Question #64*Topic 1*

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

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

**Correct Answer:** *D*

**[Brainiac](https://www.examtopics.com/user/Brainiac/)**

1 week, 6 days ago

A. Building and properly configuring a secure network infrastructure. The cloud provider is responsible for building and maintaining a secure network infrastructure to ensure the overall security of the cloud environment. This includes implementing appropriate security measures such as firewalls, intrusion detection systems, network segmentation, access controls, and other network security mechanisms. The provider should configure the network infrastructure in a way that minimizes vulnerabilities and protects against unauthorized access, data breaches, and other security threats. While the other options listed may also be important security considerations, building and properly configuring a secure network infrastructure is a fundamental responsibility of the cloud provider to ensure the overall security and protection of the cloud environment. Therefore, option A, building and properly configuring a secure network infrastructure, is the correct answer for the primary security responsibilities of the cloud provider in the management infrastructure.

upvoted 1 times

**[JoAsiaGje](https://www.examtopics.com/user/JoAsiaGje/)**

1 month, 3 weeks ago

**Selected Answer: A**

page 96 - The cloud provider is primarily responsible for building a secure network infrastructure and configuring it properly. The absolute top security priority is segregation and isolation of network traffic to prevent tenants from viewing another’s traffic. This is the most foundational security control for any multitenant network.

upvoted 1 times

**[Selmed993](https://www.examtopics.com/user/Selmed993/)**

2 months, 1 week ago

Pg. 96 - "Cloud users are primarily responsible for properly configuring their deployment of the virtual network, especially any virtual firewalls."

upvoted 1 times

**[gingyk](https://www.examtopics.com/user/gingyk/)**

3 months, 1 week ago

The primary security responsibilities of the cloud provider in compute virtualization are to enforceisolation and maintain a secure virtualization infrastructure.

upvoted 1 times

**[byfener](https://www.examtopics.com/user/byfener/)**

3 months, 2 weeks ago

Management Infrastructure Virtual networks for cloud computing always support remote management and, as such, securing the management plane/metastructure is critical. At times it is possible to create and destroy entire complex networks with a handful of API calls or a few clicks on a web console. Cloud Provider Responsibilities The cloud provider is primarily responsible for building a secure network infrastructure and configuring it properly. The absolute top security priority is segregation and isolation of network traffic to prevent tenants from viewing another's traffic. This is the most foundational security control for any multitenant network. Answer is A

upvoted 1 times

**[DERCHEF2009](https://www.examtopics.com/user/DERCHEF2009/)**

5 months, 3 weeks ago

**Selected Answer: A**

Yes vote also for A

upvoted 1 times

**[A\_Nevermind](https://www.examtopics.com/user/A_Nevermind/)**

7 months, 4 weeks ago

**Selected Answer: A**

Answer is A!

upvoted 2 times

**[beazzlebub](https://www.examtopics.com/user/beazzlebub/)**

8 months ago

**Selected Answer: A**

Direct quote from Security Guidance: "The cloud provider is primarily responsible for building a secure network infrastructure and configuring it properly."

upvoted 4 times

Question #65*Topic 1*

What is true of a workload?

* A. It is a unit of processing that consumes memory
* B. It does not require a hardware stack
* C. It is always a virtual machine
* D. It is configured for specific, established tasks
* E. It must be containerized

**Correct Answer:** *A*

**[Brainiac](https://www.examtopics.com/user/Brainiac/)**

1 week, 6 days ago

D. It is configured for specific, established tasks. A workload refers to a specific set of tasks or activities that are performed by a computing system. It represents the work or processing that needs to be executed. Workloads can vary in their nature and can include tasks such as data processing, application execution, computational tasks, or other forms of processing. Workloads can be configured to perform specific tasks based on the requirements and objectives of the system or application. They can be tailored and optimized to meet the desired outcomes and performance goals. The configuration of a workload involves setting up the necessary resources, parameters, and dependencies to carry out the intended tasks efficiently. It is important to note that workloads are not limited to virtual machines or containerized environments. They can be executed on different types of computing systems, including virtual machines, physical servers, containers, or even distributed computing environments. Therefore, option D, "It is configured for specific, established tasks," is the correct statement regarding workloads.

upvoted 1 times

**[JoAsiaGje](https://www.examtopics.com/user/JoAsiaGje/)**

1 month, 3 weeks ago

**Selected Answer: A**

(page 84) A workload is a unit of processing, which can be in a virtual machine, a container, or other abstraction. Workloads always run somewhere on a processor and consume memory.

upvoted 1 times

Question #68*Topic 1*

Which cloud security model type provides generalized templates for helping implement cloud security?

