



- Expert Verified, Online, **Free**.

All cloud services utilize virtualization technologies.

- A. False
- B. True

Correct Answer: B

Community vote distribution

B (100%)

🗨️ **BlackListRapa** 8 months, 2 weeks ago

Selected Answer: B

Cloud computing is fundamentally based on pooling resources and virtualization is the technology used to convert fixed infrastructure into these pooled resources. Virtualization provides the abstraction needed for resource pools, which are then managed using orchestration
upvoted 3 times

🗨️ **Brainiac** 10 months 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 3 times

🗨️ **JoAsiaGje** 11 months, 3 weeks ago

Selected Answer: B

agreed
upvoted 3 times

🗨️ **moota** 1 year 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 3 times

🗨️ **Phrank** 1 year, 4 months ago

No objection, all cloud systems are virtualized.
upvoted 2 times

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

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

Correct Answer: C

Community vote distribution

C (100%)

🗨️ **socian** 1 month ago

Selected Answer: C

Cloud providers typically offer some level of logging, but there may be gaps due to service limitations, lack of visibility into certain layers, or provider restrictions.

To address these gaps, organizations should enhance their logging capabilities by:

Deploying their own logging agents (e.g., AWS CloudTrail, Azure Monitor, Google Cloud Logging).

Using third-party SIEM solutions to aggregate and analyze logs.

Implementing custom monitoring tools at the application, network, or host level.

upvoted 1 times

🗨️ **Brainiac** 6 months 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 2 times

🗨️ **moota** 6 months ago

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.

upvoted 1 times

🗨️ **JoAsiaGje** 1 year, 11 months ago

Selected Answer: C

Security Guidance page 105

upvoted 3 times

🗨️ **GeoS28** 2 years, 3 months ago

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

upvoted 1 times

🗨️ **Lukasz2021** 2 years, 4 months ago

Selected Answer: C

Correct answer

upvoted 1 times

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

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

Correct Answer: C

Community vote distribution

C (100%)

JoAsiaGje **Highly Voted** 1 year, 5 months ago

Selected Answer: C

Correct, Control specification determines the risk.
upvoted 5 times

socian **Most Recent** 1 month ago

Selected Answer: C

In the Cloud Controls Matrix (CCM), a Control Specification is a measure that modifies risk. It includes processes, policies, devices, practices, or other actions that help mitigate or manage risks within a cloud environment.
upvoted 1 times

assfedassfinished 5 months, 2 weeks ago

Selected Answer: C

agreed, control specification determines the risk.
upvoted 1 times

yoyoman85 1 year, 6 months ago

Selected Answer: C

agreed, control specification determines the risk.
upvoted 3 times

moten 1 year, 6 months ago

agreed, control specification determines the risk.
upvoted 3 times

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

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

Correct Answer: E

Community vote distribution

E (100%)

anon_vzla007 4 months ago

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

upvoted 3 times

ZakySama 4 months, 1 week ago

Selected Answer: E

Cloud Provider

upvoted 2 times

moten 6 months, 3 weeks ago

agreed, cloud provider always responsible for physical security

upvoted 1 times

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

Correct Answer: A

Community vote distribution

A (100%)

 **cjkuga** Highly Voted 1 year, 11 months 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 12 times

 **beazzlebub** Highly Voted 1 year, 11 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 7 times

 **assfedassfinished** Most Recent 5 months, 2 weeks ago

Selected Answer: A

Ignore D, the answer is A. Physical location and Jurisdiction go hand in hand.

upvoted 1 times

 **KRee3** 9 months ago

The correct answer is A based on the CCSK Security Guidance

upvoted 1 times

 **TamingData** 10 months, 3 weeks ago

A is the straight up answer


upvoted 1 times

 **riee02** 1 year ago

Selected Answer: A

Based on page 64 of CCSK Security Guidance answer should be A

upvoted 2 times

 **moten** 1 year, 4 months ago

Ans should be A.

upvoted 1 times

 **jfuentesf** 1 year, 4 months ago

Selected Answer: A

the answer is A

upvoted 1 times

 **ZakySama** 1 year, 4 months ago

Selected Answer: A

A is the answer

upvoted 1 times

 **FATWENTYSIX** 1 year, 4 months 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 3 times

🗨️ **rycase** 1 year, 4 months ago

Page 37, CCSK Guide. A

upvoted 2 times

🗨️ **nitro1** 1 year, 5 months ago

answer should be A

upvoted 1 times

🗨️ **Selmed993** 1 year, 6 months ago

I think correct answer is A.

upvoted 1 times

🗨️ **vavofa5697** 1 year, 7 months 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

🗨️ **Brainiac** 1 year, 7 months ago

Correct answer should be A

upvoted 1 times

🗨️ **ngeorge** 1 year, 9 months ago

Selected Answer: A

Correct answer should be A

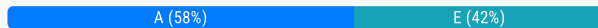
upvoted 2 times

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



FATWENTYSIX Highly Voted 1 year, 10 months 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 13 times

Jamala Most Recent 4 months, 2 weeks ago

Selected Answer: E

The cloud-based service model that enables companies to provide client-based access for partners to databases or applications is typically Software-as-a-Service (SaaS). SaaS is designed to deliver complete applications to the customer; these applications are managed by the cloud service provider and accessed by the client via the internet, often through a web browser or API

upvoted 1 times

sanju249 5 months, 1 week ago

Selected Answer: A

its access to database for clients as partners and not application users

upvoted 1 times

survivalkit 6 months 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

assfedassfinished 11 months, 2 weeks ago

Selected Answer: A

It's PaaS, we're talking about more than access to SW (SaaS), but not something barebones (IaaS). That's how I read it and would answer PaaS on the test.

upvoted 2 times

BigG83 1 year, 1 month ago

Selected Answer: A

of course the correct answer is PaaS. Despite some SaaS providers provides API interfaces to help the automation, but these don't mean direct access to the databases or to the backend application stack.

upvoted 1 times

JAMBER 1 year, 3 months ago

Selected Answer: A

pg 11: Platform as a Service (PaaS) abstracts and provides development or application platforms, such as databases, application platforms

upvoted 3 times

Alberto_M_M 1 year, 6 months ago

I was wrong. The right answer is the "A"

upvoted 1 times

🗨️ 👤 **Ungi** 1 year, 7 months ago

Selected Answer: E

Software as a Service (SaaS) is a full application that's managed and hosted by the provider. Consumers access it with a web browser, mobile app, or a lightweight client app

upvoted 2 times

🗨️ 👤 **Alcpt** 7 months, 1 week ago

Client can access data but never the actual database resource on SaaS. Not E.

upvoted 1 times

🗨️ 👤 **Alberto_M_M** 1 year, 10 months ago

Selected Answer: E

SaaS, They don't provide you any infra

upvoted 1 times

🗨️ 👤 **ZakySama** 1 year, 10 months ago

IT is A

upvoted 2 times

🗨️ 👤 **rycase** 1 year, 10 months 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 4 times

🗨️ 👤 **_AE_** 1 year, 11 months ago

It is SaaS

upvoted 1 times

🗨️ 👤 **tba** 1 year, 11 months ago

its SaaS

upvoted 1 times

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%)

 **JoAsiaGje** 5 months, 2 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 4 times

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

Community vote distribution

D (78%)

A (22%)

 **CloudSecurityMan** 6 months, 3 weeks ago

Selected Answer: D

Why correct answer is D?

VM(Virtual Machine) run on host machine hence, Virtual machine attacks have targets that are attacked as follows.

- VM snapshot and virtual image attack
- Virtualization administrator attack
- Virtual network attack
- Virtual security software issues.

upvoted 4 times


 **BlackListRapa** 8 months, 1 week ago

Selected Answer: D

D. All of the above

Virtualization technology introduces multiple attack surfaces that need to be considered for security.

upvoted 3 times

 **cyberkim** 9 months, 2 weeks ago

Selected Answer: A

Isn't the answer A - the hypervisor only? The other answers don't make sense to me in terms of the attack surface.

upvoted 2 times

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

A. False

B. True

Correct Answer: *B*

  **ElenaCyber** 4 months, 2 weeks 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.

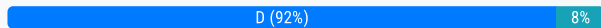
upvoted 4 times

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: D

Community vote distribution



vavofa5697 Highly Voted 2 years, 1 month 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 8 times

moota Most Recent 6 months 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

SHERLOCKAWS 1 year, 3 months ago

Selected Answer: B

Please be careful with this! > B would HAVE IMPACT on the incident response efforts while investigating logs on a VM with co-tenants. By experience cloud providers are not able to provide full logs as these include details of their other co-hosted clients.

upvoted 1 times

Brainiac 1 year, 10 months 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 2 times

Vinz_ 1 year, 10 months ago

Selected Answer: D

Answer D is the one with no impact.

upvoted 1 times

🗨️ 👤 **nitro1** 1 year, 12 months ago

answer is B just concentrate on the computing, that's the only answer that don't belong to it.
upvoted 1 times

🗨️ 👤 **Mobi333** 2 years ago

Right selection is B, just focus on characteristics of cloud as per definition.
upvoted 1 times

🗨️ 👤 **Selmed993** 2 years ago

This is confusing.
upvoted 2 times

🗨️ 👤 **felipe_g** 2 years ago

Selected Answer: D

Should rather be D, as it is not a security issue
upvoted 1 times

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

- A. False
- B. True

Correct Answer: B

Community vote distribution

B (100%)



 **Enitha** 4 months, 2 weeks ago

Selected Answer: B

Security Guidance --> page 147 --> 14.1.1 Big Data

Gartner defines it as such: "Big data is high volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization."

upvoted 3 times

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 as a result of their compliance with HIPAA/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 HIPAA/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: B

Community vote distribution

B (65%)

C (35%)

 **Petza** Highly Voted 2 years, 5 months 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 9 times

 **sanju249** Most Recent 5 months, 1 week ago

Selected Answer: B

One of the key strengths of the CCM is its alignment with leading standards, such as ISO/IEC 27001/27002, PCI Data Security Standard (DSS) (v3.2.1/v4.0), NIST, and so on. By harmonizing with these established frameworks, the CCM ensures that organizations can achieve compliance across multiple standards and regulations.

