Question #1*Topic 1*

All cloud services utilize virtualization technologies.

* B. True

**Correct Answer:** *B*  
*Community vote distribution*

B (100%)

1 week, 2 days ago

A. False While virtualization is a common technology used in many cloud services, not all cloud services rely on virtualization. There are different types of cloud services, and some may not utilize virtualization technologies. For example, in a serverless computing model, the cloud provider manages the infrastructure and runs the code on-demand without the need for the user to provision or manage virtual machines. Serverless computing abstracts away the underlying infrastructure and allows users to focus solely on their application logic without dealing with virtualization directly. Similarly, in a container-based cloud service, containers are used to package and run applications with lightweight virtualization, but it may not involve the use of traditional virtual machines. Therefore, it is not accurate to say that all cloud services utilize virtualization technologies.

upvoted 1 times

1 month, 3 weeks ago

**Selected Answer: B**

agreed

upvoted 1 times

2 months, 2 weeks ago

**Selected Answer: B**

> As mentioned in the introduction, cloud computing is fundamentally based on virtualization: It’s how we abstract resources to create pools. Without virtualization, there is no cloud.

upvoted 1 times

6 months, 1 week ago

No objection, all cloud systems are virtualized.

upvoted 1 times

Question #2*Topic 1*

If there are gaps in network logging data, what can you do?

* C. You can instrument the technology stack with your own logging.

**Correct Answer:** *C*

*Community vote distribution*

C (100%)

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

1 week, 2 days ago

C. You can instrument the technology stack with your own logging. If there are gaps in network logging data provided by the cloud provider, one option is to instrument your own technology stack with additional logging capabilities. This involves implementing logging mechanisms within your applications, systems, or network infrastructure to capture the desired data. By instrumenting your technology stack with your own logging, you can collect the specific information you need for monitoring, troubleshooting, and security purposes. This gives you more control over the logging process and allows you to fill in any gaps in the network logging data provided by the cloud provider. It's important to note that the cloud provider may have limitations or restrictions on certain aspects of logging due to security or privacy considerations. In such cases, you may need to work with the cloud provider to find an acceptable solution that meets your logging requirements while adhering to their policies.

upvoted 1 times

**Selected Answer: C**

Security Guidance page 105

**Selected Answer: C**

> Where there are gaps you can sometimes instrument the technology stack with your own logging. This can work within instances, containers, and application code in order to gain telemetry important for the investigation. Pay particular attention to PaaS and serverless application architectures; you will likely need to add custom application-level logging.

Not sure what "instrument" in this context means? "Augment" could be a better word here.

upvoted 1 times

**Selected Answer: C**

Question #3*Topic 1*

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

* C. Control Specification

**Correct Answer:** *C*

*Community vote distribution*

C (100%)

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

1 month, 3 weeks ago

**Selected Answer: C**

Correct, Control specification determines the risk.

upvoted 2 times

**[yoyoman85](https://www.examtopics.com/user/yoyoman85/)**

2 months, 3 weeks ago

**Selected Answer: C**

agreed, control specification determines the risk.

upvoted 1 times

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

3 months ago

agreed, control specification determines the risk.

upvoted 1 times

Question #4*Topic 1*

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

* E. The cloud provider

**Correct Answer:** *E*

*Community vote distribution*

E (100%)

1 week, 5 days ago

p92 of security guidance: The cloud provider will always be responsible for securing the physical infrastructure and the virtualization platform itself

upvoted 1 times

3 weeks ago

**Selected Answer: E**

Cloud Provider

upvoted 1 times

3 months ago

agreed, cloud provider always responsible for physical security

upvoted 1 times

Question #5*Topic 1*

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

* A. The physical location of the data and how it is accessed
* D. The implications of storing complex information on simple storage systems
* E. The actual size of the data and the storage format

**Correct Answer:** *D*

*Community vote distribution*

A (100%)

**Highly Voted** 7 months, 1 week ago

**Selected Answer: A**

Guide it quoted as saying: "Due to all the potential regulatory, contractual, and other jurisdictional issues, it is extremely important to understand both the logical and physical locations of data."

upvoted 8 times

**Highly Voted** 8 months ago

Personally I feel the indicated answer here (D. The implications of storing complex information on simple storage systems) is very wrong. How the data is stored is irrelevant in the context of "legal, regulatory, and jurisdictional factors" (with the occasional exception of required encryption). The answer at A is a much better answer to this question: The physical location of the data and how it is accessed.

upvoted 6 times

**Most Recent** 1 week, 4 days ago

Ans should be A.

upvoted 1 times

2 weeks, 6 days ago

**Selected Answer: A**

the answer is A

upvoted 1 times

4 weeks ago

**Selected Answer: A**

A is the answer

upvoted 1 times

4 weeks, 1 day ago

CCSK Security Guidance, pg 64: Due to all the potential regulatory, contractual, and other jurisdictional issues, it is extremely important to understand both the logical and physical locations of data

upvoted 2 times

1 month ago

Page 37, CCSK Guide. A

upvoted 2 times

2 months ago

answer should be A

upvoted 1 times

2 months, 1 week ago

I think correct answer is A.

upvoted 1 times

3 months, 2 weeks ago

**Selected Answer: A**

A. Laws and regulations around data protection, privacy, and security can vary from country to country, and even from state to state or province to province.

upvoted 2 times

4 months ago

Correct answer should be A

upvoted 1 times

6 months ago

**Selected Answer: A**

Correct answer should be A

upvoted 2 times

Question #6*Topic 1*

Which cloud-based service model enables companies to provide client-based access for partners to databases or applications?

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

**Correct Answer:** *A*

*Community vote distribution*

E (100%)

2 weeks, 5 days ago

**Selected Answer: E**

SaaS, They don't provide you any infra

upvoted 1 times

3 weeks ago

IT is A

upvoted 2 times

4 weeks, 1 day ago

CCSK Security Guide pg 11: Platform as a Service (PaaS) abstracts and provides development or application platforms,such as databases, application platforms (e.g. a place to run Python, PHP, or other code), file storage and collaboration, or even proprietary application processing (such as machine learning, big data processing, or direct Application Programming Interfaces (API) access to features of a full SaaS application). The key differentiator is that, with PaaS, you don’t manage the underlying servers, networks, or other infrastructure.

upvoted 2 times

1 month ago

Section 1.1.2.3 CCSK - Platform as a Service (PaaS) abstracts and provides development or application platforms, such as databases, application platforms (e.g. a place to run Python, PHP, or other code), file storage and collaboration, or even proprietary application processing (such as machine learning, big data processing, or direct Application Programming Interfaces (API) access to features of a full SaaS application). The key differentiator is that, with PaaS, you don’t manage the underlying servers, networks, or other infrastructure. Answer is correct, A

upvoted 2 times

1 month, 1 week ago

It is SaaS

upvoted 1 times

1 month, 3 weeks ago

**Selected Answer: E**

SaaS enables companies to provide client-based access for partners to databases or applications. In this model, software applications are hosted on the cloud, and users access them through web browsers. SaaS providers typically manage and maintain the underlying infrastructure, application, and data, which allows companies to focus on their core business rather than managing software and hardware.

upvoted 1 times

1 month, 4 weeks ago

its SaaS

upvoted 1 times

Question #7*Topic 1*

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

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

**Correct Answer:** *B*

*Community vote distribution*

B (100%)

1 month, 3 weeks ago

**Selected Answer: B**

GRM-08 "Governance and Risk Management: Policy Impact on Risk Assessments" GRM-09: "Governance and Risk Management: Policy Reviews" GRM-10 "Governance and Risk Management: Risk Assessments" GRM-11 "Governance and Risk Management: Risk Management Framework"

upvoted 1 times

Question #8*Topic 1*

Which attack surfaces, if any, does virtualization technology introduce?

* A. The hypervisor
* B. Virtualization management components apart from the hypervisor
* C. Configuration and VM sprawl issues
* D. All of the above

**Correct Answer:** *D*

Question #9*Topic 1*

APIs and web services require extensive hardening and must assume attacks from authenticated and unauthenticated adversaries.

* A. False
* B. True

**Correct Answer:** *B*

3 weeks, 1 day ago

It's B: CCSK Security Guide pg 117: APIs and web services need to be extensively hardened and assume attacks from both authenticated and unauthenticated adversaries. This includes using industry standard authentication designed specifically for APIs.

upvoted 1 times

Question #10*Topic 1*

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

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

**Correct Answer:** *B*

**Highly Voted** 3 months, 2 weeks ago

**Selected Answer: D**

The answer should be D A. --> lead to rapid deployment of resources on larger attack surface on the incident B. --> complicate the collection and analysis of data/incident evidence C. --> raise legal and regulatory issues D. --> no impact ==> the correct one E. --> complicate in locating and isolating affected resources in incident

upvoted 6 times

**Most Recent** 2 weeks ago

The option that is NOT a cloud computing characteristic that impacts incident response is: D. Object-based storage in a private cloud. Object-based storage in a private cloud is not directly related to incident response. It is a storage architecture that organizes data into discrete objects and is commonly used in cloud storage systems. While it can have implications for data management and accessibility, it does not directly impact incident response processes.

upvoted 1 times

1 month ago

**Selected Answer: D**

Answer D is the one with no impact.

upvoted 1 times

2 months ago

answer is B just concentrate on the computing, that's the only answer that don't belong to it.

upvoted 1 times

2 months, 1 week ago

Right selection is B, just focus on characteristics of cloud as per definition.

upvoted 1 times

2 months, 1 week ago

This is confusing.

upvoted 1 times

2 months, 2 weeks ago

**Selected Answer: D**

> These are the characteristics that make a cloud a cloud.. • Resource pooling... • Broad network access means that all resources are available over a network, without any need for direct physical access; the network is not necessarily part of the service. • Rapid elasticity ... • Measured service meters what is provided, to ensure that consumers only use what they are allotted, and, if necessary, to charge them for it. This is where the term utility computing comes from, since computing resources can now be consumed like water and electricity, with the client only paying for what they use.

upvoted 1 times

2 months, 3 weeks ago

**Selected Answer: D**

Should rather be D, as it is not a security issue

upvoted 1 times

Question #11*Topic 1*

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

* A. False
* B. True

**Correct Answer:** *B*

Question #12*Topic 1*

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 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.
* B. The CCM domain controls are mapped to HIPAA/HITECH Act and therefore Health4Sure could verify the CCM controls already covered as a result 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.
* 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.

**Correct Answer:** *C*

2 months, 1 week ago

Since CCM v3.0 has HIPAA/HITECH mapped in columns and the company is compliant with HIPAA/HITECH, it can disregard CCM controls mapping with HIPAA/HITECH and test CCM controls which are not mapped with HIPAA/HITECH to comply with other standards to save time on testing.

upvoted 1 times

5 months, 4 weeks ago

**Selected Answer: C**

This is a very poorly written question and even more confusing answers. Not impossible, just takes a lot of dissection and reading.

upvoted 1 times

5 months, 4 weeks ago

The problem here is that the question is intentionally misleading. They make it look like it is just for Health, hence the repeated use of HIPAA/HITECH and "health" in the company name.

upvoted 1 times

5 months, 4 weeks ago

But if you look a little more closely, regardless of their name, the goal of the company is to be a CSP and have the widest range of compliance of many frameworks. Not just HIPAA/HITECH. This is taken from this line "The company is compliant with HIPAA/HITECH Act among other industry standards."

upvoted 1 times

5 months, 4 weeks ago

Next is the overall goal; a CSP wanting to give the results to their clients so that their clients can use it as "pass thru". Now, we won't debate whether or not the CCM in the real world, is a valid document to give to customers for true pass-thru purposes (it's not). Let's just assume for the sake of argument that it is.

upvoted 1 times

5 months, 4 weeks ago

In that light, C would be the best answer because their goal is to have the widest compliance possible of many frameworks (scope applicability), not just for hipaa/hitech. A and B can be discounted simply because of their insistence on HIPAA/HITECH; whereas C says to use every control. hence giving the widest compliance results.

upvoted 1 times

7 months, 1 week ago

**Selected Answer: B**

CCM, which is part of the CSA Governance, Risk and Compliance (GRC) Stack, is mapped to multiple industry standards, regulations and frameworks that enterprises must follow, including ISO 27001/27002, PCI DSS, HIPAA and COBIT.

upvoted 4 times

7 months, 4 weeks ago

IMHO the provided answer is correct. CCM v 4 is currently mapping ISO/IEC 27001/27002/27017/27018, CCM V3.0.1, AICPA TSC (2017), CIS Controls V8, NIST 800-53r5, and PCI DSSv3.2.1 and nothing else

upvoted 2 times

7 months ago

yes, but the v3.0.1 is mapped with HIPAA. So i reckon the answer is B

upvoted 3 times

5 months, 4 weeks ago

It's C, but not for the reason Nevermind gave. The point of the question is to make you think that all it cares about is "Health", when in reality they are a CSP wanting to show the widest set of compliance to as many frameworks/standards as possible. The repeated references to HIPAA/HITECH is meant to be a red herring.

upvoted 1 times

8 months ago

The indicated answer here is clearly wrong, since the CCM controls are mapped to most of the cyber security frameworks and regulations, including HIPAA/Hitech. For me it's between A or B, and I feel B is a better answer and I would go for that.

upvoted 3 times

5 months, 4 weeks ago

The answer is C. This is because the premise of the question is intentionally misleading. It wants you to concentrate on "Health", hence A and B appear like they would be right. But they are not concentrating on just health compliance. They want to be a CSP and in such, have the widest range of compliance against as many frameworks/standards as possible. This is so they can present the results of the CCM to their clients, and their clients can use it as a pass-thru. Now obviously in the real world the CCM in itself would not be given to a client by a CSP. The CSP would go thru the certification processes such as FedRAMP/ISO/HITRUST etc, and of course a SOC2 Type 2. When you go thru these sorts of long paragraph scenarios, a good trick is to break each sentence down until you get to the core topic of it. I take part in the CISSP exam writing workshops, and we intentionally will write misleading questions like this. Albeit I would hope not as poorly written.

upvoted 1 times

Question #13*Topic 1*

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. A support table
* C. An entry log
* D. A validation process
* E. An access log

**Correct Answer:** *D*

**Highly Voted** 7 months ago

**Selected Answer: A**

It should be entitlement matrix. Validation process is not a terminology

upvoted 7 times

**Highly Voted** 7 months, 3 weeks ago

Agree, the mapping of an identity to an authorization should be documented in an entitlement matrix. That document outlines the various resources and functions allowed to be used by specific users, groups and roles.

upvoted 5 times

**Most Recent** 1 month, 4 weeks ago

**Selected Answer: A**

Definitely A. Cannot possibly be D

upvoted 2 times

2 months, 1 week ago

its E, focus on "entities in a transaction, "

upvoted 1 times

2 months, 1 week ago

Is it not an entitlement matrix?

upvoted 1 times

5 months, 4 weeks ago

**Selected Answer: A**

Yeah, they messed up here. It is entitlement matrix.

upvoted 2 times

8 months ago

For me this has to be an entitlement matrix. "Validation process" is not even a term that appears in the Security Guidance.

upvoted 4 times

Question #14*Topic 1*

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

* A. False
* B. True

**Correct Answer:** *B*

4 weeks, 1 day ago

True. Ref. Application Security. Isolated environments. Cloud applications can also leverage virtual networks and other structures, including PaaS, for hyper-segregated environments. For example, it is possible, at no additional cost, to deploy multiple application stacks on entirely separate virtual networks, eliminating the ability for an attacker to use one compromised application to attack others behind the perimeter firewalls.

upvoted 1 times

Question #15*Topic 1*

Your cloud and on-premises infrastructures should always use the same network address ranges.

