures to be used to achieve the purposes of the controller. When the service provider supplies the means and the platform, acting on behalf of the customer, it is considered to be a data processor.  
  
In a cloud services environment, it is not always easy to properly identify and assign the roles of controller and processor between the customer and the service provider. However, this is a central factor of P& DP because all liabilities are assigned to the controller role, and its country of establishment mainly determines the applicable P& DP law and jurisdiction.  
  
The following are common privacy terms and their basic meanings:  
  
**Data subject**: A subject who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity (such as telephone number or IP address).  
  
**Personal data**: Any information relating to an identified or identifiable natural person. There are many types of personal data, such as sensitive and health data and biometric data. According to the type of personal data, the P& DP laws usually set out specific privacy and data-protection obligations (such as security measures and data subject s consent for the processing).  
  
**Processing**: Operations that are performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction. Processing is undertaken for specific purposes and scopes; as a result, the P& DP laws usually set out specific privacy and data-protection obligations, such as security measures and data subject s consent for the processing.  
  
**Controller**: 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. Where the purposes and means of processing are determined by national or community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or community law.  
  
**Processor**: A natural or legal person, public authority, agency, or any other body that processes personal data on behalf of the controller.

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.

The correct answer is: Governance, Risk & Compliance is an Enterprise Responsibility across all cloud service models.  
  
The responsibilities of each role are dependent on the type of cloud service, as depicted in the diagram below from the offical CCSP study book.  
  
SaaS: The customer determines and collects the data to be processed with a cloud service, whereas the service provider essentially makes the decisions of how to carry out the processing and implement specific security controls. It is not always possible to negotiate the terms of the service between the customer and the service provider.  
  
PaaS: The customer has higher possibility to determine the instruments of processing, although the terms of the services are not usually negotiable.  
  
IaaS: The customer has a high level of control for data, processing functionalities, tools, and related operational management, thus achieving a high level of responsibility in determining purposes and means of processing.

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

The correct answer is: At the Client.  
  
The majority of object storage services offer server-side storage-level encryption, as described previously. This kind of encryption offers limited effectiveness, with the recommendation for external mechanisms to encrypt the data prior to its arrival within the cloud environments.  
  
Potential external mechanisms include the following:  
  
File-level encryption: Examples include IRM and DRM solutions, both of which can be effective when used in conjunction with file hosting and sharing services that typically rely on object storage. The encryption engine is commonly implemented at the client side and preserves the format of the original file.  
  
Application-level encryption: The encryption engine resides in the application that is utilizing the object storage. It can be integrated into the application component or by a proxy that is responsible for encrypting the data before going to the cloud. The proxy can be implemented on the customer gateway or as a service residing at the external provider.  
  
There are various Encryption storage types and each one has a specific location where the encryption engine is commonly placed.

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

The correct answer is: Legislation, regulation, and standards requirements.  
  
A data-retention policy is an organization€™s established protocol for keeping information for operational or regulatory compliance needs. The objectives of a data-retention policy are to keep important information for future use or reference, to organize information so it can be searched and accessed at a later date, and to dispose of information that is no longer needed. The policy balances the legal, regulation, and business data archival requirements against data storage costs, complexity, and other data considerations.  
  
A data-retention policy for cloud services should contain the following components:

* Legislation, regulation, and standards requirements
* Data mapping
* Data Classification
* Data-retention procedure
* Monitoring and maintenance

The following answers are inc

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".

The correct answer is:

Because an IRM contains ACLs and is embedded into the original file, IRM is agnostic to the location of the data.

DISCUSSION:

Because an Information Rights Management (IRM) contains ACLs and is embedded into the original file, IRM is agnostic to the location of the data.

IRM requires that all users with data access have matching encryption keys.

This requirement means strong identity infrastructure is a must when implementing IRM, and the identity infrastructure should expand to customers, partners, and any other organizations with which data is shared.  
  
Take a few minutes of your time to read pages 134 to 136 of the Official CCSP Study Guide Second Edition to get more info on this topic.

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

The correct answer is: Corporate Governance  
  
Corporate governance is a broad area describing the relationship between the shareholders and other stakeholders in the organization versus the senior management of the corporation. These stakeholders need to see that their interests are taken care of and that the management has a structure and a process to ensure that they execute to the goals of the organization. This requires, among other things, transparency on costs and risks. In the end, risks relating to cloud computing should be judged in relation to the corporate goals. It makes sense to develop any IT governance processes in alignment with existing corporate governance processes.

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.

The correct answer is: 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.  
  
The features you get in an object storage system are typically minimal. You can store, retrieve, copy, and delete files, as well as control which users can undertake these actions. If you want to be able to search or to have a central repository of object metadata that other applications can draw on, you generally have to implement it yourself.  
  
Amazon S3 and other object storage systems provide Representational State Transfer (REST) APIs that allow programmers to work with the containers and objects. The key issue that the CCSP has to be aware of with object storage systems is that data consistency is achieved only eventually. Whenever you update a file, you may have to wait until the change is propagated to all the replicas before requests return the latest version.  
  
This makes object storage unsuitable for data that changes frequently. However, it provides a good solution for data that does not change much, such as backups, archives, video and audio files, and VM images.  
  
The following answers are incorrect:

* Object storage is unsuitable for frequently changing data.
* Object storage offers data consistency on an "eventual " basis due to wait time while a change is propagated to all of the replicas.
* Object storage is a flat organization of containers with unique identifiers, which makes them perfect for storing operating system images for use as virtual machines

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.

The correct answer is: You should suggest that the single fuel tank is a single point of failure and the design should include a redundant fuel tank.  
  
The general rule when designing a data center is to eliminate all single points of failure - this is achieved through redundancy.  
  
A large part of data center design revolves around the redundancy in the design. Anything that can break down should be replicated. No single point of failure should remain. This means backup power, multiple independent cooling units, multiple power lines to individual racks and servers, multiple power distribution units (PDUs), multiple entrances to the building, multiple external entry points for power and network, and so on.  
  
  
The following answers are incorrect:

* You should suggest a larger fuel tank to accommodate longer power failures.
* You should suggest a battery backup unit to prevent power failures.
* 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.

The correct answer is: 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.  
  
The creation and implementation of a fully tested BCDR plan that is ready for the failover event has a great structural resemblance to any other IT implementation plan as well as other disaster response plans. It is wise to consult or even adapt existing IT project planning and risk management methodologies.  
  
When organizations are incorporating IT systems and cloud solutions on an ongoing basis, creating and reevaluating BCDR plans should be a defined and documented process.  
  
  
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.

The correct answer is: Resource exhaustion  
  
All of the other answers are cloud risks, however, a Denial of Service (DoS) attack is most closey associated with a Resource Exhuastion event.  
  
Because cloud resources are shared by definition, resource exhaustion represents a risk to customers. This can play out as being denied access to resources already provisioned or as the inability to increase resource consumption.  Examples include sudden lack of CPU or network bandwidth, which can be the result of overprovisioning to tenants by the CSP.  
  
Related to resource exhaustion are the following:

* Denial-of-service (DoS) attacks, where a common network or other resource is saturated, leading to starvation of users
* Traffic analysis
* Manipulation or interception of data in transit

Cloud-specific risks include but are not limited to the following:

* Management Plane Breach
* Resource Exhaustion
* Isolation Control Failure
* Insecure or Incomplete data deletion
* Control conflict risk
* Software Related Risks

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.

The correct answer is: Law enforcement activity, such as the seizure of a physical hard drive, has the potential to expose data of multiple customers.  
  
This questions is about legal risks associated to cloud activity. As a result of law enforcement or civil legal activity, it may be required to hand over data to authorities. The essential cloud characteristic of shared resources may make this process hard to do and may result in exposure risks to other tenants. For example, seizure and examination of a physical disk may expose the data of multiple customers.  
  