* A. Conceptual models or frameworks
* B. Design patterns
* C. Controls models or frameworks
* D. Reference architectures
* E. Cloud Controls Matrix (CCM)

**Correct Answer:** *D*

**[Brainiac](https://www.examtopics.com/user/Brainiac/)**

1 week, 6 days ago

D. Reference architectures. Reference architectures in the context of cloud security provide standardized and proven designs, patterns, and templates for implementing security controls and best practices in a cloud environment. These architectures serve as guides or blueprints that organizations can use to design and deploy their cloud infrastructure with security in mind. Reference architectures typically cover various aspects of cloud security, including network architecture, data protection, identity and access management, logging and monitoring, and incident response. They are designed to address common security challenges and provide organizations with a starting point for implementing effective security controls in their specific cloud environment. By utilizing reference architectures, organizations can benefit from the collective knowledge and experience of cloud security experts and leverage proven practices to enhance the security of their cloud deployments.

upvoted 1 times

**[JoAsiaGje](https://www.examtopics.com/user/JoAsiaGje/)**

1 month, 3 weeks ago

**Selected Answer: D**

(page 22) Reference architectures are templates for implementing cloud security, typically generalized (e.g. an IaaS security reference architecture). They can be very abstract, bordering on conceptual, or quite detailed, down to specific controls and functions.

upvoted 1 times

Question #69*Topic 1*

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

* A. Attributes belong to entities and identities belong to attributes. Each attribute can have multiple identities but only one entity.
* B. An attribute is a unique object within a database. Each attribute it has a number of identities which help define its parameters.
* C. An identity is a distinct and unique object within a particular namespace. Attributes are properties which belong to an identity. Each identity can have multiple attributes.
* D. Attributes are made unique by their identities.
* E. Identities are the network names given to servers. Attributes are the characteristics of each server.

**Correct Answer:** *D*

**[beazzlebub](https://www.examtopics.com/user/beazzlebub/)**

**Highly Voted** 8 months ago

**Selected Answer: C**

From Security Guidance: Identity: the unique expression of an entity within a given namespace. An entity can have multiple digital identities, such as a single individual having a work identity (or even multiple identities, depending on the systems), a social media identity, and a personal identity. For example, if you are a single entry in a single directory server then that is your identity Attributes: facets of an identity. Attributes can be relatively static (like an organizational unit) or highly dynamic (IP address, device being used, if the user authenticated with MFA, location, etc.)

upvoted 8 times

**[JCoutant](https://www.examtopics.com/user/JCoutant/)**

5 months, 2 weeks ago

From Security Guidance V4 Page 120: "Objects” are typically files, which are then stored using a cloud-platform specific mechanism. The difference is the work expression and object. The answer is correct.

upvoted 1 times

**[Brainiac](https://www.examtopics.com/user/Brainiac/)**

**Most Recent** 1 week, 3 days ago

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

upvoted 1 times

**[JoAsiaGje](https://www.examtopics.com/user/JoAsiaGje/)**

1 month, 3 weeks ago

**Selected Answer: C**

Identity: the unique expression of an entity within a given namespace. An entity can have multiple digital identities, such as a single individual having a work identity (or even multiple identities, depending on the systems), a social media identity, and a personal identity. For example, if you are a single entry in a single directory server then that is your identity. • Attributes: facets of an identity. Attributes can be relatively static (like an organizational unit) or highly dynamic (IP address, device being used, if the user authenticated with MFA, location, etc.).

upvoted 2 times

**[byfener](https://www.examtopics.com/user/byfener/)**

3 months, 2 weeks ago

**Selected Answer: C**

must be

upvoted 1 times

Question #70*Topic 1*

What is a potential concern of using Security-as-a-Service (SecaaS)?

* A. Lack of visibility
* B. Deployment flexibility
* C. Scaling and costs
* D. Intelligence sharing
* E. Insulation of clients

**Correct Answer:** *A*

**[Brainiac](https://www.examtopics.com/user/Brainiac/)**

1 week, 5 days ago

A potential concern of using Security-as-a-Service (SecaaS) is: C. Scaling and costs SecaaS typically operates on a subscription-based model where organizations pay for the security services provided. As the organization's needs grow and more resources are required, scaling the services can lead to increased costs. Additionally, organizations may face challenges in accurately estimating the necessary resources and cost implications, which can result in unexpected expenses.

upvoted 1 times

**[JoAsiaGje](https://www.examtopics.com/user/JoAsiaGje/)**

1 month, 3 weeks ago

**Selected Answer: A**

(page 141) Lack of visibility. Since services operate at a remove from the customer, they often provide less visibility or data compared to running one’s own operation.

upvoted 1 times

Question #71*Topic 1*

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

* A. Integrated development environments
* B. Updated threat and trust models
* C. No modification is needed
* D. Just-in-time compilers
* E. Both B and C

**Correct Answer:** *A*

**[Brainiac](https://www.examtopics.com/user/Brainiac/)**

1 week, 5 days ago

To address application security in a Cloud Computing environment, the SDLC (Software Development Life Cycle) should be modified by: E. Both B and C Updated threat and trust models: Cloud Computing introduces new security considerations and risks compared to traditional environments. It is important to update threat models and trust models to account for the unique characteristics of the Cloud, such as shared responsibility models, multi-tenancy, and potential vulnerabilities associated with virtualization and cloud infrastructure. No modification is needed: While some aspects of the SDLC may remain the same, it is crucial to recognize that Cloud Computing environments introduce new considerations and requirements. Therefore, modifications to the SDLC are necessary to address these specific challenges and ensure application security in the Cloud. By combining the updated threat and trust models with the recognition that modifications are necessary, organizations can effectively address application security within the context of Cloud Computing.

