Latest Version

Question: 1

Which is the correct sequence of Cloud Data lifecycle phases?

A. Create, Use, Store, Archive, Share, Destroy
B. Create, Store, Use, Share, Archive, Destroy
C. Create, Share, Use, Store, Archive, Destroy
D. Create, Use, Share, Store, Archive, Destroy

Answer: B

Explanation:
The correct order of data lifecycle is Create, Store, Use, Share, Archive, Destroy

Question: 2

Security Governance, Risk and Compliance(GRC) is, generally, responsibility of which of the following across all the platforms (IaaS, PaaS and SaaS)?

A. Customer
B. Cloud Service Provider
C. Shared responsibility
D. Joint Responsibility

Answer: A

Explanation:
GRC is responsibility of the customer across all service models.

Question: 3

Which of the standards is related to risk management?

A. ISO 27005
B. ISO 27001

C. ISO 27002
D. NIST 800-125

Answer: A

Explanation:
lS0 27005 'provides guidelines for information security risk management' and 'supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.'

Question: 4

"Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service. "
Which of the following characteristics defines this?

A. Broad network access
B. Resource pooling
C. Rapid elasticity
D. Measured service

Answer: D

Explanation:
Measured service is defined as "Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service. "

Question: 5

Which is the primary tool used to manage identity and access management of resources spread across hundreds of different clouds and resources?

A. Active Directory
B. Federation
C. SAML 2.0
D. Entitlement Matrix

Answer: B

Explanation:
In cloud computing, the fundamental problem is that multiple organizations are now managing the identity and access management to resources, which can greatly complicate the process. For example, imagine having to provision the same user on dozens-or hundreds-of different cloud services. Federation is the primary tool used to manage this problem, by building trust relationships between organizations and enforcing them through standards-based technologies.

Reference: CSA Security GuidelinesV.4(reproduced here for the educational purpose)

Question: 6

Which is the leading industry leading standard you will recommend to a web developer when designing web application or an API for a cloud solution?

A. ISO 27001
B. SOC2
C. FIPS 140
D. OWASP

Answer: D

Explanation:
OWASP is an open project and is leading industry standard for designing web applications and its security.

Question: 7

Where does the encryption engine and key reside when doing file-level encryption?

A. On the instance attached to the system
B. Encryption engine resides on the server and keys on the client side
C. On the KMS attached to the system
D. On the client side

Answer: A

Explanation:
File-level encryption: Database servers typically reside on volume storage. For this deployment, you are encrypting the volume or folder of the database, with the encryption engine and keys residing on the instances attached to the volume.
External file system encryption protects from media theft, lost backups, and external attack but does not protect against attacks with access to the application layer, the instances 0S, or the data

Question: 8

The management plane controls and configures the:

A. Infrastructure
B. Metastructure
C. Infostructure
D. Applistructure

Answer: B

Explanation:
The management plane controls and configures the metastructure and is also part of the metastructure itself. As a reminder, cloud computing is the act of taking physical assets(like networks and processors)and using them to build resource pools. Metastructure is the glue and guts to create, provision, and de-provision the pools. The management plane includes the interfaces for building and managing the cloud itself, but also the interfaces for cloud users to manage their own allocated resources of the cloud.
Reference: CSA Security GuidelinesV.4(reproduced here for the educational purpose)

Question: 9

Which of the following pose the biggest risk in the organization?

A. People
B. Technology
C. Access Controls
D. DDoS Attacks

Answer: A

Explanation:
People pose the biggest risk in the organization.
People form the biggest risk as they can expose the sensitive data accidentally or on purpose. Disgruntled employees or careless employees form a great threat to the organization.

Question: 10

Which of the following can lead to vendor lock-in?

A. Big Data sets
B. Large supplier Redundancy
C. Lack of transparency in terms of use
D. CSP's vendor utilisation

Answer: C

Explanation:
Lack of transparency in terms of use can lead to vendor lock-in. Contracts and SLAs should clearly define the relationship between Cloud Service Provider(CSP)and the cloud customer. Clause of data portability should be there.

Question: 11

In which of the following cloud service models is the customer required to maintain the operating system?

A. PaaS
B. Public Cloud
C. IaaS
D. SaaS

Answer: C

Explanation:
According to "The NIST Definition of Cloud Computing," in 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 OSs and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over OSs, storage, and deployed applications; and possibly limited control of select networking components (e.g, host firewalls)."