* A. False
* B. True

**Correct Answer:** *A*

4 weeks, 1 day ago

Answer is correct. With Hybrid Cloud Considerations, If the cloud uses the same network address range as your on-premises assets, it is effectively unusable.

upvoted 1 times

Question #16*Topic 1*

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

* A. Infrastructure
* B. Datastructure
* C. Infostructure
* D. Applistructure
* E. Metastructure

**Correct Answer:** *A*

**Highly Voted** 6 months, 3 weeks ago

A is the correct answer ... Domain 7 infrastructure Security ... 7.0 Introduction first paragraph..Infrastructure security is the foundation for operating securely in the cloud

upvoted 8 times

**Highly Voted** 7 months, 3 weeks ago

I disagree with this answer. In my own opinion, the infrastructure security is managed by the cloud provider so here, the most important cloud logical model is the Metastructure. That one security is the used for configuration and management of cloud deployment.

upvoted 7 times

5 months, 4 weeks ago

This is a tricky question. While the Metastructure is definitely, without a doubt important, they are combining it with answers that look like IaaS,PaaS,SaaS. But they are talking about the actual physical infrastructure, which without its 10000000% security, nothing else can be secure. This is because the physical infrastructure is what everything else is built on. Imagine if you will that the CSP is in a collocated facility and many people who are not part of the CSP can walk around the building. Now imagine if they gain access to the physical servers. Would it really matter at that point if the metastructure was "secured". No it wouldn't because physical access always beats virtual access.

upvoted 5 times

**Most Recent** 1 month ago

Infrastructure: The core components of a computing system: compute, network, and storage. The foundation that everything else is built on. The moving parts. Correct Answer : A

upvoted 1 times

2 months, 1 week ago

there is no data structure layer, follow the sequence of as mentioned in ccsk guide, infrastructure > metastructure > applistructure > infostructure so answer is infrastructure

upvoted 2 times

2 months, 1 week ago

As tralala 2 below said, refer to Domain 7 introduction. It says "Infrastructure security is the foundation for operating securely in the cloud".

upvoted 1 times

6 months, 1 week ago

Its metastructure

upvoted 2 times

Question #17*Topic 1*

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

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

**Correct Answer:** *D*

2 weeks ago

The service type of network is typically isolated on different hardware for the following reason: C. It has distinct functions from other networks. A service type of network often serves a specific purpose or function that is different from other networks within a cloud environment. Isolating it on different hardware allows for better control and management of resources dedicated to that particular network. By separating it from other networks, it becomes easier to allocate resources, optimize performance, and apply specific configurations or settings tailored to the unique requirements of that network. This isolation helps prevent interference or conflicts between different network types, ensuring efficient and reliable operation of each network within the cloud environment.

upvoted 2 times

3 months, 2 weeks ago

**Selected Answer: C**

C. A service type of network typically supports specific functions such as management, storage, or application, and therefore it is isolated on different hardware to maintain its own infrastructure and prevent it from affecting other networks in case of any failure or compromise.

upvoted 2 times

5 months, 3 weeks ago

correct answer C

upvoted 2 times

7 months ago

We most commonly see at least three different networks which are isolated onto dedicated hardware since there is no functional or traffic overlap: - The service network for communications between virtual machines and the Internet. This builds the network resource pool for the cloud consumers. - The storage network to connect virtual storage to virtual machines. A management network for management and API traffic.

upvoted 2 times

Question #18*Topic 1*

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. Legal Issues: Contracts and Electronic Discovery
* B. Infrastructure Security
* C. Compliance and Audit Management
* D. Information Governance
* E. Governance and Enterprise Risk Management

**Correct Answer:** *C*

2 weeks ago

The governance domain that deals with evaluating how cloud computing affects compliance with internal security policies and various legal requirements, such as regulatory and legislative, is: C. Compliance and Audit Management Compliance and Audit Management is responsible for ensuring that an organization's cloud computing practices adhere to internal security policies as well as legal and regulatory requirements. This governance domain involves assessing and evaluating the impact of cloud computing on compliance, managing audits and certifications, and implementing controls to address any compliance gaps or risks. It focuses on aligning cloud operations with applicable laws, regulations, industry standards, and contractual obligations to maintain a secure and compliant cloud environment.

upvoted 1 times

7 months, 4 weeks ago

**Selected Answer: C**

Compliance and Audit Management. Maintaining and proving compliance when using cloud computing. Issues dealing with evaluating how cloud computing affects compliance with internal security policies, as well as various compliance requirements (regulatory, legislative, and otherwise) are discussed here. This domain includes some direction on proving compliance during an audit

upvoted 2 times

Question #19*Topic 1*

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

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

**Correct Answer:** *A*

2 months, 3 weeks ago

**Selected Answer: A**

Without permission we cannot prform vulnerability testing

upvoted 1 times

4 months ago

The correct answer is A. You should determine whether your provider allows customers to perform a VA of their systems. If they don't, and you do it, you may find yourself blocked, because the provider won't know the source of the scan, which could be coming from bad actors.

upvoted 1 times

7 months ago

Wrong. I would say C

upvoted 1 times

4 months, 1 week ago

I tend to agree, since you are unable to test the underlying cloud infrastructure, and only the application can be tested

upvoted 1 times

Question #20*Topic 1*

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. Resource pooling
* C. Broad network access
* D. Measured service
* E. On-demand self-service

**Correct Answer:** *E*

2 weeks ago

The characteristic described as "a consumer can unilaterally provision computing capabilities such as server time and network storage as needed" is: E. On-demand self-service On-demand self-service is one of the essential characteristics of cloud services. It refers to the capability for consumers to independently and automatically provision computing resources without the need for human interaction with the cloud service provider. Users can access and allocate resources, such as server instances, storage, and network bandwidth, as per their requirements, typically through a self-service portal or API. This characteristic enables users to scale resources up or down on-demand, in a flexible and automated manner, based on their immediate needs, without relying on manual intervention from the cloud service provider.

upvoted 2 times

Question #21*Topic 1*

REST APIs are the standard for web-based services because they run over HTTPS and work well across diverse environments.

* A. False
* B. True

**Correct Answer:** *B*

3 weeks, 1 day ago

B: CCSK Security Guide pg 70; "APIs have become the standard for web-based services since they run over HTTP/S ans thus work well across diverse evnvironments".

upvoted 1 times

2 months, 2 weeks ago

**Selected Answer: B**

> APIs are typically REST for cloud services, since REST is easy to implement across the Internet. REST APIs have become the standard for web-based services since they run over HTTP/S and thus work well across diverse environments.

upvoted 1 times

4 months, 3 weeks ago

i want to see

upvoted 1 times

Question #22*Topic 1*

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

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

**Correct Answer:** *C*

2 weeks ago

The statement that is NOT a requirement of governance and enterprise risk management in a cloud environment is: C. Negotiate long-term contracts with companies who use well-vetted software application to avoid the transient nature of the cloud environment. While negotiating long-term contracts and using well-vetted software applications can be strategies organizations employ in a cloud environment, it is not specifically a requirement of governance and enterprise risk management. The other statements mentioned, A, B, and D, align with the requirements of governance and enterprise risk management in a cloud environment, which involve inspecting and accounting for risks, respecting interdependencies, communicating risk posture, and providing transparency to stakeholders.

upvoted 2 times

Question #23*Topic 1*

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

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

**Correct Answer:** *A*

1 week, 1 day ago

Security Guide, 3.1.3 electronic discovery, page 48 ----> U.S. rules around “discovery”—the process by which an opposing party obtains private documents for use in litigation—cover a wide range of potential documents.

upvoted 1 times

Question #24*Topic 1*

What item below allows disparate directory services and independent security domains to be interconnected?

* A. Coalition
* B. Cloud
* C. Intersection
* D. Union
* E. Federation

**Correct Answer:** *E*

Question #25*Topic 1*

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

* A. False
* B. True

**Correct Answer:** *B*

1 week, 4 days ago

The answer is A:

upvoted 1 times

2 months, 1 week ago

Security Guidance Page 104 "use immutable servers when possible. If an issue is detected, move workloads from compromised device onto a new instance in a known-good state.

upvoted 3 times

Question #26*Topic 1*

To understand their compliance alignments and gaps with a cloud provider, what must cloud customers rely on?

* A. Provider documentation
* B. Provider run audits and reports
* C. Third-party attestations
* D. Provider and consumer contracts
* E. EDiscovery tools

**Correct Answer:** *C*

2 days, 1 hour ago

**Selected Answer: C**

3rd Party Attestation would give unbiased view of compliance status.

upvoted 1 times

Question #27*Topic 1*

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

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

**Correct Answer:** *B*

3 months, 3 weeks ago

B is correct: 2.1.3.3 There is a greater reliance on contracts, audits, and assessments, as you lack day-to-day visibility or management.

upvoted 3 times

Question #28*Topic 1*

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

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

**Correct Answer:** *A*

2 weeks ago

The data security control that is the LEAST likely to be assigned to an IaaS (Infrastructure as a Service) provider is: A. Application logic IaaS providers primarily focus on providing the foundational infrastructure components, such as virtual machines, storage, and networking. They offer a platform for customers to build and deploy their own applications. The responsibility for application logic, including the design, development, and implementation of specific functionalities, typically lies with the customer or the software/application owner. While IaaS providers may offer some basic security measures at the infrastructure level, they are not responsible for the application logic itself. That aspect is typically the responsibility of the customer or the application owner utilizing the IaaS infrastructure.

upvoted 1 times

Question #29*Topic 1*

How does virtualized storage help avoid data loss if a drive fails?

* A. Multiple copies in different locations
* B. Drives are backed up, swapped, and archived constantly
* C. Full back ups weekly
* D. Data loss is unavoidable with drive failures
* E. Incremental backups daily

**Correct Answer:** *A*

3 weeks, 1 day ago

A: Security Guidance pg 97: "Most virtualized storage is durable and keeps multiple copies of data in different locations so that drive failures are less likely to result in data loss."

upvoted 1 times

4 weeks ago

why answer not B?

upvoted 1 times

Question #30*Topic 1*

What is the newer application development methodology and philosophy focused on automation of application development and deployment?

* A. Agile
* B. BusOps
* C. DevOps
* D. SecDevOps
* E. Scrum

**Correct Answer:** *C*

2 weeks ago

The newer application development methodology and philosophy focused on automation of application development and deployment is: C. DevOps DevOps (Development and Operations) is a software development approach that emphasizes collaboration, communication, and integration between development teams (Dev) and operations teams (Ops). It aims to streamline the application development and deployment process by breaking down silos, automating workflows, and fostering a culture of continuous integration and delivery. DevOps practices involve using automation tools and technologies to enable faster and more efficient software development, testing, deployment, and monitoring. The goal is to achieve faster time to market, improved quality, and enhanced overall efficiency in the software development lifecycle.

upvoted 2 times

3 weeks ago

pag. 125 DevOps. DevOps es una nueva metodología y filosofía de desarrollo de aplicaciones centrada en la automatización del desarrollo y la implantación de aplicaciones.

upvoted 2 times

Question #31*Topic 1*

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

* A. False
* B. True

**Correct Answer:** *B*

3 weeks, 1 day ago

B: Security Guidance p.122 "Ensure that you are protecting your data as it moves to the cloud. This necessitates understanding your provider’s data migration mechanisms, as leveraging provider mechanisms is often more secure and cost effective than “manual” data transfer methods such as Secure File Transfer Protocol (SFTP). For example, sending data to a provider’s object storage over an API is likely much more reliable and secure than setting up your own SFTP server on a virtual machine in the same provider."

upvoted 1 times

Question #32*Topic 1*

What is true of searching data across cloud environments?

* A. You might not have the ability or administrative rights to search or access all hosted data.
* B. The cloud provider must conduct the search with the full administrative controls.
* C. All cloud-hosted email accounts are easily searchable.
* D. Search and discovery time is always factored into a contract between the consumer and provider.
* E. You can easily search across your environment using any E-Discovery tool.

