



CERTBULL
FREEDOM TO RISE AND INSPIRE

CSA CCSK

CERTIFICATE OF CLOUD SECURITY KNOWLEDGE

note:

Please be aware that these free files might not be up to date. Before your exam, ensure you review our Ultra Premium File Section for the latest materials.

www.certbull.com

Warning: Keep connected with our support team
for latest updates once you are ready

QUESTION NO: 1

Which statement best describes the impact of Cloud Computing on business continuity management?

- A. Customers of SaaS providers in particular need to mitigate the risks of application lock-in.
- B. A general lack of interoperability standards means that extra focus must be placed on the security aspects of migration between Cloud providers.
- C. Clients need to do business continuity planning due diligence in case they suddenly need to switch providers.
- D. The size of data sets hosted at a Cloud provider can present challenges if migration to another provider becomes necessary.
- E. Geographic redundancy ensures that Cloud Providers provide highly available services

QUESTION NO: 2

Even with immutable infrastructures, the production environment should be actively monitored for changes and deviations from approved baselines.

- A. False
- B. True

QUESTION NO: 3

Which of the following items is NOT an example of Security as a Service (SecaaS)?

- A. Provisioning
- B. Spam filtering
- C. Web filtering
- D. Authentication
- E. Intrusion detection

QUESTION NO: 4

CCM: Which of the following statement about CSA's CCM and Security Guidance is False?

- A. CSA's Security Guidance provides a set of best practices and recommendations.
- B. CSA's Security Guidance tells you WHAT to do, the CCM tells you HOW to do it
- C. CSA's CCM provides a set of control objective against which an organization should assess cloud security.
- D. CSA's CCM tells you WHAT to do, the Guidance tells you HOW to do it

QUESTION NO: 5

Why is a service type of network typically isolated on different hardware?

- A. It has distinct functions from other networks
- B. It requires distinct access controls**
- C. It manages the traffic between other networks
- D. It manages resource pools for cloud consumers
- E. It requires unique security

QUESTION NO: 6

The NIST defines cloud computing in part by describing five essential characteristics which are: broad network access, rapid elasticity, resource pooling, measured service and which of the following?

- A. separate hardware for all cloud customers
- B. multi-tenancy for all users
- C. publicly shared resources for all customers
- D. standardized auditing for all customers
- E. On-demand self-service access for users**

QUESTION NO: 7

ENISA: Because it is practically impossible to process data in encrypted form, customers should have the following expectation of cloud providers:

- A. Provider should be PCI compliant
- B. Provider should immediately notify customer whenever data is in plaintext form
- C. Provider must be highly trustworthy and have compensating controls to protect customer data when it is in plaintext form**
- D. Homomorphic encryption should be implemented where necessary
- E. Provider should always manage customer encryption keys with hardware security module (HSM) storage

QUESTION NO: 8

When investigating an incident in an Infrastructure as a Service (IaaS) environment, what can the user investigate on their own?

- A. The CSP office spaces
- B. The network components controlled by the CSP
- C. The logs of all customers in a multi-tenant cloud
- D. Their own virtual instances in the cloud**
- E. The CSP server facility

QUESTION NO: 9

Which data security control is the LEAST likely to be assigned to an IaaS provider?

- A. Encryption solutions
- B. Application logic**
- C. Physical destruction
- D. Access controls
- E. Asset management and tracking

QUESTION NO: 10

The Software Defined Perimeter (SDP) includes which components?

- A. Controller, Firewall, and Gateway
- B. Client, Firewall, and Gateway
- C. Client, Controller, Firewall, and Gateway
- D. Client, Controller, and Firewall
- E. Client, Controller, and Gateway**

QUESTION NO: 11

A key element of the "Destroy" phase of the Data Security Lifecycle is

- A. Encryption
- B. Crypto-Shredding**
- C. Classify
- D. Assign Rights
- E. Application Security

QUESTION NO: 12

To increase network isolation, you should use SDN capabilities for multiple networks and cloud accounts or segments.

- A. False
- B. True**

QUESTION NO: 13

Big data includes high volume, high variety, and high velocity.

- A. False
- B. True**

QUESTION NO: 14

Regardless of the technology platform, container security does not include securing the tasks or code running inside the container.

- A. False**

B. True

QUESTION NO: 15

Which concept is a mapping of an identity, including roles, personas, and attributes, to an authorization?

- A. Authoritative source
- B. Access control
- C. Entitlement
- D. Federated Identity Management
- E. Authentication

QUESTION NO: 16

What are the three main aspects for data security controls?

- A. Managing, securing, and enforcing
- B. Gating, encrypting, and backing up
- C. Controlling, monitoring, and managing
- D. Controlling, encrypting, and managing
- E. Controlling, protecting, and enforcing

QUESTION NO: 17

Who is responsible for the security of the physical infrastructure and virtualization platform?

- A. It depends on the agreement
- B. The cloud consumer
- C. The responsibility is split equally
- D. The majority is covered by the consumer
- E. The cloud provider

QUESTION NO: 18

Which of the following cloud deployment models represents a composition of two or more clouds that remain unique identities but are bound together by standardized or proprietary technology that enables data and application portability?

- A. Public cloud
- B. Hybrid cloud
- C. Community cloud
- D. Segregated cloud
- E. None of the above

QUESTION NO: 19

ENISA: Lock-In is ranked as a high risk in ENISA research, a key underlying vulnerability causing lock-in is

- A. No source escrow agreement
- B. Lack of completeness and transparency in terms of use
- C. Unclear asset ownership
- D. Lack of information on jurisdictions
- E. Audit or certification not available to customers

QUESTION NO: 20

All cloud services utilize virtualization technologies.

- A. False
- B. True

QUESTION NO: 21

CCM: In the CCM tool, a is a measure that modifies risk and includes any process, policy, device, practice or any other actions which modify risk.

- A. Domain
- B. Risk Impact
- C. Control Specification

QUESTION NO: 22

On a public cloud, all communications between cloud services occurs on the same provider network to support customer monitoring and filtering.

- A. False
- B. True

QUESTION NO: 23

Audits should be robustly designed to reflect best practice, appropriate resources, and tested protocols and standards. They should also use what type of auditors?

- A. Auditors working in the interest of the cloud customer
- B. Independent auditors
- C. Certified by CSA
- D. Auditors working in the interest of the cloud provider
- E. None of the above

QUESTION NO: 24

What are the three valid options for protecting data as it moves to and within the cloud?