These risks can be grouped broadly into data protection, jurisdiction, law enforcement, and licensing, such as:

* Data Protection
* Jurisdiction
* Law Enforcement
* Licensing

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.‚

The correct answer is: Infrastructure Security is a shared responsibility in an IaaS platform and Application Security is a shared responsibility in a SaaS platform.  
  
This is intentionally a particularly confusing set of answers to choose from. This is because the chart to which the question refers appears 3 times in the official CBK text. I cannot think of a more clear warning that a question dealing with this chart will be on the exam. It is worth taking the time to memorize this chart.  
  
An easy way to remember the shared responsibilities is that Infrastructure security is shared in an Infrastructure as a Service platform, Platform Security is shared in a Platform as as a service platform, and Applications are software, and shared responsibility occurs at the Software as a Service platform.

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.

The correct answer is: Testability should be considered during the design phase of the BCDR plan.  
  
Before proceeding, two definitions need to be presented to help ensure the appropriate understanding of what BCDR is in the mind of the CCSP. The business continuity plan (BCP) allows a business to plan what it needs to do to ensure that its key products and services continue to be delivered in case of a disaster, whereas the disaster recovery plan (DRP) allows a business to plan what needs to be done immediately after a disaster to recover from the event.  
  
The objective of the design phase is to establish and evaluate candidate architecture solutions. This design phase should not just result in technical alternatives but also flesh out procedures and workflow.  
  
Following are BCDR-specific questions that should be addressed in the design phase:

* How will the BCDR solution be invoked?
* What is the manual or automated procedure for invoking the failover services?
* How will the business use of the service be affected during the failover, if at all?
* How will the BCDR be tested?

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

The correct answer is: SAML token is issued by the user's SP  
  
Security Assertion Markup Language (SAML 2.0) is by far the most commonly accepted standard used in the industry today. According to Oasis, SAML 2.0 is an XML-based framework for communicating user authentication, entitlement, and attribute information. As its name suggests, SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application.

SAML tokens carry statements that are sets of claims made by one entity about another entity. For example, in federated security scenarios, the statements are made by a security token service about a user in the system. The security token service signs the SAML token to indicate the veracity of the statements contained in the token. In addition, the SAML token is associated with cryptographic key material that the user of the SAML token proves knowledge of. This proof satisfies the relying party that the SAML token was, in fact, issued to that user. For example, in a typical scenario:

1. A client requests a SAML token from a security token service, authenticating to that security token service by using Windows credentials.
2. The security token service issues a SAML token to the client. The SAML token is signed with a certificate associated with the security token service and contains a proof key encrypted for the target service.
3. The client also receives a copy of the *proof key*. The client then presents the SAML token to the application service (the *relying party*) and signs the message with that proof key.
4. The signature over the SAML token tells the relying party that the security token service issued the token. The message signature created with the proof key tells the relying party that the token was issued to the client.

SAML is an XML-based convention for the organization and exchange of communication authentication and authorization details between security domains, often over web protocols. SAML is often used to provide a web-based SSO (single sign-on) solution. If an attacker can falsify SAML communications or steal a visitor s access token, they may be able to bypass authentication and gain unauthorized access to a site.  
  
A bit of Jargon:

An Identity Provider (IdP), also known as Identity Assertion Provider, is responsible for:  
(a) providing identifiers for users looking to interact with a system,  
(b) asserting to such a system that such an identifier presented by a user is known to the provider, and  
(c) possibly providing other information about the user that is known to the provider.  
  
This may be achieved via an authentication module which verifies a [security token](https://en.wikipedia.org/wiki/Security_token%20%20%20%20%20) that can be accepted as an alternative to repeatedly explicitly authenticating a user within a security realm. An example of this could be where a website, application or service allows users to log in with the credentials from a social networking service like Facebook or Twitter; these services will act as Identity providers. The social networking service verifies that the user is an authorized user and returns information to the website - e.g. username and email address (specific details might vary). This authentication system is called Social login.

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

The correct answer is: Assertions, Protocol, and Binding  
  
In the public cloud world, identity providers are increasingly adopting OpenID and OAuth as standard protocols. In a corporate environment, corporate identity repositories can be used. Microsoft Active Directory is a dominant example. Relevant standard protocols in the corporate world are Security Assertion Markup Language (SAML) and WS-Federation.  
  
SAML consists of a number of components that, when used together, permit the exchange of identity, authentication, and authorization information between autonomous organizations.  
  
The first component is an assertion which defines the structure and content of the information being transferred. The structure is based on the [SAML v2 assertion schema](http://docs.oasis-open.org/security/saml/v2.0/saml-schema-assertion-2.0.xsd%20%20%20).  
  
How an assertion is requested by, or pushed to, a service provider is defined as a request/response protocol encoded in its own structural guidelines: the [SAML v2 protocol schema](http://docs.oasis-open.org/security/saml/v2.0/saml-schema-protocol-2.0.xsd%20%20%20).  
  
A binding defines the communication protocols (such as HTTP or SOAP) over which the SAML protocol can be transported.  
  
Together, these three components create a profile (such as Web Browser Artifact or Web Browser POST). In general, profiles satisfy a particular use case. The following image illustrates how the components are integrated for a SAML interaction.

[Graphic From: https://www.oasis-open.org/committees/download.php/20645/sstc-saml-tech-overview-2%200-draft-10.pdf](https://www.oasis-open.org/committees/download.php/20645/sstc-saml-tech-overview-2%200-draft-10.pdf%20%20%20)

Two other components that may be included in SAML messages are:

Metadata

Metadata defines how configuration information shared between two communicating entities is structured. For instance, an entity's support for specific SAML bindings, identifier information, and public key information is defined in the metadata. The structure of the metadata is based on the [SAML v2 metadata schema](http://docs.oasis-open.org/security/saml/v2.0/saml-schema-metadata-2.0.xsd%20%20%20). The location of the metadata is defined by Domain Name Server (DNS) records.

Authentication Context  
  
In some situations, one entity may want additional information to determine the authenticity of, and confidence in, the information being sent in an assertion. Authentication context permits the augmentation of assertions with information pertaining to the method of authentication used by the principal and how secure that method might be. For example, details of a multi-factor authentication can be included.

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.

A walk-through drill/simulation test is somewhat more involved than a tabletop exercise/structured walk-through test because the participants choose a specific event scenario and apply the BCP to it. However, this test also represents a preliminary step in the overall testing process that may be used for training employees, but it is not a preferred testing methodology. It includes:

* Attendance by all operational and support personnel who are responsible for implementing the BCP procedures;
* Practice and validation of specific functional response capabilities;
* Focus on the demonstration of knowledge and skills, as well as team interaction and decision-making capabilities;
* Role playing with simulated response at alternate locations/facilities to act out critical steps, recognize difficulties, and resolve problems in a non-threatening environment;
* Mobilization of all or some of the crisis management/response team to practice proper coordination without performing actual recovery processing; and
* Varying degrees of actual, as opposed to simulated, notification and resource mobilization to reinforce the content and logic of the plan.

The 4 test scenarios (from basic to advanced) are:

* Tabletop Exercise / Structured Walk-Through Test
* Walk-Through Drill / Simulation Test
* Functional Drill / Parallel Test
* Full-Interruption / Full-Scale Test

Each test introduces greater involvement across the organization.

Ensure you carefully review this section within your study book, see reference below.

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.

The correct answer is: Yes, this is a good idea. Virtualized snapshot images should be protected because they contain sensitive information.  
  
Virtualized snapshot images ARE portable and they contain all the data associated with a live image at a particular point in time. These images should be carefully guarded and definitely not available to anyone other than those who are responsible for the organization's cloud environment.  
  