Pg. 22 in study guide of V5

upvoted 1 times

 **assfedassfinished** 11 months, 2 weeks ago

Selected Answer: B

My thought is B. While I considered C for a while, I get a warm and fuzzy with B in consideration of the inclusion of the word "overall" on the question, as it relates to the security posture.

upvoted 2 times

 **CbtL** 1 year ago

Selected Answer: C

People are really overthinking this one. In the CCM v4, on the Scope Applicability (Mappings) tab, there is no HIPAA or HIPAA/HITECH section. This tab is the mappings of the controls in the domains to various other standards. Going with C because it seems to be simple enough.

upvoted 3 times

 **sfsc91** 2 months ago

CCM maps to HIPAA/HITECH.

<https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-hipaa-us>

upvoted 1 times

 **BigG83** 1 year, 1 month ago

Selected Answer: B

There are Domain Controls in CCM and those are mapped to a lot of standards among others to HIPAA/HITECH (Omnibus rule)

upvoted 1 times

 **BiminiBoy_Cyber** 1 year, 6 months ago

As per the CSA Website:



Which Security "DOMAINS" are covered by the CCM?

Audit and Assurance, Application & Interface Security, Business Continuity...

HIPAA/HITECH is not listed among the 17 domains. <https://cloudsecurityalliance.org/research/cloud-controls-matrix/>

I hope this helps.

upvoted 1 times

  **iacini** 1 year, 8 months ago

Selected Answer: C

I would say C, because A is referring to CCM Columns and B to CCM Domain controls (there is no such thing) only C is referring to CCM Domains and I would go for that.

upvoted 1 times

  **Selmed993** 2 years 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

  **Michael_B_Morell_CISSP** 2 years, 3 months 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 3 times

  **Michael_B_Morell_CISSP** 2 years, 3 months 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

  **Michael_B_Morell_CISSP** 2 years, 3 months 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

  **Michael_B_Morell_CISSP** 2 years, 3 months 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

  **Michael_B_Morell_CISSP** 2 years, 3 months 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 2 times

  **BigG83** 1 year, 1 month ago

But the Answer C has a fully false statement: "The CCM domains are not mapped to HIPAA/HITECH Act." So this C cannot be the correct answer.

upvoted 1 times

  **A_Nevermind** 2 years, 5 months 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

  **JOKERO** 2 years, 4 months ago

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

upvoted 3 times

  **Michael_B_Morell_CISSP** 2 years, 3 months 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

  **beazzlebub** 2 years, 5 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

  **Michael_B_Morell_CISSP** 2 years, 3 months 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

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: A

Community vote distribution

A (100%)

 **ICEYNYSE** Highly Voted 1 year, 10 months ago

Selected Answer: A

It should be entitlement matrix. Validation process is not a terminology
upvoted 9 times


 **NSK_12** Highly Voted 1 year, 11 months 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

 **assfedassfinished** Most Recent 5 months, 2 weeks ago

Selected Answer: A

I haven't come across this info, but it is definitely A.
upvoted 1 times


 **BigG83** 7 months, 1 week ago

Selected Answer: A

Absolutely A, Synonym of Entitlement matrix is the Access control list.
upvoted 1 times


 **juanescast** 1 year ago

For me its A, entitlement matrix. but i'm confused for "5.1.2.2 Process. Perform a transaction on the data; update it; use it in a business processing transaction, etc." The questions says "entities in a transaction"
upvoted 1 times

 **Fripper** 1 year, 5 months ago

Selected Answer: A

Definitely A. Cannot possibly be D
upvoted 2 times

 **Mobi333** 1 year, 6 months ago

its E, focus on "entities in a transaction,"
upvoted 1 times

 **Selmed993** 1 year, 6 months ago

Is it not an entitlement matrix?
upvoted 1 times

 **Michael_B_Morell_CISSP** 1 year, 9 months ago

Selected Answer: A

Yeah, they messed up here. It is entitlement matrix.
upvoted 2 times

 **beazzlebug** 1 year, 11 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

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

- A. False
- B. True

Correct Answer: B

  **Necron** 4 months, 3 weeks 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 3 times

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

- A. False
- B. True

Correct Answer: A

  **Necron** 4 months, 3 weeks 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 3 times

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

Community vote distribution

A (67%)

E (33%)

 **NSK_12** Highly Voted 2 years, 5 months 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 12 times

 **Michael_B_Morell_CISSP** 2 years, 3 months 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 9 times

 **tralala2** Highly Voted 2 years, 4 months 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 11 times

 **ChewyBananas** Most Recent 9 months ago

E. The Metastructure has the ability to destroy your entire cloud deployment and its available on the web. The formal CSA training stressed this the most.

upvoted 1 times

 **JonHin** 10 months, 3 weeks ago

A is correct


upvoted 1 times

 **assfedassfinished** 11 months, 2 weeks ago

Selected Answer: A

Who is the audience of this question. Is it the cloud provider? Then Infrastructure definitely. If you are the cloud user, the infrastructure layer, while managed by the provider, is still critically important to secure cloud ops.


upvoted 2 times

 **BigG83** 1 year, 1 month ago

Selected Answer: E

The correct answer is the Metastructure (as others had said). Domain 6 of Security Guide is about the management plane and it is mentioned as the most important difference from Security perspective when we compare the Cloud based architectures with the Traditional ones.

upvoted 1 times

 **Sriramps** 1 year, 10 months 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

🗨️ 👤 **Mobi333** 2 years 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

🗨️ 👤 **Selmed993** 2 years 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

🗨️ 👤 **Mbnas** 2 years, 4 months ago

Its metastructure

upvoted 2 times

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: C

Community vote distribution

C (100%)

🗨️ 👤 **BigG83** 7 months, 1 week ago

Selected Answer: C

See page 78 of Security Guidance. The below mentioned clarifications are correct.

upvoted 1 times

🗨️ 👤 **BigG83** 7 months, 1 week ago

BTW the Answer D is also good if we see this text from chapter 7.2 of Security Guidance:

"If you are a cloud provider (including managing a private cloud), physical segregation of networks composing your cloud is important for both operational and security reasons. We most commonly see at least three different networks which are isolated onto dedicated hardware since there is no functional or traffic overlap:"

upvoted 1 times

🗨️ 👤 **BlackListRapa** 1 year, 2 months ago

Selected Answer: C

A service type of network, in the context of cloud computing, is typically isolated on different hardware because it serves distinct functions from other networks. In cloud environments, different types of networks are used to provide various services and functionalities.

upvoted 2 times

🗨️ 👤 **Brainiac** 1 year, 4 months 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 4 times

🗨️ 👤 **vavofa5697** 1 year, 7 months 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

🗨️ 👤 **durak** 1 year, 9 months ago

correct answer C

upvoted 2 times

🗨️ 👤 **JOKERO** 1 year, 11 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 3 times

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

Community vote distribution

C (100%)

🗨️ 👤 **Brainiac** 4 months 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 2 times

🗨️ 👤 **A_Nevermind** 11 months, 3 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 3 times

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

Community vote distribution

A (100%)

🗨️ 👤 **Ranjanarajshree** 6 months, 2 weeks ago

Selected Answer: A

Without permission we cannot perform vulnerability testing
upvoted 4 times

🗨️ 👤 **Brainiac** 7 months, 4 weeks 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 3 times

🗨️ 👤 **JOKERO** 11 months ago

Wrong. I would say C
upvoted 1 times

🗨️ 👤 **DrTee** 8 months 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

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

 **saptati** 3 months, 2 weeks ago

Answer is (E) On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider. (NIST Definition)
upvoted 2 times

 **Brainiac** 4 months 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 3 times

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

Community vote distribution

B (100%)

🗨️ 👤 **ElenaCyber** 4 months, 2 weeks ago

B: CCSK Security Guide pg 70; "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

🗨️ 👤 **moota** 6 months, 1 week 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 2 times

🗨️ 👤 **bhaipo** 8 months, 2 weeks ago

i want to see

upvoted 1 times

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

Community vote distribution

E (100%)


 **shiqna** 8 months, 3 weeks ago

Selected Answer: E

The answer is E as both B and C are correct.