- A. Password Encryption, Link/Network Encryption, Proxy-Based Encryption
- B. Client/Application Encryption, Link/Network Encryption, Hypervisor Encryption
- C. Client/Application Encryption, Cloud Encoding, Proxy-Based Encryption
- D. Client/Application Bundling, Link/Network Bundling, Proxy-Based Bundling
- E. Client/Application Encryption, Link/Network Encryption, Proxy Based Encryption

QUESTION NO: 25

CCM: A hypothetical company called "Security4Sure" provides a cloud based service to share confidential documents. The confidential documents are stored in their servers and are encrypted. How will Security4Sure ensure the protection of client data within their data center?

- A. Audit plans should not be adopted and supported by the most senior governing elements of the organization (e.g. the board and the management)
- B. Implement redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and various security devices
- C. Use a secure transfer channel (i.e.TLS)
- D. Encrypt the data at rest and put in place appropriate measures for management of encryption keys

QUESTION NO: 26

What is known as the interface used to connect with the metastructure and configure the cloud environment?

- A. Single sign-on
- B. Identity and Access Management
- C. Management plane
- D. Cloud dashboard
- E. Administrative access

QUESTION NO: 27

The key concern of data location is:

- A. Data is located only on redundant storage subsystems with high MTBF (mean time between failures)
- B. Data is stored only in geographic locations permitted by regulations
- C. Assurance that all data requested by legal authorities has been retrieved
- D. Assurance that prohibited locations cannot access the data
- E. Data should not be commingled with other customers

QUESTION NO: 28

What is a method used to decouple the network control plane from the data plane?

- A. Network Intrusion Detection Systems (NIDS)
- B. Software Defined Networking (SDN)**
- C. Information Management Policies
- D. Multi-tenancy
- E. Virtual LANs (VLANs)

QUESTION NO: 29

In which layer is the management plane?

- A. Infostructure layer
- B. Metastructure layer**
- C. Applistructure layer
- D. Overstructure layer
- E. Infrastructure layer

QUESTION NO: 30

What are the NIST defined essential characteristics of cloud computing?

- A. Broad network access, automatic patching, compliance readiness, and resource pooling
- B. Broad network access, rapid elasticity, measured service, on demand self-service, and resource pooling**
- C. Rapid elasticity, compliance readiness, and resource pooling
- D. Broad network access, measured service, multifactor configurability, and resource pooling
- E. Broad network access, rapid elasticity, automatic patching, and resource pooling

QUESTION NO: 31

Which of the following statements best describes the potential advantages of security as a service?

- A. The standardization of security software makes the outsourcing of security as a service nearly obsolete.
- B. The advantages may include flexible offering of services, greater security domain knowledge and efficiency of SecaaS providers.**
- C. The advantages are not realized until a security breach actually occurs. At that time the greater response of the security team should be obvious.
- D. Many areas of security as a service are ripe for adoption with the notable exceptions of anti-malware and anti-spam programs.

E. The higher costs and reduced flexibility are more than compensated for by the ability to pass the security responsibilities on to another firm.

QUESTION NO: 32

While the cloud consumer is responsible for implementing the security controls, the cloud provider implements the security of the workload.

A. False

B. True

QUESTION NO: 33

Cloud services exhibit five essential characteristics that demonstrate their relation to, and differences from, traditional computing approaches. Which one of the five characteristics is described as: a consumer can unilaterally provision computing capabilities such as server time and network storage as needed.

A. Broad network access

B. Rapid elasticity

C. Measured service

D. Resource pooling

E. On-demand self-service

QUESTION NO: 34

What are the components of an encryption system?

A. User, data, and encryption engine

B. Data, encryption engine, and decryption tool

C. User, encryption engine, and key management

D. User, data, and key management

E. Data, encryption engine, and key management

QUESTION NO: 35

ENISA: A reason for risk concerns of a cloud provider being acquired is

A. Provider may change physical location

B. Arbitrary contract termination by acquiring company

C. Mass layoffs may occur

D. Resource isolation may fail

E. Non-binding agreements put at risk

QUESTION NO: 36

All assets require the same continuity in the cloud.

A. False

B. True

QUESTION NO: 37

When configured properly, logs can track every code, infrastructure, and configuration change and connect it back to the submitter and approver, including the test results.

- A. False
- B. True**

QUESTION NO: 38

Why do blind spots occur in a virtualized environment, where network-based security controls may not be able to monitor certain types of traffic.

- A. The network stack is out of alignment
- B. Clouds do not occur in networked environments
- C. Traffic is undetectable in virtual machines
- D. Virtual machines may communicate with each other over a virtual network all on the same host rather than a physical network between servers**
- E. None of the above

QUESTION NO: 39

Which of the following items is one of the major regulatory compliance problems associated with cloud environments?

- A. The distributed nature of cloud storage may result in regulated information being sent across geographical boundaries**
- B. The advent of applications as a service may violate software licensing agreements
- C. The multi-tenancy model allows cloud customers to unfairly share hard drives that would otherwise have been purchased individually
- D. Transparency is improved through consolidated and centralized management platforms
- E. The lowered cost of cloud services may violate computer service embargoes

QUESTION NO: 40

What best describes the tradeoff of Infrastructure as a Service as compared to other cloud service models?

- A. Lower initial costs and greater long terms costs**
- B. Greater security features and less extensibility
- C. Less security features and greater extensibility
- D. Greater initial costs and greater security features
- E. Lower initial cost and greater security features

QUESTION NO: 41

Absent other evidence, such as tampering or hacking, documents should not be considered more or less admissible or credible because they were created or stored in the cloud.

- A. False
- B. True**

QUESTION NO: 42

Cloud provider contract enforceability should be carefully considered in light of

- A. Foreign and out of state jurisdictions**
- B. Provider controls proving inadequate for customer risks
- C. Provider key management systems
- D. Pre-production cloud deployments
- E. Costs

QUESTION NO: 43

Vulnerability assessments cannot be easily integrated into CI/CD pipelines because of provider restrictions.

- A. False**
- B. True

QUESTION NO: 44

A security failure at the root network of a cloud provider will not compromise the security of all customers because of multitenancy configuration.

- A. False**
- B. True

QUESTION NO: 45

Network logs from cloud providers are typically flow records, not full packet captures.

- A. False
- B. True**

QUESTION NO: 46

For cloud consumers to be able to properly configure and manage their network security, what must cloud providers do?

- A. Configure a default deny and enable controls as requested
- B. Provide administrator access to the tenant
- C. Expose security controls**

- D. Provide security templates
- E. Provide API access

QUESTION NO: 47

CCM: Cloud Controls Matrix (CCM) is a completely independent cloud assessment toolkit that does not map any existing standards.