**Correct Answer:** *A*

2 months, 2 weeks ago

**Selected Answer: A**

> In a cloud environment, a client may not be able to apply or use e-discovery tools that it uses in its own environment. Moreover, a client may not have the ability or administrative rights to search or access all the data hosted in the cloud.

upvoted 2 times

Question #33*Topic 1*

How does running applications on distinct virtual networks and only connecting networks as needed help?

* A. It reduces hardware costs
* B. It provides dynamic and granular policies with less management overhead
* C. It locks down access and provides stronger data security
* D. It reduces the blast radius of a compromised system
* E. It enables you to configure applications around business groups

**Correct Answer:** *D*

2 weeks ago

Running applications on distinct virtual networks and only connecting networks as needed helps in the following way: D. It reduces the blast radius of a compromised system. By running applications on separate virtual networks and connecting networks as needed, the impact of a compromised system or a security breach is contained and limited. If a system or network within a virtual network is compromised, the isolation between networks helps prevent the lateral spread of the attack to other networks or systems. This containment reduces the "blast radius" of a compromised system, minimizing the potential damage and limiting the scope of the security incident. This approach enhances the overall security posture and resilience of the cloud environment by isolating and segregating different components and applications.

upvoted 1 times

Question #34*Topic 1*

How can virtual machine communications bypass network security controls?

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

**Correct Answer:** *A*

2 weeks ago

The option that describes how virtual machine communications can bypass network security controls is: A. VM communications may use a virtual network on the same hardware host. Virtual machine communications within a virtual network on the same hardware host can bypass network security controls. Since the communication occurs within the virtualized environment of the host, it may not traverse the physical network where network security controls, such as firewalls or intrusion detection systems, are implemented. This intra-host communication can occur at the virtualization layer, enabling VMs to communicate with each other without being subject to the same network security controls and monitoring as traffic that flows through the physical network.

upvoted 1 times

Question #35*Topic 1*

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.

**Correct Answer:** *D*

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

2 weeks ago

The correct description of VM hopping according to ENISA (European Union Agency for Cybersecurity) is: D. Using a compromised VM to exploit a hypervisor, used to take control of other VMs. VM hopping refers to a scenario where a compromised virtual machine (VM) is used as a stepping stone to exploit vulnerabilities in the hypervisor or virtualization layer. The attacker aims to gain control over the hypervisor, which manages and oversees the execution of multiple VMs, and subsequently take control of other VMs hosted on the same hypervisor. By compromising one VM, the attacker attempts to "hop" from that initial foothold to gain unauthorized access to other VMs or critical resources within the virtualized environment. This type of attack can have severe consequences as it allows the attacker to move laterally across VMs and potentially compromise the entire virtualized infrastructure.

upvoted 1 times

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

1 month, 3 weeks ago

**Selected Answer: D**

ENISA (page 54) "‘VM hopping’: in which an attacker hacks a VM using some standard method and then – exploiting some hypervisor vulnerability – takes control of other VMs running on the same hypervisor"

upvoted 3 times

**[Azo\_4952](https://www.examtopics.com/user/Azo_4952/)**

7 months ago

Virtual machine hyper jumping (VM jumping) is an attack method that exploits the hypervisor’s weakness that allows a virtual machine (VM) to be accessed from another.

upvoted 4 times

Question #36*Topic 1*

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

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

**Correct Answer:** *D*

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

1 month, 3 weeks ago

**Selected Answer: D**

- Access control: restricting access to a resource. Access management is the process of managing access to the resources. - Federated Identity Management: the process of asserting an identity across different systems or organizations. This is the key enabler of Single Sign On and also core to managing IAM in cloud computing. - Authoritative source: the "root" source of an identity, such as the directory server that manages employee identities. - Entitlement: mapping an identity (including roles, personas, and attributes) to an authorization. The entitlement is what they are allowed to do, and for documentation purposes we keep these in an entitlement matrix. - Authentication: the process of confirming an identity. When you log in to a system you present a username (the identifier) and password (an attribute we refer to as an authentication factor). Also known as Authn.

upvoted 4 times

Question #37*Topic 1*

Which concept provides the abstraction needed for resource pools?

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

**Correct Answer:** *A*

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

2 weeks ago

The concept that provides the abstraction needed for resource pools is: A. Virtualization Virtualization is the concept that provides the abstraction needed for resource pools in cloud computing environments. It involves creating virtual representations of physical resources such as servers, storage, and network devices. With virtualization, physical resources are abstracted and can be divided or combined to create virtual resource pools. These virtualized resources can be allocated and managed dynamically, allowing for efficient utilization and allocation of resources based on demand. Virtualization enables the creation of resource pools that can be shared among multiple applications or users, providing flexibility and scalability in cloud environments.

upvoted 2 times

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

1 month, 3 weeks ago

**Selected Answer: A**

Virtualization provides the abstraction needed for resource pools, which are then managed using orchestration.

upvoted 1 times

Question #38*Topic 1*

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

* A. False
* B. True

**Correct Answer:** *B*

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

1 month, 3 weeks ago

**Selected Answer: B**

Network logs from a cloud provider will tend to be flow records, but not full packet capture.

upvoted 1 times

Question #39*Topic 1*

Select the best definition of `compliance` from the options below.

* A. The development of a routine that covers all necessary security measures.
* B. The diligent habits of good security practices and recording of the same.
* C. The timely and efficient filing of security reports.
* D. The awareness and adherence to obligations, including the assessment and prioritization of corrective actions deemed necessary and appropriate.
* E. The process of completing all forms and paperwork necessary to develop a defensible paper trail.

**Correct Answer:** *D*

Question #40*Topic 1*

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

**Correct Answer:** *B*

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

1 week, 2 days ago

C: Control Specifications In the CCM (Cloud Control Matrix) tool, "Encryption and Key Management" is an example of a Control Specification. The Control Specifications section of the CCM provides specific controls or measures that can be implemented to address various security requirements within the cloud environment. Encryption and key management are important controls related to protecting data confidentiality and ensuring secure access to encrypted data.

upvoted 1 times

Question #41*Topic 1*

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

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

**Correct Answer:** *D*

**[tralala2](https://www.examtopics.com/user/tralala2/)**

**Highly Voted** 7 months ago

I would say that D is the correct answer Most cloud platforms also use redundant, durable storage mechanisms that often utilize data dispersion (sometimes also known as data fragmentation of bit splitting). This process takes chunks of data, breaks them up, and then stores multiple copies on different physical storage to provide high durability. Data stored in this way is thus physically dispersed. A single file, for example, would not be located on a single hard drive.

upvoted 5 times

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

**Most Recent** 2 months, 2 weeks ago

**Selected Answer: D**

Data dispersion provides security benefits, as an attacker would need to access multiple storage devices or locations and reconstruct the entire data set in order to access the data.

upvoted 2 times

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

6 months, 2 weeks ago

The right answer is A. proxy encryption. Reference and Description: Proxy encryption In this model, you connect the volume to a special instance or appliance/ software, and then connect your instance to the encryption instance. The proxy handles all crypto operations and may keep keys either onboard or externally.

upvoted 1 times

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

1 month, 4 weeks ago

How does that help with data resiliency? I'd argue the more fitting answer is D

upvoted 1 times

**[Azo\_4952](https://www.examtopics.com/user/Azo_4952/)**

7 months ago

Proxy encryption What method is often used to support resiliency and security? 01/29/2021 – by Mod\_GuideK 0 In volume storage, what method is often used to support resiliency and security? A. proxy encryption

upvoted 4 times

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

1 month, 4 weeks ago

I disagree, Answer D is more fitting, as data dispersion helps resiliency and security

upvoted 1 times

Question #42*Topic 1*

What is true of security as it relates to cloud network infrastructure?

* A. You should apply cloud firewalls on a per-network basis.
* B. You should deploy your cloud firewalls identical to the existing firewalls.
* C. You should always open traffic between workloads in the same virtual subnet for better visibility.
* D. You should implement a default allow with cloud firewalls and then restrict as necessary.
* E. You should implement a default deny with cloud firewalls.

**Correct Answer:** *E*

Question #43*Topic 1*

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

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

**Correct Answer:** *E*

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

1 week, 4 days ago

Where did you obtain the description provided in the comments?

upvoted 1 times

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

1 week, 6 days ago

The statement that best describes the impact of Cloud Computing on business continuity management is: D. Clients need to do business continuity planning due diligence in case they suddenly need to switch providers. Cloud computing introduces new considerations for business continuity management. While cloud services can provide advantages such as scalability and redundancy, organizations must still ensure they have proper business continuity plans in place. This includes conducting due diligence in terms of understanding the provider's service-level agreements (SLAs), data backup and recovery processes, and the potential need to switch providers in case of service disruptions or other unforeseen events. Organizations need to have plans in place to handle such scenarios and ensure the continuity of their operations. Business continuity planning is crucial to mitigate risks and maintain the availability and resilience of critical systems and services, even in the cloud computing context.

upvoted 1 times

Question #44*Topic 1*

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

* A. Platform-based Workload
* B. Pod
* C. Abstraction
* D. Container
* E. Virtual machine

**Correct Answer:** *D*

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

1 week, 6 days ago

The code execution environment running within an operating system that shares and uses the resources of the operating system is known as: D. Container A container is a lightweight and isolated runtime environment that runs within an operating system. It provides an isolated execution environment for applications, allowing them to share the underlying operating system's resources efficiently. Containers are an example of operating system-level virtualization, where multiple containers can run on a single host OS. They offer a higher level of abstraction compared to virtual machines and provide a more lightweight and flexible approach to application deployment and management. Containers encapsulate the application code and dependencies, enabling consistent execution across different environments while leveraging the resources of the underlying operating system.

upvoted 2 times

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

6 months, 2 weeks ago

Correct Answer : D Reference: Containers are code execution environments that run within an operating system (for now), sharing and leveraging resources of that operating system. While a VM is a full abstraction of an operating system, a container is a constrained place to run segregated processes while still utilizing the kernel and other capabilities of the base OS.

upvoted 3 times

Question #45*Topic 1*

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

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

**Correct Answer:** *D*

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

1 month, 3 weeks ago

**Selected Answer: D**

(Security Guidance page 74) “Chaos Engineering” is often used to help build resilient cloud deployments. Since everything cloud is API-based, Chaos Engineering uses tools to selectively degrade portions of the cloud to continuously test business continuity.

upvoted 2 times

Question #46*Topic 1*

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

* A. The laws protecting customer data are based on the cloud provider and customer location only.
* B. The confidentiality agreements between companies using cloud computing services is limited legally to the company, not the provider.
* C. The companies using the cloud providers are the custodians of the data entrusted to them.
* D. The cloud computing companies are absolved of all data security and associated risks through contracts and data laws.
* E. The cloud computing companies own all customer data.

**Correct Answer:** *C*

Question #47*Topic 1*

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

* A. False
* B. True

**Correct Answer:** *B*

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

1 week, 6 days ago

B. True Dynamic Application Security Testing (DAST) involves testing the security of an application by simulating attacks and analyzing its response. In a cloud environment, DAST may have limitations or require pre-testing permission from the cloud service provider. Cloud service providers typically have policies and security measures in place to protect their infrastructure and the applications hosted on it. As a result, they may impose restrictions on conducting security testing, including DAST, without prior permission. This is done to prevent any potential impact on the stability, performance, or security of the cloud environment. Therefore, it is true that DAST might be limited or require pre-testing permission from the provider in a cloud environment. Organizations and individuals should consult and comply with the policies and procedures defined by their cloud service provider when conducting security testing activities.

upvoted 2 times

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

1 month, 3 weeks ago

**Selected Answer: B**

(Security Guidance page 114) Due to the terms of service with the cloud provider DAST may be limited and/or require pre-testing permission from the provide

upvoted 2 times

Question #48*Topic 1*

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 duration of time that a security violation can occur before the client begins assessing regulatory fines.
* C. The cost per incident for security breaches of regulated information.
* D. The regulations that are pertinent to the contract and how to circumvent them.
* E. The type of security software which meets regulations and the number of licenses that will be needed.

**Correct Answer:** *A*

Question #49*Topic 1*

Which cloud storage technology is basically a virtual hard drive for instanced or VMs?

* A. Volume storage
* B. Platform
* C. Database
* D. Application
* E. Object storage

**Correct Answer:** *A*

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

1 month, 3 weeks ago

**Selected Answer: A**

(Security Guidance page 120) Volume storage: This is essentially a virtual hard drive for instances/virtual machines.

upvoted 3 times

Question #50*Topic 1*

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

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

**Correct Answer:** *C*

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

2 months, 2 weeks ago

**Selected Answer: C**

Provisioning is not in 13.1.2 Major Categories of Security as a Service Offerings

upvoted 2 times

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

3 months, 2 weeks ago

hmm all actually example of SecaaS

upvoted 1 times

Question #51*Topic 1*

How is encryption managed on multi-tenant storage?