upvoted 1 times

**[A\_Nevermind](https://www.examtopics.com/user/A_Nevermind/)**

6 months, 1 week ago

**Selected Answer: B**

Changing threat models. The cloud provider relationship and the shared security model will need to be included in the threat model, as well as in any operational and incident response plans. Threat models also need to adapt to reflect the technical differences of the cloud provider or platform in use

upvoted 4 times

**[Petza](https://www.examtopics.com/user/Petza/)**

6 months, 3 weeks ago

**Selected Answer: A**

The given answer is correct.

upvoted 2 times

**[beazzlebub](https://www.examtopics.com/user/beazzlebub/)**

8 months ago

**Selected Answer: B**

Modification of the SDLC to use an IDE will have very little impact on application security. Although no option is very strong here B is the answer for me, use of threat and trust models.

upvoted 4 times

Question #72*Topic 1*

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

* A. Data Security and Encryption
* B. Information Governance
* C. Incident Response, Notification and Remediation
* D. Compliance and Audit Management
* E. Infrastructure Security

**Correct Answer:** *C*

**[Brainiac](https://www.examtopics.com/user/Brainiac/)**

1 week, 3 days ago

The governance domain that focuses on proper and adequate incident detection, response, notification, and remediation is: C. Incident Response, Notification, and Remediation This domain specifically deals with handling incidents effectively and efficiently within an organization. It includes activities such as incident detection, response planning, incident notification, and implementing appropriate remediation measures. By having a well-defined incident response process in place, organizations can minimize the impact of security incidents and effectively address any security breaches or vulnerabilities that arise.

upvoted 1 times

**[JoAsiaGje](https://www.examtopics.com/user/JoAsiaGje/)**

1 month, 3 weeks ago

**Selected Answer: C**

(page 25) Domain 9 : Incident Response, Notification and Remediation Proper and adequate incident detection, response, notification, and remediation. This attempts to address items that should be in place at both provider and user levels to enable proper incident handling and forensics. This domain will help you understand the complexities the cloud brings to your current incident-handling program.

upvoted 1 times

**[Petza](https://www.examtopics.com/user/Petza/)**

6 months, 3 weeks ago

**Selected Answer: C**

The given answer is correct.

upvoted 1 times

**[JOKERO](https://www.examtopics.com/user/JOKERO/)**

7 months ago

governance domain, not operational domain (D)

upvoted 1 times

Question #73*Topic 1*

Which opportunity helps reduce common application security issues?

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

**Correct Answer:** *A*

**[Brainiac](https://www.examtopics.com/user/Brainiac/)**

1 week, 3 days ago

The opportunity that helps reduce common application security issues is: D. Segregation by default Segregation by default refers to the practice of isolating different components and resources within an application or system by default. By implementing proper segregation measures, such as network segmentation and access controls, organizations can reduce the risk of unauthorized access and limit the potential impact of security breaches. This approach helps prevent lateral movement and contains the impact of any compromised component or system. By enforcing segregation as a default principle, organizations can enhance application security and minimize the potential for common security issues.

upvoted 1 times

**[Secexpert](https://www.examtopics.com/user/Secexpert/)**

1 week, 6 days ago

It's Elasticity. As it enables greater use of immutability

upvoted 1 times

**[moota](https://www.examtopics.com/user/moota/)**

2 months, 2 weeks ago

**Selected Answer: D**

10.1.5 Some of these have nothing directly to do with security, but the following trends offer opportunities to reduce common security issues: • Segregation by default

upvoted 2 times

**[jre62294](https://www.examtopics.com/user/jre62294/)**

4 months, 3 weeks ago

**Selected Answer: D**

Secuirty Guidance 10.1.5: Sgregation by default, inmmutable infra, increased use of micro-services, paas and serverless arch.

upvoted 2 times

**[vavofa5697](https://www.examtopics.com/user/vavofa5697/)**

3 months, 2 weeks ago

thanks!

upvoted 1 times

**[A\_Nevermind](https://www.examtopics.com/user/A_Nevermind/)**

6 months, 1 week ago

**Selected Answer: A**

From de guidance. Elasticity enables greater use of immutable infrastructure. When using elasticity tools like auto-scale groups each production system is launched dynamically, based on a baseline image, and may be automatically deprovisioned without human interaction.

upvoted 3 times

**[SQCISSP](https://www.examtopics.com/user/SQCISSP/)**

6 months, 2 weeks ago

Correct Answer is Option D: Segregation By Default Reference: Segregation by default: Applications can easily be run in their own isolated cloud environments. Depending on the provider, this could be a separate virtual network or account/sub-account.

upvoted 1 times

**[ICEYNYSE](https://www.examtopics.com/user/ICEYNYSE/)**

7 months ago

Elastic infrastructure is Immutable infrastructure.

upvoted 2 times

**[cjkuga](https://www.examtopics.com/user/cjkuga/)**

7 months, 1 week ago

**Selected Answer: D**

Following trends offer opportunities to reduce common security issues: Segregation by default, Immutable infrastructure, Increased use of micro-services, PaaS and "serverless" architecture.

upvoted 3 times

Question #74*Topic 1*

What is the most significant security difference between traditional infrastructure and cloud computing?