Virtualization risks include but are not limited to the following:  
  
Guest breakout: This occurs when there is a breakout of a guest OS so that it can access the hypervisor or other guests. This is presumably facilitated by a hypervisor flaw.  
  
Snapshot and image security: The portability of images and snapshots makes people forget that images and snapshots can contain sensitive information and need protecting.  
  
Sprawl: This occurs when you lose control of the amount of content on your image store.

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.

The correct answer is:

In a federated identity model, authorization is typically with the relying party whereas authentication is a function of the identity provider.

In a federated identity model, authorization typically is with the relying party whereas authentication is a function of the identity provider.

DISCUSSION:

Entities that have an identity in cloud computing include users, devices, code, organizations, and agents.

As a principle, anything that needs to be trusted has an identity. The distinguishing characteristic of an identity in cloud computing is that it can be federated across multiple collaborating parties.

It implies a split between "Identity providers" and "relying parties" who rely on identities to be issued by the providers. This leads to a model whereby an identity provider can service multiple relying parties, and a relying party can federate multiple identity providers  
  
See the relationship between identity providers and relying parties in the diagram below from the Official CCSP study book, Second Edition, on page 178:

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.

The correct answer is: Puppet and Chef.  
  
[Puppet](https://puppet.com/) - According to Puppet Labs, Puppet is a configuration management system that allows you to define the state of your IT infrastructure and then automatically enforces the correct state.  Puppet provides a standard way of delivering and operating software, no matter where it runs. With the Puppet approach, you define what you want your apps and infrastructure to look like using a common easy-to-read language. From there you can share, test and enforce the changes you want to make across your datacenter. And at every step of the way, you have the visibility and reporting you need to make decisions and prove compliance.  
  
Chef - With Chef, you can automate how you build, deploy, and manage your infrastructure. The Chef server stores your recipes as well as other configuration data. The Chef client is installed on each server, virtual machine, container, or networking device you manage (called nodes). The client periodically polls the Chef server for the latest policy and the state of your network. If anything on the node is out of date, the client brings it up to date. The goal of these applications is to ensure that configurations are updated as needed and there is consistency in versioning.  Delivery reinforces DevOps best practices for delivering applications and infrastructure faster and more safely than ever. Use Chef Delivery to ship your changes when the business wants to, with fewer defects and less effort by combining automated testing with explicit review and approval gates.

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.

The correct answer is: A Cloud web application firewall (WAF).  
  
A cloud WAF can be extremely effective in the case of a DoS attack; in several cases, a cloud WAF was used to successfully thwart DoS attacks of 350 Gbps and 450 Gbps.  
  
Supplemental security devices include the following:  
  
Web application firewall (WAF)

* A WAF is a layer-7 firewall that can understand HTTP traffic.
  + A cloud WAF can be extremely effective in the case of a DoS attack; in several cases, a cloud WAF was used to successfully thwart DoS attacks of 350 Gbps and 450 Gbps.

Database activity monitoring (DAM)

* DAM is a layer-7 monitoring device that understands SQL commands. DAM can be agent-based (ADAM) or network-based (NDAM).
  + A DAM can detect and stop malicious commands from executing on an SQL server.

XML gateways

* XML gateways transform the way services and sensitive data are exposed as APIs to developers, mobile users, and cloud users.
  + XML gateways can be either hardware or software.
  + XML gateways can implement security controls such as data loss prevention (DLP), antivirus, and antimalware services.

The following answers are incorrect:   
  
A Database activity monitor (DAM) can detect and stop malicious commands from executing on an SQL server.  
  
XML gateways can implement security controls such as data loss prevention (DLP), antivirus, and antimalware services.  
  
An API gateway can implement access control, rate-limiting, logging, metrics, and security filtering. API rate-limiting is not used against a denial of service attack.

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.

The correct answer is: 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.  
  
Data loss: Any accidental deletion by the CSP, or worse, a physical catastrophe such as a fire or earthquake, can lead to the permanent loss of customers data unless the provider takes adequate measures to back it up. Furthermore, the burden of avoiding data loss does not fall solely on the provider's shoulders.  If a customer encrypts his data before uploading it to the cloud but loses the encryption key, the data is still lost.

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.

The correct answer is: The ANF is used in conjunction with the ONF and is created for a specific application.  
  
The application normative framework (ANF) is **used in conjunction with the ONF** and is created for a specific application. **The ANF maintains the applicable portions of the ONF that are needed to enable a specific application to achieve a required level of security** or the targeted level of trust. **The ONF to ANF is a one-to-many relationship**, where one ONF is used as the basis to create multiple ANFs.  
  
Security of applications must be viewed as a holistic approach in a broad context that includes not just software development considerations but also the business and regulatory context and other external factors that can affect the overall security posture of the applications being consumed by an organization.  
  
To this end, the International Organization for Standardization (ISO) has developed and published ISO/ IEC 27034-1, ‚“Information Technology‚€ Security Techniques‚€ Application Security.‚ ISO/ IEC 27034-1 defines concepts, frameworks, and processes to help organizations integrate security within their software development lifecycle.  
  
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.

The correct answer is: Threat modeling.  
  
The goal of threat modeling is to determine any weaknesses in the application and the potential ingress, egress, and actors involved before the weakness is introduced to production. It is the overall attack surface that is amplified by the cloud, and the threat model has to take that into account. Quite often, this involves a security professional determining various ways to attack the system or connections or even performing social engineering against staff with access to the system. The CCSP should always remember that the nature of threats faced by a system changes over time. Because of the dynamic nature of a changing threat landscape, constant vigilance and monitoring are important aspects of overall system security in the cloud.

ABOUT REPUDIATION and NON-REPUDIATION  
  
To repudiate means to deny. For many years, authorities have sought to make repudiation impossible in some situations. You might send registered mail, for example, so the recipient cannot deny that a letter was delivered. Similarly, a legal document typically requires witnesses to signing so that the person who signs cannot deny having done so.

On the Internet, a [digital signature](http://searchsecurity.techtarget.com/definition/digital-signature) is used not only to ensure that a message or document has been electronically signed by the person that purported to sign the document, but also, since a digital signature can only be created by one person, to ensure that a person cannot later deny that they furnished the signature.

Since no security technology is absolutely fool-proof, some experts warn that a digital signature alone may not always guarantee nonrepudiation. It is suggested that multiple approaches be used, such as capturing unique biometric information and other data about the sender or signer that collectively would be difficult to repudiate.

Email nonrepudiation involves methods such as email tracking that are designed to ensure that the sender cannot deny having sent a message and/or that the recipient cannot deny having received it.

The following answers are incorrect:   
  
STRIDE is a specific threat model consisting of six threat types, Spoofing, Tampering, Information disclosure, Repudiation, Denial of service, Elevation of privileges.  
Black box refers to software components (or a penetration test methodology).  
Repudiation  is the Illegitimate denial of an event.   Most of time we refer to Nonrepudiation when talking about computer security.  Beware of the use of repudiation which is the opposite of nonrepudiation just to trick you of course.   Nonrepudiation is the assurance that someone cannot deny something. Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.  
  
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.

The correct answer is: Data, Functions, Processes.  
  
Organizations and practitioners alike need to understand and appreciate that cloud-based development and applications can vary from traditional or on-premises development. When considering an application for cloud deployment, you must remember that applications can be broken down to the following subcomponents:

* Data
* Functions
* Processes

The components can be broken up so that the portions that have sensitive data can be processed or stored in specified locations to comply with enterprise policies, standards, and applicable laws and regulations.  
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.

The correct answer is: SOAP only supports the XML data format.  
  
In many cloud environments, access is acquired through the means of an API. These APIs consume tokens rather than traditional usernames and passwords. This topic is discussed in greater detail in the ‚“Identity and Access Management‚ section later in this domain.  
  