* A. Single key for all data owners
* B. One key per data owner
* C. Multiple keys per data owner
* D. The answer could be A, B, or C depending on the provider
* E. C for data subject to the EU Data Protection Directive; B for all others

**Correct Answer:** *B*

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

1 week, 6 days ago

The management of encryption on multi-tenant storage can vary depending on the provider and their specific implementation. However, the most common approach is: D. The answer could be A, B, or C depending on the provider. Different cloud service providers may employ different encryption strategies for multi-tenant storage. The management of encryption keys can vary from using a single key for all data owners (option A) to assigning one key per data owner (option B) or even allowing multiple keys per data owner (option C). The chosen approach depends on the provider's security architecture, data isolation mechanisms, and the level of encryption granularity required by their customers. It's important to note that cloud service providers often offer encryption-related features and options, allowing customers to select their desired level of encryption and key management. Therefore, the specific encryption management strategy employed on multi-tenant storage can vary and should be determined based on the capabilities and offerings of the individual provider.

upvoted 1 times

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

2 days ago

Ans "A" is not aligned with a security rules, never using single key among the multiple Data owners.

upvoted 1 times

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

1 month ago

multiple keys per data owner

upvoted 3 times

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

2 months, 2 weeks ago

**Selected Answer: C**

I can't find it in the reference but I think this should be C. The major cloud providers I know allow you to at least do two: a) multiple cloud-provider managed encryption keys b) customer-managed keys

upvoted 2 times

Question #52*Topic 1*

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

* A. The devices used to access data have different storage formats.
* B. The devices used to access data use a variety of operating systems and may have different programs installed on them.
* C. The device may affect data dispersion.
* D. The devices used to access data use a variety of applications or clients and may have different security characteristics.
* E. The devices used to access data may have different ownership characteristics.

**Correct Answer:** *D*

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

1 week, 6 days ago

The statement that best describes why it is important to know how data is being accessed is: D. The devices used to access data use a variety of applications or clients and may have different security characteristics. Understanding how data is being accessed is crucial because the devices used to access data can vary in terms of the applications or clients they use and the security characteristics they possess. Different devices may have different software installed, operating systems, and security configurations. This diversity can impact the security and integrity of the data being accessed. By knowing how data is being accessed, organizations can identify potential vulnerabilities or risks associated with specific devices or applications. They can then implement appropriate security measures and controls to protect the data from unauthorized access, data breaches, or other security incidents. Understanding the device landscape helps ensure that appropriate security policies, authentication mechanisms, and encryption methods are in place to safeguard sensitive data.

upvoted 1 times

Question #53*Topic 1*

What is resource pooling?

* A. The provider's computing resources are pooled to serve multiple consumers.
* B. Internet-based CPUs are pooled to enable multi-threading.
* C. The dedicated computing resources of each client are pooled together in a colocation facility.
* D. Placing Internet (ג€cloudג€) data centers near multiple sources of energy, such as hydroelectric dams.
* E. None of the above.

**Correct Answer:** *A*

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

1 week, 6 days ago

Resource pooling refers to: A. The provider's computing resources are pooled to serve multiple consumers. Resource pooling in cloud computing refers to the practice of aggregating and sharing computing resources among multiple consumers or clients. The cloud service provider combines its computing resources, including servers, storage, and networking infrastructure, into a shared pool. These resources can then be dynamically allocated and reallocated based on the demands and needs of different consumers or applications. By pooling resources, the cloud provider can achieve higher utilization rates and optimize resource allocation, leading to improved efficiency and cost-effectiveness. Consumers benefit from this pooling by gaining access to scalable and on-demand computing resources without the need to manage and maintain their own dedicated infrastructure. Therefore, option A correctly describes resource pooling in cloud computing.

upvoted 1 times

Question #54*Topic 1*

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

* A. False
* B. True

**Correct Answer:** *A*

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

1 week, 6 days ago

B. True The statement is true: Your SLA (Service Level Agreement) with your cloud provider ensures continuity for all services. A Service Level Agreement (SLA) is a contractual agreement between a service provider and a customer that defines the level of service and performance guarantees. In the context of cloud computing, an SLA typically outlines the availability, reliability, and continuity of the services provided by the cloud provider. A well-drafted SLA ensures that the cloud provider commits to maintaining continuity for all the services they offer. This includes measures to minimize downtime, ensure data redundancy and backup, implement disaster recovery plans, and address any disruptions or incidents promptly. By signing an SLA, customers can have the assurance that their cloud provider is responsible for maintaining the continuity of the services as specified in the agreement. This helps establish a level of trust and accountability between the provider and the customer. Therefore, it is true that your SLA with your cloud provider ensures continuity for all services.

upvoted 1 times

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

1 month, 3 weeks ago

**Selected Answer: B**

LAs and Governance: Any incident using a public cloud or hosted provider requires an understanding of service level agreements (SLAs), and likely coordination with the cloud provider. Keep in mind that, depending on your relationship with the provider, you may not have direct points of contact and might be limited to whatever is offered through standard support. A custom private cloud in a third-party data center will have a very different relationship than signing up through a website and clicking through a license agreement for a new SaaS application.

upvoted 1 times

Question #55*Topic 1*

Which of the following is NOT normally a method for detecting and preventing data migration into the cloud?

* A. Intrusion Prevention System
* B. URL filters
* C. Data Loss Prevention
* D. Cloud Access and Security Brokers (CASB)
* E. Database Activity Monitoring

**Correct Answer:** *A*

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

1 week, 6 days ago

The method for detecting and preventing data migration into the cloud that is NOT normally used is: B. URL filters URL filters are primarily used for controlling and restricting access to websites based on their URLs or web addresses. They are commonly employed in web filtering and content control scenarios. However, URL filters are not typically used as a method specifically for detecting and preventing data migration into the cloud.

upvoted 1 times

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

2 months, 2 weeks ago

**Selected Answer: A**

A is correct. It's not listed in 11.1.3 Managing Data Migrations to the Cloud.

upvoted 1 times

Question #56*Topic 1*

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

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

**Correct Answer:** *C*

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

1 week, 6 days ago

The type of environment in which it is impractical to allow the customer to conduct their own audit, making it important for data center operators to provide auditing for the customers is: C. Multi-tenant environments In multi-tenant environments, multiple customers or tenants share the same physical infrastructure, such as servers, storage, and networking resources, provided by the cloud service provider. Due to the shared nature of the infrastructure, it can be challenging or impractical for individual customers to conduct their own audits of the underlying infrastructure. In such environments, data center operators play a crucial role in ensuring the security and compliance of the infrastructure. They are responsible for implementing appropriate security measures, maintaining regulatory compliance, and providing auditing capabilities to meet the requirements of different customers. The data center operators are expected to have robust auditing processes in place, allowing customers to verify the security controls and compliance measures implemented within the multi-tenant environment.

upvoted 1 times

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

4 weeks ago

C- In multi-tenant environments, multiple customers or organizations share the same infrastructure and resources provided by the data center operators. In such a scenario, it can be impractical or infeasible for each customer to conduct their own audit of the infrastructure and security measures. Due to the shared nature of the environment, allowing individual customer audits may disrupt the operations and compromise the privacy and security of other tenants' data.

upvoted 1 times

Question #57*Topic 1*

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

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

**Correct Answer:** *A*

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

1 week, 6 days ago

The key underlying vulnerability causing lock-in, as ranked by ENISA, is: A. Lack of completeness and transparency in terms of use. Lock-in refers to the situation where a customer becomes dependent on a particular cloud service provider and faces challenges or barriers in migrating to another provider or bringing the services back in-house. ENISA research identifies lock-in as a high-risk factor in cloud computing. One of the key vulnerabilities that contribute to lock-in is the lack of completeness and transparency in terms of use. This means that the terms and conditions, contractual agreements, and service-level agreements provided by the cloud service provider may not adequately disclose all the relevant information and restrictions that could impact the customer's ability to migrate or switch providers. Without a clear understanding of the terms of use and potential limitations, customers may unintentionally become locked into the services of a specific provider.

upvoted 1 times

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

1 month ago

All in One Study Guide User Provisioning Vulnerability Multiple vulnerabilities are associated with user provisioning in the ENISA document. Lack of completeness and transparency in terms of use This occurs when the provider's usage policy is unclear or lacks detail. R.1: Lock-in: Lack of completeness and transparency in Terms of Use

upvoted 1 times

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

1 month, 3 weeks ago

**Selected Answer: A**

(page 25) Vulnerabilities V13. Lack of standard technologies and solutions V46. Poor provider selection V47. Lack of supplier redundancy V31. Lack of completeness and transparency in terms of use

upvoted 1 times

Question #58*Topic 1*

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

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

**Correct Answer:** *B*

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

1 week, 6 days ago

E. Both B and D. Option B suggests maintaining customer-managed key management and revoking or deleting keys from the key management system to prevent the data from being accessed again. By managing their own keys and ensuring the revocation or deletion of those keys, customers can effectively control access to their data and prevent unauthorized access or retrieval. Option D suggests keeping the keys stored on the client side, ensuring their security, and granting users the ability to delete their own data. By having the keys securely stored and giving users control over their data, they can actively delete their data and ensure its removal from the cloud environment. By combining both options B and D, customers can exercise strong control over their data, including the ability to revoke access through key management and allowing users to delete their own data. This approach ensures that the data is properly removed from the public cloud environment, including any associated media such as backup tapes

upvoted 2 times

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

4 weeks ago

E. Both B and D. To ensure that all data has been removed from a public cloud environment, including all media such as back-up tapes, the best approach is to combine both options B and D. B. Maintaining customer-managed key management and revoking or deleting keys from the key management system: By managing their own encryption keys, customers can have greater control over their data. When data is no longer needed or when the customer wants to ensure its complete removal, revoking or deleting the encryption keys associated with that data can render it inaccessible. This ensures that even if the data is still stored in the cloud environment, it cannot be decrypted and accessed. D. Keep the keys stored on the client side: Storing encryption keys securely on the client side ensures that the keys are under the control of the customer. By having the ability to delete their own data using their keys, customers can actively manage and remove their data from the public cloud environment. This eliminates reliance on the cloud provider for data deletion.

upvoted 3 times

Question #59*Topic 1*

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

* A. Arbitrary contract termination by acquiring company
* B. Resource isolation may fail
* C. Provider may change physical location
* D. Mass layoffs may occur
* E. Non-binding agreements put at risk

**Correct Answer:** *E*

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

1 week, 6 days ago

A. Arbitrary contract termination by acquiring company. When a cloud provider is acquired by another company, there is a risk that the acquiring company may arbitrarily terminate existing contracts with customers. This can lead to service disruptions, loss of data, and potential legal and financial implications for the affected customers. The acquiring company may have different priorities, business strategies, or may not want to continue providing the same level of service to existing customers, resulting in contract termination. While the other options listed can also be potential concerns during a cloud provider acquisition, ENISA specifically highlights the arbitrary contract termination by the acquiring company as a risk concern. It emphasizes the importance of contractual agreements and the potential impact on customers when there is a change in ownership or control of the cloud provider. Therefore, option A, arbitrary contract termination by the acquiring company, is the correct answer according to ENISA.

upvoted 1 times

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

1 month, 3 weeks ago

**Selected Answer: E**

enisa page 26

upvoted 1 times

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

2 months, 2 weeks ago

**Selected Answer: E**

> The acquisition of the cloud provider (R.6) can also have a similar effect, since it increases the likelihood of sudden changes in provider policy and non-binding agreements such as terms of use (ToU).

upvoted 2 times

Question #60*Topic 1*

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

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

**Correct Answer:** *E*

Question #61*Topic 1*

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

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

**Correct Answer:** *C*

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

**Highly Voted** 8 months, 3 weeks ago

**Selected Answer: D**

D is the answer. Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together.

upvoted 6 times

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

**Most Recent** 1 week, 6 days ago

A cloud deployment of two or more unique clouds is known as: D. A Hybrid Cloud. A hybrid cloud refers to a cloud computing environment that combines two or more distinct cloud infrastructures, which can be private, public, or community clouds. In a hybrid cloud deployment, organizations can leverage the benefits of multiple cloud models to meet their specific needs. They can utilize the private cloud for sensitive or critical data and applications while leveraging the scalability and cost-effectiveness of public clouds for other workloads. The hybrid cloud allows for seamless integration and data sharing between the different cloud environments, providing flexibility and versatility to organizations. Therefore, option D, a Hybrid Cloud, is the correct answer for a cloud deployment consisting of two or more unique clouds.

upvoted 1 times

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

1 month ago

CSA Security Guidance v4 pg 11

upvoted 2 times

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

2 weeks, 3 days ago

Thank you

upvoted 1 times

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

4 months ago

I think C is correct because the term "unique" was used.

upvoted 1 times

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

4 months, 1 week ago

**Selected Answer: D**

Agree with Petza, Documentation states hybrid is the composition of two or more clouds

upvoted 1 times

Question #62*Topic 1*

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

* A. Data protection
* B. Professional negligence
* C. Globalization
* D. Intellectual property
* E. Outsourcing services and changes in control

**Correct Answer:** *C*

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

1 month, 3 weeks ago

**Selected Answer: C**

agreed with moota (enisa page 97)

upvoted 2 times

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

2 months, 2 weeks ago

**Selected Answer: C**

1. data protection a. availability and integrity b. minimum standard or guarantee 2. confidentiality 3. intellectual property 4. professional negligence 5. outsourcing services and changes in control.

upvoted 3 times

Question #63*Topic 1*

ENISA: An example high risk role for malicious insiders within a Cloud Provider includes

* A. Sales
* B. Marketing
* C. Legal counsel
* D. Auditors
* E. Accounting

**Correct Answer:** *D*

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

1 month, 3 weeks ago

**Selected Answer: D**

(enisa page 36) ...Examples of such roles include CP system administrators and auditors and managed security service providers dealing with intrusion detection reports and incident response. As cloud use increases, employees of cloud providers increasingly become targets for....

upvoted 2 times

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 #66*Topic 1*

ENISA: Which is a potential security benefit of cloud computing?