* A. Management plane
* B. Intrusion detection options
* C. Secondary authentication factors
* D. Network access points
* E. Mobile security configuration options

**Correct Answer:** *A*

**[Brainiac](https://www.examtopics.com/user/Brainiac/)**

1 week, 3 days ago

The most significant security difference between traditional infrastructure and cloud computing is: A. Management plane In traditional infrastructure, organizations have direct control over the entire management plane, including physical servers, network devices, and security configurations. They are responsible for managing and securing the infrastructure themselves. On the other hand, in cloud computing, the management plane is abstracted and provided by the cloud service provider (CSP). The CSP manages the underlying infrastructure, including servers, storage, and network, while the organization focuses on managing their applications and data. This shift in responsibility for the management plane introduces a significant security difference. In traditional infrastructure, organizations have granular control over security configurations, whereas in cloud computing, they rely on the CSP's management and security practices. It becomes crucial for organizations to understand and assess the security controls and practices provided by the CSP to ensure the protection of their applications and data in the cloud.

upvoted 1 times

**[moota](https://www.examtopics.com/user/moota/)**

2 months, 2 weeks ago

**Selected Answer: A**

Domain 6: We always have a management plane, the tools and interfaces we use to manage our infrastructure, platforms, and applications, but cloud abstracts and centralizes administrative management of resources. Instead of controlling a data center configuration with boxes and wires, it is now controlled with API calls and web consoles.

upvoted 2 times

Question #76*Topic 1*

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

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

**Correct Answer:** *E*

**[Brainiac](https://www.examtopics.com/user/Brainiac/)**

1 week, 3 days ago

When investigating an incident in an Infrastructure as a Service (IaaS) environment, the user can investigate: E. Their own virtual instances in the cloud. In an IaaS environment, users have control over their own virtual instances or virtual machines deployed within the cloud infrastructure. They have the ability to access and investigate their own virtual instances to gather logs, analyze configurations, review security settings, and identify any potential issues or indicators of compromise. However, it is important to note that users typically do not have access to investigate other customers' virtual instances or the underlying infrastructure controlled by the cloud service provider (CSP). Investigating the CSP server facility, logs of other customers in a multi-tenant cloud, network components controlled by the CSP, or the CSP office spaces would generally be outside the user's scope of investigation.

upvoted 1 times

Question #77*Topic 1*

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

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

**Correct Answer:** *D*

**[cjkuga](https://www.examtopics.com/user/cjkuga/)**

**Highly Voted** 7 months, 1 week ago

**Selected Answer: A**

From the Security Guidance document: On occasion, an actual cloud application or environment could itself be relevant to resolving a dispute. In these circumstances, the application and environment will likely be outside the control of the client and require that a subpoena or other discovery process be served on the provider directly.

upvoted 8 times

**[SQCISSP](https://www.examtopics.com/user/SQCISSP/)**

**Highly Voted** 6 months, 2 weeks ago

Correct Answer is Option A Reference: 3.1.3.2 Relevant Cloud Applications and Environment On occasion, an actual cloud application or environment could itself be relevant to resolving a dispute. In these circumstances, the application and environment will likely be outside the control of the client and require that a subpoena or other discovery process be served on the provider directly.

upvoted 5 times

**[Brainiac](https://www.examtopics.com/user/Brainiac/)**

**Most Recent** 1 week, 3 days ago

If the actual cloud application or environment is relevant to resolving a dispute in litigation or investigation, the information is likely to be obtained through: A. It may require a subpoena of the provider directly. In such cases, if the information stored or hosted in the cloud is necessary for the litigation or investigation, the party involved may need to issue a subpoena to the cloud service provider (CSP). A subpoena is a legal order that requires the CSP to provide the requested information or access to the cloud application or environment. It's important to note that the specific legal processes and requirements for obtaining information from a cloud provider may vary depending on the jurisdiction and applicable laws. Consulting legal professionals familiar with the jurisdiction and the relevant legal processes is crucial in such situations.

upvoted 1 times

**[Fripper](https://www.examtopics.com/user/Fripper/)**

1 month, 3 weeks ago

**Selected Answer: A**

Should be A, unless the provider is headquartered in a rogue state in which case it requires a declaration of war

upvoted 3 times

Question #79*Topic 1*

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

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

**Correct Answer:** *A*

**[Brainiac](https://www.examtopics.com/user/Brainiac/)**

1 week, 3 days ago

A. Enforce isolation and maintain a secure virtualization infrastructure. Cloud providers are responsible for ensuring that virtualized resources are isolated from each other, providing strong segregation between tenants. They must implement robust virtualization technologies and mechanisms to enforce this isolation, preventing unauthorized access or interference between different workloads. Additionally, cloud providers have the responsibility to maintain a secure virtualization infrastructure. This includes regularly patching and updating the underlying hypervisors, managing the host environment's security configurations, and implementing security measures to protect against vulnerabilities or attacks targeting the virtualization layer. While customers have their own security responsibilities within their virtual instances, the cloud provider's role primarily involves enforcing isolation and maintaining a secure virtualization infrastructure. Customers, on the other hand, are responsible for configuring the security settings within their virtual instances and monitoring and logging their own workloads (option B and E).

upvoted 1 times

**[JoAsiaGje](https://www.examtopics.com/user/JoAsiaGje/)**

1 month, 3 weeks ago

**Selected Answer: A**

(Security Guidance p.93) Isolation ensures that compute processes or memory in one virtual machine/container should not be visible to another. It is how we separate different tenants, even when they are running processes on the same physical hardware. • The cloud provider is also responsible for securing the underlying infrastructure and the virtualization technology from external attack or internal misuse. This means using patched and up-to-date hypervisors that are properly configured and supported with processes to keep them up to date and secure over time. The inability to patch hypervisors across a cloud deployment could create a fundamentally insecure cloud when a new vulnerability in the technology is discovered.

