CloudSecurityAlliance.CCSK.v2025-07-11.q134

Exam Code:	CCSK
Exam Name:	Certificate of Cloud Security Knowledge (v4.0) Exam
Certification Provider:	Cloud Security Alliance
Free Question Number:	134
Version:	v2025-07-11
# of views:	108
# of Questions views:	1340
https://www.freepdfdumps.com/CloudSecurityAlliance.CCSK.v2025-07-11.q134.html	

NEW QUESTION: 1
ENISA: Lock-in is ranked as a high risk in ENISA research, a key underlying vulnerability causing lock in is:
A. Audit or certification not available to customers
B. Lack of completeness and transparency in terms of use
C. Lack of information on jurisdictions
D. No source escrow agreement
E. Unclear asset ownership
Answer: B (LEAVE A REPLY)

NEW QUESTION: 2
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. Platform-based Workload
C. Abstraction
D. Container
E. Pod
Answer: (SHOW ANSWER)

NEW QUESTION: 3
Which of the following best describes an aspect of PaaS services in relation to network security controls within a cloud environment?
A. They override the VNet/VPC's network security controls by default
B. They do not interact with the VNet/VPC's network security controls
C. They require manual configuration of network security controls, separate from the VNet/VPC

D. They often inherit the network security controls of the underlying VNet/VPC
Answer: D (LEAVE A REPLY)
In a Platform as a Service (PaaS) environment, the network security controls of the underlying Virtual Network (VNet) or Virtual Private Cloud (VPC) are often inherited by the PaaS services. This means that the network security settings, such as firewalls, security groups, and access control lists (ACLs), that are applied to the VNet/VPC also extend to the PaaS services, providing a seamless security model.
While PaaS services abstract much of the infrastructure management, they still interact with the network security controls in the VNet/VPC, allowing for centralized management of network security.
PaaS services typically do not override network security controls; they integrate with them. They do interact with VNet/VPC security controls, often integrate with network security controls, and do not always require separate manual configuration.

NEW QUESTION: 4
What can be implemented to help with account granularity and limit
blast radius with laaS an PaaS?
A. Configuring secondary authentication
B. Configuring role-based authentication
C. Establishing multiple accounts
D. Implementing least privilege accounts
E. Maintaining tight control of the primary account holder credentials
Answer: C (LEAVE A REPLY)

NEW QUESTION: 5
What is the primary purpose of secrets management in cloud environments?
A. Optimizing cloud infrastructure performance
B. Managing user authentication for human access
C. Securely handling stored authentication credentials
D. Monitoring network traffic for security threats
Answer: C (LEAVE A REPLY)
Secrets management focuses on securely storing and managing sensitive information, such as API keys and passwords, to prevent unauthorized access. Reference: [Security Guidance v5, Domain 8 - Secrets Management]

NEW QUESTION: 6
Which of the following enhances Platform as a Service (PaaS) security by regulating traffic into PaaS components?
A. Intrusion Detection Systems
B. Hardware Security Modules
C. Network Access Control Lists

D. API Gateways

Answer: (SHOW ANSWER)

API Gateways enhance Platform as a Service (PaaS) security by regulating traffic into and out of PaaS components. They act as an intermediary between external requests and the PaaS applications, helping to enforce security policies such as authentication, authorization, rate limiting, input validation, and logging. API gateways help protect PaaS components by controlling which traffic is allowed to reach the services, thereby reducing exposure to potential attacks.

Intrusion Detection Systems (IDS) are used to detect potential threats in a network, but they don't specifically regulate traffic into PaaS components like API Gateways do. Hardware Security Modules (HSMs) are used for managing encryption keys and cryptographic operations but do not directly regulate traffic to PaaS components. Network Access Control Lists (NACLs) control traffic at the network layer but are generally used for controlling traffic to/from virtual machines or subnets rather than for PaaS components specifically.

NEW QUESTION: 7

Which cloud service model allows users to access applications hosted and managed by the provider, with the user only needing to configure the application?

A. Software as a Service (SaaS)

B. Database as a Service (DBaaS)

C. Platform as a Service (PaaS)

D. Infrastructure as a Service (IaaS)

Answer: (SHOW ANSWER)

SaaS enables users to access hosted applications managed by the provider, with only minor configuration by the customer. Reference: [CCSK Study Guide, Domain 1 - Service Models]

NEW QUESTION: 8

Which statement best describes why it is important to know how data is being accessed?

A. The devices used to access data use a variety of operating systems and may have different programs installed on them.

B. The device may affect data dispersion.

C. The devices used to access data use a variety of applications or clients and may have different security characteristics.

D. The devices used to access data may have different ownership characteristics.

E. The devices used to access data have different storage formats.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 9

What should every cloud customer set up with its cloud service provider (CSP) that can be utilized in the event of an incident?

A. A spill remediation kit

B. A back-up website

C. A data destruction plan

D. A communication plan

E. A rainy day fund

Answer: (SHOW ANSWER)

NEW QUESTION: 10

Which of the following best describes how cloud computing manages shared resources?

A. Through virtualization, with administrators allocating resources based on SLAs

B. Through abstraction and automation to distribute resources to customers

C. By allocating physical systems to a single customer at a time

D. Through manual configuration of resources for each user need

Answer: (SHOW ANSWER)

Cloud computing uses abstraction and automation to pool and distribute resources efficiently among multiple tenants. This allows dynamic allocation based on demand.

Reference: [CCSK v5 Curriculum, Domain 1 - Cloud Computing Models]

NEW QUESTION: 11

Which Identity and Access Management (IAM) principle focuses on implementing multiple security layers to dilute access power, thereby averting a misuse or compromise?

A. Continuous Monitoring

B. Federation

C. Segregation of Duties

D. Principle of Least Privilege

Answer: C (LEAVE A REPLY)

The principle of Segregation of Duties (SoD) focuses on implementing multiple security layers by dividing responsibilities among different individuals or systems to ensure that no single entity has enough control to misuse or compromise access. This principle helps to prevent fraud, error, and misuse by ensuring that critical tasks are divided and that sensitive actions require multiple people or processes to perform, adding an extra layer of security.

Continuous Monitoring refers to the ongoing observation of activities to detect unusual behavior, but it is not directly about diluting access power. Federation involves linking multiple identity management systems together to allow access across different domains but does not specifically address limiting access power through multiple security layers.

Principle of Least Privilege ensures that users have only the minimum necessary access to perform their tasks, but it does not directly involve dividing duties or responsibilities.

NEW QUESTION: 12
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. Physical, Network, Compute, Storage, Application or Data
B. Mappings to well-known standards and frameworks
C. SaaS, PaaS or IaaS
D. Service Provider or Tenant/Consumer
Answer: (SHOW ANSWER)

NEW QUESTION: 13
What is true of security as it relates to cloud network infrastructure?
A. You should implement a default deny with cloud firewalls.
B. You should deploy your cloud firewalls identical to the existing firewalls.
C. You should apply cloud firewalls on a per-network basis.
D. You should implement a default allow with cloud firewalls and then restrict as necessary.
E. You should always open traffic between workloads in the same virtual subnet for better visibility.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 14
What is the primary purpose of Identity and Access Management (IAM) systems in a cloud environment?
A. To encrypt data to ensure its confidentiality
B. To govern identities' access to resources in the cloud
C. To monitor network traffic for suspicious activity
D. To provide a backup solution for cloud data
Answer: B (LEAVE A REPLY)
The primary purpose of Identity and Access Management (IAM) systems in a cloud environment is to govern and control which identities (users, groups, or services) have access to which resources within the cloud. IAM systems ensure that only authorized users and services can access specific cloud resources, and they help enforce security policies such as least privilege access, role-based access control (RBAC), and multi-factor authentication (MFA).

NEW QUESTION: 15
How does cloud sprawl complicate security monitoring in an enterprise environment?
A. Cloud sprawl disperses assets, making it harder to monitor assets.
B. Cloud sprawl centralizes assets, simplifying security monitoring.
C. Cloud sprawl reduces the number of assets, easing security efforts.
D. Cloud sprawl has no impact on security monitoring.

Answer: A (LEAVE A REPLY)
Cloud sprawl leads to the distribution of assets across multiple locations, making it challenging to maintain visibility and security control over all resources. Reference: [Security Guidance v5, Domain 4 - Organization Management]

NEW QUESTION: 16
Why is governance crucial in balancing the speed of adoption with risk control in cybersecurity initiatives?
A. Only involves senior management in decision-making
B. Speeds up project execution irrespective of and focuses on systemic risk
C. Ensures adequate risk management while allowing innovation
D. Ensures alignment between global compliance standards
Answer: C (LEAVE A REPLY)
Governance in cybersecurity is crucial because it provides the framework to ensure that security risks are adequately managed while still allowing the organization to adopt new technologies and innovations at a reasonable pace. Effective governance helps organizations balance the need for security controls with the need for agility and speed in adopting new solutions. It ensures that risks are identified, assessed, and mitigated without unnecessarily slowing down progress or stifling innovation.
Without governance, there is a risk that security concerns may be overlooked, or too many restrictions might be placed on adoption, leading to delays or failure to innovate. Proper governance strikes the right balance between security and agility.