Regarding B; we do not have to 'Respect' the interdependencies but can also evaluate to mitigate the risk as well. It is based on a risk assessment whether to 'respect' them which is equivalent to accepting them and do nothing or to identify mitigating controls and reduce the risk exposure. The resultant residual risk and health of mitigating controls can be reported to the management.

upvoted 2 times

 **Brainiac** 1 year, 4 months 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

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

Community vote distribution

A (86%)

14%

 **assfedassfinished** 5 months, 2 weeks ago

Selected Answer: A

This is the definition of discovery.

upvoted 1 times

 **_jpsrob_** 6 months ago

Selected Answer: A

While a subpoena is a tool used in the discovery process to compel someone to produce documents or testify, it is not the process itself. The term "discovery" refers to the entire legal process by which opposing parties exchange information and gather evidence from each other before a trial. This process can include depositions, interrogatories, and indeed, subpoenas for documents. So, in the context of the question, "discovery" is the most accurate answer.


upvoted 1 times

 **JohnnyBG** 9 months ago

Selected Answer: A

Discovery is the process, subpoena is a document.

upvoted 1 times

 **xg33k** 11 months, 1 week ago

Selected Answer: A

3.1.3 Electronic Discovery pg. 48 - The Security Guidance for Critical Areas of Focus in Cloud Computing v4.0

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 3 times

 **ciscolangirl** 11 months, 3 weeks ago

3.1.3 Electronic Discovery pg. 48 - The Security Guidance for Critical Areas of Focus in Cloud Computing v4.0

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 2 times


 **Crotofoto** 1 year ago

Selected Answer: C

Security Guide, page 49: 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 1 times

 **Bto881** 1 year, 3 months ago

Should a cloud service provider receive, from a third party, a request to provide information; this may be in the form of a subpoena, a warrant, or a court order in which access to the client data is demanded. Should be subpoena

upvoted 1 times

 **salimhajji** 1 year, 3 months ago

C- Why is not Subpoena ?

Un subpoena est l'injonction d'apparaître devant un tribunal pour produire un témoignage ou un document

upvoted 2 times

  **Jajalmao** 1 year, 4 months 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 2 times


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

Community vote distribution

E (100%)

 **cyberkim** 9 months, 2 weeks ago

Selected Answer: E

"Federation is the primary tool used to manage this problem, by building trust relationships between organizations and enforcing them through standards-based technologies."

upvoted 3 times

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

- A. False
- B. True

Correct Answer: B

Community vote distribution

B (57%)

A (43%)

🗨️ 👤 **Selmed993** Highly Voted 👍 1 year, 6 months 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 5 times

🗨️ 👤 **_jpsrob_** Most Recent 🕒 6 months ago

Selected Answer: B

Using elastic servers and moving workloads to new instances when possible is one of the benefits of cloud computing. It allows for scalability and flexibility in resource utilization, helping businesses adjust and manage their computational needs effectively.

upvoted 2 times

🗨️ 👤 **BigG83** 7 months, 1 week ago

Selected Answer: A

See 7.4.2 Immutable Workloads Enable Security in Security Guidance.

upvoted 1 times

🗨️ 👤 **SHERLOCKAWS** 8 months, 4 weeks ago

Selected Answer: B

the term 'elastic server' is problematic

upvoted 2 times

🗨️ 👤 **riee02** 1 year ago

Selected Answer: A

This is possible in immutable server so answer is A

upvoted 2 times

🗨️ 👤 **anon_vzla007** 1 year, 4 months ago

The answer is A:

upvoted 1 times


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

Community vote distribution

C (88%) 13%

 **ciscolangirl** Highly Voted 11 months, 3 weeks ago

Pg. 56 - The Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 - Cloud customers, particularly in public cloud, must rely more on third-party attestations of the provider to understand their compliance alignment and gaps.

upvoted 6 times

 **assfedassfinished** Most Recent 5 months, 2 weeks ago


Selected Answer: C

P 55 4.1.1.1 How Cloud Changes Compliance

As with security, compliance in the cloud is a shared responsibility model. Both the cloud provider and customer have responsibilities, but the customer is always ultimately responsible for their own compliance. These responsibilities are defined through contracts, audits/assessments, and specifics of the compliance requirements.

P 56 Cloud customers, particularly in public cloud, must rely more on third-party attestations of the provider to understand their compliance alignment and gaps.

upvoted 2 times

 **BigG83** 7 months, 1 week ago

Selected Answer: C

Beside C is correct, the Answer A is also correct. See page 58 of Security Guidance about Artifacts. Answer A is about the Provider provided documentation which is also needed to understand the gaps.

upvoted 1 times

 **Crotofoto** 1 year ago

Selected Answer: D


Security Guidance, page 55: As with security, compliance in the cloud is a shared responsibility model. Both the cloud provider and customer have responsibilities, but the customer is always ultimately responsible for their own compliance. These responsibilities are defined through contracts, audits/assessments, and specifics of the compliance requirements.

upvoted 1 times

 **juanescast** 1 year ago

4.1.1.1 find the answers

upvoted 1 times

 **moten** 1 year, 3 months ago

Selected Answer: C



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

upvoted 4 times

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*

  **LauriRo** 7 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 4 times

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

 **Brainiac**  4 months 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 7 times

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

  **ElenaCyber** Highly Voted 4 months, 2 weeks 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 7 times

  **haindvn** Most Recent 4 months, 2 weeks ago

why answer not B?

upvoted 1 times

  **sfsc91** 2 months ago

While this might sound like a good practice, it doesn't accurately describe how virtualized storage typically handles redundancy. Backup and archiving are different from the real-time redundancy that virtualized storage offers.

upvoted 1 times

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

Community vote distribution

C (100%)

🗉 **Brainiac** Highly Voted 10 months, 1 week 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 7 times

🗉 **c0d2291** Most Recent 3 months, 3 weeks ago

Selected Answer: C

DevSecOps is the next evolution of DevOps, and it addresses security throughout the SDLC.

upvoted 2 times

🗉 **Alberto_M_M** 6 months, 2 weeks ago

pag 109

upvoted 1 times

🗉 **cisasama** 10 months, 2 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 3 times

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

  **ElenaCyber**  4 months, 2 weeks 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 7 times



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

Community vote distribution

A (100%)

  **moota** Highly Voted 1 year 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 6 times

  **BlackListRapa** Most Recent 8 months, 1 week ago

Selected Answer: A

In a cloud environment, the customer often does not have the same level of access or control as they would in a traditional on-premises environment. This can make it more difficult to search or access all hosted data, especially if the data is distributed across multiple cloud services or regions.

upvoted 3 times

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

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

D is the Correct Answer. A common, practical example leveraging this capability is running most, if not all, applications on their own virtual network and only connecting those networks as needed. This dramatically reduces the blast radius if an attacker compromises an individual system. The attacker can no longer leverage this foothold to expand across the entire data center. Ref: Security-Guidance-v4.0, Pg82
upvoted 6 times

  **Brainiac** Highly Voted 10 months, 1 week 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 5 times

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

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

A is the correct. For example, if two virtual machines are located on the same physical machine there is no reason to route network traffic off the box and onto the network. Thus, they can communicate directly, and monitoring and filtering tools inline on the network (or attached to the routing/switching hardware) will never see the traffic. Ref: Security-Guidance-v4.0, Pg95.

upvoted 6 times

 **Brainiac** Most Recent 10 months, 1 week 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 2 times

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

Community vote distribution

D (100%)

🗨️ 👤 **Crotofroto** 6 months ago

Selected Answer: D

ENISA page 54: Another scenario is '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 4 times

🗨️ 👤 **negevon** 7 months, 3 weeks ago

The closest answer is B - looping within the same hypervisor/physical host. D is closest to the ENISA wording but it foundationally wrong as it claims "Using a compromised VM to exploit a hypervisor". VM hopping normally does not involve exploiting the hypervisor but using an existing vulnerability that allows traffic to go where it is not supposed to go. That passive use, rather than active exploit makes D foundationally wrong

upvoted 1 times

🗨️ 👤 **riee02** 6 months, 3 weeks ago

since que talks about Enisa D is correct answer

upvoted 2 times

🗨️ 👤 **Brainiac** 10 months, 1 week 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 2 times

🗨️ 👤 **JoAsiaGje** 11 months, 2 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 4 times

🗨️ 👤 **Azo_4952** 1 year, 4 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

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

Community vote distribution

D (100%)

 **JoAsiaGje** Highly Voted 5 months, 2 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 10 times

Which concept provides the abstraction needed for resource pools?

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

Correct Answer: A

Community vote distribution

A (100%)

🗨️ 👤 **Brainiac** 4 months 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 4 times

🗨️ 👤 **JoAsiaGje** 5 months, 2 weeks ago

Selected Answer: A

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

upvoted 2 times

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

- A. False
- B. True

Correct Answer: B

Community vote distribution

B (100%)

🗨️ 👤 **saptati** 8 months, 1 week ago

Answer is True. Ref: Security-Guidance-v4.0, Pg105. "One challenge in collecting information may be limited network visibility. Network logs from a cloud provider will tend to be flow records, but not full packet capture."

upvoted 4 times

🗨️ 👤 **JoAsiaGje** 11 months, 2 weeks ago

Selected Answer: B

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

upvoted 3 times

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*

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

D is the correct answer. Compliance validates awareness of and adherence to corporate obligations. Ref: Security-Guidance-v4.0, Pg55.
upvoted 6 times

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

Community vote distribution

B (100%)

🗨️ **assfedassfinished** 5 months, 1 week ago

Selected Answer: B

In order to counter the wrong answer C, the answer is B. the CCM v3.0.1 starting in cell A44, in the domain column, we find "Encryption & Key Management..." Separately, encryption and key management are something other than domains.

upvoted 1 times

🗨️ **CloudSecurityMan** 1 year ago

`Encryption and Key Management' defined Domain of CCM v4.0.7.