upvoted 1 times

Question #80*Topic 1*

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 data destruction plan
* B. A communication plan
* C. A back-up website
* D. A spill remediation kit
* E. A rainy day fund

**Correct Answer:** *B*

**[Brainiac](https://www.examtopics.com/user/Brainiac/)**

1 week, 3 days ago

Every cloud customer should set up with its cloud service provider (CSP): B. A communication plan. A communication plan is crucial in the event of an incident or security breach within the cloud environment. It outlines the processes, procedures, and channels of communication to be followed during an incident. This includes establishing lines of communication with the CSP's incident response team, establishing escalation paths, and defining communication protocols for notifying and updating relevant stakeholders, such as internal teams, customers, partners, and regulatory authorities. Having a well-defined communication plan helps ensure effective and timely communication during an incident, facilitating coordinated response efforts and minimizing the impact on business operations. It helps maintain transparency, manage expectations, and establish clear lines of communication between the cloud customer and the CSP in order to address and resolve the incident efficiently.

upvoted 1 times

**[JoAsiaGje](https://www.examtopics.com/user/JoAsiaGje/)**

1 month, 3 weeks ago

**Selected Answer: B**

(Security Guidance p.107) • Cloud customers must set up proper communication paths with the provider that can be utilized in the event of an incident. Existing open standards can facilitate incident communication.

upvoted 2 times

Question #81*Topic 1*

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

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

**Correct Answer:** *B*

**[Brainiac](https://www.examtopics.com/user/Brainiac/)**

1 week, 3 days ago

The audits should use: B. Independent auditors. Independent auditors are external professionals or organizations that are not directly affiliated with the cloud customer or the cloud provider. They have the necessary expertise and objectivity to assess the security controls, practices, and compliance of the cloud environment. Independent auditors follow established auditing standards and frameworks and conduct audits with impartiality and integrity. Using independent auditors helps ensure a neutral and unbiased evaluation of the cloud service provider's security measures and adherence to industry best practices and standards. They provide an objective assessment of the cloud provider's security posture, offering confidence to cloud customers and other stakeholders regarding the effectiveness of security controls in place.

upvoted 1 times

**[JoAsiaGje](https://www.examtopics.com/user/JoAsiaGje/)**

1 month, 3 weeks ago

**Selected Answer: B**

(Security Guidance p57) Proper organizational governance naturally includes audit and assurance. Audits must be independently conducted and should be robustly designed to reflect best practice, appropriate resources, and tested protocols and standards. Before delving into cloud implications we need to define the scope of audit management related to information security.

upvoted 1 times

Question #82*Topic 1*

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

* A. DLP can provide options for quickly deleting all of the data stored in a cloud environment.
* B. DLP can classify all data in a storage repository.
* C. DLP never provides options for how data found in violation of a policy can be handled.
* D. DLP can provide options for where data is stored.
* E. DLP can provide options for how data found in violation of a policy can be handled.

**Correct Answer:** *E*

**[Brainiac](https://www.examtopics.com/user/Brainiac/)**

1 week, 3 days ago

E. DLP can provide options for how data found in violation of a policy can be handled. Data Loss Prevention (DLP) solutions are designed to prevent unauthorized or accidental disclosure of sensitive data. When data is detected as being in violation of a policy (e.g., containing sensitive information, violating data handling regulations), DLP solutions can offer various options for how that data can be handled. These options may include actions such as quarantining the data, encrypting it, alerting administrators or relevant personnel, blocking its transmission, or applying remediation actions to remove or redact the sensitive information. The specific handling options provided by DLP solutions can be configured according to the organization's policies and requirements.

upvoted 1 times

**[odisor](https://www.examtopics.com/user/odisor/)**

3 weeks, 4 days ago

Answer is correct: E Data Loss Prevention (DLP) solutions are designed to monitor and protect sensitive data in various environments, such as cloud storage, networks, and endpoints. When sensitive data is identified, DLP systems can provide options for handling the data based on predefined policies. These options may include actions such as blocking the data transmission, encrypting the data, alerting administrators, quarantining the data, or applying remediation measures. The goal is to prevent data loss or unauthorized exposure of sensitive information.

upvoted 2 times

Question #84*Topic 1*

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

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

**Correct Answer:** *C*

**[beazzlebub](https://www.examtopics.com/user/beazzlebub/)**

**Highly Voted** 8 months ago

**Selected Answer: A**

From Security Guidance v4. Section 3.1.2.5: It is critical for a provider to publish, and a customer to evaluate, the scope of the assessment, and which features and services are included in the assessment.

upvoted 12 times

**[Brainiac](https://www.examtopics.com/user/Brainiac/)**

**Most Recent** 1 week, 3 days ago

For third-party audits or attestations, it is critical for providers to publish and customers to evaluate: A. Scope of the assessment and the exact included features and services for the assessment. When it comes to third-party audits or attestations, the scope of the assessment is of utmost importance. Providers should clearly publish the scope of the assessment, specifying the exact features, services, and components included in the assessment. This helps customers understand which aspects of the provider's offering have been evaluated for security, compliance, or other relevant factors. By evaluating the scope, customers can assess if the assessed components align with their specific requirements, regulatory obligations, or industry standards. It provides transparency and allows customers to make informed decisions regarding the security and compliance of the provider's offerings.