APIs can be broken into multiple formats, two of which follow:  
  
Representational State Transfer (REST): A software architecture style consisting of guidelines and best practices for creating scalable web services  
  
Simple object access protocol (SOAP): A protocol specification for exchanging structured information in the implementation of web services in computer networks2

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.

The correct answer is: Performance.  
  
The software development lifecycle methodology usually contains the following stages: analysis (requirements and design), construction, testing, release, and maintenance (response).  
  
After the code is developed, it is tested against the requirements to make sure that the product is actually solving the needs gathered during the requirements phase. During this phase, unit testing, integration testing, system testing, and acceptance testing are conducted.  
  
**Planning and requirements analysis**: Business and security requirements and standards are being determined. This phase is the main focus of the project managers and stakeholders. Meetings with managers, stakeholders, and users are held to determine requirements. The software development lifecycle calls for all business requirements (functional and nonfunctional) to be defined even before initial design begins. Planning for the quality-assurance requirements and identification of the risks associated with the project are also conducted in the planning stage. The requirements are then analyzed for their validity and the possibility of incorporating them into the system to be developed.  
  
**Defining**: The defining phase is meant to clearly define and document the product requirements to place them in front of the customers and get them approved. This is done through a requirement specification document, which consists of all the product requirements to be designed and developed during the project lifecycle.  
  
**Designing**: System design helps in specifying hardware and system requirements and helps in defining overall system architecture. The system design specifications serve as input for the next phase of the model. Threat modeling and secure design elements should be undertaken and discussed here.  
  
**Developing**: Upon receiving the system design documents, work is divided into modules or units and actual coding starts. This is typically the longest phase of the software development lifecycle. Activities include code review, unit testing, and static analysis.  
  
**Testing**: After the code is developed, it is tested against the requirements to make sure that the product is actually solving the needs gathered during the requirements phase. During this phase, unit testing, integration testing, system testing, and acceptance testing are conducted.  
  
Most software development lifecycle models include a maintenance phase as their endpoint. Operations and disposal are included in some models as a way of further Most software development lifecycle models include a maintenance phase as their endpoint. Operations and disposal are included in some models as a way of further.  
  
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.

The correct answer is: Injection.  
  
**Injection:** Includes injection flaws such as SQL, OS, LDAP, and other injections. These occur when untrusted data is sent to an interpreter as part of a command or query. If the interpreter is successfully tricked, it will execute the unintended commands or access data without proper authorization.  
  
  
The following answers are incorrect: All of the other answers are incorrect.  
  
**Cross-site scripting (XSS):** 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 websites, or redirect the user to malicious sites.  
  
**Insecure direct object references:** A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.  
  
**Cross-site request forgery (CSRF):** A CSRF attack forces a logged-on victim s browser to send a forged HTTP request, including the victim s session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim s browser to generate requests that the vulnerable application thinks are legitimate requests from the victim.  
  
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.

The correct answer is: Insecure direct object reference.  
  
**Insecure direct object references:** A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.  
  
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.

The correct answer is: The Static application security test and the Dynamic application security test play different roles - one is not better than the other.  
  
Static application security testing (SAST) is generally considered a white-box test, where the application test performs an analysis of the application source code, byte code, and binaries without executing the application code. SAST is used to determine coding errors and omissions that are indicative of security vulnerabilities. SAST is often used as a test method while the tool is under development (early in the development lifecycle).  
  
Dynamic application security testing (DAST) is generally considered a black-box test, where the tool must discover individual execution paths in the application being analyzed. Unlike SAST, which analyzes code offline (when the code is not running), DAST is used against applications in their running state. DAST is mainly considered effective when testing exposed HTTP and HTML interfaces of web applications.  
  
While it is true that a Dynamic application security test is used to test the HTTP and HTML interfaces of the web applications, and a Static application security test can be used to find XSS errors, SQL injection, buffer overflows, unhandled error conditions, and potential backdoors, they are both different and one should not be considered better than the other.  
  
A full pen test is not the correct answer, as it is an exploitative test that exceeds the scope of what the application team requires.

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

The correct answer is: Stored, Reflected and DOM-based  
  
The Open Web Application Security Project (OWASP) has provided the 10 most critical web application security threats that should serve as a minimum level for application security assessments and testing.

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user s browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.  
  
Cross-site scripting attacks occur when web applications contain some type of reflected input. For example, consider a simple web application that contains a single text box asking a user to enter their name. When the user clicks Submit, the web application loads a new page that says, Hello, name. Under normal circumstances, this web application functions as designed. However, a malicious individual could take advantage of this web application to trick an unsuspecting third party.  
  
As you may know, you can embed scripts in web pages by using the HTML tags < SCRIPT > and . Suppose that, instead of entering Mike in the Name field, you enter the following text: Mike < SCRIPT > alert(' hello')   
  
When the web application reflects this input in the form of a web page, your browser processes it as it would any other web page: It displays the text portions of the web page and executes the script portions. In this case, the script simply opens a pop-up window that says hello in it. However, you could be more malicious and include a more sophisticated script that asks the user to provide a password and transmits it to a malicious third party.  
  
Early on, two primary types of [XSS](https://www.owasp.org/index.php/XSS%20%20) were identified, Stored XSS and Reflected XSS. In 2005, Amit Klein defined a third type of XSS, which he coined DOM Based XSS. These 3 types of XSS are defined as follows:

[Stored XSS](https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29#Stored_XSS_Attacks%20%20) (AKA Persistent or Type I)

Stored XSS generally occurs when user input is stored on the target server, such as in a database, in a message forum, visitor log, comment field, etc. And then a victim is able to retrieve the stored data from the web application without that data being made safe to render in the browser. With the advent of HTML5, and other browser technologies, we can envision the attack payload being permanently stored in the victim s browser, such as an HTML5 database, and never being sent to the server at all.

[Reflected XSS](https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29#Reflected_XSS_Attacks%20%20) (AKA Non-Persistent or Type II)

Reflected XSS occurs when user input is immediately returned by a web application in an error message, search result, or any other response that includes some or all of the input provided by the user as part of the request, without that data being made safe to render in the browser, and without permanently storing the user provided data. In some cases, the user provided data may never even leave the browser (see DOM Based XSS next).

[DOM Based XSS](https://www.owasp.org/index.php/DOM_Based_XSS%20%20) (AKA Type-0)

As defined by Amit Klein, who published the first article about this issue[1], DOM Based XSS is a form of XSS where the entire tainted data flow from source to sink takes place in the browser, i.e., the source of the data is in the DOM, the sink is also in the DOM, and the data flow never leaves the browser. For example, the source (where malicious data is read) could be the URL of the page (e.g., document.location.href), or it could be an element of the HTML, and the sink is a sensitive method call that causes the execution of the malicious data (e.g., document.write). "

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

The correct answer is:

Security Assertion Markup Language (SAML) 2.0

Although many federation standards exist, the Security Assertion Markup Language (SAML) 2.0 is by far the most commonly accepted standard used in the industry today.

DISCUSSION:

The choices presented are all legitimate federated identity standards.

Although many federation standards exist, the Security Assertion Markup Language (SAML) 2.0 is by far the most commonly accepted standard used in the industry today.

According to Oasis, SAML 2.0 is an XML-based framework for communicating user authentication, entitlement and attribute information. As its name suggests, SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application.

In the public cloud world, identity providers are increasingly adopting OpenID and OAuth as standard protocols. In a corporate environment, corporate identity repositories can be used. Microsoft Active Directory is a dominant example. Relevant standard protocols in the corporate world are Security Assertion Markup Language (SAML) and WS-Federation.

See the following for more information: SAML:<http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html>

The following answers are incorrect:

OAuth 2.0

OAuth is widely used for authorization services in web and mobile applications. According to RFC 6749, “The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf.”