Correct answer is B.

upvoted 3 times

🗨️ **saptati** 1 year, 2 months ago

Selected Answer: B

In the CCM (Cloud Control Matrix) Excel Sheet, Encryption & Key Management Entitlement has been defined as Control Domain. Thus, B is the right answer.

upvoted 2 times

🗨️ **Brainiac** 1 year, 4 months 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 2 times

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

Community vote distribution

D (100%)

 **tralala2**  10 months, 3 weeks 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 or 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 7 times

 **moota**  6 months, 1 week 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 3 times

 **SQCISSP** 10 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** 5 months, 3 weeks ago

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

upvoted 1 times

 **Azo_4952** 10 months, 4 weeks 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** 5 months, 3 weeks ago

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

upvoted 1 times

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

  **cyberkim** Highly Voted 9 months, 2 weeks ago

On page 90 of the guidance, it says "Implement default deny with cloud firewalls". But it also says "Always restrict traffic between workloads in the same virtual subnet using a cloud firewall (security group) policy whenever possible."

So doesn't this mean that "D" would be the better answer, oh wait, D says default "allow" not deny. Almost got trapped. The answer is E.
upvoted 6 times

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: D

Community vote distribution

D (63%)

E (38%)

🗨️ **Alcpt** 7 months, 2 weeks ago

Selected Answer: D

I have to be careful here but if I put on my Shared Responsibility Model hat here, E feels more like the CSP responsibility, while the question talks about CSC business continuity management which kinda leans more to D.

So im thinking D.

upvoted 1 times

🗨️ **_jpsrob_** 1 year ago

Selected Answer: D

D. Clients need to do business continuity planning due diligence in case they suddenly need to switch providers.

Cloud computing has indeed shifted the focus of business continuity management to vendor management, and clients need to carefully plan and consider their contracts and agreements with their cloud vendors to ensure continuity of business operations. This includes planning for potential outages, vendor discontinuance, or scenarios where they may have to switch providers. It's not just about technicalities - legal, contractual, and business aspects also play a significant role in cloud continuity management.

upvoted 1 times

🗨️ **BigG83** 1 year, 1 month ago

Selected Answer: D

beside the below mentioned references, you should consider that despite there can more AZ in a region, it doesn't mean your application is disaster resistant if you don't implement it in that way to work on Multi AZ. So finally it is up the consumer's due diligence to care with Business Continuity.

upvoted 1 times

🗨️ **JAMBER** 1 year, 3 months ago

Selected Answer: D

pg 68: 6.0.1 Business Continuity and Disaster Recovery in the Cloud. Refer to this section. Last bullet point: Considering options for portability, in case you need to migrate providers or platforms. This could be due to anything from desiring a different feature set to the complete loss of the provider if, for example, they go out of business or you have a legal dispute.

upvoted 2 times

🗨️ **BFCrypto** 1 year, 5 months ago

I think D is the answer. Not all cloud providers provide the Geographical Redundancy mentioned (or it could be an extra charge). While the provider Geographic redundancy will help in case of a datacentre DR event, what if a critical system (e.g. IaaS) fails in the cloud -> Geographical Redundancy I dont think will help you, so for that you need to do your own BCP Planning. I would go with D but it is a badly worded question, me thinks :-).

upvoted 1 times

🗨️ **byfener** 1 year, 7 months ago

Selected Answer: E

In option D, the customer's responsibility is expressed, and in option E, the provider's statement "Geographic redundancy ensures that Cloud Providers provide highly available services." has a significant impact on ensuring business continuity. As if option E was a more correct answer I

think. The question asked about the impact of the provider side.

upvoted 3 times

🗨️ 👤 **saptati** 1 year, 8 months ago

Although the question is a little vague, here is my opinion: E is not the right response because it cannot be categorized as impact.

As stated on page 73 of Security-Guidance-v4.0, "For example, the odds of a major IaaS provider going out of business or changing their entire business model are low, but this isn't all that uncommon for a smaller venture-backed SaaS provider". Thus, the following statement sounds like an impact to me: "Clients need to do business continuity planning due diligence in case they suddenly need to switch providers.". Thus, I will go with option D.

upvoted 2 times

🗨️ 👤 **anon_vzla007** 1 year, 10 months ago

Where did you obtain the description provided in the comments?

upvoted 1 times

🗨️ 👤 **Brainiac** 1 year, 10 months 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

🗨️ 👤 **SSG786** 1 year, 8 months ago

I don't think so D is correct because you need to understand to switch the provider is not easy, how we can move on-going operations, business applications when services are down, Hence I still say E is the correct answer.

upvoted 1 times

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** 4 months 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 4 times

🗨️ 👤 **SQCISSP** 10 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 4 times

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

Community vote distribution

D (100%)



 **JoAsiaGje** Highly Voted 5 months, 2 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 6 times


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

Community vote distribution

C (100%)

 **saptati** 8 months, 1 week ago

Selected Answer: C

According to , "Before getting into legal details it is worth noting that the customers of cloud providers may vary in type (from private to public entities) and size (from SMEs to large companies) and, thus, in the extent to which they are in a position to negotiate. This is very relevant from the legal point of view, because the relationship between the cloud providers and their customers will be mostly regulated by means of contracts", (Ref: ENISA, Page 97).

Therefore, companies considering a cloud computing business relationship should pay close attention to the contracts and agreements they enter into with cloud providers, as these will determine the rights and responsibilities of both parties. The text does not support options A, B, D, or E. Option C is partially true, as the companies using cloud providers are responsible for ensuring the security of the data entrusted to them, but they may also have legal protections and obligations related to data protection. Thus, I will go with answer C.

upvoted 3 times

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

- A. False
- B. True

Correct Answer: B

Community vote distribution

B (100%)

 **Brainiac** 4 months 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 3 times

 **JoAsiaGje** 5 months, 2 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 3 times

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

Community vote distribution

A (100%)



🗨️ 👤 **saptati** 8 months, 1 week ago

Selected Answer: A

Will go with option A. Other options like B, C, D, and E are important considerations as well, but they are not typically included in the SLA.
upvoted 2 times

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

Community vote distribution

A (100%)



 **JoAsiaGje** Highly Voted 5 months, 2 weeks ago

Selected Answer: A

(Security Guidance page 120) Volume storage: This is essentially a virtual hard drive for instances/virtual machines.
upvoted 5 times

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


Community vote distribution

C (100%)

 **moota** Highly Voted 6 months, 1 week ago

Selected Answer: C

Provisioning is not in 13.1.2 Major Categories of Security as a Service Offerings
upvoted 5 times

 **vavofa5697** Most Recent 7 months, 1 week ago

hmm all actually example of SecaaS
upvoted 1 times

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

Community vote distribution

B (50%) C (25%) D (25%)

🗨️ **ChewyBananas** 9 months ago

Selected Answer: B

How is it managed vs. how should it be managed. Should have one key per owner at least but could have multiple keys or a single key for everyone.

upvoted 2 times

🗨️ **_jpsrob_** 1 year ago

Selected Answer: D

This is a poorly formulated question but i believe the answer could still be D

In an ideal scenario, "One key per data owner" would be a recommended practice for maintaining the highest level of security in a multi-tenant environment. However, the original question was about how encryption is managed on multi-tenant storage, without specifying it to the best or recommended practice. That's why the answer can still be "The answer could be A, B, or C depending on the provider," because in reality, encryption management can vary widely across different providers. It's always important for customers to inquire about a provider's security practices to ensure they are suitable for their specific needs, and to ideally look for a provider that uses the most secure practices, such as one key per data owner.

upvoted 3 times

🗨️ **MrN0body** 1 year, 6 months ago

This is another poorly written question. If the authors of the CCSK exam want the question to be aligned with security, it should read: How should encryption be managed on multi-tenant storage? To @Brainiac's point, I've seen CSP that either facilitate 1 key per customer or do not support unique keys at all. The Security Guidance even states it is recommended to use per-customer keys when possible...when possible being the key phrase here.

upvoted 3 times

🗨️ **byfener** 1 year, 7 months ago

Selected Answer: B

According Security-Guidance-v4.0, Pg 125 : "It is recommended to use percustomer keys when possible, in order to better enforce multitenancy isolation." Answer must be B

upvoted 4 times

🗨️ **negevon** 1 year, 7 months ago

No answer here is correct - The right answer should be "B or C" but without the relations to regulations. A is not meeting cloud security basics and cannot be part of an answer

upvoted 1 times

🗨️ **saptati** 1 year, 8 months ago

B is the correct answer. For multi-tenant storage, it is recommended to use per-customer keys when possible, in order to better enforce multitenancy isolation. Ref: Security-Guidance-v4.0, Pg 125.

upvoted 3 times

🗨️ **Brainiac** 1 year, 10 months 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 2 times

🗨️ 👤 **moten** 1 year, 9 months ago

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

upvoted 2 times

🗨️ 👤 **FATWENTYSIX** 1 year, 11 months ago

multiple keys per data owner

upvoted 3 times

🗨️ 👤 **moota** 2 years 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 3 times

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

🗨️ 👤 **saptati** 8 months, 1 week ago

D is the correct answer. Data today is accessed using a variety of different devices. These devices have different security characteristics and may use different applications or clients. Ref: Security-Guidance-v4.0, Pg 65.

upvoted 1 times

🗨️ 👤 **Brainiac** 10 months, 1 week 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 3 times

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 (cloud) data centers near multiple sources of energy, such as hydroelectric dams.
- E. None of the above.