upvoted 1 times

**[SKUNK1](https://www.examtopics.com/user/SKUNK1/)**

3 months, 4 weeks ago

Agree with beazzlebub too

upvoted 1 times

**[A\_Nevermind](https://www.examtopics.com/user/A_Nevermind/)**

6 months, 1 week ago

**Selected Answer: A**

It is A

upvoted 2 times

**[cjkuga](https://www.examtopics.com/user/cjkuga/)**

7 months, 1 week ago

**Selected Answer: A**

Agree with beazzlebub's answer

upvoted 4 times

Question #85*Topic 1*

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

* A. Create, Store, Use, and Share
* B. Create and Store
* C. Create and Use
* D. Create, Store, and Use
* E. Create, Use, Store, and Delete

**Correct Answer:** *A*

**[Brainiac](https://www.examtopics.com/user/Brainiac/)**

1 week, 3 days ago

D. Create, Store, and Use. To effectively process data throughout its lifecycle, the following functions are necessary: 1. Create: This involves the creation or generation of data, such as capturing user input, generating reports, or creating new records. The data is initially created or collected during this phase. 2. Store: Data needs to be stored or persisted in a secure and accessible manner. This includes activities such as data storage, database management, backup, and data retention. 3. Use: This refers to utilizing the data for various purposes, such as analysis, reporting, decision-making, or providing services. Data is processed, manipulated, and accessed during this phase to derive value or fulfill specific requirements. By combining these functions—Create, Store, and Use—organizations can effectively manage and leverage data throughout its lifecycle. However, it's important to note that there may be additional functions involved in the overall data lifecycle, such as sharing or deletion, depending on specific requirements and compliance obligations (option E).

upvoted 1 times

**[mattch](https://www.examtopics.com/user/mattch/)**

1 month, 1 week ago

**Selected Answer: C**

From Security Guidance v4. Section 5.1.2.2, Table 1--Information Lifecycle Phases: Function "Read" to ALL phases, Function "Process" to Create & Use, and Function "Store" to Store & Archive.

upvoted 2 times

**[edwoos](https://www.examtopics.com/user/edwoos/)**

3 months ago

It is C

upvoted 2 times

**[A\_Nevermind](https://www.examtopics.com/user/A_Nevermind/)**

6 months, 1 week ago

**Selected Answer: C**

From the table in the guidance. THe answer is C

upvoted 2 times

**[SQCISSP](https://www.examtopics.com/user/SQCISSP/)**

6 months, 2 weeks ago

Correct Answer is Option C Process. Perform a transaction on the data; update it; use it in a business processing transaction, etc. Create Function Use Action Archive Location Store Share Destroy Process : Create and Use

upvoted 3 times

**[Petza](https://www.examtopics.com/user/Petza/)**

6 months, 3 weeks ago

**Selected Answer: C**

Answer C!

upvoted 4 times

Question #87*Topic 1*

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

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

**Correct Answer:** *C*

**[Brainiac](https://www.examtopics.com/user/Brainiac/)**

1 week, 3 days ago

C. Measured service. Measured service is one of the key characteristics of cloud computing, according to NIST's definition. It refers to the capability of cloud computing providers to measure and monitor resource usage by the consumers of cloud services. The resource usage can include computing power, storage, network bandwidth, or other relevant metrics. By implementing measured service, cloud providers can provide transparency and accountability to their customers by accurately measuring and reporting resource usage. This allows customers to be billed based on their actual usage and provides insights for optimization and cost management.

upvoted 1 times

**[JoAsiaGje](https://www.examtopics.com/user/JoAsiaGje/)**

1 month, 3 weeks ago

**Selected Answer: C**

Security Guidance page 10 table

upvoted 2 times

Question #88*Topic 1*

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

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

**Correct Answer:** *B*

**[Brainiac](https://www.examtopics.com/user/Brainiac/)**

1 week, 3 days ago

B. A number of requirements to be implemented, based upon numerous standards and regulatory requirements. The Cloud Control Matrix (CCM) is a framework developed by the Cloud Security Alliance (CSA) that provides a catalog of security controls and best practices for cloud computing. It is designed to assist organizations in assessing the security risks associated with cloud computing and implementing appropriate security measures. The CCM includes a comprehensive set of controls and requirements that should be considered and implemented by cloud service providers and cloud customers. These controls cover various domains such as governance and risk management, compliance, data security, physical security, and incident response, among others. The requirements are derived from industry-accepted standards, frameworks, and regulatory requirements.

upvoted 1 times

Question #90*Topic 1*

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

* A. Use strong multi-factor authentication
* B. Secure backup processes for key management systems
* C. Segregate keys from the provider hosting data
* D. Stipulate encryption in contract language
* E. Select cloud providers within the same country as customer