- A. False
- B. True

QUESTION NO: 48

At a minimum, how often should incident response testing occur?

- A. Semi-annually
- B. Quarterly
- C. Annually and whenever a significant change occurs
- D. Whenever an event occurs
- E. Monthly

QUESTION NO: 49

When attempting to contain, eradicate, and recover from a cloud based incident, what is the first step you should do?

- A. Terminate all super user/administrative access
- B. Make sure the cloud management plane is free of an attacker
- C. Isolate the infected devices
- D. Put the device in stand by mode
- E. Kill all network access

QUESTION NO: 50

What is a challenge of application security in a cloud environment?

- A. Non-unified interface
- B. Limited detailed visibility
- C. Isolated environments
- D. Responsiveness
- E. Decreased application scope

QUESTION NO: 51

Sending data to a provider's storage over an API is likely as much more reliable and secure than setting up your own SFTP server on a VM in the same provider.

- A. False
- B. True

QUESTION NO: 52

Database Activity Monitoring and File Activity Monitoring are specifically recommended for what type of data migrations into the cloud?

- A. Small, stealthy data migrations
- B. Complex, long-term migrations**
- C. Small, external data migrations
- D. Large, internal data migrations
- E. Simple, homogenous migrations

QUESTION NO: 53

When associating the functions to an actor, what is used to restrict a list of possible actions down to allowed actions?

- A. Location
- B. Functions
- C. Permissions**
- D. Controls
- E. Actions

QUESTION NO: 54

Which process is used to break up data and store the information on multiple copies on different physical storage for higher durability?

- A. Data displacement
- B. Data diversion
- C. Data segregation
- D. Data crypting
- E. Data dispersion**

QUESTION NO: 55

If a provider's infrastructure is not in scope, who is responsible for building compliant applications and services?

- A. No one. It is an accepted risk that is written into the terms and conditions with customers.
- B. The provider must update or fix whatever is not in compliance.
- C. It is up to the customer and provider to negotiate the solution.
- D. The provider must create a separate tenant for each customer based on the various compliance regulations.
- E. The customer is responsible for compliant applications and services.**

QUESTION NO: 56

Generally speaking, in the United States, a party is obligated to take reasonable steps to prevent the destruction or modification of data in its possession that it reasonably should know, is relevant to an anticipated litigation or government investigation.

- A. False
- B. True**

QUESTION NO: 57

Which of the following is a perceived advantage or disadvantage of managing enterprise risk for cloud deployments?

- A. More physical control over assets and processes
- B. Greater reliance on contracts, audits, and assessments due to lack of visibility or management**
- C. Decreased requirement for proactive management of relationship and adherence to contracts
- D. Increased need, but reduction in costs, for managing risks accepted by the cloud provider
- E. None of the above

QUESTION NO: 58

When the application components communicate directly with the cloud service, the management plane and metastructure might fall within the application security scope.

- A. False
- B. True**

QUESTION NO: 59

Which of the following statements best describes an identity federation?

- A. Identities which share similar attributes
- B. A library of data definitions
- C. Several countries which have agreed to define their identities with similar attributes
- D. The connection of one identity repository to another**
- E. A group of entities which have decided to exist together in a single cloud

QUESTION NO: 60

Security Assertion Markup Language (SAML) 2.0 is an OASIS standard for federated identity management that supports authentication and authorization.

A. False

B. True

QUESTION NO: 61

What is known as a code execution environment running within an operating system that shares and uses the resources of the operating system?

A. Virtual machine

B. Pod

C. Abstraction

D. Container

E. Platform-based Workload

QUESTION NO: 62

Which action is part of the containment phase of the incident response lifecycle?

A. Configuring and validating alerts

B. Analyzing what happened

C. Evaluating infrastructure by proactive scanning and network

D. monitoring, vulnerability assessments, and performing risk assessments

E. Making considerations for data loss versus service availability

F. Planning notification and coordination of activities

QUESTION NO: 63

How can cloud providers support a secure use of virtualization for cloud consumers?

A. By creating a secure chain of processes from the image used to run the VM through to a boot process with security and integrity.

B. By locking, denying, or preventing access and then gradually enabling items as needed

C. By providing professional services to assist the consumer with configurations

D. Unfortunately, this is not a possible option for cloud consumers

E. By enabling full access to the consumer

QUESTION NO: 65

When mapping functions to lifecycle phases, which functions are required to successfully process data?

A. Create, Store, Use, and Share

B. Create, Use, Store, and Delete

C. Create, Store, and Use

D. Create and Store o

E. Create and Use

QUESTION NO: 66

Identified issues, risks, and recommended remediations are included when determining compliance.

A. True

B. False

QUESTION NO: 67

Which layer is the most important for securing because it is considered to be the foundation for secure cloud operations?

A. Metastructure

B. Datastructure

C. Infostructure

D. Applistructure

E. Infrastructure

QUESTION NO: 68

Who is responsible for the security of the physical infrastructure and virtualization platform?

A. The majority is covered by the consumer

B. It depends on the agreement

C. The cloud consumer

D. The responsibility is split equally

E. The cloud provider

QUESTION NO: 69

How can web security as a service be deployed for a cloud consumer?

A. By proxying or redirecting web traffic to the cloud provider

B. By utilizing a partitioned network drive

C. On the premise through a software or appliance installation

D. Both A and C

E. None of the above

QUESTION NO: 70

Which meta-phase does the Cloud Security Alliance use to focus on the security and testing activities when moving code from an isolated development environment to production?

A. Secure Design and Development

B. Secure Scaling

C. Secure Deployment

D. Secure Networking

E. Secure Operations

QUESTION NO: 71

What is the most important reason for knowing where the cloud service provider will host the data?

A. To enable data location transparency for the consumer.

B. To allow compliance with local laws regarding data privacy and safeguarding.

C. Such knowledge is a prerequisite to implementing the required measures to ensure compliance with local laws that restrict the crossborder flow of data.

D. To facilitate comprehensive disaster planning.

E. Enable the data controller to register with the local Data Protection Officer(s), where appropriate.

QUESTION NO: 72

Which SDP component terminates network traffic and enforces communication policies?

A. Client

B. Access Manager

C. Gateway

D. Firewall

E. Controller

QUESTION NO: 73

Database Activity Monitoring and File Activity Monitoring are specifically recommended for what type of data migrations into the cloud?

A. Simple, homogenous migrations

B. Large, internal data migrations

C. Small, stealthy data migrations

D. Small, external data migrations

E. Complex, long-term migrations

QUESTION NO: 74

Because virtual networks are software constructs, the use of multiple separate virtual networks might offer extensive compartmentalization advantages not possible on traditional physical networks.