Correct Answer: A

 **Brainiac** 4 months 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 4 times

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

- A. False
- B. True

Correct Answer: A

Community vote distribution

A (75%)

B (25%)

🗳️ 👤 **Kneebee** 8 months ago

False (Option A): SLAs typically provide a specified level of service. Even with a high SLA, it doesn't guarantee absolute continuity because there may still be instances of downtime that could affect service availability.

upvoted 3 times

🗳️ 👤 **JAMBER** 8 months, 4 weeks ago

Selected Answer: A

False. A written agreement can't/won't ensure anything but the CP intent. If the security mechanisms (hardware/software) are breached then the SLA is violated.

upvoted 2 times

🗳️ 👤 **JohnnyBG** 9 months ago

Selected Answer: A

False, even if you have an SLA of 99.999% nothing guarantee you they will make it. You will get money back if they don't, that's it.

upvoted 1 times

🗳️ 👤 **BFCrypto** 10 months, 4 weeks ago

The SLA may state an availability figure - e.g. 99.99% for each service. It does not "ensure" continuity for all services - in fact it may indicate when the service may not be available - another poorly written question.

upvoted 2 times

🗳️ 👤 **Brainiac** 1 year, 4 months 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** 1 year, 5 months ago

Selected Answer: B

SLAs 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


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

Community vote distribution

A (100%)

  **_jpsrob_** 6 months ago



Selected Answer: A

A. Intrusion Prevention System

Intrusion Prevention Systems (IPS) are primarily used for identifying and preventing malicious activities and attacks on a network or system, not specifically toward detecting and preventing data migration into the cloud. Methods like URL filters, Data Loss Prevention (DLP), Cloud Access Security Brokers (CASB), and Database Activity Monitoring are more aligned with controlling and monitoring data migration into the cloud, as they focus on data protection, detect data breaches, control access to cloud services, and monitor database activities.



reference page 121 for more information

upvoted 1 times

  **moten** 1 year, 3 months ago

URL filters are typically used for web content filtering and blocking access to specific websites or web resources based on URL criteria. While URL filters can help enforce browsing policies and restrict access to certain websites, they are not primarily designed for detecting and preventing data migration into the cloud.

upvoted 4 times

  **Brainiac** 1 year, 4 months 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 3 times

  **a2m2** 11 months, 2 weeks ago

Hola. De cierto modo si ya que mediante un filtrado de URL puede detectar la ruta, servicio en nube que esta usando para hacer la transferencia de datos y de cierto modo llegar a bloquear o permitirlo según sean las políticas de la empresa.



upvoted 1 times

  **moota** 1 year, 6 months ago

Selected Answer: A

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

upvoted 3 times

  **saptati** 1 year, 2 months ago

I agree, A is the correct answer. Ref: Security-Guidance-v4.0, Pg121.

upvoted 1 times

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

🗨️ 👤 **saptati** 8 months, 1 week ago

C is correct. Customers should understand that providers can (and often should) consider on-premises audits a security risk when providing multitenant services. Multiple on-premises audits from large numbers of customers present clear logistical and security challenges, especially when the provider relies on shared assets to create the resource pools. Ref: Security-Guidance-v4.0, Pg 57-58.

upvoted 2 times

🗨️ 👤 **Brainiac** 10 months, 1 week 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 2 times

🗨️ 👤 **odisor** 10 months, 3 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 2 times

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

Community vote distribution

A (100%)

🗨️ **Brainiac** 4 months 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 2 times

🗨️ **FATWENTYSIX** 4 months, 3 weeks 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** 5 months, 2 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 3 times

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

Community vote distribution

E (67%)

B (33%)

BigG83 7 months, 1 week ago

Selected Answer: B

I forgot to vote in my previous comment. B as D doesn't allow customer to directly delete data.

upvoted 1 times

BigG83 7 months, 1 week ago

I would agree with E, but that point in answer D is problematic: storing the keys on customer side doesn't mean the customer has all permissions to delete all data from the Cloud. Of course the access of data can be prevented by the own-hosted keys, but it is not equal with the data deletion.

upvoted 1 times

BFCrypto 10 months, 4 weeks ago

Selected Answer: E

Both B and D are ways to ensure the data is deleted.

upvoted 2 times

moten 1 year, 3 months ago

The best way to ensure that all data has been removed from a public cloud environment, including all media such as backup tapes, is by selecting option E: Both B and D.

Option B, maintaining customer-managed key management and revoking or deleting keys from the key management system, ensures that the data cannot be accessed again by revoking the encryption keys. This prevents unauthorized access to the data even if the cloud provider still possesses the encrypted data.

Option D, keeping the keys stored on the client side, provides an additional layer of security. By securely storing the encryption keys on the client side, the users have the ability to delete their own data when necessary. This gives the users more control over their data and ensures that it is properly removed from the cloud environment.

upvoted 1 times

Brainiac 1 year, 4 months 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 3 times

  **odisor** 1 year, 4 months 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

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

Community vote distribution

E (83%)

A (17%)

🗨️ 👤 **c0d2291** 3 months, 3 weeks ago

Selected Answer: A

I see A as a much bigger risk than E.

Does anyone have a link to the ENISA documentation? There are so many docs on their website.

upvoted 1 times

🗨️ 👤 **Crotofroto** 6 months ago

Selected Answer: E

ENISA page 32: Acquisition of the cloud provider could increase the likelihood of a strategic shift and may put non-binding agreements at risk.

upvoted 1 times

🗨️ 👤 **Brainiac** 10 months, 1 week 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 2 times

🗨️ 👤 **JoAsiaGje** 11 months, 2 weeks ago

Selected Answer: E

enisa page 26

upvoted 1 times

🗨️ 👤 **moota** 1 year 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 3 times

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

  **saptati** 8 months, 1 week ago

E is correct answer. "APIs are typically the underlying communications method for components within a cloud, some of which (or an entirely different set) are exposed to the cloud user to manage their resources and configurations." Ref: Security-Guidance-v4.0, Pg 14.

upvoted 1 times

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: D

Community vote distribution

D (100%)

 **Petza** Highly Voted 1 year, 6 months 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 10 times

 **SSG786** Most Recent 8 months, 1 week ago

D: Security Guidance clearly talk on this page # 11 "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"

upvoted 4 times

 **moten** 9 months, 3 weeks ago

Correct Ans D:

A cloud deployment of two or more unique clouds is known as a Hybrid Cloud. In a hybrid cloud, organizations utilize a combination of public and private cloud infrastructure to meet their specific needs. This allows for greater flexibility, scalability, and the ability to leverage the benefits of both public and private cloud environments. By integrating multiple clouds, organizations can optimize their workload placement, resource allocation, and data management strategies.

A community cloud is a cloud deployment model where infrastructure and resources are shared by a specific community or group of organizations with common interests or requirements. It is designed to meet the specific needs of a particular community and can be managed by the organizations themselves or a third-party provider. This type of cloud deployment allows for collaboration, data sharing, and resource pooling within the community while maintaining a certain level of control and security.

upvoted 2 times

 **Brainiac** 10 months, 1 week 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** 10 months, 4 weeks ago

CSA Security Guidance v4 pg 11

upvoted 3 times

  **ZakySama** 10 months, 1 week ago



Thank you

upvoted 1 times

  **Brainiac** 1 year, 1 month ago

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

upvoted 1 times

  **DrTee** 1 year, 2 months ago

Selected Answer: D

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

upvoted 1 times

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

Community vote distribution

C (100%)

🗨️ **Crotofroto** 6 months ago

Selected Answer: C

ENISA page 97:

Five key legal issues have been identified which are common across all the scenarios:

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 2 times

🗨️ **moten** 9 months, 3 weeks ago

Globalization is not one of the five key legal issues common across all scenarios identified by ENISA. The four key legal issues common across all scenarios are data protection, professional negligence, intellectual property, and outsourcing services and changes in control. These legal issues are relevant in various contexts and industries and are important considerations in managing and securing information and technology assets.

upvoted 1 times

🗨️ **JoAsiaGje** 11 months, 2 weeks ago

Selected Answer: C

agreed with mooto (enisa page 97)

upvoted 2 times

🗨️ **mooto** 1 year 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 4 times

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

Community vote distribution

D (100%)