NEW QUESTION: 17
In a cloud computing incident, what should be the initial focus of analysis due to the ephemeral nature of resources and centralized control mechanisms?
A. Management plane activity logs
B. Network perimeter monitoring
C. Endpoint protection status
D. Physical hardware access
Answer: (SHOW ANSWER)

In a cloud computing incident, the initial focus of analysis should be on the management plane activity logs due to the ephemeral nature of resources and centralized control mechanisms in cloud environments. The management plane controls and monitors the overall cloud infrastructure, and its activity logs provide crucial information about changes to configurations, access controls, resource provisioning, and administrative actions that can help identify the root cause of an incident.
Network perimeter monitoring and endpoint protection status are also important, but in cloud environments where resources can be rapidly provisioned and decommissioned, the management plane logs provide the most immediate insight into administrative actions and the overall state of the cloud environment.
Physical hardware access is generally the responsibility of the cloud provider and less relevant in the initial stages of a cloud incident analysis, especially when focusing on virtualized and managed resources.

NEW QUESTION: 18
Which term describes the practice in cloud compliance where a customer acquires a set of pre-approved regulatory or standards-based controls from a compliant provider?
A. Automated compliance
B. Attestation inheritance
C. Audit inheritance
D. Compliance inheritance
Answer: D (LEAVE A REPLY)
Compliance inheritance refers to the practice in cloud compliance where a customer leverages a set of pre- approved regulatory or standards-based controls that have been established and validated by a compliant cloud provider. Essentially, the cloud provider implements these controls, and the customer inherits the provider's compliance framework to meet their own regulatory requirements. This allows customers to benefit from the provider's compliance efforts without having to implement everything themselves.
Automated compliance refers to automating compliance tasks and processes but does not describe the practice of inheriting compliance controls. Attestation inheritance is not a standard term used in cloud compliance; attestation typically refers to formally certifying or declaring compliance. Audit inheritance would relate to the inheritance of audit reports or records, but it doesn't describe the broader process of inheriting compliance controls.

NEW QUESTION: 19
Which of the following is the MOST common cause of cloud-native security breaches?
A. Inability to monitor cloud infrastructure for threats
B. IAM failures
C. Lack of encryption for data at rest
D. Vulnerabilities in cloud provider's physical infrastructure
Answer: B (LEAVE A REPLY)

IAM failures are a leading cause of cloud-native breaches, often due to misconfigurations or inadequate access control mechanisms. Reference: [Security Guidance v5, Domain 5 - IAM]

NEW QUESTION: 20
What is the purpose of access policies in the context of security?
A. Access policies encrypt sensitive data to protect it from disclosure and unrestricted access.
B. Access policies define the permitted actions that can be performed on resources.
C. Access policies determine where data can be stored.
D. Access policies scan systems to detect and remove malware infections.
Answer: B (LEAVE A REPLY)
Access policies are a critical component of security frameworks that specify and enforce the permitted actions that users or systems can perform on resources, such as files, applications, or services. These policies help ensure that only authorized individuals or systems have access to certain resources and that they can only perform authorized actions, such as reading, writing, or modifying the resources. Access policies are fundamental in managing security and preventing unauthorized access, misuse, or attacks. Access policies encrypt sensitive data is incorrect because encryption of sensitive data is typically handled by encryption policies, not access policies. Access policies determine where data can be stored is more related to data management policies rather than access control. Access policies scan systems for malware is related to security measures such as antivirus or anti-malware tools, not the scope of access control policies.

NEW QUESTION: 21
CCM: In the CCM tool, ais a measure that modifies risk and includes any process, policy, device, practice or any other actions which modify risk.
A. Domain
B. Control Specification
C. Risk Impact
Answer: B (LEAVE A REPLY)

NEW QUESTION: 22
If the management plane has been breached, you should confirm the templates/configurations for your infrastructure or applications have not also been compromised.
A. True
B. False
Answer: B (LEAVE A REPLY)

NEW QUESTION: 23

What does it mean if the system or environment is built automatically from a template?
A. Nothing.
B. Changes made in production are overwritten by the next code or template change.
C. It depends on how the automation is configured.
D. Changes made in test are overwritten by the next code or template change.
E. Changes made in production are untouched by the next code or template change.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 24
In a containerized environment, what is fundamental to ensuring runtime protection for deployed containers?
A. Implementing real-time visibility
B. Deploying container-specific antivirus scanning
C. Using static code analysis tools in the pipeline
D. Full packet network monitoring
Answer: A (LEAVE A REPLY)
Real-time visibility allows for monitoring container behavior during runtime, helping to identify and respond to security incidents as they occur. Reference: [Security Guidance v5, Domain 8 - Cloud Workload Security]

NEW QUESTION: 25
In securing virtual machines (VMs), what is the primary role of using an "image factory" in VM deployment?
A. To encrypt data within VMs for secure storage
B. To facilitate direct manual intervention in VM deployments
C. To enable rapid scaling of virtual machines on demand
D. To ensure consistency, security, and efficiency in VM image creation
Answer: (SHOW ANSWER)
An image factory is used in VM deployment to create standardized and secure virtual machine images. The primary role of the image factory is to automate the creation of these images, ensuring that all VMs deployed from the image are consistent in terms of configuration, security settings, and performance. By using an image factory, organizations can ensure that their VMs are secure (with the necessary security patches and settings), efficient (optimized for performance), and consistent (following the same configuration). This process minimizes the risk of configuration drift and reduces manual intervention in VM deployment, leading to more efficient and secure operations.

NEW QUESTION: 26
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. None of the above

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. 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
Answer: A (LEAVE A REPLY)

NEW QUESTION: 27
Which of the following best describes a primary risk associated with the use of cloud storage services?
A. Increased cost due to redundant data storage practices
B. Unauthorized access due to misconfigured security settings
C. Inherent encryption failures within all cloud storage solutions
D. Complete data loss due to storage media degradation
Answer: B (LEAVE A REPLY)
One of the primary risks associated with cloud storage services is unauthorized access due to misconfigured security settings. Cloud storage providers typically offer a range of configuration options for managing access, but if these settings are not properly configured (e.g., improper access control lists, missing encryption, or inadequate permissions), it can lead to unauthorized users gaining access to sensitive data. This is a common and significant risk in cloud environments, which is why securing and correctly configuring access controls is critical.

NEW QUESTION: 28
In the Incident Response Lifecycle, which phase involves identifying potential security events and examining them for validity?
A. Post-Incident Activity
B. Detection and Analysis
C. Preparation
D. Containment, Eradication, and Recovery
Answer: B (LEAVE A REPLY)
The Detection and Analysis phase involves identifying incidentsand determining their impact. It is crucial to validate events to understand if they constitute a security incident.
Reference: [Security Guidance v5, Domain
11 - Incident Response]

NEW QUESTION: 29
Which principle reduces security risk by granting users only the permissions essential for their role?
A. Role-Based Access Control

B. Unlimited Access
C. Mandatory Access Control
D. Least-Privileged Access
Answer: D (LEAVE A REPLY)
The principle of least privilege limits access to only necessary permissions, reducing the risk of misuse and exposure of sensitive data. Reference: [CCSK v5 Curriculum, Domain 5 - IAM]

NEW QUESTION: 30
Which of the following cloud essential characteristics refers to the capability of the service to scale resources up or down quickly and efficiently based on demand?
A. On-Demand Self-Service
B. Broad Network Access
C. Resource Pooling
D. Rapid Elasticity
Answer: D (LEAVE A REPLY)
Rapid Elasticity refers to the capability of cloud services to scale resources up or down quickly and efficiently in response to varying demand. This characteristic allows cloud environments to dynamically adjust resource allocation (such as computing power, storage, or bandwidth) to meet the needs of users, ensuring that resources are available when required and minimizing waste when demand decreases.
This ability is a key advantage of cloud computing, providing flexibility and cost efficiency for businesses.

NEW QUESTION: 31
For third-party audits or attestations, what is critical for providers to publish and customers to evaluate?
A. Full API access to all required services
B. Provider infrastructure information including maintenance windows and contracts
C. Scope of the assessment and the exact included features and services for the assessment
D. Network or architecture diagrams including all end point security devices in use
E. Service-level agreements between all parties
Answer: D (LEAVE A REPLY)

NEW QUESTION: 32
Which practice best helps mitigate security risks by minimizing root/core access and restricting deployment creation?
A. Enforcing the principle of trust and eventually verily on demand'
B. Disabling multi-factor authentication for staff and focusing on decision makers' accounts
C. Deploying applications with full access and applying restrictions based on the need to object
D. Enforcing the principle of least privilege
Answer: D (LEAVE A REPLY)
Enforcing the principle of least privilege is the practice of granting users and systems the minimum level of access necessary to perform their tasks. By limiting root or core access and restricting the creation of deployments to only those who absolutely need it, the risk of unauthorized access, misuse, or damage is minimized. This helps ensure that critical systems and sensitive data are protected by reducing the number of people or services with high-level access.
Trust and verify on demand is not a standard security practice and could create security gaps. Disabling multi- factor authentication is a poor security practice, as multi-factor authentication (MFA) enhances security by adding an additional layer of verification. Deploying applications with full access) contradicts the principle of least privilege and could expose the system to unnecessary risks.