OAuth 2.0

WS-Federation Version 1.2

OAuth is widely used for authorization services in web and mobile applications. According to RFC 6749, “The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf.”

WS-Federation: According to the WS-Federation Version 1.2 OASIS standard, “this specification 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 are managed in other realms.”

OAuth 2.0

WS-Federation Version 1.2

OpenID Connect

OAuth is widely used for authorization services in web and mobile applications. According to RFC 6749, “The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf.”

WS-Federation: According to the WS-Federation Version 1.2 OASIS standard, “this specification 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 are managed in other realms.”

According to the OpenID Connect FAQ, this is an interoperable authentication protocol based on the OAuth 2.0 family of specifications. According to OpenID, “Connect lets developers authenticate their users across websites and apps without having to own and manage password files. For the app builder, it provides a secure verifiable answer to the question: ‘What is the identity of the person currently using the browser or native app that is connected to me?’”

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

The correct answer is:

Crypto-shredding

Crypto-shredding is effectively summed up as the deletion of the key used to encrypt data that's stored in the cloud.

The only reasonable method to properly destroying cloud data is encrypting the data. The process of encrypting the data to dispose of it is called digital shredding or crypto-shredding. Crypto-shredding is the process of deliberately destroying the encryption keys that were used to encrypt the data originally. The data is encrypted with the keys, so the data is rendered unreadable (at least until the encryption protocol used can be broken or is capable of being brute-forced by an attacker).  
  
To perform proper crypto-shredding, consider the following:

* The data should be encrypted completely without leaving clear text remaining.
* The technique must make sure that the encryption keys are completely unrecoverable.

This can be hard to accomplish if an external CSP or other third party manages the keys.

DISCUSSION:

Crypto-shredding is effectively summed up as the deletion of the key used to encrypt data that's stored in the cloud.  
  
For long-term archive storage, I would encrypt your data and then send it to a cloud data storage vendor. This way you hold and control the cryptographic keys. This segregation of encryption key management from the cloud provider hosting the data also creates a chain of separation, which helps protect both the cloud provider and you in the event of compliance issues. Crypto-shredding is also an effective technique for mitigating cloud computing risks. This is where the provider destroys all copies of the key ensuring that any data that's outside your physical control is rendered inaccessible. If you manage your own keys, crypto-shredding should be an important part of your strategy too.  
  
The ISC2 study book describes the process as:  
  
The only reasonable method to properly destroying cloud data is encrypting the data. The process of encrypting the data to dispose of it is called digital shredding or crypto-shredding. Crypto-shredding is the process of deliberately destroying the encryption keys that were used to encrypt the data originally. The data is encrypted with the keys, so the data is rendered unreadable (at least until the encryption protocol used can be broken or is capable of being brute-forced by an attacker).  
  
To perform proper crypto-shredding, consider the following:

* The data should be encrypted completely without leaving clear text remaining.

Question 15

At what stage does one identify the programming language and architecture to be used for development of an application?

1. Design Phase
2. Testing
3. Defining
4. Development Phase

The correct answer is:

Design Phase

This is the phase in which one decides what the interface would look like. This is also where one identifies the programming language such as (Python etc), and the architecture such as SOAP.

DISCUSSION:

The cloud-secure software development life cycle (SDLC) has the same foundational structure as the traditional SDLC, although there are some factors when dealing with the cloud that need to be taken into account. Just like data, software has a useful life cycle based on phases or stages of development and use.

Although the name and number of stages can be debated, they generally include at least the following core stages:

* Defining
* Designing
* Development
* Testing

In the design phase, we begin to develop user stories (what the user will want to accomplish and how to go about it), what the interface will look like, and whether it will require the use or development of any APIs.

This is also where we would identify what programming language (Python, Visual Basic, and so on) and architecture (REST, SOAP, and so on) we will use.

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

The correct answer is:

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a [client/server](http://searchnetworking.techtarget.com/definition/client-server) protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access

DISCUSSION:

Oauth

OAuth (Open Authorization) is an open standard for token-based authentication and authorization on the Internet. OAuth, which is pronounced "oh-auth," allows an end user's account information to be used by third-party services, such as Facebook, without exposing the user's password.

OpenID Connect

OpenID Connect is a simple identity layer on top of the OAuth 2.0 protocol, which allows computing clients to verify the identity of an end-user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end-user in an interoperable and REST-like manner.

WS-Federation

WS-Security, WS-Trust, and WS-SecurityPolicy provide a basic model for federation between Identity Providers and Relying Parties. These specifications define mechanisms for codifying claims (assertions) about a requestor as security tokens which can be used to protect and authorize web services requests in accordance with policy. WS-Federation extends this foundation by describing how the claim transformation model inherent in security token exchanges can enable richer trust relationships and advanced federation of services. This enables high-value scenarios where authorized access to resources managed in one realm can be provided to security principals whose identities and attributes are managed in other realms. WS-Federation includes mechanisms for brokering of identity, attribute discovery and retrieval, authentication and authorization claims between federation partners, and protecting the privacy of these claims across organizational boundaries. These mechanisms are defined as extensions to the Security Token Service (STS) model defined in WS-Trust. In addition, WS-Federation defines a mapping of these mechanisms, and the WS-Trust token issuance messages, onto HTTP such that WS-Federation can be leveraged within Web browser environments. The intention is to provide a common infrastructure for performing Federated Identity operations for both web services and browser-based applications. A common protocol provides economies with regard to development, testing, deployment and maintenance for vendors and customers alike.

SAML

Security Assertion Markup Language (SAML, pronounced *sam-el)* is an open standard for exchanging authentication and authorization data between parties, in particular, between an [identity provider](https://en.wikipedia.org/wiki/Identity_provider_(SAML)) and a [service provider](https://en.wikipedia.org/wiki/Service_provider_(SAML)). As its name implies, SAML is a XML-based markup language (for security assertions etc.) but SAML is also:

* A set of XML-based protocol messages
* A set of protocol message bindings
* A set of profiles (utilizing all of the above)

The single most important use case that SAML addresses is web browser single sign-on (SSO). Single sign-on is relatively easy to accomplish within a security domain (using [cookies](https://en.wikipedia.org/wiki/HTTP_cookie), for example) but extending SSO across security domains is more difficult and resulted in the proliferation of non-interoperable proprietary technologies. Hence the SAML Web Browser SSO profile[[](https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language#cite_note-SAMLProf20-2)was specified and standardized. (For comparison, the more recent [OpenID Connect](https://en.wikipedia.org/wiki/OpenID_Connect) protocol is an alternative approach to web browser SSO.)

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a [client/server](http://searchnetworking.techtarget.com/definition/client-server) protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it's easier to track usage for billing and for keeping network statistics. Created by Livingston (now owned by Lucent), RADIUS is a de facto industry standard used by a number of network product companies and is a proposed [IETF](http://searchsoa.techtarget.com/definition/IETF) standard.

Operations

Question 1

How is security best accomplished at the SaaS level?

Through collaboration.

Security must be provided by the cloud consumer.

Security is provided through traditional firewalls.

Security is negotiated as part of the Service Level Agreement.

The correct answer is: Security is negotiated as part of the Service Level Agreement.  
  
When working with an external service, be sure to review any SLA (service-level agreements) to ensure security is a prescribed component of the contracted services. This could include customization of service-level requirements for your specific needs.  
  
Service levels, security, governance, compliance, and liability expectations of the service and provider are contractually stipulated, managed to, and enforced, when a service level agreement (SLA s), is offered to the consumer.  
  
There are two types of SLA s, negotiable and non negotiable.  
  
In the absence of an SLA, the consumer administers all aspects of the cloud under its control.  
  
When a non negotiable SLA is offered, the provider administers those portions stipulated in the agreement.  
  