🗨️ **moten** 3 months, 3 weeks ago

Auditors are an example of a high-risk role for malicious insiders within a cloud provider. Auditors have access to sensitive information and systems during the auditing process. If a malicious insider in an auditing role intentionally manipulates or alters data, it can lead to significant security breaches or financial fraud. It is crucial for cloud providers to have strict controls and monitoring mechanisms in place to detect and prevent such malicious activities by insiders in auditing positions.

upvoted 1 times

🗨️ **JoAsiaGje** 5 months, 2 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 3 times

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: A

Community vote distribution

A (100%)

JoAsiaGje Highly Voted 1 year, 5 months 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 7 times

jpsrob Most Recent 6 months ago

Selected Answer: A

A. The cloud provider is primarily responsible for building a secure network infrastructure and configuring it properly

p96

upvoted 1 times

moten 1 year, 3 months ago

The primary security responsibilities of the cloud provider in the management infrastructure include:

A. Building and properly configuring a secure network infrastructure: The cloud provider is responsible for establishing and maintaining a secure network infrastructure that protects the underlying infrastructure and prevents unauthorized access.

upvoted 2 times

Brainiac 1 year, 4 months 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 4 times

Selmed993 1 year, 6 months ago

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

upvoted 2 times

gingyk 1 year, 7 months ago

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

upvoted 1 times

🗨️ 👤 **byfener** 1 year, 7 months 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** 1 year, 9 months ago

Selected Answer: A

Yes vote also for A

upvoted 2 times

🗨️ 👤 **A_Nevermind** 1 year, 11 months ago

Selected Answer: A

Answer is A!

upvoted 3 times

🗨️ 👤 **beazzlebug** 1 year, 11 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

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

Community vote distribution

A (100%)

 **JoAsiaGje** Highly Voted 11 months, 2 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 8 times

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

Its correct check the guide p84

upvoted 5 times

 **Brainiac** Most Recent 10 months, 1 week 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 2 times

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

Community vote distribution

A (100%)

 **Crotofroto** 6 months 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 3 times

 **Brainiac** 10 months, 1 week 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 2 times

 **JoAsiaGje** 11 months, 2 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 3 times

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

Community vote distribution

A (100%)

 **Crotofroto** Highly Voted 6 months ago

Selected Answer: A

Security Guidance 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 5 times

 **moten** Most Recent 9 months, 3 weeks ago

The SDP architecture involves the use of a client software or agent on the user's device, a controller that manages the access policies and authentication, and a gateway that provides secure connectivity to the protected resources. These components work together to establish a secure and controlled network environment for users accessing applications and services.

upvoted 1 times

 **JoAsiaGje** 11 months, 2 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 3 times

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

Community vote distribution

D (100%)

🗨️ 👤 **Brainiac** 4 months 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 3 times

🗨️ 👤 **JoAsiaGje** 5 months, 2 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 4 times


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: C

Community vote distribution

C (100%)

 **beazzlebug** Highly Voted 1 year, 5 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 12 times

 **drhtater** 4 months, 4 weeks ago

Security Guidance pg 131

upvoted 2 times

 **JCoutant** 1 year, 3 months 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

 **moten** Most Recent 9 months, 3 weeks ago

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.

In this context, identities refer to distinct and unique objects within a specific namespace, such as users, entities, or objects. Attributes, on the other hand, are properties or characteristics that are associated with an identity. Each identity can have multiple attributes that help define its properties, attributes, or qualities. The relationship is such that attributes belong to identities and help describe or define them.

upvoted 1 times

 **Brainiac** 10 months 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** 11 months, 2 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** 1 year, 1 month ago

Selected Answer: C

must be

upvoted 1 times


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

Community vote distribution

A (100%)

 **saptati** 8 months, 1 week ago

Selected Answer: A

According to Security-Guidance-v4.0, Pg 141, 13.1.1.2, Potential Concerns --> 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. The SecaaS provider may not reveal details of how it implements its own security and manages its own environment.. Therefore, the answer is A.

upvoted 3 times

 **moten** 9 months, 3 weeks ago

A. Lack of visibility.

When organizations rely on a third-party service provider for security services, they may have limited visibility into the inner workings of the security infrastructure and operations. This lack of visibility can make it challenging to assess the effectiveness of the security measures, monitor for potential vulnerabilities or threats, and ensure compliance with regulatory requirements. Organizations may have to rely on the service provider's reporting and assurance mechanisms to gain insights into the security posture of their systems and data.

upvoted 4 times

 **Brainiac** 10 months, 1 week 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

 **Yahealborini** 8 months, 3 weeks ago

no not correct check the guide page 140

upvoted 2 times

 **JoAsiaGje** 11 months, 2 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 3 times

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: B

Community vote distribution

B (84%)

A (16%)

🗨️ **A_Nevermind** Highly Voted 1 year, 4 months 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 9 times

🗨️ **MrN0body** Most Recent 6 months, 1 week ago

Selected Answer: B

CSA CCSK Security Guidance pg. 112

Design: During the application design process, especially when PaaS is involved, the focus for security in cloud is on architecture, the cloud provider's baseline capabilities, cloud provider features, and automating and managing security for deployment and operations. We find that

there are often significant security benefits to integrating security into the application architecture since there are opportunities to leverage the provider's own security capabilities. For example, inserting a serverless load balancer or message queue could completely block certain network attack paths. This is also where you perform threat modeling, which must also be cloud and provider/platform specific.

If threat modeling must be cloud and provider/platform specific, it stands to reason that the threat and trust models must be modified in the event you switch CSPs or move from one platform to another.

upvoted 3 times

🗨️ **negevon** 7 months, 3 weeks ago

I don't see how using cloud infra makes any difference for the importance of use of IDEs

upvoted 1 times

🗨️ **Brainiac** 10 months, 1 week 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

🗨️ 👤 **Petza** 1 year, 4 months ago

Selected Answer: A

The given answer is correct.

upvoted 3 times

🗨️ 👤 **beazzlebug** 1 year, 5 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

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

Community vote distribution

C (100%)

🗨️ **Brainiac** 4 months 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** 5 months, 2 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 2 times

🗨️ **Petza** 10 months, 2 weeks ago

Selected Answer: C

The given answer is correct.

upvoted 1 times

🗨️ **JOKERO** 11 months ago

governance domain, not operational domain (D)

upvoted 1 times

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: D

Community vote distribution

D (73%)

A (27%)

🗳️ 👤 **romaso82** 7 months, 1 week ago

B. Default deny: This is a security principle where access is denied by default, and only explicitly permitted actions are allowed. This approach minimizes the attack surface by ensuring that unauthorized access is not allowed, which helps reduce common application security issues like unauthorized access and privilege escalation.

upvoted 3 times

🗳️ 👤 **romaso82** 7 months, 2 weeks ago

The answer is B: Default Deny

upvoted 1 times

🗳️ 👤 **BFCrypto** 1 year, 4 months ago

Selected Answer: A

I think both A and D are correct, however the answer sought is 'A', as it is specifically worded as, Which "opportunity" helps ? If you refer to "opportunities" in Domain 10 "Elasticity" is listed as an Opportunity Heading, including the justification.

upvoted 1 times

🗳️ 👤 **negevon** 1 year, 7 months ago

Selected Answer: D

Definitely D, even some choices seems to be selected from the text some quoted below (reversing, for example, the "Increased use of Micro services" to confuse)

upvoted 1 times

🗳️ 👤 **moten** 1 year, 9 months ago

Segregation by default can indeed help reduce common application security issues. By implementing segregation by default, applications and systems are designed to separate different components, resources, or user access by default. This approach helps prevent unauthorized access, limit the impact of security breaches, and reduce the attack surface.

upvoted 1 times

🗳️ 👤 **Brainiac** 1 year, 10 months 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** 1 year, 10 months ago

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

upvoted 1 times

🗳️ 👤 **moota** 2 years 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 4 times

🗨️ 👤 **jre62294** 2 years, 2 months ago

Selected Answer: D

Security Guidance 10.1.5: Segregation by default, immutable infra, increased use of micro-services, paas and serverless arch.

upvoted 3 times

🗨️ 👤 **vavofa5697** 2 years, 1 month ago

thanks!

upvoted 1 times

🗨️ 👤 **A_Nevermind** 2 years, 4 months ago

Selected Answer: A

From the 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** 2 years, 4 months 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** 2 years, 4 months ago

Elastic infrastructure is Immutable infrastructure.

upvoted 2 times

🗨️ 👤 **cjkuga** 2 years, 5 months 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

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

Community vote distribution

A (100%)

🗨️ 👤 **SSG786** 8 months, 1 week ago

Correct A: Security-Guidance Page# 67 "The management plane is the single most significant security difference between traditional infrastructure and cloud computing."

upvoted 1 times

🗨️ 👤 **Brainiac** 10 months 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** 1 year 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 3 times

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

Community vote distribution

A (90%)

10%

 **moota** Highly Voted 1 year 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 9 times

 **byfener** 7 months, 3 weeks ago

I agree with moota after check 7.3.4 Additional Considerations for Cloud Providers or Private Clouds topics. A is correct answer

upvoted 2 times

 **Anantwgupta** Most Recent 3 months ago

Selected Answer: B

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

upvoted 1 times

 **Brainiac** 10 months 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 2 times

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** Highly Voted 4 months 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 6 times

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: A

Community vote distribution

A (100%)