NEW QUESTION: 33
Containers are highly portable code execution environments.
A. False
B. True
Answer: B (LEAVE A REPLY)

NEW QUESTION: 34
What is a key advantage of using Policy-Based Access Control (PBAC) for cloud-based access management?
A. PBAC eliminates the need for defining and managing user roles and permissions.
B. PBAC is easier to implement and manage compared to Role-Based Access Control (RBAC).
C. PBAC allows enforcement of granular, context-aware security policies using multiple attributes.
D. PBAC ensures that access policies are consistent across all cloud providers and platforms.
Answer: C (LEAVE A REPLY)

PBAC enables highly specific access control based on multiple attributes, enhancing flexibility and security in cloud environments. Reference: [CCSK v5 Curriculum, Domain 5 - IAM][16†source].

NEW QUESTION: 35
A cloud deployment of two or more unique clouds is known as:
A. A Community Cloud
B. A Hybrid Cloud
C. Infrastructures as a Service
D. A Private Cloud
E. Jericho Cloud Cube Model
Answer: A (LEAVE A REPLY)

NEW QUESTION: 36
What is known as the interface used to connect with the metastructure and configure the cloud environment?
A. Administrative access
B. Identity and Access Management
C. Management plane
D. Cloud dashboard
E. Single sign-on
Answer: C (LEAVE A REPLY)

NEW QUESTION: 37
Which aspect of cloud architecture ensures that a system can handle growing amounts of work efficiently?
A. Reliability
B. Security
C. Performance
D. Scalability
Answer: (SHOW ANSWER)
Scalability is a fundamental aspect of cloud architecture that allows a system to grow in capacity to meet increased workload demands effectively. Reference: [Security Guidance v5, Domain 1 - Cloud Characteristics]

NEW QUESTION: 38
Which benefit of automated deployment pipelines most directly addresses continuous security and reliability?
A. They enable consistent and repeatable deployment processes
B. They enhance collaboration through shared tools
C. They provide detailed reports on team performance

D. They ensure code quality through regular reviews

Answer: A (LEAVE A REPLY)

The most direct benefit of automated deployment pipelines in addressing continuous security and reliability is that they enable consistent and repeatable deployment processes. This ensures that the same steps are followed every time code is deployed, reducing human error and inconsistencies that could introduce vulnerabilities or reliability issues. Automated pipelines can also include security checks, such as static code analysis, vulnerability scanning, and automated testing, all of which help ensure that security and reliability are maintained continuously.

Enhancing collaboration through shared tools is a benefit of automated pipelines but doesn't directly address security and reliability. Providing detailed reports on team performance is useful for team management but doesn't directly contribute to security or reliability. Ensure code quality through regular reviews can improve security indirectly but is not the most direct benefit when it comes to continuous security and reliability in the deployment process.

NEW QUESTION: 39

How is encryption managed on multi-tenant storage?

A. Single key for all data owners

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

C. One key per data owner

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

E. Multiple keys per data owner

Answer: (SHOW ANSWER)

NEW QUESTION: 40

In preparing for cloud incident response, why is updating forensics tools for virtual machines (VMs) and containers critical?

A. To comply with cloud service level agreements (SLAs)

B. To streamline communication with cloud service providers and customers

C. To ensure compatibility with cloud environments for effective incident analysis

D. To increase the speed of incident response team deployments

Answer: C (LEAVE A REPLY)

Updating forensics tools for virtual machines (VMs) and containers is critical because cloud environments can differ significantly from traditional on-premises environments. As cloud technologies evolve, it is important to ensure that forensic tools are compatible with the latest cloud infrastructure, such as VMs, containers, and serverless architectures. This ensures that the tools can effectively collect, analyze, and preserve evidence in the event of a security incident, allowing for accurate and efficient incident analysis.

Complying with cloud service level agreements (SLAs)) is not the primary reason for updating forensics tools, although some SLAs may require certain levels of incident

response capabilities. Streamlining communication with cloud service providers and customers) is important, but the primary concern is the ability to analyze incidents, not just communication. Increasing the speed of incident response team deployments) is a consideration, but ensuring the tools are up to date and compatible is the main priority for effective incident analysis.

NEW QUESTION: 41
Which attack surfaces, if any, does virtualization technology introduce?
A. All of the above
B. Virtualization management components apart from the hypervisor
C. The hypervisor
D. Configuration and VM sprawl issues
Answer: A (LEAVE A REPLY)

NEW QUESTION: 42
Which term describes any situation where the cloud consumer does
not manage any of the underlying hardware or virtual machines?
A. Virtual machineless
B. Abstraction
C. Container
D. Serverless computing
E. Provider managed
Answer: D (LEAVE A REPLY)

NEW QUESTION: 43
In volume storage, what method is often used to support resiliency and security?
A. random placement
B. proxy encryption
C. data rights management
D. hypervisor agents
E. data dispersion
Answer: (SHOW ANSWER)

NEW QUESTION: 44
According to NIST, what is cloud computing defined as?
A. A shared set of resources delivered over the Internet
B. A model for more-efficient use of network-based resources
C. Services that are delivered over the Internet to customers
D. A model for on-demand network access to a shared pool of configurable resources
Answer: D (LEAVE A REPLY)

NIST defines cloud computing as on-demand network access to a shared pool of configurable resources, aligning with the essential characteristics of cloud services. Reference: [Security Guidance v5, Domain 1 - Cloud Computing Models]

NEW QUESTION: 45
Which layer is the most important for securing because it is considered to be the foundation for secure cloud operations?
A. Datastructure
B. Infostructure
C. Infrastructure
D. Metastructure
E. Applistructure
Answer: C (LEAVE A REPLY)

NEW QUESTION: 46
How does running applications on distinct virtual networks and only connecting networks as needed help?
A. It reduces hardware costs
B. It enables you to configure applications around business groups
C. It locks down access and provides stronger data security
D. It reduces the blast radius of a compromised system
E. It provides dynamic and granular policies with less management overhead
Answer: D (LEAVE A REPLY)

NEW QUESTION: 47
What's the difference between DNS Logs and Flow Logs?
A. They represent the logging of different networking solutions, and DNS Logs are more suitable for a ZTA implementation
B. DNS Logs record domain name resolution requests and responses, while Flow Logs record info on source, destination, protocol
C. They play identical functions and can be used interchangeably

D. DNS Logs record all the information about the network behavior, including source, destination, and protocol, while Flow Logs record users' applications behavior

Answer: B (LEAVE A REPLY)

DNS logs capture information on domain name resolution, while Flow logs capture details about network traffic, including source, destination, and protocol. Reference: [CCSK Study Guide, Domain 7 - Infrastructure
& Networking]

NEW QUESTION: 48

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. Rapid elasticity

B. Broad network access

C. On-demand self-service

D. Resource pooling

E. Measured service

Answer: (SHOW ANSWER)

NEW QUESTION: 49

What key characteristic differentiates cloud networks from traditional networks?

A. Cloud networks are software-defined networks (SDNs)

B. Cloud networks rely on dedicated hardware appliances

C. Cloud networks are less scalable than traditional networks

D. Cloud networks have the same architecture as traditional networks

Answer: A (LEAVE A REPLY)

The key characteristic that differentiates cloud networks from traditional networks is that cloud networks are often software-defined networks (SDNs). This means that network management, configuration, and provisioning in the cloud are handled through software, rather than relying on traditional hardware-based network components. SDNs allow for greater flexibility, scalability, and automation, enabling cloud providers to dynamically adjust resources to meet changing demands.

NEW QUESTION: 50

Dynamic Application Security Testing (DAST) might be limited or require pre-testing permission from the provider.

A. True

B. False

Answer: A (LEAVE A REPLY)

NEW QUESTION: 51
CCM: In the CCM tool, "Encryption and Key Management" is an example of which of the following?
A. Risk Impact
B. Domain
C. Control Specification
Answer: B (LEAVE A REPLY)

NEW QUESTION: 52
Which type of application security testing tests running applications and includes tests such as web vulnerability testing and fuzzing?
A. Static Application Security Testing (SAST)
B. Code Review
C. Dynamic Application Security Testing (DAST)
D. Functional Testing
E. Unit Testing
Answer: (SHOW ANSWER)

NEW QUESTION: 53
Why is consulting with stakeholders important for ensuring cloud security strategy alignment?
A. IT simplifies the cloud platform selection process
B. It reduces the overall cost of cloud services.
C. It ensures that the strategy meets diverse business requirements.
D. It ensures compliance with technical standards only.
Answer: (SHOW ANSWER)
Consulting with stakeholders is crucial for ensuring that the cloud security strategy aligns with the overall business objectives and needs. Stakeholders - such as business leaders, IT teams, legal, and compliance officers - bring unique perspectives on what the cloud strategy needs to accomplish, from security to compliance, scalability, and performance. By involving stakeholders, organizations can ensure that the security strategy supports business goals, addresses various concerns, and is comprehensive.
Simplifying the cloud platform selection process is a potential benefit but not the primary reason for consulting stakeholders. Selecting the right cloud platform is part of the broader strategy. Reducing the overall cost of cloud services is not necessarily the outcome of involving stakeholders, although cost considerations may be part of the discussion.
Ensuring compliance with technical standards only is too narrow; stakeholders help ensure compliance with both technical and business requirements.

NEW QUESTION: 54

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

A. True

B. False

Answer: (SHOW ANSWER)

NEW QUESTION: 55

Which of the following best describes an authoritative source in the context of identity management?