In the case of PaaS or IaaS, it is usually the responsibility of the consumer 's system administrators to effectively manage the residual services specified in the SLA, with some offset expected by the provider for securing the underlying platform and infrastructure components to ensure basic service availability and security.  
  
[NIST Draft Publication SP 800-146 says](http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf%20%20%20%20):  
A subscriber s terms of service for a cloud are determined by a legally binding agreement between the two parties often contained in two parts: (1) a service agreement, and (2) a Service Level Agreement (SLA). Generally, the service agreement is a legal document specifying the rules of the legal contract between a subscriber and provider, and the SLA is a shorter document stating the technical performance promises made by a provider including remedies for performance failures. For simplicity, this NIST publication and most publications refers to the combination of these two documents as an SLA.  
  
The self-service aspect of clouds implies that a subscriber either (1) accepts a provider s pricing and SLA, or (2) finds a provider with more acceptable terms, potential subscribers anticipating heavy use of cloud resources may be able to negotiate more favorable terms. For the typical subscriber, however, a cloud s pricing policy and SLA are nonnegotiable.  
  
Published SLAs between subscribers and providers can typically be terminated at any time by either party, either for cause such as a subscriber s violation of a cloud s acceptable use policies, or for failure of a subscriber to pay in a timely manner.  
  
Further, an agreement can be terminated for no reason at all. Subscribers should analyze provider termination and data retention policies.  
  
Provider promises, including explicit statements regarding limitations, are codified in their SLAs. A provider s SLA has three basic parts:  
(1) a collection of promises made to subscribers,  
(2) a collection of promises explicitly not made to subscribers, i.e., limitations, and  
(3) a set of obligations that subscribers must accept.  
  
**Negotiated SLA**  
If the terms of the default SLA do not address all subscriber needs, the subscriber should discuss modifications of the SLA with the provider prior to use.  
  
**TIP:** **It should be clear in all cases that one can assign/transfer responsibility but not necessarily accountability.**  
  
  
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:

Hosting racks of physical infrastructure with each server in a separate "coop" to form a clear demarcation from other tenant equpment.

Hosting racks of physical infrastructure with each virtual switch in a separate environment to protect against "cam bus wolf-packs".

Hosting of racks of physical infrastructure within long rectangles with isolated power strips, thereby reducing electrical anomalies.

Hosting of racks of physical infrastructure within long rectangles with a long side facing the prevailing wind, thereby allowing natural cooling.

The correct answer is: Hosting of racks of physical infrastructure within long rectangles with a long side facing the prevailing wind, thereby allowing natural cooling.  
  
One example of this trend can be seen in the design of the chicken coop data center, which is designed to host racks of physical infrastructure within long rectangles with a long side facing the prevailing wind, thereby allowing natural cooling. 1 Facebook, in its open compute design, places air intakes and outputs on the second floor of its data centers so that cool air can enter the building and drop on the machines, while hot air rises and is evacuated by large fans.  
  
 Yahoo has been using the chicken coop design to drive its data center architecture:  
[http:// www.datacenterknowledge.com/ archives/ 2010/ 04/ 26/ yahoo-computing-coop-the-shape-of-things-to-come/](http://www.datacenterknowledge.com/archives/2010/04/26/yahoo-computing-coop-the-shape-of-things-to-come/)   
  
  
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.

The correct answer is: 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.  
  
Essentially, the air conditioning system moves heat generated by equipment in the data center outside, allowing the data center to maintain a stable temperature range for the operating equipment.  
  
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.

The correct answer is: 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.  
  
The text specifically warns against oversubscription.  
  
**Oversubscription**   
  
Beware of oversubscription. It occurs when more users are connected to a system than can be fully supported at the same time. Networks and servers are almost always designed with some amount of oversubscription with the assumption that users do not all need the service simultaneously. If they do, delays are certain and outages are possible.  
  
Oversubscription is permissible on general-purpose LANs, but you should not use an oversubscribed configuration for iSCSI.  
  
Here s best practice:  
To have a dedicated local area network (LAN) for iSCSI traffic.  
Not to share the storage network with other network traffic such as management, fault tolerance, or vMotion/ Live Migration.  
  
  
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.

The correct answer is: There is a misperception that cloud computing removes data compliance responsibility; however, the data owner is still fully responsible for compliance.  
  
Compliance with government regulations, such as the Sarbanes-Oxley Act (SOX), the Gramm-Leach-Bliley Act (GLBA), and the Health Insurance Portability and Accountability Act (HIPAA), and industry standards such as the PCI DSS are much more challenging in the SaaS environment. There is a perception that cloud computing removes data compliance responsibility; however, the data owner is still fully responsible for compliance. Those who adopt cloud computing must remember that it is the responsibility of the data owner, not the service provider, to secure valuable data.  
The following answers are incorrect:   
All of the other answers are incorrect.

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.

The correct answer is: Broadcast packets sent by one of the workstations can reach all the others in the VLAN.  
In simple terms, a VLAN is a set of workstations within a LAN that can communicate with each other as though they were on a single, isolated LAN.  
The following answers are incorrect:  
All of the other answers are incorrect.

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".

The correct answer is: Another name for a DNSKEY is a "Trust Anchor ".  
  
DNSSEC11 is a suite of extensions that adds security to the domain name system (DNS) protocol by enabling DNS responses to be validated. Specifically, DNSSEC provides origin authority, data integrity, and authenticated denial of existence. With DNSSEC, the DNS protocol is much less susceptible to certain types of attacks - particularly DNS spoofing attacks.

In DNSSEC a secure response to a query is one which is cryptographically signed and validated. An individual signature is validated by following a chain of signatures to a key which is trusted for some extra-protocol reason.

ICANN, as IANA Functions Operator, is responsible for the publication of trust anchors for the root zone of the Domain Name System.  
  
A trust anchor is a [DNSKEY,](https://www.dnssec-tools.org/wiki/index.php?title=DNSKEY%20) usually a *Key Signing Keys* ([KSK](https://www.dnssec-tools.org/wiki/index.php?title=KSK%20)) that is placed into a validating resolver so that the validator can cryptographically validate the results for a given request back to a known public key (the trust anchor).

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

The correct answer is: Spoofing  
When a DNS server accepts and uses incorrect information from a host that has no authority giving that information. DNS spoofing is in fact malicious cache poisoning where forged data is placed in the cache of the name servers.  
  
Another attack on a DNS Server is when an attacker attempts to deny the availability of network services by flooding one or more DNS servers in the network with queries**.** This is called a DOS or Denial-of-service attack.  
  
  
The following answers are incorrect:  
  
**Redirection:** When an attacker can redirect queries for DNS names to servers that are under the control of the attacker.  
  
**Data modification:** An attempt by an attacker to spoof valid IP addresses in IP packets that the attacker has created. This gives these packets the appearance of coming from a valid IP address in the network. With a valid IP address, the attacker can gain access to the network and destroy data or conduct other attacks.  
  
**Footprinting:** The process by which an attacker obtains DNS zone data, including DNS domain names, computer names,  
and IP addresses for sensitive network resources.  
  
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.

The correct answer is: 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

The correct answer is: Access Control   
  
The following answers are incorrect: All of the other answers are incorrect.  
While Access Control monitoring is important from a security standpoint, it is not part of a performance Monitoring stategy.  
Performance monitoring is essential for the secure and reliable operation of a cloud environment. Data on the performance of the underlying components may provide early indications of hardware failure.  
Traditionally, four key subsystems are recommended for monitoring in cloud environments:  
**Network:** Excessive dropped packets  
**Disk:** Full disk or slow reads and writes to the disks (input/ output operations per second [IOPS])  
**Memory:** Excessive memory usage or full utilization of available memory allocation   
**CPU:** Excessive CPU utilization

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.

