In-Class Practice Questions

1. Which of the following terms best describes the ability for cloud consumers to access evidence, actions, controls and processes that were performed by a user?
   1. SLA
   2. Portability
   3. Auditability
   4. Regulatory Compliance
2. Which of the following is a true statement?
   1. Organizational goals that require technology, especially cloud technology, are best met when technology is considered at the forefront.
   2. The choice to deploy a cloud solution is primarily a technical decision.
   3. Funding and technology decisions for a movement to the cloud should be made with the business direction at the core.
   4. Deployment of a cloud solution is always a technology decision.
3. Privacy in the cloud is most often achieved through which of the following?
   1. Privacy is best achieved through regulatory compliance.
   2. Privacy is achieved through the security provided by the cloud provider in addition to the cloud customer.
   3. Privacy must be outlined in the Service Level Agreement with the cloud provider.
   4. Privacy is one of the essential elements of cloud computing and need to be addressed as part of the resource pooling.
4. Paul 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 Paul can give the board members?
   1. The board member is correct in stating that the perimeter is clearly the demarcation point.
   2. There is not a clear perimeter in cloud networks.
   3. The perimeter transforms into a series of highly dynamic “micro borders” for some cloud providers.
   4. The classic definition of a network perimeter takes on different meanings under different guises and deployment models.
5. 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 administrator
   2. Cloud architect
   3. Cloud operator
   4. Cloud storage administrator
6. Which of the following approaches is typically used for SaaS environments and cloud deployments?
   1. Segregated Key Management
   2. Client Side Key Management
   3. Hybrid Key Management
   4. Remote Key Management Service
7. 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 for providing access to end users. What are we referring to?
   1. Centralized key management
   2. Migration and transference
   3. Provisioning and de-provisioning
   4. Multi-factor authentication and resource access
8. A system design that does not create a single point of failure is the best defense against which of the following common threats?
   1. Malicious Insider
   2. Abuse of Cloud Service
   3. Traffic Hijacking
   4. Denial of Service
9. Which of the following is true of “bolt-on” components to cloud API’s?
   1. Bolt-on components are bad because they decrease complexity of cloud security.
   2. Bolt-on components are bad because they increase complexity and decrease security.
   3. Bolt-on components are good because they build extra security into an existing API.
   4. Bolt-on components are good because they increase productivity.
10. 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 act of investigation and understanding the risks a company faces, and due diligence is the development and implementation of policies and procedures to aid in protecting the company, its assets, and its people from threats.
    2. 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.
    3. Due care is the methodology required for certifying a site as “cloud ready”, and due diligence in the process of accreditation of a site.
    4. Due diligence is the act of investigating and understanding the risks a company faces, and due care is the development and implementation of policies and procedures to aid in protecting the company, its assets, and its people from threats.
11. 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 true, because simply powering off a VM makes it safe against an infection or attack against the Operating System or applications.
    2. This is true, because simply powering off a VM renders it inaccessible to the system on which it resides.
    3. This is false, because simply powering off a VM does not stop the processes from running, leading to VM sprawl.
    4. This is false, because simply powering off a VM still leaves the image files susceptible to malware infections and missed patching.
12. 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. Resource Pools
    3. Strict Segmentation
    4. No physical endpoints
13. 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 due to its decreased complexity, which decreases a defense-in-depth approach.
    2. 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.
    3. A single point of access to a VM environment is a security threat because it creates strict network topologies, which are counter-productive.
    4. A single point of access to a VM environment is a security threat because it creates too many physical endpoints, increasing complexity.
14. Susan 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 good design because it is efficient and operationally expedient.
    3. This is a bad design because it creates the threat of Insecure Direct Object Reference.
    4. This is a bad design because it creates the threat of Cross-Site Request Forgery (CSRF).
15. 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. Store
    2. Process
    3. Destroy
    4. Access
16. Service Organization Control (SOC) reports are broken into 3 types. Which type is of most interest to a technical audience due to its Trust Service Principles?
    1. SOC I, Type I
    2. SOC I, Type II
    3. SOC II
    4. SOC III
17. Which of the following is an example of Unstructured Data?
    1. Text and Multimedia content
    2. IAM information
    3. Relational Database content
    4. Raw Device Mapping
18. Which phase of the cloud data lifecycle typically occurs nearly simultaneously with data creation?
    1. Storage
    2. Encryption
    3. Use
    4. Classification
19. At which point in the cloud data lifecycle phases is data considered most vulnerable?
    1. Storage
    2. In use
    3. Archived
    4. Deletion
20. Each cloud service model uses different data storage types. Which storage type is associated with the PaaS cloud service model?