A. True

B. False

QUESTION NO: 75

CCM: The Architectural Relevance column in the CCM indicates the applicability of the cloud security control to which of the following elements?

- A. SaaS, PaaS or IaaS
- B. Physical, Network, Compute, Storage, Application or Data
- C. Service Provider or Tenant/Consumer

QUESTION NO: 76

Which phase of the incident response lifecycle includes creating and validating alerts?

- A. Preparation
- B. Post-mortem
- C. Auditing & Logging
- D. Containment, Eradication, Recovery
- E. Detection & Analysis

QUESTION NO: 77

What are the primary security responsibilities of the cloud consumer in the management infrastructure?

- A. Building and properly configuring a secure network infrastructure
- B. Providing as many API endpoints as possible for custom access and configurations
- C. Properly configuring the deployment of the virtual network, except the firewalls
- D. Configuring second factor authentication across the network
- E. Properly configuring the deployment of the virtual network, especially the firewalls

QUESTION NO: 78

What is a benefit of application security in a cloud environment?

- A. Increased application scope
- B. Reduced transparency
- C. Non-unified interface
- D. Isolated environments
- E. Limited detailed visibility

QUESTION NO: 79

ENISA: As it relates to public cloud computing, in the European Data Protection law, the customer is considered to be the:

- A. Data controller
- B. Data manager
- C. Data processor
- D. Data owner
- E. Certificate holder

QUESTION NO: 80

In the case of Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) the responsibility to effectively manage the security of the application running in the cloud primarily belongs to who?

- A. The cloud consumer's administrators
- B. The government
- C. The software as a service (SaaS) provider
- D. The provider's system administrators
- E. The internet service provider (ISP)

QUESTION NO: 81

What is the best way to ensure that all data has been removed from a public cloud environment including all media such as back-up tapes?

- A. Allowing the cloud provider to manage your keys so that they have the ability to access and delete the data from the main and back-up storage.
- B. Maintaining customer managed key management and revoking or deleting keys from the key management system to prevent the data from being accessed again.
- C. Practice Integration of Duties (IOD) so that everyone is able to delete the encrypted data.
- D. Keep the keys stored on the client side so that they are secure and so that the users have the ability to delete their own data.
- E. Both B and D.

QUESTION NO: 82

What type of information is contained in the Cloud Security Alliance's Cloud Control Matrix?

- A. The command and control management hierarchy of a typical cloud company
- B. A list of cloud configurations including traffic logic and efficient routes
- C. Federal legal business requirements for all cloud operators
- D. A number of requirements to be implemented, based upon numerous standards and regulatory requirements
- E. Network traffic rules for cloud environments

QUESTION NO: 83

The level of attention and scrutiny paid to enterprise risk assessments should be directly related to what?

- A. The size of the cloud computing environment
- B. The value of the information at risk
- C. The operating system and firewall type
- D. Whether the cloud is IaaS, PaaS, or SaaS
- E. Both A and C

QUESTION NO: 84

CCM: A hypothetical company called "InfrastructureASure" provides Infrastructure as a Service (IaaS) to its clients. A customer wants to review InfrastructureASure's hypervisor security implementation measures. Which of the following measures should InfrastructureASure implement?

- A. Choose a hypervisor with a smaller footprint for a reduced attack surface.
- B. Harden the hypervisor's configuration to increase areas of vulnerability (e.g., disabling memory sharing between VMs running within the same hypervisor hosts).
- C. Connect unused physical hardware devices and enable clipboard or file-sharing services.
- D. Monitor for signs of compromise by analyzing hypervisor logs on an ongoing basis.
- E. A and D

QUESTION NO: 85

For third-party audits or attestations, what is critical for providers to publish and customers to evaluate?

- A. Scope of the assessment and the exact included features and services for the assessment
- B. Full API access to all required services
- C. Service-level agreements between all parties
- D. Provider infrastructure contracts information including maintenance windows and contracts
- E. Network or architecture diagrams including all end point security devices in use

QUESTION NO: 86

What makes single cloud assets less resilient compared with a traditional infrastructure?

- A. API access
- B. Not scalable
- C. Greater fragility of virtualized resources
- D. Less cost effective
- E. Less management oversight

QUESTION NO: 87

A cloud deployment of two or more unique clouds is known as:

- A. Infrastructures as a Service
- B. Jericho Cloud Cube Model
- C. A Hybrid Cloud
- D. A Private Cloud
- E. A Community Cloud

QUESTION NO: 88

In which type of environment is it impractical to allow the customer to conduct their own audit, making it important that the data center operators are required to provide auditing for the customers?

- A. Single tenant environments
- B. Long distance relationships
- C. Multi-tenant environments
- D. Distributed computing arrangements
- E. Multi-application, single tenant environments

QUESTION NO: 89

Which architecture for hybrid cloud connectivity allows you to connect multiple, different cloud networks to a data center using a single hybrid connection?

- A. Hybrid
- B. Multiconnect
- C. Transitional
- D. Dataconnect
- E. Bastion

QUESTION NO: 90

Which security advantage considers that anything that goes into production is created by the CI/CD pipeline on approved code and configuration templates?

- A. Standardization
- B. SecDevOps/DevSecOps and Rugged DevOps
- C. Immutable**
- D. Improved auditing and change management
- E. Automated testing

QUESTION NO: 91

In which deployment model do cloud customers have a reduced ability to govern operations because the cloud provider is responsible for the management and governance of the infrastructure?

- A. Public Cloud**
- B. Hybrid Cloud
- C. Community Cloud
- D. Hosted Cloud
- E. Private Cloud

QUESTION NO: 92

Which common component of big data is focused on the mechanisms used to ingest large volumes of data, often of a streaming nature?

- A. Distributed data collection**
- B. Distributed information
- C. Distributed processing
- D. Distributed attribution
- E. Distributed storage

QUESTION NO: 93

Your SLA with your cloud provider ensures continuity for all services.

- A. True
- B. False**

QUESTION NO: 94

ENISA: To mitigate credential compromise or theft, cloud provider can implement:

- A. HR background checks
- B. Anomaly detection capabilities**
- C. Portable applications using open APIs
- D. Hardening of virtual machines according to industry standard guidelines.
- E. Data-at-rest encryption

QUESTION NO: 95

Which of the following is one of the five essential characteristics of cloud computing as defined by NIST?