Question: 12

Which of the following adds abstraction layer on top of networking hardware and decouples network control plane from the data plane?

A. VLANs
B. Software Defined Networks
C. Virtual Private Networks
D. Converged Networks

Answer: B

Explanation:
Software Defined Networking(SDN):A more complete abstraction layer on top of networking hardware, SDNs decouple the network control plane from the data. This allows us to abstract networking from the traditional limitations of a LAN.
Reference: CSA Security GuidelinesV.4(reproduced here for the educational purpose)

Question: 13

Which of the following are communications method for components within a cloud, some of which (or an entirely different set) are exposed to the cloud user to manage their resources and configurations?

A. Data Identifiers
B. Application Programming Interfaces (API)
C. API Gateway
D. IPSEC

Answer: B

Explanation:
All this is facilitated using Application Programming Interfaces, APIs are typically the underlying communications method for components within a cloud. some of which (or an entirely different set) are exposed to the cloud user to manage their resources and configurations. Most cloud APIs these days use REST (Representational State Transfer). which runs over the HTTP protocol, making it extremelywe11 suited for Internet services.
Ref: CSA Security Guidelines V4.0

Question: 14

Multi-tenancy and shared resources are defining characteristics of cloud computing. However, mechanisms separating storage, memory, routing may fail due to several reasons. What risk are we talking about?

A. Isolation Failure
B. Isolation Escalation
C. Separation of Duties
D. Route poisoning

Answer: A

Explanation:
According to ENISA (European Network and Information Security Agency) document on Security risk and recommendation, Isolation failure is considered as one of the top risk and is defined as follows Multi-tenancy and shared resources are defining characteristics of cloud computing. This risk category covers the failure of mechanisms separating storage, memory, routing and even reputation between different tenants (e.g, so-called guest-hopping attacks). However it should be considered that attacks on resource isolation mechanisms (e.g. against hypervisors) are still less numerous and much more difficult for an attacker to put in practice compared to attacks on traditional Oss.

Question: 15

Which one of the following is NOT a level of CSA star program?

A. Self-assessment
B. Third-party attestation
C. Continuous-monitoring program
D. Technology Audit program

Answer: D

Explanation:
"Technology Audit Program" is not one of the levels of CSA star program

The three levels of CSA Star program are
1) Self Assessment
2) Third-party Attestment
3) Continuous Monitoring program

Question: 16

Which of the following is a key consideration in Data security but does not feature in Data Security Life cycle?

A. Storage Location
B. Storage Device
C. Storage protocol
D. Access Method

Answer: A

Explanation:
The lifecycle represents the phases information passes through but doesnt address its location or how it is accessed.

Question: 17

Which of the cloud service model has least maintenance or administration from a cloud customer perspective?

A. IaaS
B. PaaS
C. SaaS
D. XaaS

Answer: C

Explanation:
SaaS requires least maintenance from the customer as all the infrastructure up to application is managed by the cloud service provider

Question: 18

Which standard offers guidelines for information security controls applicable to the provision and use of cloud services?

A. ISO 27018
B. ISO 27017
C. ISO 15048

D. ISO 27034

Answer: A

Explanation:
ISO 270017 provides guidance on the information security aspects of cloud computing. recommending and assisting with the implementation of cloud-specific information security controls supplementing the guidance in ISO/IEC 27002 and other ISO 27k standards.

Question: 19

Which of the following is key component of regulated PII components?

A. Mandatory Breach Reporting
B. Cloud Service Provider Consent
C. E-discovery
D. Data disclosure

Answer: A

Explanation:
The key component and differentiator related to regulated PII is mandatory breach reporting requirements. At present. 47 states and territories within the United States, including the District of Columbia. Puerto Rico. and the Virgin Islands, have legislation in place that requires both private and government entities to notify and inform individuals of any security breaches involving PII.

Question: 20

Which of the following is NOT one of the common networks underlying in Cloud Infrastructure?

A. Service Network
B. Management Network
C. Security Network
D. Storage Network

Answer: C

Explanation:
If you are a cloud provider (including managing a private cloud), physical segregation of networks composing your cloud is important for both operational and security reasons. We most commonly see at least three different networks which are isolated onto dedicated hardware since there is no functional or traffic overlap:
1. The service network for communications between virtual machines and the Internet. This builds the network resource pool for the cloud users.
2. The storage network to connect virtual storage to virtual machines.