**The correct answer is:** An IDS generates a large number of false positives and false negatives.  
**The following answers are incorrect:**  All of the other answers are incorrect.  
An IDS is passive by design. It is a detection system that works in tandem with an Intrusion Prevention System (IPS).  The IPS has the active responsibility of taking action on suspicious traffic.  
The IDS does not need to sit inline with traffic, and that has no impact on its ability to "see" all the network traffic.  
An IDS has deep visibility into the network. It does not lack visibility.  
  
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).

The correct answer is:  Infrastructure As a Service (IaaS)  
The following answers are incorrect:All of the other answers are incorrect.  
With IaaS, the CCSP does not typically collect or have access to the log data of the VMs; the collection of log data is the customer‚„¢s responsibility. In a PaaS or SaaS environment, the CCSP may collect application- or OS-level log data.

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

The correct answer is: HIPAA  
  
HIPAA is the Health Insurance Portability and Accountability Act. It was enacted to protect health care records.  
  
The following answers are incorrect: All of the other answers are incorrect.  
  
- **SOX is the Sarbanes-Oxley** law that was enacted to protect consumers from fraudulent accounting practices.  
  
- **NIST is the National Institute of Standards and Technology.** NIST produces documentation in the form of "Special Publications (SP) " that are used for guidance.  
  
- **GLBA is the Graham-Leach-Bliley Act** which was enacted to protect consumer data sharing by financial institutions.  
  
The following reference(s) were/was used to create this question: Gordon, Adam. [The Official (ISC)2 Guide to the CCSP CBK Second Edition](http://www.amazon.com/gp/product/B01EYG54U6?ie=UTF8&tag=thecisspopens-20&linkCode=xm2&camp=1789&creativeASIN=%B01EYG54U6%20%20) Page 293 or Kindle Locations 7165-7171.

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.

The correct answer is: A SIEM system maps to and supports the implementation of the Critical Controls for Effective Cyber-Defense.  
A SIEM system can be set up locally or hosted in an external cloud-based environment.  
A SIEM system can support early detection of these events. A locally hosted SIEM system offers easy access and lower risk of external disclosure. An external SIEM system may prevent tampering of data by an attacker. SIEM systems are also beneficial because they map to and support the implementation of the Critical Controls for Effective Cyber-Defense.  
  
The Critical Controls for Effective Cyber-Defense (the Controls) are a recommended set of actions for cyber-defense that provide specific and actionable ways to stop today s most pervasive attacks.  
  
You can get a copy of the controls at: [www.counciloncybersecurity.org/critical-controls/](http://www.counciloncybersecurity.org/critical-controls/%20)  
  
  
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.

The correct answer is: A Logical network design lacks specific details such as technologies and standards while focusing on the needs at a general level.  
  
A Logical network design is always very general. This "abstraction " is done to describe complex ideas in a simple way.  
The one item of specifics is the use of the customer's business vocabulary. The use of specific business vocabulary helps to align the design to the requirement set for a solution to a customer problem.

Question 16

What is most important for the Cloud Security Professional to consider before performing system repair and maintenance?

When scheduling system repair and maintenance, the CSP needs to ensure adequate resources are available to meet expected demand and SLA requirements.

When scheduling system repair and maintenance, a host system must be placed into maintenance mode before starting any work on it.

When scheduling system repair and maintenance, a host system must be powered off or moved to another host before starting any work on it.

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.

The correct answer is: When scheduling system repair and maintenance, the CSP needs to ensure adequate resources are available to meet expected demand and SLA requirements.  
  
All of the procedures are legitimate considerations when performing any repairs or maintenance, however, the question is seeking the answer to what should be done BEFORE the maintenance begins.  When considering management-related activities and the need to control and organize them to ensure accuracy and impact, you need to think about the impact of change. It is important to schedule system repair and maintenance, as well as customer notifications, to ensure that they do not disrupt the organization‚„¢s systems. When scheduling maintenance, the CSP needs to ensure adequate resources are available to meet expected demand and SLA requirements. You should make sure that appropriate change-management procedures are implemented and followed for all systems and that scheduling and notifications are communicated effectively to all parties that will potentially be affected by the work.  
  
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

The correct answer is: Availability  
From the perspective of the cloud customer, business continuity elements include the relevant security pillars of availability, integrity, and confidentiality.  
  
The availability of the relevant resources and services is often the key requirement, along with the uptime and ability to access these on demand. Failure to ensure this results in significant impacts, including loss of earnings, loss of opportunities, and loss of confidence for the customer and provider.  
  
Many security professionals struggle to keep their business continuity processes current once they have started to utilize cloud-based services. Equally, many fail to adequately update, amend, and keep their business continuity plans up to date in terms of complete coverage of services.

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.

The correct answer is: Readily available independent security vendor reports.  
  
Many vendors do not make security reports available to customers or the public unless the report is sanitized and specifically requested.  
  
Communicating in a structured and standardized way is part of an effective distributed information technology (IT) model.  
Communication may be enhanced in a structured environment when change management controls are improved.  
  
Clearly assigned and identified requirements that are documented in SLAs avoids being penalized monetarily and are also part of an effective distributed information technology (IT) model.  
  
Project management:  Effective project management helps to ensure successful technology delivery and solutions.  
  
The following answers are incorrect:

Question 2

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

Executive Committee and Directors.

Vendor Management, Compliance and Audit teams.

IT, Information Security, Logistics and Risk teams.

Legal, Finance and Operations teams.

The following answers are incorrect:   
  
The stakeholders listed below are all teams and business units within the organization acting as relevant stakeholders.  
  
Vendor Management, Compliance and Audit teams;  
Legal, Finance and Operation teams, and  
Executive Committee and Directors  
  
In addition, IT, Information Security, Risk and Data Protection and Privacy teams may also be identified as relevant cloud computing stakeholders across an organization.

Question 3

Organizational policies are not useful in helping to reduce:

Retrievable data loss.

Financial loss.

Misuse and abuse of systems and resources.

Reputational, regulatory and legal issues.

The correct answer is: Retrievable data loss.  
  
Organizational policies help to reduce "Irretrievable loss of data. " Retrievable loss of data is a distractor. If data is loss, you would want to retrieve that data. Organizational policies help reduce the likelihood of irretrievable loss of data.  
  
  
The following answers are incorrect:   
  
All of the answers below are incorrect because organizational policies help to reduce those issues.  
  
Financial loss, Reputational,  
Regulatory and Legal issues and  
Misuse and abuse of systems and resources are incorrect answers because organizational policies help to reduce these things.  
  
  
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

The correct answer is: Unenforceable governmental request.

The term, unenforceable governmental request is a distractor. A governmental request can be **enforceable** and granted based on the government s order.  
  
The following list is a general guide designed to help you focus on some of the areas and legislative items that might impact your cloud environments:  
  
**International law**: International law is the term given to the rules that govern relations between states or countries.  
  
**State law**: State law typically refers to the law of each U.S. state (50 states in total, each treated separately), with their own state constitutions, state governments, and state courts.  
  
**Copyright and piracy law**: Copyright infringement can be performed for financial or nonfinancial gain. It typically occurs when copyright material is infringed upon and made available to or shared with others by a party who is not the legal owner of the information.  
  
**Enforceable governmental request**: An enforceable governmental request is a request or order that is capable of being performed on the basis of the government s order.  
  
**Intellectual property right**: Intellectual property describes creations of the mind such as words, logos, symbols, other artistic creations, and literary works. Patents, trademarks, and copyright protection exist to protect a person s or a company s intellectual entitlements.  
  
**Privacy law**: Privacy can be defined as the right of an individual to determine when, how, and to what extent she will release personal information.  
  
**The doctrine of the proper law**: When a conflict of laws occurs, this determines in which jurisdiction the dispute will be heard, based on contractual language professing an express selection or a clear intention through a choice-of-law clause.  
  