**Correct Answer:** *C*

Question #95*Topic 1*

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

**Correct Answer:** *B*

**[Brainiac](https://www.examtopics.com/user/Brainiac/)**

1 week, 3 days ago

The statement that best describes the Data Security Lifecycle is: B. The Data Security Lifecycle has six stages, can be non-linear, and varies in that some data may never pass through all stages. The Data Security Lifecycle typically consists of six stages: Identify, Protect, Detect, Respond, Recover, and Review. These stages represent different activities and processes involved in securing data throughout its lifecycle. However, the lifecycle is not strictly linear, and the progression through these stages can vary depending on the specific data and its context. Some data may not pass through all stages of the Data Security Lifecycle. For example, not all data may require the same level of protection or may not be subjected to the same detection and response mechanisms. The lifecycle is flexible and adaptable to different data types, risk levels, and security requirements.

upvoted 1 times

**[JoAsiaGje](https://www.examtopics.com/user/JoAsiaGje/)**

1 month, 3 weeks ago

from Security Guidance, page 63: The lifecycle includes six phases from creation to destruction. Although it is shown as a linear progression, once created, data can bounce between phases without restriction, and may not pass through all stages (for example, not all data is eventually destroyed).

upvoted 2 times

Question #96*Topic 1*

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. Media encryption
* C. Asymmetric encryption
* D. Object encryption
* E. Client/application encryption

**Correct Answer:** *E*

**[Brainiac](https://www.examtopics.com/user/Brainiac/)**

1 week, 3 days ago

D. Object encryption Object encryption involves encrypting individual objects or files stored in the object storage system. It ensures that each object is encrypted before being stored and can only be decrypted by authorized users or applications with the appropriate encryption keys. Object encryption provides granular control over the encryption of data at rest, making it suitable for securing data stored in object storage. It helps protect the confidentiality and integrity of the stored objects, even if the underlying storage infrastructure is compromised. The other encryption methods mentioned are not specifically tailored for object storage scenarios: A. Database encryption typically refers to encrypting data within a database management system, which is different from object storage. B. Media encryption involves encrypting storage media such as hard drives or tapes, rather than individual objects within an object storage system. E. Client/application encryption refers to encrypting data at the client or application level before it is sent to the storage system, which is independent of the specific storage backend being used.

upvoted 1 times

**[moota](https://www.examtopics.com/user/moota/)**

2 months, 2 weeks ago

**Selected Answer: E**

11.1.4.2 Client-side encryption: When object storage is used as the back-end for an application (including mobile applications), encrypt the data using an encryption engine embedded in the application or client.

upvoted 2 times

Question #97*Topic 1*

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

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

**Correct Answer:** *D*

**[Brainiac](https://www.examtopics.com/user/Brainiac/)**

1 week, 3 days ago

D. Cloud Provider In the SaaS model, the cloud provider is responsible for managing and securing the underlying infrastructure, including the network, servers, storage, and physical data centers. They are also responsible for implementing security measures at the platform level, such as access controls, authentication mechanisms, and data encryption. The cloud provider ensures the availability, scalability, and reliability of the SaaS application, as well as the protection of customer data stored within the service. They employ various security measures to safeguard against threats and vulnerabilities that could impact the SaaS environment.

upvoted 1 times

Question #98*Topic 1*

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

* A. Encryption
* B. Organization
* C. Knowledge management
* D. IDS
* E. Insulation

**Correct Answer:** *E*

**[SQCISSP](https://www.examtopics.com/user/SQCISSP/)**

**Highly Voted** 6 months, 2 weeks ago

Encryption makes more sense as Insulation has a completely different meaning with reference to the question itself.

upvoted 5 times

**[Brainiac](https://www.examtopics.com/user/Brainiac/)**

**Most Recent** 1 week, 3 days ago

A. Encryption Data fragmentation involves dividing data into smaller pieces or fragments and distributing them across different locations or systems. This technique can help mitigate the impact of a data breach by making it more difficult for an attacker to access and reconstruct the complete data set. However, data fragmentation alone does not provide confidentiality for the individual data fragments. To ensure the confidentiality of each fragment, encryption can be used. By applying encryption to the fragmented data, even if an attacker gains access to one or more fragments, they would not be able to decipher the sensitive information without the encryption key. This provides an additional layer of security and confidentiality to the fragmented data.

upvoted 1 times

**[FATWENTYSIX](https://www.examtopics.com/user/FATWENTYSIX/)**

1 month ago

Definitely not E. CCSK Study Guide pg 141: Insulation of clients. In some cases, SecaaS can intercept attacks before they hit the organization directly. For example, spam filtering and cloud-based Web Application Firewalls are positioned between the attackers and the organization. They can absorb certain attacks before they ever reach the customer’s assets

upvoted 2 times

**[moota](https://www.examtopics.com/user/moota/)**

2 months, 2 weeks ago

**Selected Answer: A**

In the context of data fragmentation, A is the closer answer compared to E.

upvoted 3 times

**[Petza](https://www.examtopics.com/user/Petza/)**

7 months, 1 week ago

**Selected Answer: A**

Answer A & only A

upvoted 4 times

Question #99*Topic 1*

Which of the following statements best defines the "authorization" as a component of identity, entitlement, and access management?