A. A list of permissions assigned to different users

B. A network resource that handles authorization requests

C. A database containing all entitlements

D. A trusted system holding accurate identity information

Answer: (SHOW ANSWER)

An authoritative source in the context of identity management refers to a trusted system that contains accurate identity information. This system is considered the source of truth for identities, and other systems or services within the organization rely on it for the most up-to-date and verified identity details, such as usernames, attributes, roles, and permissions.

A list of permissions assigned to different users represents access control data but is not considered the authoritative source of identity. A network resource that handles authorization requests refers to authorization mechanisms but is not the authoritative source for identity. A database containing all entitlements could be part of an identity management system but is not necessarily the authoritative source for identity itself; it focuses more on access rights and entitlements.

NEW QUESTION: 56

What is true of companies considering a cloud computing business relationship?

A. The cloud computing companies own all customer data.

B. The companies using the cloud providers are the custodians of the data entrusted to them.

C. The confidentiality agreements between companies using cloud computing services is limited legally to the company, not the provider.

D. The cloud computing companies are absolved of all data security and associated risks through contracts and data laws.

E. The laws protecting customer data are based on the cloud provider and customer location only.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 57

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

A. True
B. False
Answer: B (LEAVE A REPLY)

NEW QUESTION: 58
Which governance domain focuses on proper and adequate incident detection, response, notification, and remediation?
A. Compliance and Audit Management
B. Infrastructure Security
C. Data Security and Encryption
D. Information Governance
E. Incident Response, Notification and Remediation
Answer: (SHOW ANSWER)

NEW QUESTION: 59
Why is snapshot management crucial for the virtual machine (VM) lifecycle?
A. It allows for quick restoration points during updates or changes
B. It is used for load balancing VMs
C. It enhances VM performance significantly
D. It provides real-time analytics on VM applications
Answer: A (LEAVE A REPLY)
Snapshots serve as recovery points, enabling quick rollback to previous states if issues arise during updates or changes. This is crucial for VM lifecycle management. Reference: [Security Guidance v5, Domain 7 - Infrastructure & Networking]

NEW QUESTION: 60
Which aspect is most important for effective cloud governance?
A. Formalizing cloud security policies
B. Implementing best-practice cloud security control objectives
C. Negotiating SLAs with cloud providers
D. Establishing a governance hierarchy
Answer: (SHOW ANSWER)
A governance hierarchy provides a structured approach to managing cloud services, ensuring policies and controls are effectively enforced. Reference: [Security Guidance v5, Domain 2 - Cloud Governance]

NEW QUESTION: 61
What is the most effective way to identify security vulnerabilities in an application?
A. Performing code reviews of the application source code just prior to release
B. Relying solely on secure coding practices by the developers without any testing
C. Waiting until the application is fully developed and performing a single penetration test

D. Conducting automated and manual security testing throughout the development

Answer: D (LEAVE A REPLY)

The most effective way to identify security vulnerabilities in an application is to conduct automated and manual security testing throughout the development lifecycle. This approach ensures that security is continuously evaluated at every stage of development, rather than waiting until the end. Automated tools can help identify common vulnerabilities quickly, while manual testing allows for more in-depth analysis, including testing for complex, contextual security issues. This proactive and ongoing approach reduces the risk of vulnerabilities being overlooked and helps ensure that security is integrated into the application from the start.

Performing code reviews just prior to release is valuable, but it's not comprehensive enough. Security testing should be done early and continuously, not just before release.

Relying solely on secure coding practices is important but not sufficient. Even with secure coding practices, testing is essential to identify vulnerabilities.

Waiting for a single penetration test after development is not effective because waiting until the end can allow many vulnerabilities to go unnoticed during development, leaving the application exposed.

NEW QUESTION: 62

What is a key consideration when handling cloud security incidents?

A. Monitoring network traffic

B. Focusing on technical fixes

C. Cloud service provider service level agreements

D. Hiring additional staff

Answer: C (LEAVE A REPLY)

SLAs play a key role in cloud incident management as they define response expectations and support arrangements between CSPs and CSCs. Reference: [CCSK Study Guide, Domain 11 - Incident Response]

NEW QUESTION: 63

What is the primary objective of posture management in a cloud environment?

A. Automating incident response procedures

B. Optimizing cloud cost efficiency
C. Continuous monitoring of configurations
D. Managing user access permissions
Answer: C (LEAVE A REPLY)
The primary objective of posture management in a cloud environment is to ensure that cloud configurations are continuously monitored to ensure compliance with security policies, best practices, and regulatory requirements. Posture management involves assessing and maintaining the security posture by identifying misconfigurations, vulnerabilities, or non-compliant resources, and ensuring that the cloud environment remains secure and aligned with organizational policies.
Automating incident response procedures is important but is not the primary focus of posture management, which focuses more on proactive configuration and security monitoring. Optimizing cloud cost efficiency is a key concern in cloud management, but it is not the main focus of posture management, which deals with security and compliance.
Managing user access permissions is related to Identity and Access Management (IAM), which is a separate aspect of cloud security from posture management.

NEW QUESTION: 64
What are the key outcomes of implementing robust cloud risk management practices?
A. Ensuring the security and resilience of cloud environments
B. Negotiating shared responsibilities
C. Transferring compliance to the cloud service provider via inheritance
D. Reducing the need for compliance with regulatory requirements
Answer: (SHOW ANSWER)
The key outcomes of implementing robust cloud risk management practices focus on ensuring the security and resilience of cloud environments. This involves identifying, assessing, and mitigating risks associated with the use of cloud services, such as security threats, data privacy issues, and service availability concerns.
By adopting strong risk management practices, organizations can better protect their data, ensure business continuity, and maintain compliance with regulations, which ultimately strengthens the overall security and reliability of their cloud environments.
Negotiating shared responsibilities is an important aspect of cloud security but is not the direct outcome of risk management practices. It's about clarifying roles between the customer and provider. Transferring compliance to the cloud service provider via inheritance is not the complete picture. While cloud service providers may help with compliance, the responsibility for compliance and risk management is still shared.
Reducing the need for compliance with regulatory requirements is incorrect. Robust risk management practices help ensure compliance with regulatory requirements, not reduce the need for them.

NEW QUESTION: 65

Which component is primarily responsible for filtering and monitoring HTTP/S traffic to and from a web application?

A. Anti-virus Software

B. Load Balancer

C. Web Application Firewall

D. Intrusion Detection System

Answer: C (LEAVE A REPLY)

A Web Application Firewall (WAF) is primarily responsible for filtering and monitoring HTTP/S traffic to and from a web application. It is designed to protect web applications by filtering and monitoring traffic for malicious requests, such as SQL injection, cross-site scripting (XSS), and other common application-layer attacks. A WAF helps secure web applications by analyzing the HTTP/S traffic and blocking any harmful requests before they reach the application.

Anti-virus Software is used to detect and remove malicious software on endpoints and devices but is not designed to filter HTTP/S traffic specifically for web applications. Load Balancer is used to distribute network traffic across multiple servers to ensure performance and reliability, but it does not focus on security filtering. Intrusion Detection System (IDS) monitors network traffic forsuspicious activity but operates at a different level of the network stack and is not focused solely on web application traffic.

NEW QUESTION: 66

Which aspect of cybersecurity can AI enhance by reducing false positive alerts?

A. Anomaly detection

B. Assisting analysts

C. Threat intelligence

D. Automated responses

Answer: (SHOW ANSWER)

AI can enhance anomaly detection in cybersecurity by analyzing large volumes of data and identifying patterns that deviate from normal behavior. By using machine learning algorithms, AI can improve the accuracy of anomaly detection, reducing false positive alerts. This helps security teams focus on genuine threats while minimizing distractions from irrelevant alerts.

Assisting analysts is a valid benefit of AI, but reducing false positives directly improves anomaly detection capabilities. Threat intelligence refers to gathering and analyzing information about potential threats but isn't directly focused on reducing false positives in the same way as anomaly detection. Automated responses can be part of AI's role in cybersecurity, but reducing false positives is more directly related to improving anomaly detection.

NEW QUESTION: 67

How does centralized logging simplify security monitoring and compliance?