**Criminal law**: Criminal law is a body of rules and statutes that defines conduct that is prohibited by the government and is set out to protect the safety and well being of the public. Besides defining prohibited conduct, criminal law defines the punishment when the law is breached.  
  
**Tort law**: This is a body of rights, obligations, and remedies that sets out reliefs for persons suffering harm as a result of the wrongful acts of others.  
  
**Restatement (second) conflict of laws**: A restatement is a collation of developments in the common law (that is, judge made law, not legislation) that inform judges and the legal world of updates in the area. Conflict of laws relates to a difference between the laws.  
  
  
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

The correct answer is:

Copyright laws protect logos and symbols

The correct answer is: Copyright laws protect logos and symbols.  
  
This statement describes the protection provided by trademarks which makes it FALSE.  
  
Copyright laws offer protection against improperly sharing information and protects product of the mind.

Question 6

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

Define audit policies.

Refine the audit process.

Define audit scope and conduct audit.

Define audit objectives.

The correct answer is: Define audit policies.  
  
Defining audit polices is not a phase of audit planning. In the context of audit planning, defining audit policies is a distractor.  
  
Policies would be produced prior to you validating them through an audit, not the opposite.  
  
  
The following answers are incorrect:  
  
You are being asked to define activities that are **not** included in the audit planning phase. The following statements are incorrect because they are part of (help to define) the audit planning phase.  
  
Define audit objectives is included in the audit planning phase. The define audit objective phase includes: defining audit ouputs, audit focus, defining number of auditors and subject matter experts.  
  
Define audit scope and conduct audit is included in the audit planning phase. The define audit scope phase includes documenting services and resources utilized from CSPs,key points of contacts, risk managment processes and; defining things such as cloud services to be audited, locations for audits to be conducted, escalation and communication points and criteria to which CSP will be assessed. The conduct audit phase includes having adequate staff and tools, as well as properly supervising the audit.  
  
Refine the audit process is included in the audit planning phase. The refine phase includes ensuring that the audit approach and scope are still relevant to the audit, reporting details are clear and concise and, that the auditors are competent and are able to provide accurate audit reports.  
  
  
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.

The correct answer is: Technical assessments.  
  
The ability to meet SLAs, contractural requirements, and industry best practice standards and frameworks are all part of cloud-based audits.  
  
This questions is asking that you identify what generally is **NOT i**ncluded in most cloud-based audits.  
  
The majority of cloud-based audits do not focus on technical assessments, but rather testing is focused on the ability to meet SLAs, contractural requirements, and 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?

Disclosure to third parties, Security for privacy, Quality, Monitoring and enforcement

Management, Notice, Choice and consent

Collection, Use, Rention and disposal, Access

Confidentiality, Integrity, Availability

The correct answer is: Confidentiality, Integrity, Availability  
  
A brief overview of ten main GAPP:  
  
Defines, documents, communicates and assigns accountability for its privacy prolicies and procedures **(Management)**  
Provides notice about its privacy and procedures policy **(Notice)**  
Describes choices available to individuals and obtains consent for the use of personal information **(Choice and consent)**  
Collects personal information as described **(Collection)**  
Limits the use of, and retains and disposes of personal information appropriately **(Use, rention, disposal)**  
Provides individuals access to their personal information **(Access)**  
Discloses personal information to third parties with consent **(Disclosure to third parties)**  
Protects personal information from unauthorized access **(Security for privacy)**  
Maintains accurate, complete, relevant personal information **(Quality)**   
Monitors compliance with its privacy policies and procedures **(Monitoring and enforcement)**  
  
  
Question 9

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

Risk

Confidentiality, Integrity, Availability

Resiliency

Interoperability

The correct answer is:  Risk    
  
The following answers are incorrect:  Interoperability, Confidentiality, Integrity, Availability and Resiliency are incorrect answers.  Interoperability refers to the ease of moving and reusing applicaton components regardless of provider, platform, OS, infrastructure, location, storge, fomat of data or APIs. Interoperability is also related to how well the applications work together with new and existing architecture. Interoperability is not a key focus of the CSP and cloud customer.   Confidentiality, Integrity and Availability are basic foundational tenants of information security.  Resiliency is the ability of a cloud service's data center and its related components to continue operating during a disruption.  Resiliency is not a key focus of the CSP and cloud customer.      
  
The CSP and cloud customer must focus on risk.  To this end the CSP's and cloud customer's policies and procedures should be aligned.  The customer (organization) must determine its acceptable level of risk, conduct a risk assessment and review it against cloud-computing services, CSP and understand the effects of using cloud based services.   
  
What statement concerning the Service Level Agreement (SLA) is false?

The SLA should reference compliance and best practice activities.

SLAs tend to be structured in favor of the customer as penalty clauses within the SLA is a form of transferring risks.

Customers pay for time and costs associated with making changes to existing SLAs.

The SLA is critical in establishing secure business and operational requirements.

The correct answer is:  
  
SLAs tend to be structured in favor of the customer as penalty clauses within the SLA is a form of transferring risks is the correct answer because it is a false statement. The question is asking that you identify the false statement.  SLAs tend to be written in favor of the provider, not the customer; thereby, exposing the provider to less risk.  Addressing financial penalties are important in SLAs but, penalties usually do not provide adequate compensation to the customer for associated losses.  Penalty clauses encourage providers to meet the terms of the SLA, but penalty clauses are not a form of risk transference for the customer.     
  
The following answers are incorrect:  
  
This question is asking you to identify incorrect answers.  Customers pay for time and costs associated with making changes to existing SLAs is a true statement.  The SLA is critical in establishing secure business and operational requirements is a true statement.  The SLA should reference compliance and best practice activities is a true statement.  
  
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) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Is not encrypted.

Relevant to a pending or reasonably anticipated litigation or government investigation.

Contains credit card information, in conjunction with PCI DSS requirements.

Provides enough PII to jeopardize a customer's Right to Privacy.

**The correct answer is**: Relevant to a pending or reasonably anticipated litigation or government investigation.  
  
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, is relevant to a pending or reasonably anticipated litigation or government investigation. Depending on the cloud service and deployment model that a client is using, preservation in the cloud can be very similar to preservation in other IT infrastructures, or it can be significantly more complex.  
  
In the European Union, information preservation is governed under Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006. Japan, South Korea, and Singapore have similar data protection initiatives. Within South America, Brazil and Argentina have the Azeredo Bill, and the Argentina Data Retention Law 2004, Law No. 25.873, 6 February 2004, respectively.  
  
  
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 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Data that does NOT include Personably Identifying Information of employees.

Data that does NOT include Personably Identifying Information of customers.

Data that are within its possession, custody or control.

Data as listed in the Graham / Livingston Act of 2007.

**The correct answer is:** Data that are within its possession, custody or control.  
  
In most jurisdictions in the United States, **a party's obligation to produce relevant information is limited to documents and data within its possession, custody or control**.  
  
Hosting relevant data at a third-party, even a cloud provider, generally does not obviate a party's obligation to produce information as it may have a legal right to access or obtain the data.  However, not all data hosted by a cloud provider may be under the control of a client (e.g., disaster recovery systems, certain metadata created and maintained by the cloud provider to operate its environment).  Distinguishing the data that is and is not available to the client may be in the interest of the client and provider.  The obligations of the cloud service provider as cloud data handler with regard to the production of information in response to legal process is an issue left to each jurisdiction to resolve.   
  
  
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

The correct answer is:

Cloud Customer

The customer has all the responsibility and liability for protecting the information

DISCUSSION:

The customer has all the responsibility and liability for protecting the information according to legal standards and regulation but often cannot mandate the actual protections and security measures in order to accomplish this. This is a very strange, unnatural situation.