- A. Multi-tenancy
- B. Hybrid clouds
- C. Unlimited bandwidth
- D. Nation-state boundaries
- E. Measured service

QUESTION NO: 96

What are the primary security responsibilities of the cloud provider in compute virtualizations?

- A. Enforce isolation and maintain a secure virtualization infrastructure
- B. Enforce isolation and monitor and log workloads
- C. Maintain a secure virtualization infrastructure and configure the security settings
- D. Monitor and log workloads and configure the security settings
- E. Enforce isolation and configure the security settings

QUESTION NO: 97

Without virtualization, there is no cloud.

- A. True
- B. False

QUESTION NO: 98

CCM: In the CCM tool, a _____ is a measure that modifies risk and includes any process, policy, device, practice or any other actions which modify risk.

- A. Control Specification
- B. Risk Impact
- C. Domain

QUESTION NO: 99

Which statement best describes the options for PaaS encryption?

- A. PaaS is very diverse and would most likely include file/folder and instance-managed encryption.
- B. PaaS is limited to public networks.
- C. PaaS is very diverse and may include client/application, database, and proxy encryption as well as other options.

- D. PaaS is sensitive to application updates and therefore must be constantly refreshed with relevant keys.
- E. PaaS is strictly limited to client/application, database and proxy encryption.

QUESTION NO: 100

Consumers of Infrastructure as a Service (IaaS) are primarily responsible for containment, eradication, and recovery from incidents.

- A. True
- B. False

QUESTION NO: 101

Which of the following is NOT a method of object storage encryption?

- A. Externally managed encryption
- B. Client/application encryption
- C. Proxy encryption
- D. File/folder encryption
- E. Enterprise digital rights management

QUESTION NO: 102

Which regulation affects data controllers with business in Japan?

- A. Act on the Protection of Personal Information
- B. General Data Protection Regulation (GDPR)
- C. 1995 Data Protection Directive
- D. Personal Information Protection and Electronic Documents Act (PIPEDA)
- E. Privacy Act 1988

QUESTION NO: 103

Which concept is defined as the unique expression of an entity within a given namespace?

- A. Identity
- B. Role
- C. Attribute
- D. Persona
- E. Identifier

QUESTION NO: 104

How can key management be leveraged to prevent cloud providers from inappropriately accessing customer data?

- A. Use strong multi-factor authentication
- B. Select cloud providers within the same country as customer

- C. Stipulate encryption in contract language
- D. Secure backup processes for key management systems
- E. Segregate keys from the provider hosting data

QUESTION NO: 105

CCM: A company wants to use the IaaS offering of some CSP. Which of the following options for using CCM is NOT suitable for the company as a cloud customer?

- A. Submit the CCM on behalf of the CSP to CSA Security, Trust & Assurance Registry (STAR), a free, publicly accessible registry that documents the security controls provided by CSPs.
- B. Use CCM to build a detailed list of requirements and controls that they want their CSP to implement.
- C. Use CCM to help assess the risk associated with the CSP.
- D. None of the above

QUESTION NO: 106

Which security concept includes the policy, process, and internal controls comprising how an organization is run - including the structures and policies of the leadership and other mechanisms for management?

- A. Compliance
- B. Information risk management
- C. Enterprise risk management
- D. Information security
- E. Governance

QUESTION NO: 107

What factor(s), if any, allows for more efficient and effective containment and recovery in a cloud environment than in a non-cloud environment.

- A. Virtualization technologies, and the elasticity inherent in cloud computing platforms
- B. no part of incident response is easier in a cloud environment
- C. frequent back-up routines
- D. encrypted data files
- E. multi-tenancy and software as a service models

QUESTION NO: 108

You have a business relationship with a cloud provider for all sales management functionality. Through the APIs and SDKs, you have customized the interface and some functionality, but the back end service is done through the cloud provider. In this relationship, which service is completed by the cloud provider?

- A. Software-as-a-service (SaaS)
- B. Desktop-as-a-service (DaaS)
- C. Infrastructure-as-a-service (IaaS)
- D. Identity-as-a-service (IDaaS)
- E. Platform-as-a-service (PaaS)

QUESTION NO: 109

IaaS volume storage encryption protects from which following security risk(s)?

- A. Protects volumes from snapshot cloning/exposure
- B. Protects volumes from being moved to another part of the cloud
- C. Protects volumes from being viewed by the cloud provider's employees
- D. Both A and B
- E. Both A and C

QUESTION NO: 110

Which deployment model is commonly used to describe a non-cloud data center bridged directly to a cloud provider?

- A. Public Cloud
- B. Hybrid Cloud
- C. Community Cloud
- D. Hosted Cloud
- E. Private Cloud

QUESTION NO: 111

You should disable remote access when working with immutable workloads.

- A. True
- B. False

QUESTION NO: 112

A defining set of rules composed of claims and attributes of the entities in a transaction, which is used to determine their level of access to cloud-based resources is called what?

- A. An access log
- B. A support table
- C. An entry log
- D. A validation process
- E. An entitlement matrix

QUESTION NO: 113

The hub and spoke architecture uses internal identity providers or sources connected directly to cloud providers.

- A. True
- B. False**

QUESTION NO: 114

Which security advantage considers that CI/CD pipelines can track everything, down to individual character changes in source files tied to the person submitting the change, with the entire application stack history?

- A. Standardization
- B. SecDevOps/DevSecOps and Rugged DevOps
- C. Immutable
- D. Improved auditing and change management**
- E. Automated testing

QUESTION NO: 115

What are six phases of the Data Security Lifecycle?

- A. Create, Classify, Use, Store, Retain, Destroy
- B. Assign, Define, Store, Process, Transmit, Destroy
- C. Create, Store, Use, Share, Archive, Destroy**
- D. Assign, Define, Create, Process, Store, Destroy
- E. Create, Classify, Use, Store, Archive, Destroy

QUESTION NO: 116

What makes the metastructure layer of cloud computing so different from traditional computing?

- A. It includes the data and information components.
- B. It includes the underlying application services.
- C. It is automatically patch and scalable.
- D. It eliminates the need for the Infostructure layer.
- E. It includes the management plane components, which are network enabled and remotely accessible.**

QUESTION NO: 117

What method can be utilized along with data fragmentation to enhance security?

- A. Insulation
- B. IDS
- C. Knowledge management

D. Organization

E. Encryption

QUESTION NO: 118

Compute virtualization abstracts the running of code, not including the operating systems, from the underlying hardware.

A. False

B. True

QUESTION NO: 119

What is a benefit of application security in a cloud environment?

A. Reduced transparency

B. Non-unified interface

C. Limited detailed visibility

D. Isolated environments

E. Increased application scope

QUESTION NO: 120

How should an SDLC be modified to address application security in a Cloud Computing environment?