* A. More efficient and timely system updates
* B. ISO 27001 certification
* C. Provider can obfuscate system O/S and versions
* D. Greater compatibility with customer IT infrastructure
* E. Lock-In

**Correct Answer:** *A*

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

1 week, 6 days ago

A. More efficient and timely system updates. Cloud computing can provide more efficient and timely system updates compared to traditional on-premises environments. Cloud service providers are responsible for managing and maintaining the underlying infrastructure, including software and hardware updates. They often have dedicated teams and automated processes in place to ensure that security patches, bug fixes, and system updates are promptly applied across their infrastructure. This helps in reducing the window of vulnerability and mitigating security risks associated with outdated software or known vulnerabilities. Regular and timely system updates play a crucial role in enhancing security by addressing vulnerabilities, improving system resilience, and incorporating the latest security measures. Cloud providers, through their centralized management and update processes, can offer more efficient and timely system updates to their customers, enabling them to benefit from the latest security enhancements without the need for individual patch management.

upvoted 1 times

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

1 month, 3 weeks ago

**Selected Answer: A**

(enisa page 8) MORE TIMELY, EFFECTIVE AND EFFICIENT UPDATES AND DEFAULTS: default virtual machine images and software modules used by customers can be pre-hardened and updated with the latest patches and security settings according to fine-tuned processes; IaaS cloud service APIs also allow snapshots of virtual infrastructure to be taken regularly and compared with a baseline. Updates can be rolled out many times more rapidly across a homogenous platform than in traditional client-based systems that rely on the patching model.

upvoted 1 times

Question #67*Topic 1*

The Software Defined Perimeter (SDP) includes which components?

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

**Correct Answer:** *A*

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

1 month, 3 weeks ago

**Selected Answer: A**

(page 82) SDP includes three components: • An SDP client on the connecting asset (e.g. a laptop). • The SDP controller for authenticating and authorizing SDP clients and configuring the connections to SDP gateways. • The SDP gateway for terminating SDP client network traffic and enforcing policies in communication with the SDP controller.

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 #75*Topic 1*

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

* A. False
* B. True

**Correct Answer:** *A*

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

1 week, 3 days ago

B. True A security failure at the root network of a cloud provider will generally not compromise the security of all customers due to the multitenancy configuration. In a multitenancy environment, multiple customers or tenants share the same physical infrastructure, but their resources and data are logically separated and isolated from each other. The cloud provider implements various security measures to ensure the isolation and protection of customer data. This includes network segmentation, virtualization, access controls, and security mechanisms at various levels. These measures are designed to prevent cross-customer data breaches and limit the impact of any security failures to the affected tenant only. While no system is completely immune to security breaches, the multitenancy configuration in cloud computing helps mitigate the risk of widespread security compromises across different customers in the event of a security failure at the root network of the cloud provider.

upvoted 1 times

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

2 months, 2 weeks ago

**Selected Answer: A**

7.3.4 A security failure at the root network will likely compromise the security of all customers. And this security must be managed for arbitrary communications and multiple tenants, some of which must be considered adversarial.

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 #78*Topic 1*

The containment phase of the incident response lifecycle requires taking systems offline.

* A. False
* B. True

**Correct Answer:** *B*

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

1 week, 3 days ago

B. True In the incident response lifecycle, the containment phase involves taking systems offline as a measure to prevent further damage or spread of the incident. By isolating affected systems or network segments, organizations can limit the impact and reduce the risk of additional compromise or data loss. Taking systems offline during the containment phase allows security teams to assess the situation, investigate the incident, and implement necessary remediation measures without the interference of ongoing malicious activity. It also helps to prevent the incident from spreading to other parts of the infrastructure or affecting additional systems or users. While the specific actions taken during the containment phase may vary depending on the nature of the incident and organizational policies, temporarily taking systems offline is a common and effective step to contain and control the situation.

upvoted 1 times

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

1 month, 3 weeks ago

**Selected Answer: B**

from security guidance page 102: Containment: Taking systems offline. Considerations for data loss versus service availability. Ensuring systems don’t destroy themselves upon detection.

upvoted 1 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 #83*Topic 1*

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

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

**Correct Answer:** *C*

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

**Highly Voted** 8 months ago

**Selected Answer: B**

From CCM: Architectural Relevance Phys Network Compute Storage App Data

upvoted 8 times

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

**Highly Voted** 8 months, 2 weeks ago

**Selected Answer: B**

B. Physical, Network, Compute, Storage, Application or Data These are the columns of the CCM document

upvoted 5 times

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

**Most Recent** 1 week, 3 days ago

The Architectural Relevance column in the Cloud Controls Matrix (CCM) indicates the applicability of the cloud security control to: B. Physical, Network, Compute, Storage, Application, or Data The CCM is a framework that provides a catalog of security controls and best practices for various elements of cloud computing. The Architectural Relevance column in the CCM specifies the specific architectural components or elements to which the security control is relevant or applicable. These elements can include physical infrastructure, network components, compute resources, storage systems, application layers, and data. The CCM helps organizations assess and align their security controls with the relevant architectural elements in a cloud computing environment, ensuring comprehensive coverage and addressing the specific security considerations associated with each component.

upvoted 1 times

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

4 months, 1 week ago

**Selected Answer: B**

Checking the CCM, Clearly it is Phys Net Comp Stor App Data

upvoted 3 times

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

6 months, 1 week ago

**Selected Answer: B**

From ccm file

upvoted 4 times

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

6 months, 2 weeks ago

Answer B "Infrastructure & Virtualization Security Network Architecture" IVS-13 X X X X X X

upvoted 4 times

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

7 months, 1 week ago

**Selected Answer: B**

In CCM v4.0.5, Phys, Network, Compute, Storage, App, Data

upvoted 4 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 #86*Topic 1*

When designing an encryption system, you should start with a threat model.

* A. False
* B. True

**Correct Answer:** *B*

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

1 week, 3 days ago

B. True When designing an encryption system, it is highly recommended to start with a threat model. A threat model helps identify potential risks, vulnerabilities, and attack vectors that the encryption system may face. It involves analyzing the system's assets, potential adversaries, and the potential impact of successful attacks. By understanding the threats and risks, designers can make informed decisions about the appropriate encryption algorithms, key management practices, and overall system architecture. Threat modeling allows designers to identify potential weaknesses in the encryption system and make proactive decisions to mitigate those risks. It helps ensure that the encryption system is designed to effectively protect sensitive data and withstand potential attacks. Therefore, starting the design process with a threat model is an important step in developing a robust and secure encryption system.

upvoted 1 times

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

1 month, 1 week ago

From Security Guidance v4. Section 11.1.4.2, Page 124: When designing an encryption system, you should start with a threat model. For example, do you trust a cloud provider to manage your keys? How could the keys be exposed? Where should you locate the encryption engine to manage the threats you are concerned with?

upvoted 1 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 #89*Topic 1*

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

* A. False
* B. True

**Correct Answer:** *A*

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

1 week, 3 days ago

A. False Vulnerability assessments can be integrated into CI/CD (Continuous Integration/Continuous Deployment) pipelines, and it is not accurate to say that they cannot be easily integrated due to provider restrictions. In fact, integrating vulnerability assessments into CI/CD pipelines is a recommended practice to ensure the security of software applications throughout the development lifecycle. By incorporating vulnerability scanning and testing tools into the CI/CD pipeline, organizations can automate the process of identifying and addressing security vulnerabilities early on. Cloud service providers typically offer APIs, SDKs, and tools that allow developers to integrate security testing and vulnerability assessments into their CI/CD pipelines. These tools can scan the application code, dependencies, and container images for known vulnerabilities, configuration weaknesses, and common security issues.

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 #91*Topic 1*

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

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

**Correct Answer:** *D*

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

**Highly Voted** 7 months, 1 week ago

**Selected Answer: A**

I don't believe a customer can submit the CCM on behalf of the CSP to CSA Security. As a result I marked A for answer.

upvoted 5 times

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

**Most Recent** 1 week, 3 days ago

The option that is NOT suitable for the company as a cloud customer when using the Cloud Control Matrix (CCM) is: A. Submit the CCM on behalf of the CSP to CSA Security, Trust & Assurance Registry (STAR), a free, publicly accessible registry that documents the security controls provided by CSPs. Submitting the CCM on behalf of the cloud service provider (CSP) to CSA STAR is not a suitable option for the company as a cloud customer. The CSA STAR registry is intended for CSPs to document and demonstrate their security controls and practices to customers and the public. It is not meant for cloud customers to submit the CCM on behalf of their CSP.

upvoted 1 times

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

2 months, 2 weeks ago

**Selected Answer: A**

In https://cloudsecurityalliance.org/star/, you can ask your CSP to submit to the registry.

upvoted 2 times

Question #92*Topic 1*

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

* A. False
* B. True

**Correct Answer:** *A*

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

1 month ago

CCSK Study Guide, pg 106: If there is concern that the management plane is breached, be sure to confirm that the templates or configurations for new infrastructure/ applications have not been compromised.

upvoted 1 times

**[Neo0](https://www.examtopics.com/user/Neo0/)**

2 months ago

new infrastructure/applications

upvoted 1 times

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

3 months, 2 weeks ago

even by common sense it should B

upvoted 1 times

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

6 months, 1 week ago

**Selected Answer: B**

From the guidance as mentioned by cjkuga

upvoted 1 times

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

7 months, 1 week ago

**Selected Answer: B**

9.1.2.3 If there is concern that the management plane is breached, be sure to confirm that the templates or configurations for new infrastructure/applications have not been compromised.

upvoted 3 times

Question #93*Topic 1*

CCM: A hypothetical start-up company called "ABC" provides a cloud based IT management solution. They are growing rapidly and therefore need to put controls in place in order to manage any changes in their production environment. Which of the following Change Control & Configuration Management production environment specific control should they implement in this scenario?

* A. Policies and procedures shall be established for managing the risks associated with applying changes to business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations, infrastructure network and systems components.
* B. Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g. issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.
* C. All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.
* D. None of the above

**Correct Answer:** *A*

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

1 week, 3 days ago

A. Policies and procedures shall be established for managing the risks associated with applying changes to business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations, infrastructure network and systems components. As a growing start-up with a cloud-based IT management solution, it is crucial for "ABC" to have proper policies and procedures in place to manage changes in their production environment effectively. This control ensures that any changes made to business-critical applications, customer-impacting systems, API designs and configurations, and infrastructure network and system components are carefully managed and their associated risks are assessed.

upvoted 1 times

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

1 month, 3 weeks ago

**Selected Answer: A**

CCC-05

upvoted 1 times

Question #94*Topic 1*

Containers are highly portable code execution environments.

* A. False
* B. True

**Correct Answer:** *B*

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

1 week, 3 days ago

B. True Containers are indeed highly portable code execution environments. Containers provide a lightweight and isolated runtime environment that encapsulates an application and its dependencies. This allows the containerized application to run consistently and reliably across different computing environments, such as development machines, testing environments, and production servers. Containers achieve portability by bundling the application code, runtime dependencies, libraries, and configuration files into a single package. This package, known as a container image, can be easily distributed and deployed on various host systems that have a compatible container runtime, such as Docker or Kubernetes. Containers abstract away the underlying infrastructure and operating system differences, making it possible to run the same containerized application consistently across different environments.

upvoted 1 times

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 #101*Topic 1*

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

* A. False
* B. True

**Correct Answer:** *B*

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

1 week, 3 days ago

B. True When logs are properly configured, they can track and record every code, infrastructure, and configuration change made within a system or environment. This includes capturing information about the submitter and approver of the changes, as well as any associated test results. Logs play a crucial role in maintaining an audit trail and providing accountability for changes made in a system. By analyzing logs, organizations can track the history of changes, identify potential issues or security breaches, and ensure compliance with policies and regulations. Therefore, the statement is true.

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 #103*Topic 1*

Without virtualization, there is no cloud.

* A. False
* B. True

**Correct Answer:** *B*

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

1 week, 3 days ago

B. True Virtualization is a fundamental technology that underlies cloud computing. It enables the abstraction and virtualization of computing resources, such as servers, storage, and networks, allowing for the efficient allocation and utilization of these resources across multiple users or tenants. Cloud computing relies on virtualization to provide the flexibility, scalability, and isolation required to deliver on-demand services over the internet. Without virtualization, the key characteristics of cloud computing, such as resource pooling, rapid elasticity, and multi-tenancy, would not be possible. Virtualization enables the creation of virtual machines (VMs) or containers that can run multiple instances of operating systems and applications on a single physical server. Therefore, the statement is true. Without virtualization, there would be no cloud computing as we understand it today.

upvoted 1 times

Question #104*Topic 1*

All assets require the same continuity in the cloud.

* A. False
* B. True

**Correct Answer:** *A*

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

7 months, 1 week ago

6.0.1.1

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?

* A. Code Review
* B. Static Application Security Testing (SAST)
* C. Unit Testing
* D. Functional Testing
* E. Dynamic Application Security Testing (DAST)

**Correct Answer:** *E*

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

1 week, 3 days ago

E. Dynamic Application Security Testing (DAST) Dynamic Application Security Testing (DAST) is a type of application security testing that involves testing running applications to identify vulnerabilities and security weaknesses. It simulates real-world attacks on the application and examines how it responds to those attacks. DAST typically includes tests such as web vulnerability scanning, penetration testing, and fuzzing. DAST tools send various inputs and payloads to the application, analyze the responses, and identify potential vulnerabilities such as injection flaws, cross-site scripting (XSS), and insecure configurations. Unlike Static Application Security Testing (SAST), which analyzes the application's source code, DAST focuses on the application in its deployed state. Therefore, the correct answer is E. Dynamic Application Security Testing (DAST).

upvoted 1 times

Question #106*Topic 1*

CCM: The Cloud Service Delivery Model Applicability column in the CCM indicates the applicability of the cloud security control to which of the following elements?

* A. Mappings to well-known standards and frameworks
* B. Service Provider or Tenant/Consumer
* C. Physical, Network, Compute, Storage, Application or Data
* D. SaaS, PaaS or IaaS

**Correct Answer:** *D*

Question #107*Topic 1*

Any given processor and memory will nearly always be running multiple workloads, often from different tenants.