3. A management network for management and API traffic.
Ref: Reference: CSA Security GuidelinesV.4 (reproduced here for the educational purpose)

Question: 21

Which of the following best describes the relationship between a cloud provider and the customer?

A. Contract
B. Operational level Agreement
C. Service Level Agreement
D. Privacy Level Agreement

Answer: A

Explanation:
Contract is the most suitable answer here. It can be argued that Service Level Agreement could also be an answer but SLA is a negotiation/agreement for minimum service-levels expected. Contract is the document that defines the relation-ship between Cloud service provider and customer

Question: 22

Which is the most important trust mechanism between cloud service provider and cloud customer?

A. Meeting SLA requirements
B. Contract
C. Audit reports
D. Logging and Monitoring reports

Answer: B

Explanation:
Contract is the most important document which defines trust and relationship between cloud service provider and the customer.

Question: 23

Which of the following type of risk assessment most effectively supports cost-benefit analyses of alternative risk responses or courses of action?

A. Qualitative Analysis
B. Quantitative Analysis
C. Third party Risk Analysis
D. Outsourced risk analysis

Answer: B

Explanation:
Quantitative assessments typically employ a set of methods, principles, or rules for assessing risk based on the use of numbers This type of assessment most effectively supports cost-benefit analyses of alternative risk responses or courses of action.

Question: 24

Which of the following is a key component that allows programmatic management of the cloud?

A. APIs
B. Firewall
C. API Gateway
D. Control Plane

Answer: A

Explanation:
Application Programming Interfaces allow for programmatic management of the cloud. They are the glue that holds the cloud's components together and enables their orchestration. Since not everyone wants to write programs to manage their cloud, web consoles provide visual interfaces. In many cases web consoles merely use the same APIs you can access directly.
Reference: CSA Security Guidelines V.4 (reproduced here for the educational purpose)

Question: 25

Identifying the specific threats against servers and determine the effectiveness of existing security controls in counteracting the threats. is known as:

A. Risk Mitigation
B. Risk Assessment
C. Risk Management
D. Risk Determination

Answer: C

Explanation:
like this, which has similar-looking answers should be carefully answered
Risk Management is overall process which covers from identifying threats to ultimately review the effectiveness of the controls.

Question: 26

You, as a cloud customer, will more control on event and diagnostic data in SaaS environment than in the PaaS or IaaS environment.

A. True
B. False

Answer: B

Explanation:
This is false because it will be exactly opposite. In SaaS environment, you will least amount of controls on event and diagnostic data. Your control will, in fact, increase as you for from SaaS to PaaS and eventually, in IaaS, you will have full control Event and diagnostic data (except of platform logs which is maintained by the cloud service provider).

Question: 27

Which of the following is most commonly used to program Application Programming Interface(API)?

A. SOAP
B. JSON
C. HTTP
D. REST

Answer: D

Explanation:
APIs are typically REST for cloud services, since REST is easy to implement across the Internet. REST APIs have become the standard for web-based services since they run over Hl'-P/S and thus work well across diverse environments.
Reference: CSA Security GuidelinesV.4 (reproduced here for the educational purpose)

Question: 28

In cloud services. risks and responsibilities are shared between the cloud provider and customer. however. which of the following holds true?

A. Cloud provider has ultimate legal liability for unauthorised and illicit data disclosures
B. Cloud Customer liability is limited to financial responsibility
C. Cloud Provider liability is limited to financial responsibility
D. Cloud Customer has ultimate legal liability for unauthorised and illicit data disclosures

Answer: D

Explanation:

In a shared responsibility model. Data security is responsibility of the cloud consumer and he is legally liable.

Question: 29

Credentials and cryptographic keys must not be embedded in source code or distributed in public facing repositories such as GitHub.

A. True
B. False

Answer: A

Explanation:
This is true. Credentials and cryptographic keys must not be embedded in source code or distributed in public facing repositories such as GitHub, because there is a significant chance of discovery and misuse. Keys need to be appropriately secured and a well- secured public key infrastructure (PKI) is needed to ensure key-management activities are carried out.

Question: 30

In Platform as a Service (PaaS), platform security is a responsibility of:

A. Customer
B. Cloud service provider
C. It's a shared responsibility
D. Neither of them

Answer: C

Explanation:
This is a very confusing question and we need to understand that its a shared responsibility between cloud service provider and customer.