A. Integrated development environments

B. Updated threat and trust models

C. No modification is needed

D. Just-in-time compilers

E. Both B and C

QUESTION NO: 121

Which type of application security testing tests running applications and includes tests such as web vulnerability testing and fuzzing?

A. Dynamic Application Security Testing (DAST)

B. Functional Testing

C. Unit Testing

D. Static Application Security Testing (SAST)

E. Code Review

QUESTION NO: 122

ENISA: Because it is practically impossible to process data in encrypted form, customers should have the following expectation of cloud providers:

A. Homomorphic encryption should be implemented where necessary.

B. Provider should be PCI compliant.

C. Provider should immediately notify customer whenever data is in plaintext form.

D. Provider must be highly trustworthy and have compensating controls to protect customer data when it is in plaintext form.

E. Provider should always manage customer encryption keys with hardware security module (HSM) storage.

QUESTION NO: 123

Which components typically comprise Infrastructure-as-a-Service (IaaS) providers?

A. Presentation modality, APIs, Applications, and Hardware

B. Hardware, APIs, and Core Connectivity & Delivery

C. Integration & Middleware, APIS, and Data

D. Hardware, APIs, and Data o

E. Presentation modality, APIs, Applications, and Data

QUESTION NO: 124

If the management plane has been breached, you should confirm the templates/configurations for your infrastructure or applications have not also been compromised.

A. False

B. True

QUESTION NO: 125

What is true about the security for a private cloud platform in the shared security model?

A. The provider and consumer split the security responsibilities

B. Whoever maintains the platform must ensure all layers are secure

C. The cloud consumer must ensure all layers are secure

D. The responsibility of security depends on the platform layer

E. The cloud provider must ensure all layers are secure

QUESTION NO: 126

Select the statement below which best describes the relationship between identities and attributes.

A. Identities are the network names given to servers. Attributes are the characteristics of each server.

B. Attributes are made unique by their identities.

C. An identity is a distinct and unique object within a particular namespace. Attributes are properties which belong to an identity. Each identity can have multiple attributes.

D. An attribute is a unique object within a database. Each attribute it has a number of identities which help define its parameters.

E. Attributes belong to entities and identities belong to attributes. Each attribute can have multiple identities but only one entity.

QUESTION NO: 127

If in certain litigations and investigations, the actual cloud application or environment itself is relevant to resolving the dispute in the litigation or investigation, how is the information likely to be obtained?

A. It would never be obtained in this situation

B. It would require a previous contractual agreement to obtain the application or access to the environment.

C. It would require an act of war

D. It would require a previous access agreement

E. It may require a subpoena of the provider directly

QUESTION NO: 128

Which statement best describes a data (information) dispersion fragmentation scheme?

A. A file is split into fragments; all of the fragments are sent to multiple physical storage repositories.

B. A network is split into nodes; all of the nodes store only certain types of files.

C. Fragmented files are signed and stored together on a local server; data retrieval is arbitrary.

D. File fragments are sequentially placed on servers based on the physical location of the data user.

E. A cloud is split into cloudlets; each cloudlet stores a portion of the files based on an encryption algorithm.

QUESTION NO: 129

Which of the following cloud deployment models represents a composition of two or more clouds that remain unique identities but are bound together by standardized or proprietary technology that enables data and application portability?

A. Public cloud

B. Hybrid cloud

C. Community cloud

- D. Segregated cloud
- E. None of the above

QUESTION NO: 130

Immutable workloads make it faster to roll out updated versions because applications must be designed to handle individual nodes going down.

- A. False
- B. True

QUESTION NO: 131

Which of the following is NOT a common storage option with Infrastructure as a Service.

- A. Volume Storage
- B. Content Delivery Network
- C. Big Data as a Service
- D. Object Storage
- E. SSD based volume storage

QUESTION NO: 132

Which facet is focused on protecting the management plane components, such as web and API servers, from attacks?

- A. Logging and alerting
- B. Customer authentication
- C. Perimeter security
- D. Authorization and entitlements
- E. External authentication

QUESTION NO: 133

In volume storage, what method is often used to support resiliency and security?

- A. data rights management
- B. hypervisor agents
- C. proxy encryption
- D. data dispersion
- E. random placement

QUESTION NO: 134

Which of the following statements are NOT requirements of governance and enterprise risk management in a cloud environment?

- A. Inspect and account for risks inherited from other members of the cloud supply chain and take active measures to mitigate and contain risks through operational resiliency.
- B. Respect the interdependency of the risks inherent in the cloud supply chain and communicate the corporate risk posture and readiness to consumers and dependent parties.
- C. Negotiate long-term contracts with companies who use well-vetted software applications to avoid the transient nature of the cloud environment.
- D. Provide transparency to stakeholders and shareholders demonstrating fiscal solvency and organizational transparency.
- E. Both B and C

QUESTION NO: 135

Which of the following is NOT a cloud computing characteristic that impacts incidence response?

- A. Privacy concerns for co-tenants regarding the collection and analysis of telemetry and artifacts associated with an incident.
- B. The possibility of data crossing geographic or jurisdictional boundaries
- C. The on demand self-service nature of cloud computing environments
- D. Object-based storage in a private cloud
- E. The resource pooling practiced by cloud services, in addition to the rapid elasticity offered by cloud infrastructures

QUESTION NO: 136

Which concept provides the abstraction needed for resource pools?

- A. Applistructure
- B. Hypervisor
- C. Virtualization
- D. Metastructure
- E. Orchestration

QUESTION NO: 137

When associating the functions to an actor, what is used to restrict a list of possible actions down to allowed actions?

- A. Controls
- B. Location
- C. Functions
- D. Permissions
- E. Actions

QUESTION NO: 138

Of the choices below which option allows for the most interoperability in security authentication in a cloud environment?

- A. SAML
- B. SCORM
- C. WEP
- D. XHTML
- E. WPA or WPA-2

QUESTION NO: 139

CCM: The following list of controls belong to which domain of the CCM? GRM 06 - Policy GRM 07 - Policy Enforcement GRM 08 - Policy Impact on Risk Assessments GRM 09 - Policy Reviews GRM 10 - Risk Assessments GRM 11 - Risk Management Framework

- A. Governance and Retention Management
- B. Governance and Risk Management
- C. Governing and Risk Metrics

QUESTION NO: 140

Virtual appliances can become bottlenecks because they cannot fail open and must intercept all traffic.