    1. Structured and Unstructured
    2. Volume and Object
    3. Raw and Ephemeral
    4. Volume and File
21. Regarding data dispersion, what is the underlying technology where segments of data are encrypted and dispersed across the network and makes dispersion possible?
    1. Erasure coding is the technology that chunks a data object into the segments.
    2. Encryption algorithmic dispersion is the technology that chunks a data object into the segments.
    3. Data blocking is the technology that chunks a data object into the segments.
    4. Tokenization masking is the technology that chunks a data object into the segments.
22. An organization has asked their Cloud Security Professional how to setup 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 should 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 should be deployed where the data resides, usually on one or more subsystems.
    3. In a “Data in Motion” topology, the DLP monitoring engine should be deployed at the endpoint, where the data is processed.
    4. In a “Data in Motion” topology, the DLP monitoring engine should be deployed in an unstructured database.
23. 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 requires forced collusion to occur if unauthorized access is attempted.
    2. Separation of duties requires that a manager approves the action in order to proceed with the key management function.
    3. Separation of duties shifts the responsibility to the Board of Directors.
    4. Separation of duties has no impact on key management.
24. When working with Privacy and Data Protection, to what entity are all liabilities assigned?
    1. All liabilities are assigned to the Controller role, and its country of establishment mainly determines the applicable Privacy and Data Protection law and jurisdiction.
    2. All liabilities are assigned to the Processor role, and its country of establishment mainly determines the applicable Privacy and Data Protection law and jurisdiction.
    3. Liabilities cannot be assigned to any particular role, due to varying Privacy and Data Protection laws in the countries of establishment and their jurisdictions.
    4. All liabilities are assigned to the Controller and Processors 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.
25. Which of the following is considered to be the only reasonable method of data disposal in a cloud environment?
    1. Degaussing
    2. Physical Destruction
    3. Overwriting
    4. Crypto-shredding
26. What statement is most accurate about cloud object storage?
    1. 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.
    2. Object storage features offer increased, real-time data consistency, making them perfect for frequently changing data.
    3. Object storage features offer the most robust advantages when using granular file-level controls.
    4. Object storage features are never for storing operating system images.
27. Regulatory compliance is most closely aligned with which of the following?
    1. The requirement of an organization to access, report, and obtain evidence of organization controls.
    2. The requirement of an organization to define processes and procedures.
    3. The focus of an organization to produce information about actions of the users.
    4. The requirement of an organization to adhere to relevant laws, guidelines and specifications relevant to its business.
28. Which of the following protocols is NOT used to protect data in transit?
    1. IPSEC
    2. KMS
    3. SSL
    4. TLS
29. Which of the following essential characteristics of the cloud most closely resembles the scalability of traditional computing?
    1. Rapid Elasticity
    2. Measured Self-Service
    3. Broad Network Access
    4. On-Demand Self-Service
30. 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. Private
    3. Community
    4. Hybrid
31. 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 SLA.
    4. Through collaboration.
32. What is a key activity for any organization considering moving to the cloud?
    1. All of the others are considerations.
    2. Determining the best cloud formation for the business.
    3. Classifying the organizations data to determine the requirements for the cloud engagement.
    4. Understanding if the cloud is the correct choice for the business of the organization.
33. Why is a Type I hypervisor less vulnerable to attack than other hypervisor types?
    1. The limited access and strong control over the Operating System(OS) greatly increases reliability and robustness of Type I hypervisors.
    2. Type 2 hypervisors security is limited in its patch availability.
    3. The Type I hypervisors are not less vulnerable to attack than the Type 2 hypervisors.
    4. The operating system-based hypervisor in standardized, making it less vulnerable.
34. A MitM attack against a cloud consumer is most closely aligned with which of the following common threats?
    1. Cruzr attack
    2. Denial of Service
    3. Low Orbit Ion Cannon Attack
    4. Traffic Hijacking
35. Which of the following would NOT be included as input into the requirements gathering for an application or system?
    1. Users
    2. Management
    3. Regulators
    4. Auditors
36. The final phase of the cloud data lifecycle is the destroy phase, where data is ultimately deleted and done so in a secure manner to ensure it cannot be recovered or reconstructed. Which cloud service category poses the most challenges to data destruction or the cloud customer?