* A. False
* B. True

**Correct Answer:** *B*

Question #108*Topic 1*

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. Public
* B. PaaS
* C. Private
* D. IaaS
* E. Hybrid

**Correct Answer:** *E*

Question #109*Topic 1*

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

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

**Correct Answer:** *B*

Question #110*Topic 1*

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

* A. Nothing.
* B. It depends on how the automation is configured.
* C. Changes made in production are overwritten by the next code or template change.
* 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.

**Correct Answer:** *D*

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

2 months, 2 weeks ago

**Selected Answer: C**

10.1.3.4 If the system or environment is built automatically from a template, likely from a CI/ CD pipeline, then any changes made in production will be overwritten by the next code or template change.

upvoted 1 times

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

6 months ago

Actually C and D are correct, but in single-choice question, I would go for C, as it has the more significant security implications.

upvoted 1 times

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

6 months, 1 week ago

**Selected Answer: C**

I think it is C. these environments are automatically built for us from a set of source file definitions (templates), they can also be immutable. This means that any changes that are manually implemented will be overwritten the next time a template is run

upvoted 1 times

**[tralala2](https://www.examtopics.com/user/tralala2/)**

7 months ago

**Selected Answer: C**

In this one I would go with C (personally I would go with C & D) but I think C is the best According to Domain 10 • Elasticity. 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 .............. operational requirements mean you never want to allow an administrator to log into a system and make changes, since they will be lost during a normal auto-scale activity

upvoted 2 times

Question #111*Topic 1*

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

* A. Code Review
* B. Static Application Security Testing (SAST)
* C. Unit Testing
* D. Functional Testing
* E. Dynamic Application Security Testing (DAST)

**Correct Answer:** *D*

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

**Highly Voted** 7 months, 1 week ago

**Selected Answer: A**

10.1.3, Code Review: This is a manual activity that's not necessarily integrated into automated testing...

upvoted 5 times

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

**Most Recent** 4 weeks, 1 day ago

CCSK Study Guide pg 114: Code Review: This is a manual activity that’s not necessarily integrated into automated testing

upvoted 1 times

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

2 months, 2 weeks ago

Code review

upvoted 1 times

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

3 months, 4 weeks ago

Answer A is correct!

upvoted 1 times

Question #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?

* A. Secure Networking
* B. Secure Scaling
* C. Secure Deployment
* D. Secure Operations
* E. Secure Design and Development

**Correct Answer:** *C*

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

3 months, 4 weeks ago

Secure Deployment: The security and testing activities when moving code from an isolated development environment into production.

upvoted 1 times

Question #113*Topic 1*

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

* A. False
* B. True

**Correct Answer:** *B*

Question #114*Topic 1*

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

* A. Virtual environments
* B. Sparsely populated areas
* C. Without licenses
* D. Legal jurisdictions
* E. None of the above

**Correct Answer:** *D*

Question #115*Topic 1*

The key concern of data location is:

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

**Correct Answer:** *D*

Question #116*Topic 1*

ENISA: Licensing Risks refer to:

* A. Use of country-issued drivers licenses for user identification
* B. Cloud provider employees not maintaining operating system license files
* C. Risk that software company may go out of business, leading to expiration of licenses for mission critical software
* D. A traditional software licensing scheme may lead to high costs or lack of compliance in cloud systems
* E. Cloud provider may not have all appropriate government operating licenses

**Correct Answer:** *C*

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

**Highly Voted** 7 months ago

**Selected Answer: D**

R.24 Licensing Risk For example, if software is charged on a per instance basis every time a new machine is instantiated then the cloud customer’s licensing costs may increase exponentially even though they are using the same number of machine instances for the same duration.

upvoted 5 times

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

**Most Recent** 1 week ago

D: Licensing conditions, such as per-seat agreements, and online licensing checks may become unworkable in a cloud environment. For example, if software is charged on a per instance basis every time a new machine is instantiated then the cloud customer’s licensing costs may increase exponentially even though they are using the same number of machine instances for the same duration. In the case of PaaS and IaaS, there is the possibility for creating original work in the cloud (new applications, software etc). As with all intellectual property, if not protected by the appropriate contractual clauses (see ANNEX I – Cloud computing – Key legal issues , Intellectual Property), this original work may be at risk.

upvoted 1 times

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

6 months ago

Definitely D, see R.24 in ENISA document

upvoted 1 times

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

6 months, 2 weeks ago

The correct answer is Option D Reference: Licensing conditions, such as per-seat agreements, and online licensing checks may become unworkable in a cloud environment. For example, if software is charged on a per instance basis every time a new machine is instantiated then the cloud customer’s licensing costs may increase exponentially even though they are using the same number of machine instances for the same duration. In the case of PaaS and IaaS, there is the possibility for creating original work in the cloud (new applications, software etc). As with all intellectual property, if not protected by the appropriate contractual clauses (see ANNEX I – Cloud computing – Key legal issues , Intellectual Property), this original work may be at risk.

upvoted 2 times

**[tralala2](https://www.examtopics.com/user/tralala2/)**

6 months, 3 weeks ago

**Selected Answer: D**

should be D

upvoted 3 times

Question #117*Topic 1*

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

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

**Correct Answer:** *D*

Question #118*Topic 1*

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

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

**Correct Answer:** *D*

Question #119*Topic 1*

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

* A. Federation bridges, software compatibility, and implementation
* B. Delegations, bipartisan tenancy, and implementation
* C. Single tenancy and vendor lock-in
* D. Provisioning, federation, and compliance
* E. Compliance, multi-tenancy, and vendor lock-in

**Correct Answer:** *E*

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

3 months, 4 weeks ago

E: Regulation differences: Given global regulatory requirements, SecaaS providers may be unable to assure compliance in all jurisdictions that an organization operates in Data leakage: As with any cloud computing service or product, there is always the concern of data from one cloud user leaking to another. SecaaS providers should be held to the highest standards of multitenant isolation and segregation. Changing providers: organizations may be concerned about lock-in due to potentially losing access to data, including historical data needed for compliance or investigative support.

upvoted 1 times

Question #120*Topic 1*

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

* A. XHTML
* B. SAML
* C. SCORM
* D. WEP
* E. WPA or WPA2

**Correct Answer:** *B*

Question #121*Topic 1*

The key concern of data backup and recovery schemes is:

* A. Data aggregation should not cause breaches
* B. They must prevent data loss, unwanted data overwrite and destruction
* C. Assurance that cloud provider has multiple data centers for disaster recover
* D. Assurance that deleted data is in fact unrecoverable
* E. Data should not be commingled with other customers

**Correct Answer:** *E*

Question #122*Topic 1*

Which regulation affects data controllers with business in Japan?

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

**Correct Answer:** *E*

Question #123*Topic 1*

Which component is a key part of software container systems?

* A. Operating system
* B. Workload tools
* C. An automated controller.
* D. The execution environment
* E. A client

**Correct Answer:** *D*

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

1 week ago

D: SecGuiv4, P.85: Containers: Containers are code execution environments that run within an operating system (for now), sharing and leveraging resources of that operating system. While a VM is a full abstraction of an operating system, a container is a constrained place to run segregated processes while still utilizing the kernel and other capabilities of the base OS. Multiple containers can run on the same virtual machine or be implemented without the use of VMs at all and run directly on hardware. The container provides code running inside a restricted environment with only access to the processes and capabilities defined in the container configuration. This allows containers to launch incredibly rapidly, since they don’t need to boot an operating system or launch many (sometimes any) new services; the container only needs access to already-running services in the host OS and some can launch in milliseconds.

upvoted 1 times

Question #124*Topic 1*

CCM: What is the role of the Scope Applicability column in the CCM?

* A. It show which architectural elements are related to a given control
* B. It describes the applicability of the overall domain
* C. It maps the existing industry standards to the controls in the domains
* D. It describes the applicability of the controls in the domains
* E. None of the above

**Correct Answer:** *C*

Question #125*Topic 1*

When considering business continuity and disaster recovery with a cloud provider, which layer of the logical stack includes code and message queues?

* A. Applistructure
* B. Datastructure
* C. Infostructure
* D. Infrastructure
* E. Metastructure

**Correct Answer:** *A*

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

1 week ago

A: SecGuiV4, P.74: Applistructure: Applistructure includes all of the above, but also the application assets like code, message queues, etc. When a cloud user builds their own cloud applications they’re usually built on top of IaaS and/or PaaS, so resiliency and recovery are inherently tied to those layers. But Applistructure includes the full range of everything in an application.

upvoted 1 times

Question #126*Topic 1*

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

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

**Correct Answer:** *E*

Question #127*Topic 1*

What is true of cloud built-in firewalls?

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

**Correct Answer:** *D*

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

1 week ago

D. They typically offer fewer features that newer physical firewalls SecGuiV4, P.96: All modern cloud platforms offer built-in firewalls, which may offer advantages over corresponding physical firewalls. These are software firewalls that may operate within the SDN or the hypervisor. They typically offer fewer features than a modern, dedicated next-generation firewall, but these capabilities may not always be needed due to other inherent security provided by the cloud provider.

upvoted 1 times

Question #128*Topic 1*

What are the NIST defined essential characteristics of cloud computing?

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

**Correct Answer:** *D*

Question #129*Topic 1*

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

* A. False
* B. True

**Correct Answer:** *B*

Question #130*Topic 1*

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

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

**Correct Answer:** *E*

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

2 months, 2 weeks ago

**Selected Answer: D**

Looks like D according to 11.1.2

upvoted 1 times

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

6 months, 3 weeks ago

**Selected Answer: D**

11.1.2 Cloud Data Storage Types Application/platform: Examples of these would be a content delivery network (CDN), files stored in SaaS, caching, and other novel options. I would go for D.

upvoted 3 times

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

7 months ago

**Selected Answer: C**

Content delivery Network is not an storage mean. According to wiki "CDN is a geographically distributed network of proxy servers and their data centers. The goal is to provide high availability and performance by distributing the service spatially relative to end users."

upvoted 3 times

Question #131*Topic 1*

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

* A. Recovery
* B. Ballistics
* C. Detection
* D. Forensics
* E. Preparation

**Correct Answer:** *D*

Question #132*Topic 1*

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

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

**Correct Answer:** *B*

Question #133*Topic 1*

How can you monitor and filter data in a virtual network when traffic might not cross the physical network?

* A. Route traffic to the physical network for capturing
* B. Route traffic to a virtual appliance on the same virtual network
* C. Route traffic to a virtual network monitoring or filtering tool on the same hardware
* D. A and B
* E. B and C

**Correct Answer:** *E*

Question #134*Topic 1*

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

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

**Correct Answer:** *D*

**[Azo\_4952](https://www.examtopics.com/user/Azo_4952/)**

**Highly Voted** 7 months, 1 week ago

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.

upvoted 6 times

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

**Most Recent** 1 week ago

E. Identity SecGui v4 P.131: 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. • Identifier: the means by which an identity can be asserted. For digital identities this is often a cryptological token. In the real world it might be your passport.

upvoted 1 times

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

1 week, 5 days ago

It's E

upvoted 1 times

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

2 months, 2 weeks ago

**Selected Answer: E**

12.1 Identity: the unique expression of an entity within a given namespace.

upvoted 2 times

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

3 months, 4 weeks ago

E: Identity is correct!

upvoted 1 times

Question #135*Topic 1*

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

* A. Information Management Policies
* B. Multitenancy
* C. Network Intrusion Detect on Systems (NIDS)
* D. Software Defined Networking (SDN)
* E. Virtual LANs (VLANs)

**Correct Answer:** *D*

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

1 week ago

SecGuiV4 P.79 D: Software Defined Networking (SDN): A more complete abstraction layer on top of networking hardware, SDNs decouple the network control plane from the data plane. This allows us to abstract networking from the traditional limitations of a LAN

upvoted 1 times

Question #136*Topic 1*

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

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

**Correct Answer:** *E*

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

1 week ago

A: Expose security controls Hard to say, but according to the book: A. Expose security controls, is the rigth answer. SecGuiV4 P.83: Providers must also expose security controls to the cloud users so they can properly configure and manage their network security.

upvoted 1 times

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

4 weeks, 1 day ago

Answer A: CCSK Study Guide, pg 84, Providers must also expose security controls to the cloud users so they can properly configure and manage their network security.

upvoted 1 times

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

2 months, 2 weeks ago

**Selected Answer: A**

7.3.4 Providers must also expose security controls to the cloud users so they can properly configure and manage their network security.

upvoted 1 times

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

5 months, 2 weeks ago

**Selected Answer: A**

According to the documentation A is the right answer

upvoted 1 times

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

6 months, 2 weeks ago

The correct answer is Option A Reference: Providers must also expose security controls to the cloud users so they can properly configure and manage their network security.

upvoted 4 times

Question #137*Topic 1*

What is true of Software Defined Network firewalls?

* A. They are policy sets that can only be applied to similar grouped assets
* B. They require the use of static IP addresses
* C. They are more difficult to manage
* D. They are limited based on physical topology
* E. They are not limited based on physical topology

**Correct Answer:** *E*

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

1 week ago

E. They are not limited based on physical topology

upvoted 1 times

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

6 months, 1 week ago

**Selected Answer: E**

they aren’t limited based on physical topology

upvoted 2 times

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

6 months, 2 weeks ago

Option A SDN firewalls (e.g., security groups) can apply to assets based on more flexible criteria than hardware-based firewalls, since they aren’t limited based on physical topology. (Note that this is true of many types of software firewalls, but is distinct from hardware firewalls). SDN firewalls are typically policy sets that define ingress and egress rules that can apply to single assets or groups of assets, regardless of network location (within a given virtual network). For example, you can create a set of firewall rules that apply to any asset with a particular tag. Keep in mind this gets slightly difficult to discuss, since different platforms use different terminology and have different capabilities to support this kind of capability, so we are trying to keep things at a conceptual level.

upvoted 1 times

Question #138*Topic 1*

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

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

**Correct Answer:** *D*

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

3 weeks, 6 days ago

Hybrid: CCSK Security Study Guide, pg 12: Hybrid is also commonly used to describe a non-cloud data center bridged directly to a cloud provider.

upvoted 1 times

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

1 month, 3 weeks ago

**Selected Answer: B**

Its B. B!!!!

upvoted 1 times

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

6 months ago

Agree, option B is correct. MANY MANY incorrect "professionally reviewed" answers in here...

upvoted 1 times

**[tralala2](https://www.examtopics.com/user/tralala2/)**

7 months ago

**Selected Answer: B**

B Hybrid Cloud

upvoted 2 times

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

7 months, 1 week ago

**Selected Answer: B**

Hybrid is also commonly used to describe a non-cloud data center bridged directly to a cloud provider

upvoted 3 times

**[Azo\_4952](https://www.examtopics.com/user/Azo_4952/)**

7 months, 1 week ago

The term hybrid cloud is also commonly used to describe a non-cloud data centre bridged directly to a cloud provider. Cloud service models the answer is hybrid cloud

upvoted 2 times

Question #139*Topic 1*

What is a core tenant of risk management?