A. It consolidates logs into a single location.
B. It decreases the amount of data that needs to be reviewed.
C. It encrypts all logs to prevent unauthorized access.
D. It automatically resolves all detected security threats.
Answer: A (LEAVE A REPLY)
Centralized logging aggregates logs in one location, making it easier to monitor, analyze, and comply with regulatory requirements. Reference: [Security Guidance v5, Domain 6 - Security Monitoring]

NEW QUESTION: 68
What primary purpose does object storage encryption serve in cloud services?
A. It compresses data to save space
B. It speeds up data retrieval times
C. It monitors unauthorized access attempts
D. It secures data stored as objects
Answer: (SHOW ANSWER)
Encryption in object storage is used to secure stored data and protect it from unauthorized access, ensuring confidentiality. Reference: [Security Guidance v5, Domain 9 - Data Security]

NEW QUESTION: 69
Which of the following items is NOT an example of Security as a Service (SecaaS)?
A. Provisioning
B. Authentication
C. Web filtering
D. Spam filtering
E. Intrusion detection
Answer: A (LEAVE A REPLY)

NEW QUESTION: 70
Which of the following statements best describes an identity federation?
A. The connection of one identity repository to another
B. A library of data definitions
C. Several countries which have agreed to define their identities with similar attributes
D. Identities which share similar attributes
E. A group of entities which have decided to exist together in a single cloud
Answer: A (LEAVE A REPLY)

NEW QUESTION: 71

Which of the following statements best reflects the responsibility of organizations regarding cloud security and data ownership?
A. Cloud providers are responsible for everything under the 'limited O responsibilities clauses.' The customer and the provider have joint accountability.
B. Cloud providers assume full responsibility for the security obligations, and cloud customers are accountable for overall compliance.
C. Data ownership rights are solely determined by the cloud provider, leaving organizations with no control or accountability over their data.
D. Organizations are accountable for the security and compliance of their data and systems, even though they may lack full visibility into their cloud provider's infrastructure.
Answer: D (LEAVE A REPLY)
TheShared Responsibility Modelin cloud computing establishes that:
* Cloud providersare responsible for securing the underlyinginfrastructure, networking, and hardware.
* Customers (organizations)are responsible for securingdata, identity and access management (IAM), encryption, and complianceobligations.
* Data ownershipremainswith the customer, even though visibility into cloud infrastructure may be limited.
The major security challenge in cloud computing is thatorganizations lack full control over cloud infrastructurebut must still ensure that security policies align withregulatory requirements (e.g., GDPR, HIPAA, PCI DSS).
This principle is outlined in:
* CCSK v5 - Security Guidance v4.0, Domain 2 (Governance and Enterprise Risk Management)
* Cloud Security Alliance's (CSA) Cloud Controls Matrix (CCM) - Data Security and Governance.

NEW QUESTION: 72
What is the primary purpose of the CSA Security, Trust, Assurance, and Risk (STAR) Registry?
A. To provide cloud service rate comparisons
B. To certify cloud services for regulatory compliance
C. To document security and privacy controls of cloud offerings
D. To manage data residency and localization requirements
Answer: (SHOW ANSWER)
The CSA STAR Registry provides transparency by listing security and privacy controls of CSPs, helping customers assess provider security. Reference: [CCSK Overview, STAR Registry]

NEW QUESTION: 73
Which aspect of assessing cloud providers poses the most significant challenge?

A. Inconsistent policy standards and the proliferation of provider requirements.
B. Limited visibility into internal operations and technology.
C. Excessive details shared by the cloud provider and consequent information overload.
D. Poor provider documentation and over-reliance on pooled audit.
Answer: (SHOW ANSWER)
One of the biggest challenges incloud security risk assessmentisthe lack of transparencyregardingcloud provider operations and security controls.
Key Issues with Limited Visibility:
* Cloud providers manage infrastructure at a global scale:
* Customerscannot directly inspectsecurity implementations.
* Rely onthird-party attestationslikeSOC 2, ISO 27001, CSA STARinstead of direct assessments.
* Multi-tenancy complexities:
* Cloud customersshare infrastructurewith other tenants.
* Data isolation mechanisms (e.g., virtual private clouds, encryption)must be trustedwithout direct verification.
* Regulatory compliance challenges:
* Organizations handling sensitive data (e.g., healthcare, finance)requirestrict controls.
* Cloud providers may not offer sufficient audit logsor control overdata residency and processing.
* Incident response limitations:
* In traditional IT, organizations controllog access, forensic analysis, and recovery.
* In the cloud,incident investigation depends on the provider's logging and notification practices.
Thisvisibility issueis extensively covered in:
* CCSK v5 - Security Guidance v4.0, Domain 4 (Compliance and Audit Management)
* ENISA's Cloud Computing Risk Assessment (Limited visibility into cloud provider security policies)

NEW QUESTION: 74
ENISA: An example high risk role for malicious insiders within a Cloud Provider includes
A. Sales
B. Marketing
C. Auditors
D. Legal counsel
E. Accounting
Answer: (SHOW ANSWER)

NEW QUESTION: 75
What is a primary objective during the Detection and Analysis phase of incident response?
A. Developing and updating incident response policies

B. Validating alerts and estimating the scope of incidents
C. Performing detailed forensic investigations
D. Implementing network segmentation and isolation
Answer: (SHOW ANSWER)
During the Detection and Analysis phase of incident response, the primary objective is to validate alerts to determine whether they represent a genuine security incident, and to estimate the scope of the incident to understand the potential impact on the organization. This phase involves analyzing evidence, confirming the nature of the incident, and gathering the necessary information to move forward with containment and remediation. Developing and updating incident response policies is important but occurs more during the preparation phase, not during the detection and analysis of an active incident. Performing detailed forensic investigations typically takes place during later phases, such as Containment, Eradication, & Recovery or Post-Incident Analysis. Implementing network segmentation and isolation may be part of the Containment phase but is not the primary focus during the Detection and Analysis phase.

NEW QUESTION: 76
Which of the following encryption methods would be utilized when object storage is used as the back-end for an application?
A. Database encryption
B. Object encryption
C. Media encryption
D. Client/application encryption
E. Asymmetric encryption
Answer: D (LEAVE A REPLY)

NEW QUESTION: 77
Which statement best describes the Data Security Lifecycle?
A. The Data Security Lifecycle has six stages, is strictly linear, and never varies.
B. The Data Security Lifecycle has five stages, can be non-linear, and is distinct in that data must always pass through all phases.

C. The Data Security Lifecycle has six stages, can be non-linear, and varies in that some data may never pass through all stages.
D. The Data Security Lifecycle has five stages, is circular, and varies in that some data may never pass through all stages.
E. The Data Security Lifecycle has six stages, can be non-linear, and is distinct in that data must always pass through all phases.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 78
What is a core tenant of risk management?
A. The consumers are completely responsible for all risk.
B. The provider is accountable for all risk management.
C. You can manage, transfer, accept, or avoid risks.
D. Risk insurance covers all financial losses, including loss of customers.
E. If there is still residual risk after assessments and controls are in place, you must accept the risk.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 79
Without virtualization, there is no cloud.
A. False
B. True
Answer: (SHOW ANSWER)

NEW QUESTION: 80
ENISA: "VM hopping" is:
A. Improper management of VM instances, causing customer VMs to be commingled with other customer systems.
B. Looping within virtualized routing systems.
C. Lack of vulnerability management standards.
D. Using a compromised VM to exploit a hypervisor, used to take control of other VMs.
E. Instability in VM patch management causing VM routing errors.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 81
In the cloud provider and consumer relationship, which entity
manages the virtual or abstracted infrastructure?
A. Only the cloud provider
B. Only the cloud consumer
C. Both the cloud provider and consumer
D. It is determined in the agreement between the entities

E. It is outsourced as per the entity agreement
Answer: C (LEAVE A REPLY)

NEW QUESTION: 82
Which governance domain deals with evaluating how cloud computing affects compliance with internal security policies and various legal requirements, such as regulatory and legislative?
A. Infrastructure Security
B. Information Governance
C. Legal Issues: Contracts and Electronic Discovery
D. Compliance and Audit Management
E. Governance and Enterprise Risk Management
Answer: D (LEAVE A REPLY)

NEW QUESTION: 83
APIs and web services require extensive hardening and must assume attacks from authenticated and unauthenticated adversaries.
A. False
B. True
Answer: (SHOW ANSWER)

NEW QUESTION: 84
What tool allows teams to easily locate and integrate with approved cloud services?
A. Contracts
B. Shared Responsibility Model
C. Service Registry
D. Risk Register
Answer: C (LEAVE A REPLY)
A Service Registry lists approved services, making it easy for teams to find and integrate compliant services.
Reference: [CCSK Knowledge Guide, Domain 3 - Risk and Compliance Tools]

NEW QUESTION: 85
What is the primary purpose of implementing a systematic data/asset classification and catalog system in cloud environments?
A. To automate the data encryption process across all cloud services
B. To reduce the overall cost of cloud storage solutions
C. To apply appropriate security controls based on asset sensitivity and importance
D. To increase the speed of data retrieval within the cloud environment
Answer: C (LEAVE A REPLY)

Classification and cataloging help assign security controls and manage data based on its sensitivity and criticality. Reference: [CCSK v5 Curriculum, Domain 9 - Data Security]

NEW QUESTION: 86
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. Both B and D.
B. 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.
C. Practice Integration of Duties (IOD) so that everyone is able to delete the encrypted data.
D. 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.
E. Maintaining customer managed key management and revoking or deleting keys from the key management system to prevent the data from being accessed again.
Answer: E (LEAVE A REPLY)

NEW QUESTION: 87
In the context of FaaS, what is primarily defined in addition to functions?
A. Data storage
B. Network configurations
C. User permissions
D. Trigger events
Answer: (SHOW ANSWER)
In the context of Function as a Service (FaaS), trigger events are primarily defined in addition to the functions themselves. FaaS allows you to run individual functions in response to events, such as HTTP requests, file uploads, database changes, or messages in a queue. These trigger events initiate the execution of the serverless function, making them a core part of FaaS architecture.
Data storage is not directly defined by FaaS, as storage is typically managed separately (e.g., cloud storage or databases). Network configurations are not the main focus of FaaS, since cloud providers manage the underlying network infrastructure. User permissions may be relevant but are typically handled through identity and access management (IAM), not directly tied to the definition of a FaaS function.