* A. The process of specifying and maintaining access policies
* B. Checking data storage to make sure it meets compliance requirements
* C. Giving a third party vendor permission to work on your cloud solution
* D. Establishing/asserting the identity to the application
* E. Enforcing the rules by which access is granted to the resources

**Correct Answer:** *D*

**[MassoudAbedian](https://www.examtopics.com/user/MassoudAbedian/)**

**Highly Voted** 7 months, 1 week ago

**Selected Answer: E**

12.1 Overview Authorization: allowing an identity access to something (e.g. data or a function). Also known as Authz.

upvoted 6 times

**[Brainiac](https://www.examtopics.com/user/Brainiac/)**

**Most Recent** 1 week, 3 days ago

E. Enforcing the rules by which access is granted to the resources Authorization is the process of determining and enforcing the rules or permissions by which access is granted to specific resources or functionalities within a system. It involves evaluating the privileges and entitlements associated with an identity or user and deciding whether they have the necessary permissions to perform a requested action or access a particular resource. Authorization typically works in conjunction with authentication, which verifies the identity of the user or entity requesting access. Once the authentication is successful, the authorization component determines the level of access rights and permissions associated with that identity and enforces them. By enforcing access control rules and permissions, authorization ensures that users are only granted access to the resources they are entitled to, based on their role, privileges, or other defined criteria. This helps protect sensitive data, maintain system integrity, and prevent unauthorized access or misuse of resources.

upvoted 1 times

Question #100*Topic 1*

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

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

**Correct Answer:** *A*

**[Brainiac](https://www.examtopics.com/user/Brainiac/)**

1 week, 3 days ago

D. Both A and C 1. By proxying or redirecting web traffic to the cloud provider: The cloud consumer can direct their web traffic through a web security service provided by the cloud provider. The provider's security service will then analyze and filter the web traffic, applying security controls such as web application firewalls, anti-malware scanning, content filtering, and other security mechanisms. 2. On-premise through a software or appliance installation: Alternatively, the cloud consumer can deploy web security as a service on their own premises by installing dedicated software or appliances provided by a third-party vendor. This software or appliance acts as a gateway or intermediary between the cloud consumer's network and the internet, intercepting and inspecting web traffic for security threats. By combining these approaches, the cloud consumer can leverage both the cloud provider's web security service and deploy their own on-premise solution to enhance their web security posture.

upvoted 1 times

**[anon\_vzla007](https://www.examtopics.com/user/anon_vzla007/)**

1 week, 4 days ago

**Selected Answer: D**

Web Security involves real-time protection, offered either on-premises through software and/or appliance installation, or via the Cloud by proxying or redirecting web traffic to the cloud provider (or a hybrid of both

upvoted 1 times

**[NJALPHA](https://www.examtopics.com/user/NJALPHA/)**

2 months, 2 weeks ago

D- Explanation :Web Security involves real-time protection, offered either on-premises through software and/or appliance installation, or via the Cloud by proxying or redirecting web traffic to the cloud provider (or a hybrid of both).

upvoted 1 times

**[moota](https://www.examtopics.com/user/moota/)**

2 months, 2 weeks ago

**Selected Answer: D**

I go for D. From 13.1.2.3: > ...via the Cloud by proxying or redirecting web traffic to the cloud provider (or a hybrid of both)

upvoted 1 times

**[cjkuga](https://www.examtopics.com/user/cjkuga/)**

7 months, 1 week ago

**Selected Answer: D**

Both A and C, 13.1.2.3

upvoted 3 times

**[DrTee](https://www.examtopics.com/user/DrTee/)**

4 months, 1 week ago

Questions asks about Web Sec as a Service, the answer should only be A

upvoted 1 times

Question #102*Topic 1*

What of the following is NOT an essential characteristic of cloud computing?

* A. Broad Network Access
* B. Measured Service
* C. Third Party Service
* D. Rapid Elasticity
* E. Resource Pooling

**Correct Answer:** *C*

**[Brainiac](https://www.examtopics.com/user/Brainiac/)**

1 week, 3 days ago

C. Third Party Service While third-party services are often associated with cloud computing and can be utilized within cloud environments, they are not considered one of the essential characteristics of cloud computing. The essential characteristics of cloud computing, as defined by the National Institute of Standards and Technology (NIST), include: On-Demand Self-Service: Users can provision and manage cloud resources without requiring interaction with the cloud provider. Broad Network Access: Cloud services are accessible over the network via standard mechanisms. Resource Pooling: Cloud provider's computing resources are pooled to serve multiple users, with different physical and virtual resources dynamically assigned and reassigned. Rapid Elasticity: Computing resources can be rapidly scaled up or down based on demand. Measured Service: Cloud systems automatically control and optimize resource usage, and resource usage can be monitored, controlled, and reported, providing transparency and accountability. Therefore, the correct answer is C. Third Party Service.

upvoted 1 times

Question #105*Topic 1*

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

* E. Dynamic Application Security Testing (DAST)

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?

* E. Hybrid

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

* B. Management plane

What does it mean if the system or environment is built automatically from a template?

* C. Changes made in production are overwritten by the next code or template change.

Which type of application security testing involves manual activity that is not necessarily integrated into automated testing?

* A. Code ReviewQuestion #112*Topic 1*

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

* C. Secure DeploymentQuestion #113*Topic 1*

Highly regulated industries such as finance and health care should consider the impact of cloud providers operating in diverse geographic locations and  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

* D. Legal jurisdictions

The key concern of data location is:

* D. Data is stored only in geographic locations permitted by regulations

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

* D. Bastion

What are the barriers to developing full confidence in security as a service (SecaaS)?

* E. Compliance, multi-tenancy, and vendor lock-in

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

* B. SAML

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

* D. Big Data as a Service