* A. If there is still residual risk after assessments and controls are in place, you must accept the risk.
* B. Risk insurance covers all financial losses, including loss of customers.
* C. The consumers are completely responsible for all risk.
* D. The provider is accountable for all risk management.
* E. You can manage, transfer, accept, or avoid risks.

**Correct Answer:** *E*

Question #140*Topic 1*

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

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

**Correct Answer:** *B*

Question #141*Topic 1*

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

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

**Correct Answer:** *E*

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

1 week ago

D. Virtual machines may communicate with each other over a virtual network all on the same host rather than a physical network between servers

upvoted 1 times

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

6 months, 1 week ago

**Selected Answer: D**

In my opinion is D

upvoted 1 times

**[tralala2](https://www.examtopics.com/user/tralala2/)**

7 months ago

D should be the correct answer, the question is why do blind spots occur ... and one of the reason it could be that the vm's are on the same host

upvoted 2 times

**[Boo\_boo12](https://www.examtopics.com/user/Boo_boo12/)**

8 months, 1 week ago

Would choose D too

upvoted 4 times

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

8 months, 1 week ago

Please check the answer, i feel below should be the answer D. Virtual machines may communicate with each other over a virtual network all on the same host rather than a physical network between servers

upvoted 4 times

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

7 months ago

your VMs are not always on the same host

upvoted 1 times

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

5 months, 4 weeks ago

That's not what the answer implicates, as it says VMs MAY (!) communicate over a virtual network all on the same host, not that they necessarily need to be. So many incorrectly marked answers in here, it's actually not worth the money.

upvoted 1 times

Question #142*Topic 1*

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

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

**Correct Answer:** *B*

Question #143*Topic 1*

Which type of application security testing should incorporate checks on API calls to the cloud service?

* A. Dynamic Application Security Testing (DAST)
* B. Unit Testing
* C. Functional Testing
* D. Static Application Security Testing (SAST)
* E. All of the above

**Correct Answer:** *D*

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

2 months, 2 weeks ago

**Selected Answer: D**

10.1.3 Static Application Security Testing (SAST): On top of the normal range of tests, these should ideally incorporate checks on API calls to the cloud service. They should also look for any static embedded credentials for those API calls, which is a growing problem.

upvoted 1 times

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

3 months, 4 weeks ago

Static Application Security Testing (SAST): On top of the normal range of tests, these should ideally incorporate checks on API calls to the cloud service.

upvoted 2 times

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

6 months, 1 week ago

**Selected Answer: E**

API calls should be tested with all the methods reported

upvoted 1 times

Question #144*Topic 1*

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

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

**Correct Answer:** *D*

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

3 months, 3 weeks ago

D: Perimeter security: Protecting from attacks against the management plane’s components itself, such as the web and API servers. It includes both lower-level network defenses as well as higher-level defenses against application attacks.

upvoted 1 times

Question #145*Topic 1*

In a cloud environment, how can you best determine data/information security risks and potential controls?

* A. understand the cloud storage architecture in use
* B. run a search on user data file
* C. encrypt everything
* D. identify the major operating system(s)
* E. understand the related regulatory requirements

**Correct Answer:** *A*

Question #146*Topic 1*

What is it called when a customer's information and/or processes are compromised by the actions of another customer in a multi-tenancy environment?

* A. Information leakage
* B. Data loss
* C. Failure to thrive
* D. Relationship failure
* E. Isolation failure

**Correct Answer:** *E*

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

1 week ago

ENISAPg. 9: ISOLATION FAILURE: multi-tenancy and shared resources are defining characteristics of cloud computing. This risk category covers the failure of mechanisms separating storage, memory, routing and even reputation between different tenants (e.g., so-called guest-hopping attacks). However it should be considered that attacks on resource isolation mechanisms (e.g.,. against hypervisors) are still less numerous and much more difficult for an attacker to put in practice compared to attacks on traditional OSs.

upvoted 1 times

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

4 weeks ago

It should be A: CCSK Study Guide pg 143; Data leakage. As with any cloud computing service or product, there is always the concern of data from one cloud user leaking to another. This risk isn’t unique to SecaaS, but the highly sensitive nature of security data (and other regulated data potentially exposed in security scanning or incidents) does mean that SecaaS providers should be held to the highest standards of multitenant isolation and segregation.

upvoted 1 times

Question #147*Topic 1*

What are the three main aspects for data security controls?

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

**Correct Answer:** *A*

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

1 week ago

E. Controlling, protecting, and enforcing SecGuiV4 Pg.120: 11.1.1 Data Security Controls: Controlling, protecting, and enforcing

upvoted 1 times

**[tralala2](https://www.examtopics.com/user/tralala2/)**

6 months, 3 weeks ago

**Selected Answer: E**

E is the correct answer

upvoted 2 times

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

6 months, 3 weeks ago

**Selected Answer: E**

11.1.1 Data Security Controls Controlling, Protecting, Enforcing

upvoted 4 times

Question #148*Topic 1*

Which SDP component is used for authentication and authorization?

* A. Client
* B. Controller
* C. Access Manager
* D. Gateway
* E. Firewall

**Correct Answer:** *B*

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

1 week ago

B: Controller SecGui Pg.82 - The SDP controller for authenticating and authorizing SDP clients and configuring the connections to SDP gateways.

upvoted 1 times

Question #149*Topic 1*

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

* A. True
* B. False

**Correct Answer:** *A*

Question #150*Topic 1*

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

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

**Correct Answer:** *D*

Question #151*Topic 1*

What are major factors to building and managing a secure management plane?

* A. Perimeter security; customer authentication; internal authentication and credential passing; authorization and entitlements; and logging, monitoring, and alerting
* B. API management; end point security; logging; and authentication and authorization
* C. Device patching and maintenance; internal authentication and credential passing; access management and logging, monitoring, and alerting
* D. Perimeter security; customer authentication; internal authentication and credential passing; authorization and entitlements; and governance auditing
* E. Perimeter patching; log authentication; external entitlement passing; credential alerting and customer security

**Correct Answer:** *A*

Question #152*Topic 1*

Cloud storage will most often utilize the same types of data storage used in traditional data storage technologies.

* A. True
* B. False

**Correct Answer:** *B*

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

3 months, 3 weeks ago

B: 11.1.2, Since cloud storage is virtualized it tends to support different data storage types than used in traditional storage technologies. Below the virtualization layer these might use well-known data storage mechanisms, but the cloud storage virtualization technologies that cloud users access will be different.

upvoted 2 times

Question #153*Topic 1*

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

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

**Correct Answer:** *D*

Question #154*Topic 1*

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

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

**Correct Answer:** *B*

Question #155*Topic 1*

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

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

**Correct Answer:** *D*

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

**Highly Voted** 6 months, 3 weeks ago

**Selected Answer: A**

11.1.3.1. There are a few options for in-transit encryption depending on what the cloud platform supports. One way is to encrypt before sending to the cloud (client-side encryption). Network encryption (TLS/SFTP/etc.) is another option. Most cloud provider APIs use Transport Layer Security (TLS) by default; if not, pick a different provider, since this is an essential security capability. Proxy-based encryption may be a third option, where you place an encryption proxy in a trusted area between the cloud user and the cloud provider and the proxy manages the encryption before transferring the data to the provider.

upvoted 6 times

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

**Most Recent** 2 months, 2 weeks ago

A is the right answer

upvoted 1 times

**[tralala2](https://www.examtopics.com/user/tralala2/)**

6 months, 3 weeks ago

**Selected Answer: A**

A is correct

upvoted 3 times

Question #156*Topic 1*

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

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

**Correct Answer:** *D*

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

4 weeks ago

Answer is B: CCSK Study Security Guide pg 37: highlights some of the legal issues raised by moving data to the cloud; contracting with cloud service providers; and handling electronic discovery requests in litigation. Our overview here cannot address every potential legal situation. To address your specific issues, you should consult with legal counsel in the jurisdiction(s) in which you intend to operate and/or in which your customers reside. In addition, be aware that laws and regulations change frequently, and thus you should verify the relevancy of information contained in this domain before relying on it. Domain 3 is concerned primarily with the legal implications of public cloud computing and third party-hosted private clouds.

upvoted 1 times

**[tralala2](https://www.examtopics.com/user/tralala2/)**

6 months, 3 weeks ago

**Selected Answer: B**

B is correct

upvoted 1 times

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

6 months, 3 weeks ago

**Selected Answer: B**

3.0 Introduction This domain highlights some of the legal issues raised by moving data to the cloud; contracting with cloud service providers; and handling electronic discovery requests in litigation. Our overview here cannot address every potential legal situation. To address your specific issues, you should consult with legal counsel in the jurisdiction(s) in which you intend to operate and/or in which your customers reside.

upvoted 3 times

Question #157*Topic 1*

ENISA: A key area of controls for cloud provider network architecture is

* A. Patch management
* B. SAFECode software assurance
* C. Hardening of virtual machines according to industry standard guidelines
* D. Distributed Denial of Service mitigation
* E. Antivirus

**Correct Answer:** *D*

Question #158*Topic 1*

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

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

**Correct Answer:** *A*

Question #159*Topic 1*

While a virtual machine is a full abstraction of an operating system, a container is a constrained place to run segregated processes while still using the kernel and other OS capabilities.

* A. True
* B. False

**Correct Answer:** *A*

Question #160*Topic 1*

What are the main considerations for key management?

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

**Correct Answer:** *D*

**[tralala2](https://www.examtopics.com/user/tralala2/)**

6 months, 3 weeks ago

**Selected Answer: D**

D is correct

upvoted 2 times

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

6 months, 3 weeks ago

**Selected Answer: D**

11.1.4.3 Key Management (Including Customer-Managed Keys) The main considerations for key management are performance, accessibility, latency, and security.

upvoted 3 times

Question #161*Topic 1*

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

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

**Correct Answer:** *B*

Question #162*Topic 1*

CCM: A hypothetical start-up company called "IT4Sure" provides a cloud based IT management solution. They are growing rapidly and have some security measures in place but the employees are still using their personal mobile devices for storing and communicating company confidential information. So they decide to provide the employees with company mobile devices and implement a Mobile Device Management policy. Two months later, a customer wants to review  
IT4Sure's mobile device security practices. Which of the following basic protection measures should the client look for in the company's Mobile Device  
Management policy?

* A. Registration of mobile devices
* B. Requirements for physical protection
* C. Requirements for mobile device software versions and for applying patches
* D. Malware protection
* E. All of the above

**Correct Answer:** *E*

Question #163*Topic 1*

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

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

**Correct Answer:** *E*

Question #164*Topic 1*

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

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

**Correct Answer:** *B*

Question #165*Topic 1*

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

* A. True
* B. False

**Correct Answer:** *A*

Question #166*Topic 1*

What are the encryption options available for SaaS consumers?

* A. Provider-managed and (sometimes) proxy encryption
* B. Any encryption option that is available for volume storage, object storage, or PaaS
* C. Volume storage encryption
* D. Client/application and file/folder encryption
* E. Object encryption

**Correct Answer:** *A*

Question #167*Topic 1*

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

* A. True
* B. False

**Correct Answer:** *A*

Question #168*Topic 1*

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

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

**Correct Answer:** *A*

Question #169*Topic 1*

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

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

**Correct Answer:** *E*

Question #170*Topic 1*

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

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

**Correct Answer:** *B*

Question #171*Topic 1*

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

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

**Correct Answer:** *C*

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

3 months, 3 weeks ago

Voted for C: V39 V38. Misconfiguration V39. System or OS vulnerabilities V6. Lack of resource isolation V41. Lack of, or a poor and untested, business continuity and disaster recovery PLAN

upvoted 1 times

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

5 months, 1 week ago

**Selected Answer: E**

E is correct

upvoted 1 times

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

5 months, 1 week ago

Sorry C is correct. P48 , R 26

upvoted 1 times

Question #172*Topic 1*

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

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

**Correct Answer:** *D*

Question #173*Topic 1*

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

* A. True
* B. False

**Correct Answer:** *A*

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

7 months, 1 week ago

**Selected Answer: A**

Audits and assessments are mechanisms to document compliance with internal or external requirements (or identify deficiencies). Reporting needs to include a compliance determination, as well as a list of identified issues, risks, and remediation recommendations.

upvoted 1 times

Question #174*Topic 1*

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

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

**Correct Answer:** *D*

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

6 days, 22 hours ago

D: Distributed data collection SegGuiV4 p.147 - Distributed data collection: Mechanisms to ingest large volumes of data, often of a streaming nature. This could be as “lightweight” as web-click streaming analytics and as complex as highly distributed scientific imaging or sensor data. Not all big data relies on distributed or streaming data collection, but it is a core big data technology.

upvoted 1 times

Question #175*Topic 1*

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

* A. A network is split into nodes; all of the nodes store only certain types of files.
* B. Fragmented files are signed and stored together on a local server; data retrieval is arbitrary.
* C. File fragments are sequentially placed on servers based on the physical location of the data user.
* D. A cloud is split into cloudlets; each cloudlet stores a portion of the files based on an encryption algorithm.
* E. A file is split into fragments; all of the fragments are sent to multiple physical storage repositories.