 **cjkuga** Highly Voted 2 years, 5 months 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 11 times

 **SQCISSP** Highly Voted 2 years, 4 months 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 6 times

 **ChewyBananas** Most Recent 9 months ago

Selected Answer: A

Page 52 - 3.1.3.11 Response to a Subpoena or Search Warrant Should a cloud service provider receive, from a third party, a request to provide information; this may be in the form of a subpoena, a warrant, or a court order in which access to the client data is Security Guidance v4.0 © Copyright 2021, Cloud Security Alliance. All rights reserved 53 demanded. The client may want to have the ability to fight the request for access in order to protect the confidentiality of their data. To this end, the cloud service agreement should require the cloud service provider to notify the customer that a subpoena was received and give the company time to fight the request for access.

upvoted 1 times

 **Brainiac** 1 year, 10 months 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 2 times

 **Fripper** 1 year, 11 months 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

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

- A. False
- B. True

Correct Answer: B

Community vote distribution

B (100%)

 **Brainiac** 4 months 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 3 times

 **JoAsiaGje** 5 months, 2 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 3 times

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

Community vote distribution

A (100%)

 **Brainiac** 4 months 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 2 times

 **JoAsiaGje** 5 months, 2 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 2 times

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

Community vote distribution

B (100%)

 **Brainiac** 4 months 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 3 times

 **JoAsiaGje** 5 months, 2 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 4 times

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

Community vote distribution

B (100%)

🗨️ 👤 **Brainiac** 4 months 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 2 times

🗨️ 👤 **JoAsiaGje** 5 months, 2 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 3 times

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

Community vote distribution

E (100%)

 **overarch384** 5 months, 2 weeks ago

Selected Answer: E

Answer found in 11.1.7.2

upvoted 2 times


 **Brainiac** 1 year, 4 months 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** 1 year, 4 months 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 3 times


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: B

Community vote distribution

B (100%)

 **beazzlebug** Highly Voted 1 year, 11 months ago

Selected Answer: B

From CCM:
Architectural Relevance
Phys Network Compute Storage App Data
upvoted 11 times

 **Gulagulagu** Highly Voted 2 years ago

Selected Answer: B

B. Physical, Network, Compute, Storage, Application or Data
These are the columns of the CCM document
upvoted 7 times

 **ahijada** Most Recent 3 months, 3 weeks ago

Selected Answer: B

on CCM: Column D3:I3: Phys, Network, Compute, Storage, App, Data
upvoted 1 times

 **Ungi** 1 year ago

Selected Answer: B

Architectural Relevance - Cloud Stack Components
Phys Network Compute Storage App Data
From CCM table
upvoted 3 times

 **Brainiac** 1 year, 4 months 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 2 times

 **DrTee** 1 year, 8 months ago

Selected Answer: B

Checking the CCM, Clearly it is Phys Net Comp Stor App Data
upvoted 3 times

 **A_Nevermind** 1 year, 10 months ago

Selected Answer: B

From ccm file



upvoted 4 times

  **SQCISSP** 1 year, 10 months ago

Answer B

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

upvoted 4 times

  **cjkuga** 1 year, 11 months ago

Selected Answer: B

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

upvoted 4 times


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: A

Community vote distribution

A (100%)

 **beazzlebub** Highly Voted 1 year, 5 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 17 times

 **negevon** Most Recent 7 months, 3 weeks ago

Selected Answer: A

its clearly A

upvoted 2 times

 **Brainiac** 10 months 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** 1 year, 1 month ago

Agree with beazzlebub too


upvoted 1 times

 **A_Nevermind** 1 year, 4 months ago

Selected Answer: A

It is A

upvoted 2 times

 **cjkuga** 1 year, 5 months ago

Selected Answer: A

Agree with beazzlebub's answer

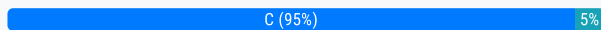
upvoted 4 times

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: C

Community vote distribution



CloudSecurityMan Highly Voted 6 months, 3 weeks ago

Selected Answer: C

In CSA's Cloud Security Guidance v4.0, find to page 65, Section 5.1.2.2. Table 1 Data process relate to Create and Use.

upvoted 6 times

byfener Most Recent 7 months, 3 weeks ago

Selected Answer: C

it is absolutely C From Security Guidance v4. Section 5.1.2.2, Table 1

upvoted 3 times

moten 9 months, 3 weeks ago

Selected Answer: D

When mapping functions to lifecycle phases, the functions of creating, storing, and using data are all required to successfully process data.

The "create" function involves generating or capturing data.

The "store" function involves securely storing the data for future use.

The "use" function involves accessing and processing the stored data for various purposes.

The answer option D includes all three essential functions for data processing.

upvoted 1 times

Brainiac 10 months 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 2 times

mattch 11 months, 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 4 times

🗨️ 👤 **edwoos** 1 year ago

It is C

upvoted 2 times

🗨️ 👤 **A_Nevermind** 1 year, 4 months ago

Selected Answer: C

From the table in the guidance. The answer is C

upvoted 3 times

🗨️ 👤 **SQCISSP** 1 year, 4 months 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** 1 year, 4 months ago

Selected Answer: C

Answer C!

upvoted 4 times

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

- A. False
- B. True

Correct Answer: B

Community vote distribution

B (100%)

 **Crotofoto** 6 months ago

Selected Answer: B

Security Guidance 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 3 times

 **Brainiac** 10 months 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 3 times

 **match** 11 months, 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 2 times

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

Community vote distribution

C (100%)

🗨️ 👤 **Brainiac** 4 months 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 3 times

🗨️ 👤 **JoAsiaGje** 5 months, 2 weeks ago

Selected Answer: C

Security Guidance page 10 table

upvoted 2 times

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**  4 months 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 7 times



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

- A. False
- B. True

Correct Answer: A

Community vote distribution



A (100%)

  **overarch384** 5 months, 2 weeks ago

Selected Answer: A

Found in 10.1.3.1

upvoted 1 times

  **saptati** 1 year, 2 months ago

According to Security-Guidance-v4.0, Pg 114: "Vulnerability assessment can be integrated into CI/CD pipelines and implemented in cloud fairly easily, but it nearly always requires compliance with the provider's terms of service."

upvoted 2 times

  **Brainiac** 1 year, 4 months 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


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

Community vote distribution


C (100%)

 **overarch384** 5 months, 2 weeks ago

Selected Answer: C

Found in 11.1.4.3

upvoted 1 times

 **saptati** 1 year, 2 months ago

The right answer is C., Segregate keys from the provider hosting data, can be leveraged to prevent cloud providers from inappropriately accessing customer data. According to Security-Guidance-v4.0, Pg126, "You may be able to store the keys externally from the provider and only pass them over on a per-request basis."

upvoted 2 times

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: A

Community vote distribution

A (100%)

🗨️ **MassoudAbedian** Highly Voted 1 year, 4 months 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 9 times

🗨️ **byfener** Most Recent 7 months, 3 weeks ago

Selected Answer: A

This option is NOT suitable for the company as a cloud customer. The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) is a framework that provides a structured set of controls that can be used by customers to assess the security posture of their cloud providers. It's designed for customers to use when evaluating potential cloud service providers (CSPs) and their offerings.

Submitting the CCM on behalf of the CSP to the CSA STAR registry would involve the cloud customer submitting information about the CSP's security controls and practices. However, the CCM is typically intended for customers to evaluate the CSP's security, rather than for the CSP to submit their own information. The responsibility for submitting accurate and up-to-date security information to the STAR registry lies with the CSP themselves. Therefore, option A is not suitable as a use of CCM by the company as a cloud customer.

upvoted 1 times

🗨️ **Brainiac** 10 months 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 2 times

🗨️ **moota** 1 year ago

Selected Answer: A

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

upvoted 3 times

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: B

Community vote distribution

B (91%)

9%

  **cjkuga** Highly Voted  11 months 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 7 times

  **moten** Most Recent  3 months, 2 weeks ago

Selected Answer: A

Option A is the most appropriate control in this scenario, as it specifically addresses the need to manage changes in business-critical or customer-impacting applications, system designs, and configurations in the production environment.

upvoted 1 times

  **moten** 3 months, 2 weeks ago

Selected Answer: B

If the management plane of a cloud environment has been breached, it is important to confirm that the templates and configurations for infrastructure or applications have not been compromised as well. The management plane is responsible for managing and controlling the cloud resources, including the templates and configurations used to provision and manage those resources. A breach in the management plane can potentially lead to unauthorized access or modifications to the templates and configurations, compromising the overall security of the cloud environment. Therefore, it is necessary to verify the integrity of these templates and configurations after a management plane breach.

upvoted 1 times

  **FATWENTYSIX** 4 months, 3 weeks 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 4 times

  **Neo0** 5 months, 3 weeks ago

new infrastructure/applications

upvoted 1 times

  **vavofa5697** 7 months, 1 week ago

even by common sense it should B

upvoted 1 times

  **A_Nevermind** 10 months ago

Selected Answer: B

From the guidance as mentioned by cjkuga

upvoted 2 times

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

Community vote distribution

A (100%)

 **byfener** 7 months, 3 weeks ago

Selected Answer: A

In the context of a rapidly growing start-up like "ABC" providing a cloud-based IT management solution, implementing controls for Change Control & Configuration Management is essential to manage changes effectively in their production environment. Option A outlines a specific control related to managing the risks associated with changes to critical applications, customer-impacting systems, and infrastructure components. Given that ABC is dealing with cloud-based IT management and providing services to customers, ensuring that changes are controlled and assessed for potential impacts is crucial for maintaining the stability and security of their production environment.