NEW QUESTION: 88
When designing an encryption system, you should start with a threat model.
A. True
B. False
Answer: (SHOW ANSWER)

NEW QUESTION: 89
In the context of cloud security, what is the primary benefit of implementing Identity and Access Management (IAM) with attributes and user context for access decisions?
A. Enhances security by supporting authorizations based on the current context and status
B. Reduces log analysis requirements
C. Simplifies regulatory compliance by using a single sign-on mechanism
D. These are required for proper implementation of RBAC
Answer: A (LEAVE A REPLY)
Context-aware IAM enables access decisions that account for real-time conditions, enhancing security by adapting to changes in user and resource status. Reference: [CCSK Study Guide, Domain 5 - IAM]

NEW QUESTION: 90
What is the most significant security difference between traditional infrastructure and cloud computing?
A. Intrusion detection options
B. Mobile security configuration options
C. Network access points
D. Secondary authentication factors
E. Management plane
Answer: (SHOW ANSWER)

NEW QUESTION: 91
What of the following is NOT an essential characteristic of cloud computing?
A. Rapid Elasticity
B. Measured Service
C. Third Party Service
D. Broad Network Access
E. Resource Pooling
Answer: (SHOW ANSWER)

NEW QUESTION: 92

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

NEW QUESTION: 93
Which of the following best describes a primary focus of cloud governance with an emphasis on security?
A. Enhancing user experience with intuitive interfaces.
B. Maximizing cost savings through resource optimization.
C. Increasing scalability and flexibility of cloud solutions.
D. Ensuring compliance with regulatory requirements and internal policies.
Answer: (SHOW ANSWER)
Cloud governancefocuses onsecurity, risk management, and complianceto ensuredata protection, audit readiness, and regulatory adherence.
Key Elements of Cloud Security Governance:
* Regulatory Compliance:
* Organizations must comply withGDPR, HIPAA, PCI DSS, ISO 27001.
* Cloud Security Posture Management (CSPM)helpsenforce complianceautomatically.
* Security Policies & Controls:
* Cloud governance frameworks includeIAM (Identity and Access Management), encryption policies, and workload isolation.
* Organizations muststandardize security settingsacross multiple cloud environments.
* Audit & Risk Management:
* Implementcontinuous monitoring, security logging, and forensic readiness.
* Risk-based access control policiesensuredata security across workloads.
* Data Protection & Privacy:
* Enforcingcloud-native security frameworks (e.g., Zero Trust, CASB, SIEM).
* Data retention, access control, andincident responseareessential governance practices.
This is covered in:
* CCSK v5 - Security Guidance v4.0, Domain 2 (Governance and Risk Management)
* Cloud Security Alliance's Cloud Controls Matrix (CCM) - Cloud Governance and Compliance Standards

NEW QUESTION: 94
How can the use of third-party libraries introduce supply chain risks in software development?
A. They are usually open source and do not require vetting
B. They might contain vulnerabilities that can be exploited
C. They fail to integrate properly with existing continuous integration pipelines
D. They might increase the overall complexity of the codebase
Answer: (SHOW ANSWER)
The use of third-party libraries in software development can introduce supply chain risks because these libraries might contain vulnerabilities that can be exploited. Since third-party libraries often come from external sources, they might not be thoroughly vetted or maintained with the same level of scrutiny as in- house code. Vulnerabilities in these libraries can lead to security breaches, data leaks, or other forms of exploitation if not properly managed and updated.
Although many third-party libraries are open-source, they still require proper vetting for security and compatibility. Integration issues, while a concern, are not directly related to the supply chain risks posed by vulnerabilities. While increased complexity is a challenge, it does not directly relate to security risks or supply chain concerns.

NEW QUESTION: 95
Why is identity management at the organization level considered a key aspect in cybersecurity?
A. It replaces the need to enforce the principles of the need to know
B. It ensures only authorized users have access to resources
C. It automates and streamlines security processes in the organization
D. It reduces the need for regular security training and auditing, and frees up cybersecurity budget
Answer: B (LEAVE A REPLY)
Identity management at the organizational level is a key aspect of cybersecurity because it ensures that only authorized users can access specific resources, systems, or data. By controlling and managing user identities, roles, and permissions, identity management helps enforce security policies, preventing unauthorized access and potential breaches. This is a fundamental practice in maintaining confidentiality, integrity, and availability within an organization.

NEW QUESTION: 96
In a cloud environment spanning multiple jurisdictions, what is the most important factor to consider for compliance?
A. Relying on the cloud service provider's compliance certifications for all jurisdictions

B. Focusing on the compliance requirements defined by the laws, regulations, and standards enforced in the jurisdiction where the company is based
C. Relying only on established industry standards since they adequately address all compliance needs
D. Understanding the legal and regulatory requirements of each jurisdiction where data originates, is stored, or processed
Answer: D (LEAVE A REPLY)
In a cloud environment that spans multiple jurisdictions, it is crucial to understand the legal and regulatory requirements of each jurisdiction where data originates, is stored, or is processed. Different regions or countries have varying laws, regulations, and compliance standards regarding data privacy, protection, and security. Organizations must ensure they meet all applicable requirements in each jurisdiction to avoid potential legal issues, fines, and reputational damage.

NEW QUESTION: 97
How does serverless computing impact infrastructure management responsibility?
A. Requires extensive on-premises infrastructure
B. Shifts more responsibility to cloud service providers
C. Increases workload for developers
D. Eliminates need for cloud service providers
Answer: B (LEAVE A REPLY)
Serverless computing shifts infrastructure management responsibility to the CSP, allowing customers to focus on application logic rather than infrastructure. Reference: [Security Guidance v5, Domain 8 - Cloud Workload Security]

NEW QUESTION: 98
To understand their compliance alignments and gaps with a cloud provider, what must cloud customers rely on?
A. Provider documentation
B. Third-party attestations
C. Provider and consumer contracts
D. EDiscovery tools
E. Provider run audits and reports
Answer: B (LEAVE A REPLY)

NEW QUESTION: 99
What are the most important practices for reducing vulnerabilities in virtual machines (VMs) in a cloud environment?
A. Disabling unnecessary VM services and using containers
B. Encryption for data at rest and software bill of materials
C. Using secure base images, patch and configuration management

D. Network isolation and monitoring

Answer: (SHOW ANSWER)

To reduce vulnerabilities in virtual machines (VMs) in a cloud environment, it is critical to use secure base images that are free from known vulnerabilities, ensure regular patching to fix any discovered security issues, and implement configuration management to ensure that VMs are properly configured according to security best practices. This combination of practices ensures that VMs are both secure from the start and remain secure over time as new vulnerabilities are discovered.

Disabling unnecessary VM services and using containers is a good security practice but does not directly address vulnerabilities in VMs specifically. Encryption and SBOM is important for securing data and understanding dependencies but does not specifically focus on reducing vulnerabilities in VMs. Network isolation and monitoring are key network security practices but do not directly address the security of the VMs themselves.

NEW QUESTION: 100

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

A. Providing as many API endpoints as possible for custom access and configurations

B. Properly configuring the deployment of the virtual network, especially the firewalls

C. Configuring second factor authentication across the network

D. Properly configuring the deployment of the virtual network, except the firewalls

E. Building and properly configuring a secure network infrastructure

Answer: (SHOW ANSWER)

NEW QUESTION: 101

In federated identity management, what role does the identity provider (IdP) play in relation to the relying party?

A. The IdP relies on the relying party to authenticate and authorize users.

B. The relying party makes assertions to the IdP about user authorizations.

C. The IdP and relying party have no direct trust relationship.

D. The IdP makes assertions to the relying party after building a trust relationship.

Answer: D (LEAVE A REPLY)

In federated identity management, the identity provider (IdP) is responsible for authenticating users and making assertions about their identity to the relying party (which could be a service or application that trusts the IdP). The IdP and the relying party establish a trust relationship in advance, which allows the IdP to assert that a user is authenticated, often in the form of security tokens or assertions like SAML or OpenID Connect.

The IdP that authenticates users and makes assertions, not the relying party. The relying party does not make assertions to the IdP; the relying party relies on assertions made by

the IdP. The IdP and relying party do have a direct trust relationship in federated identity management.