- A. False
- B. True

QUESTION NO: 141

ENISA: which of the following is among the vulnerabilities contributing to a high risk ranking for Network Management?

- A. System or O/S vulnerabilities
- B. Hypervisor vulnerabilities
- C. AAA vulnerabilities
- D. Inadequate physical security procedures
- E. User provisioning vulnerabilities

QUESTION NO: 142

When deploying Security as a Service in a highly regulated industry or environment, what should both parties agree on in advance and include in the SLA?

- A. The duration of time that a security violation can occur before the client begins assessing regulatory fines.
- B. The cost per incident for security breaches of regulated information

C. The metrics defining the service level required to achieve regulatory objectives

D. The regulations that are pertinent to the contract and how to circumvent them

E. The type of security software which meets regulations and the number of licenses that will be needed

QUESTION NO: 143

What method can be utilized along with data fragmentation to enhance security?

A. Insulation

B. IDS

C. Knowledge management

D. Organization

E. Encryption

QUESTION NO: 144

Which governance domain focuses on proper and adequate incident detection, response, notifications, and remediation?

A. Infrastructure Security

B. Compliance and Audit Management

C. Incident response, Notification and Remediation

D. Information Governance

E. Data Security and Encryption

QUESTION NO: 145

CCM: The cloud service delivery model applicability column in the CCM indicates the applicability of the cloud security control to which of the following elements?

A. Mappings to well known standards and frameworks

B. Physical, Network, Compute, Storage, Application or Data

C. Service Provider or Tenant/Consumer

D. SaaS, PaaS or IaaS

QUESTION NO: 146

What is known as the interface used to connect with the metastructure and configure the cloud environment?

A. Cloud dashboard

B. Single sign-on

C. Identity and Access Management

D. Management plane

E. Administrative access

QUESTION NO: 147

The cloud consumer has more tactical responsibility for implementing and managing security controls in which cloud service model?

- A. Platform as a service
- B. Infrastructure as a service**
- C. Jericho cloud cube model
- D. Security as a service
- E. Software as a service

QUESTION NO: 148

CCM: In the CCM tool, _____ is a measure that modifies risk and includes any process, policy, device, practice or any other actions which modify risk.

- A. Risk impact
- B. Domain
- C. Control specification**

QUESTION NO: 149

What is a more secure and cost-effective approach to data security and encryption?

- A. Initially using a deny all and locking everything down until requirements are met
- B. Applying a data-driven approach
- C. Applying a risk-based approach**
- D. Using the same policies applied to the traditional network
- E. Applying a blanket security policy to anything cloud

QUESTION NO: 150

What is the order of the main phases of secure application design and development?

- A. Train, Analyse, Develop, Test, Implement
- B. Analyse, Design, Develop, Test, Implement
- C. Analyse, Define, Design, Develop, Test
- D. Train, Define, Develop, Test, Implement
- E. Train, Define, Design, Develop, Test**

QUESTION NO: 151

How is encryption managed on multi-tenant storage?

- A. Single key for all data owners.
- B. One key per data owner.
- C. Multiple keys per data owner.

D. The answer could be A, B, or C depending on the provider.

E. C for data subject to the EU Data Protection Directive; B for all others.

QUESTION NO: 152

CCM: In the Identity & Access Management (IAM) domain, what does the number '04' in IAM-04 signify?

A. There are 4 controls in that particular domain

B. The control ID is a random number assigned to the control

C. It is the 4th control in the IAM domain

D. None of the above

QUESTION NO: 153

Which of the following statements is true in regards to Data Loss Prevention (DLP)?

A. DLP can provide options for quickly deleting all of the data stored in a cloud environment.

B. DLP can classify all data in a storage repository.

C. DLP never provides options for how data found in violation of a policy can be handled.

D. DLP can provide options for where data is stored.

E. DLP can provide options for how data found in violation of a policy can be handled.

QUESTION NO: 154

Which of the following is NOT a method of object storage encryption?

A. Externally managed encryption

B. File/folder encryption

C. Enterprise digital rights management

D. Proxy encryption

E. Client/application encryption

QUESTION NO: 155

Virtual appliances can become bottlenecks because they cannot fail open and must intercept all traffic.

A. False

B. True

QUESTION NO: 156

Which part of the incident response process is greatly complicated by the resource pooling and rapid elasticity of cloud infrastructure?

A. Preparation

- B. Recovery
- C. Forensics
- D. Detection
- E. Ballistics

QUESTION NO: 157

How can you reduce the blast radius if an attacker compromises one system?

- A. Configure distinct firewall rules.
- B. Use different cloud providers.
- C. Configure applications on distinct virtual networks only connecting where needed.
- D. Configure a default deny.
- E. Configure role-based access controls.

QUESTION NO: 158

What are the main considerations for key management?

- A. Performance, control, immutability, and security
- B. Accessibility, control, latency, and security
- C. Performance, accessibility, immutability, and security
- D. Performance, accessibility, latency, and security
- E. Performance, control, accessibility, and security

QUESTION NO: 159

In the cloud provider and consumer relationship, which entity manages the virtual or abstracted infrastructure?

- A. Only the cloud provider
- B. It is determined in the agreement between the entities
- C. Only the cloud consumer
- D. Both the cloud provider and consumer
- E. It is outsourced as per the entity agreement

QUESTION NO: 160

What factors should you understand about the data specifically due to legal, regulatory, and jurisdictional factors?

- A. The actual size of the data and the storage format.
- B. The implications of storing complex information on simple storage systems.
- C. The physical location of the data and how it is accessed.
- D. The language of the data and how it affects the user.
- E. The fragmentation and encryption algorithms employed.

QUESTION NO: 161

If a provider's infrastructure is not in scope, who is responsible for building compliant applications and services?

- A. The customer is responsible for compliant applications and services.
- B. It is up to the customer and provider to negotiate the solution.
- C. The provider must update or fix whatever is not in compliance.
- D. No one. It is an accepted risk that is written into the terms and conditions with customers.
- E. The provider must create a separate tenant for each customer based on the various compliance regulations.

QUESTION NO: 162

Which term is used to describe the use of tools to selectively degrade portions of the cloud to continuously test business continuity?

- A. Organized Downtime
- B. Chaos Engineering
- C. Planned Outages
- D. Expected Engineering
- E. Resiliency Planning

QUESTION NO: 163

What is defined as the process by which an opposing party may obtain private documents for use in litigation?

- A. Scope
- B. Risk Assessment
- C. Discovery
- D. Subpoena
- E. Custody

QUESTION NO: 164

How can web security as a service be deployed for a cloud consumer?