Therefore, in this scenario, option A is the most suitable control to implement for Change Control & Configuration Management in ABC's rapidly growing cloud-based IT management start-up.

upvoted 2 times

 **moten** 9 months, 3 weeks ago

Selected Answer: A

Option A is the most appropriate control in this scenario, as it specifically addresses the need to manage changes in business-critical or customer-impacting applications, system designs, and configurations in the production environment.

upvoted 1 times

 **Brainiac** 10 months 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 3 times

 **JoAsiaGje** 11 months, 2 weeks ago

Selected Answer: A

CCC-05

upvoted 3 times

Containers are highly portable code execution environments.

- A. False
- B. True

Correct Answer: B

🗨️ 👤 **saptati** 8 months ago

As stated in Security-Guidance-v4.0, Pg 85, "Containers are code execution environments that run within an operating system (for now), sharing and leveraging resources of that operating system" They are designed to be highly portable and can run on different operating systems and cloud platforms. Thus, the statement is True.

upvoted 1 times

🗨️ 👤 **Brainiac** 10 months 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 2 times

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

Community vote distribution

B (100%)

JoAsiaGje **Highly Voted** 11 months, 2 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 7 times

c0d2291 **Most Recent** 3 months, 3 weeks ago

Selected Answer: B

Once created, data can bounce in between phases without restriction, and may not pass through all stages (not all data is eventually destroyed).

<https://cloudsecurityalliance.org/blog/2021/10/14/the-6-phases-of-data-security>

upvoted 1 times

moten 9 months, 3 weeks ago

Selected Answer: B

B is the Answer,

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: Create, Store, Use, Share, Archive, and Destroy. However, the lifecycle is not strictly linear, and the flow of data through these stages can vary based on the specific requirements and characteristics of the data. Some data may not pass through all stages, depending on factors such as data type, sensitivity, retention requirements, and legal/regulatory obligations. The Data Security Lifecycle is flexible and adaptable to the unique needs of each organization and the data they handle.

upvoted 4 times

Brainiac 10 months 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 2 times

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

Community vote distribution

E (80%)

D (20%)

🗨️ **c0d2291** 3 months, 3 weeks ago

Selected Answer: D

Object encryption is an out-of-the-box feature - e.g. in S3.

The in-transit encryption would be via HTTPS.

upvoted 1 times

🗨️ **overarch384** 11 months, 3 weeks ago

Selected Answer: E

11.1.4.2, pg 124. 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

🗨️ **BFCrypto** 1 year, 4 months ago

Selected Answer: E

Correct Answer is E. The application or client should encrypt the data before storing in the object. If it was implemented by the server or cloud provider then they would have to hold the key which is not recommended, so best your own application has access to the key and encrypts the object before storing. This is consistent with 11.1.4.2

upvoted 2 times

🗨️ **byfener** 1 year, 7 months ago

Selected Answer: D

When object storage is used as the back-end for an application, the appropriate encryption method would typically involve object encryption. Object encryption involves encrypting each individual object (or file) stored within the object storage system. This ensures that data remains secure even when stored in a potentially shared or publicly accessible environment.

Client/application encryption (E) might refer to encryption applied by the client or application before sending data to the storage, which could be an additional layer of security but might not be the encryption method applied within the storage system itself.

So, among the options provided, the most appropriate encryption method when using object storage as the back-end for an application is D. Object encryption.

upvoted 1 times

🗨️ **byfener** 1 year, 7 months ago

but accordingly 11.1.4.2 Client-side encryption: answer is E. we should stick guidance I think

upvoted 4 times

🗨️ **salimhajji** 1 year, 9 months ago

The explications of Brainiac are clear and exactly but the answer of Moota are from the docs.

What s the real response for the question : the definition or the words used on the references

upvoted 1 times

🗨️ **Brainiac** 1 year, 10 months 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 2 times

  **moota** 2 years 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 4 times


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

Community vote distribution


D (100%)

 **overarch384** 5 months, 2 weeks ago

Selected Answer: D

1.2.1 - Software as a Service: The cloud provider is responsible for nearly all security, since the cloud user can only access and manage their use of the application, and can't alter how the application works.

upvoted 1 times

 **Brainiac** 1 year, 4 months 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 2 times

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: A

Community vote distribution

A (100%)

 **SQCISSP** Highly Voted 10 months, 1 week ago

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

upvoted 5 times

 **moten** Most Recent 3 months, 2 weeks ago

Selected Answer: A

The correct answer is A. Encryption. Data fragmentation alone may not provide sufficient security measures to protect data. However, when encryption is combined with data fragmentation, it can significantly enhance security. Encryption ensures that even if an unauthorized entity gains access to fragmented data, the encrypted pieces are unintelligible without the corresponding encryption keys. This adds an additional layer of protection to the fragmented data and helps safeguard its confidentiality.

upvoted 2 times

 **Brainiac** 4 months 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** 4 months, 3 weeks 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** 6 months, 1 week ago

Selected Answer: A

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

upvoted 3 times

 **Petza** 11 months ago

Selected Answer: A

Answer A & only A

upvoted 4 times

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: E

Community vote distribution

E (87%)

7%

 **MassoudAbedian** Highly Voted 1 year, 4 months 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 11 times

 **Crotofoto** Most Recent 6 months ago

Selected Answer: C

Security Guidance page 137: An authorization is permission to do something—access a file or network, or perform a certain function like an API call on a particular resource.

The correct answer is C because you give permission.


upvoted 1 times

 **riee02** 6 months, 3 weeks ago

Selected Answer: E

sometimes more than one answer can sound correct always choose the best suited answer to quetion

upvoted 1 times

 **byfener** 7 months, 3 weeks ago

Selected Answer: A

A. The process of specifying and maintaining access policies

Authorization, as a component of identity, entitlement, and access management, refers to the process of specifying and maintaining access policies. It involves defining rules and permissions that determine what actions and resources a user or entity is allowed to access based on their identity and assigned roles or attributes. Authorization ensures that individuals and entities can only access the resources and perform the actions that they have been granted permission for, following established policies.

upvoted 1 times

 **moten** 9 months, 3 weeks ago

Selected Answer: E

The correct answer is E. Enforcing the rules by which access is granted to the resources. Authorization, as a component of identity, entitlement, and access management (IAM), refers to the process of determining and enforcing the rules or policies that dictate access to resources. It involves verifying whether an authenticated user or entity has the necessary permissions or privileges to perform specific actions or access certain resources within a system or application. Authorization ensures that users are granted appropriate access based on their roles, permissions, and the established security policies.

upvoted 1 times

 **Brainiac** 10 months 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 2 times

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: D

Community vote distribution

D (87%) 13%

🗨️ **Crotofoto** 12 months ago

Selected Answer: D

Security Guidance page 143: 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 3 times

🗨️ **Ungi** 1 year ago

Selected Answer: D

13.1.2.3 Web Security (Web Security Gateways)

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

🗨️ **negevon** 1 year, 1 month ago

Selected Answer: A

I understand peopel that say C is also correct and soem WaaS vendors can land or manage on-premise equipment but "As a service" is more aligned to cloud so 'C' is a bit weak here (though not strictly false)

upvoted 2 times

🗨️ **moten** 1 year, 3 months ago

Selected Answer: D

The correct answer is D. Both A and C. Web security as a service (WaaS) can be deployed for a cloud consumer through a combination of proxying or redirecting web traffic to the cloud provider and deploying it on-premise through a software or appliance installation.

upvoted 2 times

🗨️ **Brainiac** 1 year, 4 months 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** 1 year, 4 months 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** 1 year, 6 months 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** 1 year, 6 months 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 2 times

🗨️ 👤 **chkuga** 1 year, 11 months ago

Selected Answer: D

Both A and C, 13.1.2.3

upvoted 4 times

🗨️ 👤 **DrTee** 1 year, 8 months ago

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

upvoted 2 times

🗨️ 👤 **wakandakindom** 7 months, 2 weeks ago

That's true. The question of WEB need to be taking in consideration

upvoted 1 times

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

Community vote distribution

B (100%)

🗨️ 👤 **ChewyBananas** 9 months ago

Selected Answer: B

10.1.3.3 Deployment Pipeline Security page 114

upvoted 1 times

🗨️ 👤 **Brainiac** 1 year, 10 months 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

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** 4 months 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 3 times

Without virtualization, there is no cloud.

- A. False
- B. True

Correct Answer: B

 **Brainiac** 4 months 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 2 times

All assets require the same continuity in the cloud.


- A. False
- B. True

Correct Answer: A

Community vote distribution


A (100%)



 **overarch384** 5 months, 2 weeks ago

Selected Answer: A

6.0.1.1 - "Overall, a risk-based approach is key: Not all assets need equal continuity."
upvoted 1 times

 **cjkuga** 1 year, 11 months ago

6.0.1.1
upvoted 2 times

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** 4 months 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 2 times