NEW QUESTION: 102
Which approach creates a secure network, invisible to unauthorized users?
A. Firewalls
B. Software-Defined Perimeter (SDP)
C. Virtual Private Network (VPN)
D. Intrusion Detection System (IDS)
Answer: B (LEAVE A REPLY)
An SDP creates a "dark" network, visible only to authorized users, enhancing security by hiding infrastructure from potential attackers. Reference: [Security Guidance v5, Domain 7 - Infrastructure & Networking]

NEW QUESTION: 103
How does SASE enhance traffic management when compared to traditional network models?
A. It solely focuses on user authentication improvements
B. It replaces existing network protocols with new proprietary ones
C. It filters traffic near user devices, reducing the need for backhauling
D. It requires all traffic to be sent through central data centers
Answer: C (LEAVE A REPLY)
SASE reduces latency and enhances performance by filtering traffic closer to the user, avoiding the need to backhaul traffic to a central data center. Reference: [Security Guidance v5, Domain 7 - Network Security]

NEW QUESTION: 104
Why is early integration of pre-deployment testing crucial in a cybersecurity project?
A. It identifies issues before full deployment, saving time and resources.
B. It increases the overall testing time and costs.
C. It allows skipping final verification tests.
D. It eliminates the need for continuous integration.
Answer: A (LEAVE A REPLY)
Integrating testing early helps identify security vulnerabilities and configuration issues before they reach production, reducing remediation costs and time. Reference: [Security Guidance v5, Domain 10 - Application Security]

NEW QUESTION: 105
Which of the following best describes a key aspect of cloud risk management?
A. A structured approach for performance optimization of cloud services
B. A structured approach to identifying, assessing, and addressing risks

C. A structured approach to establishing the different what/if scenarios for cloud vs on-premise decisions
D. A structured approach to SWOT analysis
Answer: B (LEAVE A REPLY)
A key aspect of cloud risk management is taking a structured approach to identify, assess, and address risks related to using cloud services. Thisincludes evaluating potential risks such as security vulnerabilities, data privacy issues, service outages, and compliance challenges. Effective risk management helps organizations proactively mitigate potential threats, ensuring the cloud environment is secure, compliant, and resilient.
A structured approach for performance optimization of cloud services is more related to performance management, not risk management. A structured approach to establishing the different what/if scenarios for cloud vs on-premise decisions refers to decision-making scenarios, not the identification and management of risks. A structured approach to SWOT analysis) is a strategic planning tool that focuses on strengths, weaknesses, opportunities, and threats, but it is not specifically focused on cloud risk management.

NEW QUESTION: 106
How does artificial intelligence pose both opportunities and risks in cloud security?
A. AI enhances security without any adverse implications
B. AI mainly reduces manual work with no significant security impacts
C. AI enhances detection mechanisms but could be exploited for sophisticated attacks
D. AI is only beneficial in data management, not security
Answer: C (LEAVE A REPLY)
While AI improves threat detection, it also introduces risks as attackers can use it to develop advanced attack methods. Organizations must balance these risks. Reference: [CCSK Study Guide, Domain 12 - AI and Security]

NEW QUESTION: 107
What is a primary benefit of using Identity and Access Management (IAM) roles/identities provided by cloud providers instead of static secrets?
A. They lower storage costs
B. They reduce the risk of credential leakage

C. They facilitate data encryption
D. They improve system performance
Answer: B (LEAVE A REPLY)
Using IAM roles/identities provided by cloud providers instead of static secrets (like passwords or API keys) significantly reduces the risk of credential leakage. IAM roles enable dynamic and temporary credentials, meaning that they are automatically rotated and do not need to be manually stored or managed. This eliminates the need for hardcoding sensitive credentials into code or configuration files, which can often lead to accidental exposure or misuse if not properly secured.
Lowering storage costs is not a direct benefit of using IAM roles over static secrets. Facilitating data encryption is important for security, but IAM roles are not specifically focused on data encryption. Improving system performance is not a primary benefit of using IAM roles over static secrets. The main advantage is security-related, specifically the reduction in credential leakage risks.

NEW QUESTION: 108
Why is it important to capture and centralize workload logs promptly in a cybersecurity environment?
A. To simplify application debugging processes
B Primarily to reduce data storage costs
B. Logs may be lost during a scaling event
C. To comply with data privacy regulations
Answer: C (LEAVE A REPLY)
In a cybersecurity environment, it is important to capture and centralize workload logs promptly because logs may be lost during a scaling event. When workloads are scaled up or down, such as when cloud resources are dynamically allocated, logs may not be properly captured or may be overwritten if they are not centralized and stored in a reliable, persistent location. Centralizing logs ensures that valuable security data is not lost during these events and can be accessed for incident detection, analysis, and response.

NEW QUESTION: 109
Which cloud service model typically places the most security responsibilities on the cloud customer?
A. Platform as a Service (PaaS)
B. Infrastructure as a Service (IaaS)
C. The responsibilities are evenly split between cloud provider and customer in all models.
D. Software as a Service (SaaS)
Answer: B (LEAVE A REPLY)
InInfrastructure as a Service (IaaS), the customer has themost control and security responsibilitybecause:
* The provider only secures physical infrastructure (data centers, networking, hardware).

* Customers must configure and manage firewalls, network security, operating system patches, and IAM.
* Data security, encryption, and application security are entirely the customer's responsibility.
In contrast:
* PaaS (Platform as a Service)places some security responsibility on the provider (e.g., runtime environments, managed databases).
* SaaS (Software as a Service)places most security responsibility on the provider, with customers mainly managingidentity and access controls.
This is extensively discussed in:
* CCSK v5 - Security Guidance v4.0, Domain 1 (Cloud Computing Concepts and Architectures)
* Cloud Controls Matrix (CCM) - Infrastructure and Application Security Controls.

NEW QUESTION: 110
Which of the following is a perceived advantage or disadvantage of managing enterprise risk for cloud deployments?
A. None of the above.
B. More physical control over assets and processes.
C. Increased need, but reduction in costs, for managing risks accepted by the cloud provider.
D. Decreased requirement for proactive management of relationship and adherence to contracts.
E. Greater reliance on contracts, audits, and assessments due to lack of visibility or management.
Answer: E (LEAVE A REPLY)

NEW QUESTION: 111
What is resource pooling?
A. The provider's computing resources are pooled to serve multiple consumers.
B. The dedicated computing resources of each client are pooled together in a colocation facility.
C. None of the above.
D. Internet-based CPUs are pooled to enable multi-threading.
E. Placing Internet ("cloud") data centers near multiple sources of energy, such as hydroelectric dams.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 112
If there are gaps in network logging data, what can you do?
A. Ask the cloud provider to open more ports.

B. Ask the cloud provider to close more ports.
C. Nothing. There are simply limitations around the data that can be logged in the cloud.
D. You can instrument the technology stack with your own logging.
E. Nothing. The cloud provider must make the information available.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 113
Why is it essential to include key metrics and periodic reassessment in cybersecurity governance?
A. To meet legal requirements and avoid fines
B. To ensure effective and continuous improvement of security measures
C. To document all cybersecurity incidents and monitor them overtime
D. To reduce the number of security incidents to zero
Answer: (SHOW ANSWER)
Including key metrics and periodic reassessment in cybersecurity governance is essential for ensuring the effective and continuous improvement of security measures. Metrics provide a way to assess the current state of security, identify gaps, and measure progress over time. Periodic reassessment allows organizations to adapt to emerging threats and vulnerabilities, ensuring that security controls remain relevant and effective as the threat landscape evolves.
While meeting legal requirements is important, the primary reason for metrics and reassessment is continuous improvement, not just legal compliance. Documenting cybersecurity incidents is important, but the main focus of key metrics and reassessment is improving and adapting security strategies. Zero security incidents is not feasible; the goal is to reduce incidents and manage risk, not to eliminate all incidents entirely.

NEW QUESTION: 114
CCM: A hypothetical company called: "Health4Sure" is located in the United States and provides cloud based services for tracking patient health. The company is compliant with HIPAA/HITECH Act among other industry standards. Health4Sure decides to assess the overall security of their cloud service against the CCM toolkit so that they will be able to present this document to potential clients.
Which of the following approach would be most suitable to assess the overall security posture of Health4Sure' s cloud service?
A. The CCM domain controls are mapped to HIPAA/HITECH Act and therefore Health4Sure could verify the CCM controls already covered as aresult of their compliance with HIPPA/HITECH Act. They could then assess the remaining controls thoroughly. This approach saves time while being able to assess the company's overall security posture in an efficient manner.
B. The CCM columns are mapped to HIPAA/HITECH Act and therefore Health4Sure could verify the CCM controls already covered ad a result of their compliance with

HIPPA/HITECH Act. They could then assess the remaining controls. This approach will save time.
C. The CCM domains are not mapped to HIPAA/HITECH Act. Therefore Health4Sure should assess the security posture of their cloud service against each and every control in the CCM. This approach will allow a thorough assessment of the security posture.
Answer: (SHOW ANSWER)

NEW QUESTION: 115
How does virtualized storage help avoid data loss if a drive fails?
A. Data loss is unavoidable with drive failures
B. Full back ups weekly
C. Multiple copies in different locations
D. Drives are backed up, swapped, and archived constantly
E. Incremental backups daily
Answer: (SHOW ANSWER)

NEW QUESTION: 116
Which aspect of a Cloud Service Provider's (CSPs) infrastructure security involves protecting the interfaces used to manage configurations and resources?
A. Management plane
B. Virtualization layers
C. Physical components
D. PaaS/SaaS services
Answer: A (LEAVE A REPLY)
The management plane refers to the interfaces used to manage configurations and resources in a cloud environment. It is responsible for handling administrative tasks, such as provisioning, configuration management, and monitoring of resources. Protecting the management plane is crucial because it is where sensitive configurations and access control policies are set, which can potentially be exploited if not properly secured. Securing the management plane involves ensuring that only authorized users and systems can make changes to the cloud infrastructure and resources, protecting these interfaces from unauthorized access or malicious activity.