- A. By proxying or redirecting web traffic to the cloud provider
- B. By utilizing a partitioned network drive
- C. On the premise through a software or appliance installation
- D. Both A and C
- E. None of the above

QUESTION NO: 165

If in certain litigations and investigations, the actual cloud application or environment itself is relevant to resolving the dispute in the litigation or investigation, how is the information likely to be obtained?

- A. It may require a subpoena of the provider directly
- B. It would require a previous access agreement
- C. It would require an act of war
- D. It would require a previous contractual agreement to obtain the application or access to the environment.
- E. It would never be obtained in this situation

QUESTION NO: 166

How can virtual machine communications bypass network security controls?

- A. Most network security systems do not recognize encrypted VM traffic
- B. VM images can contain rootkits programmed to bypass firewalls
- C. VM communications may use a virtual network on the same hardware host
- D. Hypervisors depend upon multiple network interfaces
- E. The guest OS can invoke stealth mode

QUESTION NO: 167

Which technique uses the management plane to detect various activities, such as file uploads or configuration changes?

- A. Event-driven security
- B. Static Application Security Testing (SAST)
- C. Action security
- D. Auditing and logging
- E. Dynamic Application Security Testing (DAST)

QUESTION NO: 168

When configuring SDN firewalls, after adding all assets, what is typically the first configuration you must address?

- A. Creating update rules
- B. Configuring logging
- C. Configuring additional access
- D. Opening connections
- E. Disconnecting previous firewalls

QUESTION NO: 169

Use elastic servers when possible and move workloads to new instances.

- A. False
- B. True**

QUESTION NO: 170

Why, in the event that an enterprise seeks a new provider for Security as a Service, must they concern themselves with the problems of translating and transporting existing data and log files in a forensically sound manner?

- A. The logging and reporting files are often heavily encrypted
- B. Providers may operate in foreign languages
- C. Providers don't want to lose business so they do not help the customer move out
- D. Logging and reporting is often treated haphazardly
- E. Providers often have proprietary standards for logging and reporting**

QUESTION NO: 171

To what extent does the CSA Guidance document suffice for legal advice in setting up relationships with cloud service providers?

- A. The CSA Guidance document provides adequate legal advice under certain circumstances.
- B. The CSA Guidance document provides sufficient guidance to substitute for legal advice.
- C. The CSA Guidance document provides an overview of selected issues and it is not a substitute for obtaining legal advice.**
- D. The CSA Guidance document does not discuss any legal issues at all.
- E. The CSA Guidance document provides copious amounts of relevant case law to enable legal inferences to be developed.

QUESTION NO: 172

Which communication methods within a cloud environment must be exposed for partners or consumers to access database information using a web application?

- A. Application Programming Interface (API)**
- B. Application Binary Interface (ABI)
- C. Software Development Kits (SDKs)
- D. Extensible Markup Language (XML)
- E. Resource Description Framework (RDF)

QUESTION NO: 173

A key element of the "Destroy" phase of the Data Security Lifecycle is

- A. Application Security
- B. Classify

C. Crypto-Shredding

- D. Encryption
- E. Assign Rights

QUESTION NO: 174

Which opportunity helps reduce common application security issues?

- A. Elastic infrastructure
- B. Default deny
- C. Decreased use of micro-services
- D. Segregation by default**
- E. Fewer serverless configurations

QUESTION NO: 175

CCM: The following list of controls belong to which domain of the CCM? GRM 06 - Policy GRM 07 - Policy Enforcement GRM 08 - Policy Impact on Risk Assessments GRM 09 - Policy Reviews GRM 10 - Risk Assessments GRM 11 - Risk Management Framework

- A. Governance and Risk Management**
- B. Governance and Retention Management
- C. Governing and Risk Metrics

QUESTION NO: 176

An important consideration when performing a remote vulnerability test of a cloud-based application is to.

- A. Schedule vulnerability test at night
- B. Use network layer testing tools exclusively
- C. Obtain provider permission for test**
- D. Use application layer testing tools exclusively
- E. Use techniques to evade cloud provider's detection systems

QUESTION NO: 177

Prominent recommended standards to enable federation of identity in cloud environments include

- A. FIDO
- B. X.509
- C. Kerberos
- D. SAML**
- E. SSO

QUESTION NO: 178

Your SLA with your cloud provider ensures continuity for all services.

- A. False
- B. True

QUESTION NO: 179

Which of the following is NOT a cloud computing characteristic that impacts incidence response?

- A. The resource pooling practiced by cloud services, in addition to the rapid elasticity offered by cloud infrastructures.
- B. Object-based storage in a private cloud.
- C. The on demand self-service nature of cloud computing environments.
- D. The possibility of data crossing geographic or jurisdictional boundaries.
- E. Privacy concerns for co-tenants regarding the collection and analysis of telemetry and artifacts associated with an incident.

QUESTION NO: 180

What is true of cloud built-in firewalls?

- A. They provide identical configurations to physical firewalls
- B. They operate exclusively outside of the hypervisor
- C. They typically offer fewer features than newer physical firewalls
- D. They operate exclusively outside of the SDN
- E. Whichever features are not provided in the firewall, the cloud provider has an alternative

QUESTION NO: 181

In the case of Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) the responsibility to effectively manage the security of the application running in the cloud primarily belongs to who?

- A. The cloud consumer's administrators
- B. The provider's system administrators
- C. The internet service provider (ISP)
- D. The software as a service (SaaS) provider
- E. The government

QUESTION NO: 182

In volume storage, what method is often used to support resiliency and security?

- A. random placement
- B. data dispersion

- C. proxy encryption
- D. hypervisor agents
- E. data rights management

QUESTION NO: 183

The hub and spoke architecture uses internal identity providers or sources connected directly to cloud providers.

- A. False
- B. True

QUESTION NO: 184

In the Software-as-a-service relationship, who is responsible for the majority of the security?

- A. Application Consumer
- B. Database Manager
- C. Application Developer
- D. Cloud Provider
- E. Web Application CISO

QUESTION NO: 185

Cloud applications can use virtual networks and other structures, for hyper-segregated environments.

- A. False
- B. True

QUESTION NO: 186

Who is responsible for the proper rights management and configuration of exposed controls in the management plane?

- A. The cloud provider
- B. The responsibility is split equally
- C. The cloud consumer
- D. It depends on the agreement
- E. The majority is covered by the provider

QUESTION NO: 187

ENISA: Which is not one of the five key legal issues common across all scenarios:

- A. Data protection
- B. Professional negligence
- C. Globalization
- D. Intellectual property

E. Outsourcing services and changes in control