    1. Platform
    2. Software
    3. Infrastructure
    4. Desktop
37. Which phase of the cloud data lifecycle also typically entails the process of data classification?
    1. Use
    2. Store
    3. Create
    4. Archive
38. At which layer does the IPSec protocol operate to encrypt and protect communications between two parties?
    1. Network
    2. Application
    3. Transport
    4. Data link
39. The Cloud Security Alliance's (CSA's) Cloud Controls Matrix (CCM) addresses all the following security architecture elements except \_\_\_\_\_\_\_\_\_\_\_\_.
    1. Physical security
    2. IaaS
    3. Application security
    4. Business drivers
40. Which of the following characteristics is associated with digital rights management (DRM) solutions (sometimes referred to as information rights management, or IRM)?
    1. Mapping to existing access control lists (ACLs)
    2. Delineating biometric catalogs
    3. Preventing multifactor authentication
    4. Prohibiting unauthorized transposition
41. The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing. A cloud customer that does not perform sufficient due diligence can suffer harm if the cloud provider they've selected goes out of business.

What do we call this problem?

* 1. Vendor lock-in
  2. Vendor lock-out
  3. Vendor incapacity
  4. Unscaled

1. Which of the following contract terms most incentivizes the cloud provider to meet the requirements listed in the SLA?
   1. Regulatory oversight
   2. Financial penalties
   3. Performance details
   4. Desire to maintain customer satisfaction
2. Which of the following is considered an administrative control?
   1. Access control process
   2. Keystroke logging
   3. Door locks
   4. Biometric authentication
3. Administrative penalties for violating the General Data Protection Regulation (GDPR) can range up to \_\_\_\_\_\_\_\_\_\_\_\_.
   1. US$100,000
   2. 1,000,000 euros
   3. 20,000,000 euros
   4. 4,000,000 euros
4. When designing a cloud data center, which of the following aspects is not necessary to ensure continuity of operations during contingency operations?
   1. Access to clean water
   2. Broadband data connection
   3. Extended battery backup
   4. Physical access to the data center
5. A web application firewall (WAF) can understand and act on \_\_\_\_\_\_\_\_ traffic.
   1. Malicious
   2. SMTP
   3. ICMP
   4. HTTP
6. You are a consultant performing an external security review on a large manufacturing firm. You determine that its newest assembly plant, which cost $24 million, could be completely destroyed by a fire but that a fire suppression system could effectively protect the plant. The fire suppression system costs $15 million. An insurance policy that would cover the full replacement cost of the plant costs $1 million per month. In order to establish the true annualized loss expectancy (ALE), you would need all of the following information except \_\_\_\_\_\_\_\_\_\_\_\_.
   1. The amount of revenue generated by the plant
   2. The rate at which the plant generates revenue
   3. The length of time it would take to rebuild the plant
   4. The amount of product the plant creates
7. Which security certification serves as a general framework that can be applied to any type of system or application?
   1. ISO/IEC 27001
   2. PCI DSS
   3. FIPS 140-2
   4. NIST SP 800-53
8. You work for a company that operates a production environment in the cloud. Another company using the same cloud provider is under investigation by law enforcement for racketeering. Your company should be concerned about this because of the cloud characteristic of \_\_\_\_\_\_\_\_\_\_\_\_.
   1. Virtualization
   2. Pooled resources
   3. Elasticity
   4. Automated self-service
9. You are the security manager for an online retail sales company with 100 employees and a production environment hosted in a PaaS model with a major cloud provider. Your company policies have allowed for a BYOD workforce that work equally from the company offices and their own homes or other locations. The policies also allow users to select which APIs they install and use on their own devices in order to access and manipulate company data. Of the following, what is a security control you'd like to implement to offset the risk(s) incurred by this practice?
   1. Regular and widespread integrity checks on sampled data throughout the managed environment
   2. More extensive and granular background checks on all employees, particularly new hires
   3. Inclusion of references to all applicable regulations in the policy documents
   4. Increased enforcement of separation of duties for all workflows
10. Your company has just been served with an eDiscovery order to collect event data and other pertinent information from your application during a specific period of time, to be used as potential evidence for a court proceeding. Which of the following, apart from ensuring that you collect all pertinent data, would be the MOST important consideration?
    1. Encryption
    2. Chain of custody
    3. Compression
    4. Confidentiality
11. It is important to include \_\_\_\_\_\_\_ in the design of underfloor plenums if they are also used for wiring.
    1. Mantraps
    2. Sequestered channels
    3. Heat sinks
    4. Tight gaskets
12. Which of the following is not typically included in the list of critical assets specified for continuity during BCDR contingency operations?