NEW QUESTION: 117
Which of the following is one of the five essential characteristics of cloud computing as defined by NIST?
A. Hybrid clouds
B. Unlimited bandwidth
C. Nation-state boundaries
D. Multi-tenancy
E. Measured service

Answer: (SHOW ANSWER)

NEW QUESTION: 118
In the context of server-side encryption handled by cloud providers, what is the key attribute of this encryption?
A. The data is encrypted using symmetric encryption.
B. The data is not encrypted in transit.
C. The data is encrypted using customer or provider keys after transmission to the cloud.
D. The data is encrypted before transmission to the cloud.
Answer: C (LEAVE A REPLY)
In the context of server-side encryption handled by cloud providers, the data is encrypted after transmission to the cloud using either provider-managed keys or customer-managed keys. The cloud provider takes responsibility for encrypting the data when it is stored in the cloud, ensuring that the data at rest is protected.
Server-side encryption typically uses symmetric encryption for performance reasons, but this attribute is not what defines the encryption process. Also, server-side encryption focuses on protecting data once it's in the cloud, not before transmission. Encryption in transit is typically handled separately from server-side encryption and applies to data as it moves between the client and the cloud.

NEW QUESTION: 119
What primary aspects should effective cloud governance address to ensure security and compliance?
A. Encryption, redundancy, data integrity, and scalability
B. Decision making, prioritization, monitoring, and transparency
C. Service availability, disaster recovery, load balancing, and latency
D. Authentication, authorization, accounting, and auditing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 120
What is the primary reason dynamic and expansive cloud environments require agile security approaches?
A. To reduce costs associated with physical hardware
B. To simplify the deployment of virtual machines
C. To quickly respond to evolving threats and changing infrastructure
D. To ensure high availability and load balancing
Answer: (SHOW ANSWER)
Agile security approaches allow organizations to adapt to the rapid changes and emerging threats characteristic of cloud environments. Reference: [Security Guidance v5, Domain 4 - Organization Management]

NEW QUESTION: 121
Which areas should be initially prioritized for hybrid cloud security?
A. Cloud storage management and governance
B. Data center infrastructure and architecture
C. IAM and networking
D. Application development and deployment
Answer: C (LEAVE A REPLY)
Identity and Access Management (IAM) and networking are essential for secure hybrid cloud environments, as they control access and communication across diverse environments. Reference: [Security Guidance v5, Domain 5 - IAM]

NEW QUESTION: 122
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 entitlement matrix
B. An access log
C. A support table
D. An entry log
E. A validation process
Answer: E (LEAVE A REPLY)

NEW QUESTION: 123
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 metrics defining the service level required to achieve regulatory objectives.
B. The regulations that are pertinent to the contract and how to circumvent them.
C. The type of security software which meets regulations and the number of licenses that will be needed.
D. The duration of time that a security violation can occur before the client begins assessing regulatory fines.
E. The cost per incident for security breaches of regulated information.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 124
Which of the following best describes the concept of AI as a Service (AIaaS)?
A. Selling AI hardware to enterprises for internal use
B. Hosting and running AI models with customer-built solutions
C. Offering pre-built AI models to third-party vendors
D. Providing software as an AI model with no customization options
Answer: (SHOW ANSWER)
AI as a Service (AIaaS) refers to cloud-based services that provide organizations with access to pre-built or customizable AI models and infrastructure. These services allow businesses to host and run AI models, often with the ability to tailor them to meet their specific needs. AIaaS enables customers to leverage AI capabilities without needing to build the underlying infrastructure or develop complex AI models from scratch.

NEW QUESTION: 125
Which cloud security model type provides generalized templates for helping implement cloud security?
A. Conceptual models or frameworks
B. Cloud Controls Matrix (CCM)
C. Reference architectures
D. Controls models or frameworks
E. Design patterns
Answer: C (LEAVE A REPLY)

NEW QUESTION: 126
What is a primary benefit of consolidating traffic through a central bastion/transit network in a hybrid cloud environment?
A. It minimizes hybrid cloud sprawl and consolidates security.
B. It reduces the need for physical network hardware.
C. It increases network redundancy and fault tolerance.
D. It decreases the latency of data transfers across the cloud network.
Answer: A (LEAVE A REPLY)
Acentralized bastion or transit networkimproves hybrid cloud security by:
* Reducing cloud sprawlthrough a unified security control point.
* Centralizing firewall, logging, and security monitoringfor betterthreat detection and response.
* Enforcing consistent security policiesacross different cloud platforms (AWS, Azure, on-premises data centers).
* Minimizing unauthorized lateral movementwithin hybrid cloud environments.
This concept is extensively covered in:
* CCSK v5 - Security Guidance v4.0, Domain 7 (Infrastructure Security)

* Cloud Controls Matrix (CCM) - Network Security and Monitoring.

NEW QUESTION: 127
What is a key advantage of using Infrastructure as Code (IaC) in application development?
A. It removes the need for manual testing.
B. It eliminates the need for cybersecurity measures.
C. It enables version control and rapid deployment.
D. It ensures zero configuration drift by default.
Answer: (SHOW ANSWER)
Infrastructure as Code (IaC)allows organizations toautomate cloud infrastructure managementusing code-based templatesinstead of manual configuration.
Key Benefits of IaC:
* Version Control & Automation
* IaC uses version control systems (e.g., Git) to track changes in infrastructure.
* Developers can quickly deploy infrastructure updates, reducing human errors.
* Ensuresconsistent, repeatable deploymentsacross environments.
* Rapid & Scalable Deployments
* EnablesCI/CD (Continuous Integration/Continuous Deployment)pipelines.
* Automates infrastructure provisioning, reducingdeployment time from hours to minutes.
* Works withTerraform, AWS CloudFormation, Ansible, and Kubernetes manifests.
* Security & Compliance Enhancements
* Policies as Code (PaC) & Security as Code (SaC) enforce security best practices.
* Cloud Security Posture Management (CSPM)scans IaC for misconfigurations.
* Reducesshadow IT risksby enforcingpre-approved infrastructure templates.
* Prevents Configuration Drift
* RegularIaC re-application (desired state enforcement)ensuresconsistent infrastructure settings.
* Eliminatesmanual misconfigurations that lead to security vulnerabilities.
This is extensively covered in:
* CCSK v5 - Security Guidance v4.0, Domain 6 (Management Plane and Business Continuity)
* Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) - Infrastructure and Configuration Management Controls.

NEW QUESTION: 128
Any given processor and memory will nearly always be running multiple workloads, often from different tenants.
A. True
B. False
Answer: A (LEAVE A REPLY)

NEW QUESTION: 129
Which cloud-based service model enables companies to provide client-based access for partners to databases or applications?
A. Desktop-as-a-service (DaaS)
B. Infrastructure-as-a-service (IaaS)
C. Identity-as-a-service (IDaaS)
D. Software-as-a-service (SaaS)
E. Platform-as-a-service (PaaS)
Answer: E (LEAVE A REPLY)

NEW QUESTION: 130
Which of the following best explains how Multifactor Authentication (MFA) helps prevent identity-based attacks?
A. MFA relies on physical tokens and biometrics to secure accounts.
B. MFA requires multiple forms of validation that would have to compromise.
C. MFA requires and uses more complex passwords to secure accounts.
D. MFA eliminates the need for passwords through single sign-on.
Answer: B (LEAVE A REPLY)
MFA enhances security by requiring multiple independent forms of authentication, making it harder for attackers to gain unauthorized access. Reference: [Security Guidance v5, Domain 5 - IAM]

NEW QUESTION: 131
What is a common characteristic of default encryption provided by cloud providers for data at rest?
A. It is not available without an additional premium service
B. It always requires the customer's own encryption keys
C. It uses the cloud provider's keys, often at no additional cost
D. It does not support encryption for data at rest
Answer: C (LEAVE A REPLY)
Many cloud providers offer default encryption for data at rest, which is typically enabled automatically for data stored within the cloud. In these cases, the encryption is often done using the cloud provider's keys as part of the provider's security infrastructure, and it is usually provided at no additional cost to the customer.
This ensures that data is protected while at rest, reducing the risk of unauthorized access.

NEW QUESTION: 132
In which deployment model should the governance strategy consider the minimum common set of controls comprised of the Cloud Service Provider contract and the organization's internal governance agreements?
A. Private

B. IaaS
C. Public
D. Hybrid
E. PaaS
Answer: (SHOW ANSWER)

NEW QUESTION: 133
Which of the following statements are NOT requirements of governance and enterprise risk management in a cloud environment?
A. Negotiate long-term contracts with companies who use well-vetted software application to avoid the transient nature of the cloud environment.
B. Both B and C.
C. Provide transparency to stakeholders and shareholders demonstrating fiscal solvency and organizational transparency.
D. 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.
E. 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.
Answer: (SHOW ANSWER)

NEW QUESTION: 134
What is critical for securing serverless computing models in the cloud?
A. Disabling console access completely or using privileged access management
B. Validating the underlying container security
C. Managing secrets and configuration with the least privilege
D. Placing serverless components behind application load balancers
Answer: C (LEAVE A REPLY)
In serverless computing models, the primary security concern is ensuring that secrets (such as API keys, database credentials, etc.) and configuration settings are handled securely. The principle of least privilege means that these secrets and configurations should only be accessible by the minimum set of functions or services that truly need them, reducing the attack surface. Proper management of secrets and configurations ensures that unauthorized access or misuse is prevented.
Disabling console access completely or using privileged access management is important for securing any environment, but it is not specifically tied to serverless models. Validating the underlying container security is more relevant to containerized environments rather than serverless computing, which abstracts away infrastructure management. Placing serverless components behind application load balancers is useful for routing traffic but is not specifically critical for securing the serverless model itself. Managing secrets and access controls is a more direct concern for securing serverless environments.