**Correct Answer:** *E*

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

6 days, 22 hours ago

E: data dispersion (sometimes also known as data fragmentation of bit splitting). This process takes chunks of data, breaks them up, and then stores multiple copies on different physical storage to provide high durability. Data stored in this way is thus physically dispersed. A single file, for example, would not be located on a single hard drive.

upvoted 1 times

Question #176*Topic 1*

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

* A. False
* B. True

**Correct Answer:** *B*

Question #177*Topic 1*

Installing security software designed for physical servers onto a virtualized server can result in severe degradation in performance.

* A. False
* B. True

**Correct Answer:** *B*

Question #178*Topic 1*

CCM: A hypothetical company called "lnfrastructure4Sure" provides Infrastructure as a Service (IaaS) to its clients. A customer wants to review Infrastructure4Sure's hypervisor security implementation measures. Which of the following measures should Infrastructure4Sure implement?

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

**Correct Answer:** *A*

Question #179*Topic 1*

CCM: What security requirements does the Identity and Access Management domain in the CCM address?

* A. The requirement to ensure that all files are properly backed up.
* B. The requirement to ensure inappropriate access to resources and to enable the right individuals to access the right resources.
* C. There is no such domain as Identity and Access Management in the CCM.
* D. The requirement to ensure appropriate access to resources and to enable the right individuals to access the right resources at the right times for the right reasons.

**Correct Answer:** *D*

Question #180*Topic 1*

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

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

**Correct Answer:** *C*

**[Wllfgnlnrb18](https://www.examtopics.com/user/Wllfgnlnrb18/)**

2 months, 2 weeks ago

Answer is Hybrid cloud - 1.1.2.3: Hybrid Cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or

upvoted 1 times

Question #181*Topic 1*

What are six phases of the Data Security Lifecycle?

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

**Correct Answer:** *A*

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

2 days, 4 hours ago

D is the correct answer.

upvoted 1 times

Question #182*Topic 1*

Which tool is the primary tool between the cloud provider and consumer that extends governance into business partners and providers?

* A. Compliance Reporting
* B. Supplier Assessments
* C. Consumer Assessments
* D. Contracts
* E. Service-level Agreements (SLAs)

**Correct Answer:** *E*

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

4 weeks ago

D: CCSK Study Security Guide, pg 29, 2.1.1.1

upvoted 1 times

**[cloud\_guru\_1909](https://www.examtopics.com/user/cloud_guru_1909/)**

2 months, 1 week ago

**Selected Answer: D**

Contracts: The primary tool of governance is the contract between a cloud provider and a cloud customer (this is true for public and private cloud). The contract is your only guarantee of any level of service or commitment—assuming there is no breach of contract which, tosses everything into a legal scenario. Contracts are the primary tool to extend governance into business partners and providers.

upvoted 1 times

Question #183*Topic 1*

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

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

**Correct Answer:** *D*

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

4 weeks ago

D is the most logical answer. This is a two part question, and the plaintext wording is a distractor. There is no mention of Homomorphic encryption as an option in any of the study guides. CCSK Study Guide pg 126, 11.1.4.3 references HSM as a viable option.

upvoted 1 times

**[cloud\_guru\_1909](https://www.examtopics.com/user/cloud_guru_1909/)**

2 months, 1 week ago

**Selected Answer: C**

V10. IMPOSSIBILITY OF PROCESSING DATA IN ENCRYPTED FORM Encrypting data at rest is not difficult, but despite recent advances in homomorphic encryption (27), there is little prospect of any commercial system being able to maintain this encryption during processing. In one article, Bruce Schneier estimates that performing a web search with encrypted keywords -- a perfectly reasonable simple application of this algorithm -- would increase the amount of computing time by about a trillion (28). This means that for a long time to come, cloud customers doing anything other than storing data in the cloud must trust the cloud provider.

upvoted 2 times

Question #184*Topic 1*

Which statement best describes the options for PaaS encryption?

* A. PaaS is very diverse and may include client/application, database, and proxy encryption as well as other options.
* B. PaaS is strictly limited to client/application, database and proxy encryption.
* C. PaaS is sensitive to application updates and therefore must be constantly refreshed with relevant keys.
* D. PaaS is very diverse and would most likely include file/folder and instance-managed encryption.
* E. PaaS is limited to public networks.

**Correct Answer:** *A*

Question #185*Topic 1*

What can be implemented to help with account granularity and limit blast radius with IaaS an PaaS?

* A. Maintaining tight control of the primary account holder credentials
* B. Configuring secondary authentication
* C. Implementing least privilege accounts
* D. Establishing multiple accounts
* E. Configuring role-based authentication

**Correct Answer:** *D*

Question #186*Topic 1*

Which of the following statements best defines the "authentication" component of identity, entitlement, and access management (IdEA).

* A. A guarantee that data in a repository is 100% unregulated
* B. Updating security protocols to the latest version
* C. Establishing/asserting the identity to the application
* D. The process of specifying and maintaining access policies
* E. None of the above

**Correct Answer:** *E*

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

6 days, 22 hours ago

The correct answer is: C. Establishing/asserting the identity to the application Authentication is the process of verifying and confirming the identity of a user or entity attempting to access a system, application, or resource. It involves presenting credentials (such as username and password, biometric data, or digital certificates) to prove one's identity and gain access to the desired resource. The authentication component of identity, entitlement, and access management (IdEA) is responsible for validating and asserting the identity of users or entities interacting with an application or system.

upvoted 1 times

Question #187*Topic 1*

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

* A. The standardization of security software makes the outsourcing of security as a service nearly obsolete.
* B. The advantages may include flexible offering of services, greater security domain knowledge and efficiency of SecaaS providers.
* C. The advantages are not realized until a security breach actually occurs. At that time the greater response of the security team should be obvious.
* D. The higher costs and reduced flexibility are more than compensated for by the ability to pass the security responsibilities on to another firm.
* E. Many areas of security as a service are ripe for adoption with the notable exceptions of anti-malware and anti-spam programs.

**Correct Answer:** *B*

Question #188*Topic 1*

What is true of how the management plane is to be secured in the cloud?

* A. The cloud provider is responsible for securing the management plane and exposing the required security features, while the cloud consumer is responsible for configuring access to the management plane.
* B. The cloud consumer is responsible for securing the management plane, exposing the required security features, and configuring access to the management plane.
* C. The cloud consumer is responsible for securing the management plane and exposing the required security features, while the cloud provider is responsible for configuring access to the management plane.
* D. The cloud provider is responsible for securing the management plane, exposing the required security features, and configuring access to the management plane.
* E. The cloud provider is responsible exposing the required security features, while the cloud consumer is responsible for securing the management plane and configuring access to the management plane.

**Correct Answer:** *A*

Question #189*Topic 1*

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

* A. Evaluating infrastructure by proactive scanning and network monitoring, vulnerability assessments, and performing risk assessments
* B. Planning notification and coordination of activities
* C. Making considerations for data loss versus service availability
* D. Configuring and validating alerts
* E. Analyzing what happened

**Correct Answer:** *C*

Question #190*Topic 1*

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

* A. Such knowledge is a prerequisite to implementing the required measures to ensure compliance with local laws that restrict the cross-border flow of data.
* B. Enable the data controller to register with the local Data Protection Officer(s), where appropriate.
* C. To facilitate comprehensive disaster planning.
* D. To enable data location transparency for the consumer.
* E. To allow compliance with local laws regarding data privacy and safeguarding.

**Correct Answer:** *E*

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

6 days, 21 hours ago

A. Such knowledge is a prerequisite to implementing the required measures to ensure compliance with local laws that restrict the cross-border flow of data. Knowing where the cloud service provider will host the data is crucial for ensuring compliance with local laws and regulations regarding the cross-border transfer of data. Many countries have specific requirements and restrictions on the transfer of personal or sensitive data outside their borders. By knowing the location of the data hosting, the data controller can take appropriate measures to comply with these laws, such as implementing data protection safeguards or obtaining necessary permissions or agreements. It allows the organization to ensure that the data is handled in accordance with applicable legal requirements and helps mitigate the risk of non-compliance and potential legal consequences.

upvoted 2 times

Question #191*Topic 1*

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

* A. Hardware, APIs, and Core Connectivity & Delivery
* B. Integration & Middleware, APIS, and Data
* C. Hardware, APIs, and Data
* D. Presentation modality, APIs, Applications, and Data
* E. Presentation modality, APIs, Applications, and Hardware

**Correct Answer:** *A*

**[cloud\_guru\_1909](https://www.examtopics.com/user/cloud_guru_1909/)**

2 months, 1 week ago

**Selected Answer: A**

Thus IaaS consists of a facility, hardware, an abstraction layer, an orchestration (core connectivity and delivery) layer to tie together the abstracted resources, and APIs to remotely manage the resources and deliver them to consumers.

upvoted 1 times

Question #192*Topic 1*

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

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

**Correct Answer:** *A*

Question #193*Topic 1*

ENISA: In Infrastructure as a Service (IaaS), who is responsible for guest systems monitoring?

* A. Customer
* B. Cloud Provider
* C. Shared responsibility
* D. Internet Service Provider (ISP)
* E. Data Commissioner

**Correct Answer:** *A*

Question #194*Topic 1*

What are the components of an encryption system?

* A. User, data, and encryption engine
* B. Data, encryption engine, and decryption tool
* C. User, encryption engine, and key management
* D. Data, encryption engine, and key management
* E. User, data, and key management

**Correct Answer:** *D*

Question #195*Topic 1*

What is the main data source for detection and analysis of an incident?

* A. Logs
* B. Data repositories
* C. The Pew Research Center
* D. Blogs
* E. Database

**Correct Answer:** *A*

Question #196*Topic 1*

Which cloud storage technology would include a content delivery network (CON), files stored in SaaS, and caching?

* A. Database
* B. Volume storage
* C. Application
* D. Object storage
* E. Service

**Correct Answer:** *C*

**[cloud\_guru\_1909](https://www.examtopics.com/user/cloud_guru_1909/)**

2 months, 1 week ago

**Selected Answer: C**

Application/platform: Examples of these would be a content delivery network (CDN), files stored in SaaS, caching, and other novel options.

upvoted 1 times

Question #197*Topic 1*

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

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

**Correct Answer:** *B*

Question #198*Topic 1*

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

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

**Correct Answer:** *D*

Question #199*Topic 1*

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

* A. There are 4 controls in that particular domain
* B. The control ID is a random number assigned to the control
* C. It is the 4th control in the IAM domain
* D. None of the above

**Correct Answer:** *C*

Question #200*Topic 1*

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

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

**Correct Answer:** *C*

Question #201*Topic 1*

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

* A. False
* B. True

**Correct Answer:** *B*

Question #202*Topic 1*

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

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

**Correct Answer:** *A*

**[dotcom21](https://www.examtopics.com/user/dotcom21/)**

3 weeks, 4 days ago

Refer – section 8.1.2.2 Management Infrastructure The cloud user is, again, responsible for proper rights management and configuration of exposed controls in the management plane.

upvoted 1 times

Question #203*Topic 1*

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

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

**Correct Answer:** *A*

Question #204*Topic 1*

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

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

**Correct Answer:** *A*

Question #205*Topic 1*

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

* A. False
* B. True

**Correct Answer:** *B*

Question #206*Topic 1*

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

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

**Correct Answer:** *A*

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

4 days, 23 hours ago

Event driven security: Certain cloud providers support event-driven code execution. In these cases, the management plane detects various activities—such as a file being uploaded to a designated object storage location or a configuration change to the network or identity management—which can in turn trigger code execution through a notification message, or via serverless hosted code. Security can define events for security actions and use the event-driven capabilities to trigger automated notification, assessment, remediation, or other security processes.

upvoted 1 times

Question #207*Topic 1*

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

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

**Correct Answer:** *C*

Question #208*Topic 1*

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

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

**Correct Answer:** *E*

Question #209*Topic 1*

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

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

**Correct Answer:** *E*

Question #210*Topic 1*

In which layer is the management plane?

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

**Correct Answer:** *C*

Question #211*Topic 1*

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

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

**Correct Answer:** *A*

Question #212*Topic 1*

Cloud provider contract enforceability should be carefully considered in light of

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

**Correct Answer:** *D*

Question #213*Topic 1*

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

* A. False
* B. True

**Correct Answer:** *B*

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

4 days, 22 hours ago

A is the correct answer. Free-form: internal identity providers/sources (often directory servers) connect directly to cloud providers. Hub and spoke: internal identity providers/sources communicate with a central broker or repository that then serves as the identity provider for federation to cloud providers.

upvoted 1 times

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

1 week, 6 days ago

It's false. • Free-form: internal identity providers/sources (often directory servers) connect directly to cloud providers. • Hub and spoke: internal identity providers/sources communicate with a central broker or repository that then serves as the identity provider for federation to cloud providers.

upvoted 1 times

**[dotcom21](https://www.examtopics.com/user/dotcom21/)**

3 weeks, 4 days ago

correct is : A

upvoted 1 times

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

3 weeks, 6 days ago

False: CCSK Study Security Guide, 12.1.2, pg 136: •• Free-form: internal identity providers/sources (often directory servers) connect directly to cloud providers. •• Hub and spoke: internal identity providers/sources communicate with a central broker or repository that then serves as the identity provider for federation to cloud providers.

upvoted 1 times

Question #214*Topic 1*

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

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

**Correct Answer:** *C*