    1. Systems
    2. Data
    3. Cash
    4. Personnel
13. With cloud computing crossing many jurisdictional boundaries, it is a virtual certainty that conflicts will arise between differing regulations. What is the major impediment to resolving conflicts between multiple jurisdictions to form an overall policy?
    1. Language differences
    2. Technologies used
    3. Licensing issues
    4. Lack of international authority
14. You are performing an audit of the security controls used in a cloud environment. Which of the following would best serve your purpose?
    1. The business impact analysis (BIA)
    2. A copy of the VM baseline configuration
    3. The latest version of the company's financial records
    4. A SOC 3 report from another (external) auditor
15. You are the security manager for a small retail business involved mainly in direct ecommerce transactions with individual customers (members of the public). The bulk of your market is in Asia, but you do fulfill orders globally. Your company has its own data center located within its headquarters building in Hong Kong, but it also uses a public cloud environment for contingency backup and archiving purposes. Your company has decided to expand its business to include selling and monitoring lifesupport equipment for medical providers. What characteristic do you need to ensure is offered by your cloud provider?
    1. Full automation of security controls within the cloud data center
    2. Tier 4 of the Uptime Institute certifications
    3. Global remote access
    4. Prevention of ransomware infections
16. You are the security subject matter expert (SME) for an organization considering a transition from the legacy environment into a hosted cloud provider's data center. One of the challenges you're facing is whether the provider will have undue control over your data once it is within the provider's data center; will the provider be able to hold your organization hostage because they have your data? This is a(n) \_\_\_\_\_\_\_\_\_ issue.
    1. Interoperability
    2. Portability
    3. Availability
    4. Security
17. Which of the following is an example of useful and sufficient data masking of the string "CCSP"?
    1. XCSP
    2. PSCC
    3. TtLp
    4. 3X91
18. The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "injection." In most cases, what is the method for reducing the risk of an injection attack?
    1. User training
    2. Hardening the OS
    3. Input validation/bounds checking
    4. Physical locks
19. Firewalls can detect attack traffic by using all these methods except \_\_\_\_\_\_\_\_\_\_\_\_.
    1. Known past behavior in the environment
    2. Identity of the malicious user
    3. Point of origination
    4. Signature matching
20. Bob is staging an attack against Alice's website. He is able to embed a link on her site that will execute malicious code on a visitor's machine, if the visitor clicks on the link. This is an example of which type of attack?
    1. Cross-site scripting
    2. Broken authentication/session management
    3. Security misconfiguration
    4. Insecure cryptographic storage
21. Although indirect identifiers cannot alone point to an individual, the more of them known can lead to a specific identity. Which strategy can be used to avoid such a connection being made?
    1. Masking
    2. Anonymization
    3. Obfuscation
    4. Encryption
22. Software-defined networking (SDN) is intended to separate different network capabilities and allow for the granting of granular configurations, permissions, and features to non- network staff or customers. Which network capability is separated from forwarding of traffic?
    1. Routing
    2. Firewalling
    3. Filtering
    4. IPS
23. Who is ultimately responsible for a data breach that includes personally identifiable information (PII), in the event of negligence on the part of the cloud provider?
    1. The user
    2. The subject
    3. The cloud provider
    4. The cloud customer
24. What could be the result of failure of the cloud provider to secure the hypervisor in such a way that one user on a virtual machine can see the resource calls of another user's virtual machine?
    1. Unauthorized data disclosure
    2. Inference attacks
    3. Social engineering
    4. Physical intrusion
25. Which of the following are not examples of personnel controls?
    1. Background checks
    2. Reference checks
    3. Strict access control mechanisms
    4. Continuous security training
26. Which of the following data-sanitation approaches are always available within a cloud environment?
    1. Physical destruction
    2. Shredding
    3. Overwriting
    4. Cryptographic erasure
27. Aside from the fact that the cloud customer probably cannot locate/reach the physical storage assets of the cloud provider, and that wiping an entire storage space would impact other customers, why would degaussing probably not be an effective means of secure sanitization in the cloud?
    1. All the data storage space in the cloud is already gaussed.
    2. Cloud data storage may not be affected by degaussing.
    3. Federal law prohibits it in the United States.
    4. The blast radius is too wide.
28. a
    1. m