



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



CERTIFICATION TEST

- CertificationTest.net - Cheap & Quality Resources With Best Support

When briefing senior management on the creation of a governance process, the MOST important aspect should be:

- A. knowledge required to analyze each issue
- B. information security metrics
- C. linkage to business area objectives
- D. baseline against which metrics are evaluated

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ 👤 **RamingoRoad** 1 month ago

Selected Answer: C

Answer is C.

upvoted 1 times

🗨️ 👤 **huaze_lei** 1 year, 3 months ago

Selected Answer: C

When it comes to the senior management, the most important supporting factor that the management will give is how the proposed governance process will link to the business objectives. In the profit and loss (P&L) corporate environment, it is important to portray to the management what benefits the governance process will bring about, which will then garner the support for the governance process.

upvoted 1 times

🗨️ 👤 **hwwgs** 3 years, 1 month ago

Answer is C.

upvoted 1 times

🗨️ 👤 **Manix** 3 years, 2 months ago

Selected Answer: C

I agree, C is correct

upvoted 1 times

🗨️ 👤 **boyladdudeman** 4 years, 9 months ago

C is correct

upvoted 1 times

Which of the following should be determined while defining risk management strategies?

- A. Organizational objectives and risk tolerance
- B. Enterprise disaster recovery plans
- C. Risk assessment criteria
- D. IT architecture complexity

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **RamingoRoad** 1 month ago

Selected Answer: A

Answer is A.

upvoted 1 times

🗳️ 👤 **Naida** 5 months, 2 weeks ago

Selected Answer: A

A risk strategy should be established at the early stage of risk assessment.

upvoted 1 times

🗳️ 👤 **letsdoitnow** 1 year, 6 months ago

Selected Answer: A

A is the correct answer

upvoted 1 times

🗳️ 👤 **hwwgs** 1 year, 7 months ago

Answer is A.

upvoted 1 times

🗳️ 👤 **Sovattha** 1 year, 9 months ago

Selected Answer: A

A is correct answer

upvoted 1 times

🗳️ 👤 **boyladdudeman** 3 years, 3 months ago

A is correct

upvoted 1 times

Which of the following is the MOST important benefit of an effective security governance process?

- A. Senior management participation in the incident response process
- B. Better vendor management
- C. Reduction of security breaches
- D. Reduction of liability and overall risk to the organization

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **RamingoRoad** 1 month ago

Selected Answer: D

Answer is D

upvoted 1 times

🗳️ 👤 **goodwin1027** 1 year, 6 months ago

Selected Answer: D

Makes the most sense from a corporate governance standpoint. Thats the goal.

upvoted 1 times

🗳️ 👤 **arifbhatkar** 2 years ago

option C , will be right answer as security breaches are often a direct manifestation of risks and can have immediate and significant impacts on an organization.

upvoted 1 times

🗳️ 👤 **hwwgs** 2 years, 7 months ago

Answer is D

upvoted 1 times

🗳️ 👤 **certguy0001** 2 years, 7 months ago

All are good but most important is the overall Risk reduction

upvoted 1 times

🗳️ 👤 **mmus** 3 years, 1 month ago

D. Reduction of liability and overall risk to the organization is correct answer

upvoted 1 times

A global retail organization is looking to implement a consistent Disaster Recovery and Business Continuity Process across all of its business units.

Which of the following standards and guidelines can BEST address this organization's need?

- A. International Organization for Standardizations 22301 "€λ (ISO-22301)
- B. Information Technology Infrastructure Library (ITIL)
- C. Payment Card Industry Data Security Standards (PCI-DSS)
- D. International Organization for Standardizations 27005 "€λ (ISO-27005)

Suggested Answer: A

Community vote distribution

A (100%)

🗲️ 👤 **RamingoRoad** 1 month ago

Selected Answer: A

Answer is A.

upvoted 1 times

🗲️ 👤 **goodwin1027** 1 year, 6 months ago

I didn't know what ISO 22301 was, however, I did a process of elimination to reach the correct answer.

upvoted 1 times

🗲️ 👤 **hwwgs** 2 years, 7 months ago

Answer is A.

upvoted 1 times

🗲️ 👤 **letsdoitnow** 4 years ago

Verified, ISO 22301 is correct

upvoted 1 times

🗲️ 👤 **boyladdudeman** 4 years, 3 months ago

A is correct: ISO 22301:2019, Security and resilience – Business continuity management systems

upvoted 1 times

A security manager regularly checks work areas after business hours for security violations; such as unsecured files or unattended computers with active sessions.

This activity BEST demonstrates what part of a security program?

- A. Compliance management
- B. Audit validation
- C. Physical control testing
- D. Security awareness training

Suggested Answer: A

Community vote distribution

A (100%)

🗲️ 👤 **RC2073** 1 year, 4 months ago

Selected Answer: A

Correct answer is A

upvoted 2 times

🗲️ 👤 **arifbhatkar** 1 year, 6 months ago

Option B : Audit Validation is right option

upvoted 1 times

🗲️ 👤 **hwwgs** 2 years, 1 month ago

Answer is A. Compliance Management.

upvoted 1 times

Which of the following is the MAIN reason to follow a formal risk management process in an organization that hosts and uses privately identifiable information (PII) as part of their business models and processes?

- A. Need to comply with breach disclosure laws
- B. Fiduciary responsibility to safeguard credit information
- C. Need to transfer the risk associated with hosting PII data
- D. Need to better understand the risk associated with using PII data

Suggested Answer: D

Community vote distribution

D (100%)

🗨️ 👤 **RamingoRoad** 1 month ago

Selected Answer: D

question regards risk so answer is D.

upvoted 1 times

🗨️ 👤 **hwwgs** 1 year, 1 month ago

Answer is D.

upvoted 3 times

A method to transfer risk is to_____.

- A. Implement redundancy
- B. Move operations to another region
- C. Align to business operations
- D. Purchase breach insurance

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **RamingoRoad** 1 month ago

Selected Answer: D

Answer is D.

upvoted 1 times

🗳️ 👤 **letsdoitnow** 1 year, 6 months ago

D is correct.

upvoted 1 times

🗳️ 👤 **hwwgs** 1 year, 7 months ago

Answer is D. Purchase insurance to transfer risk.

upvoted 1 times

🗳️ 👤 **letsdoitnow** 3 years ago

Agreed! When insurance is purchased, risk is transferred to the Insurer.

upvoted 1 times

🗳️ 👤 **boyladdudeman** 3 years, 3 months ago

D is correct

upvoted 1 times

An organization licenses and uses personal information for business operations, and a server containing that information has been compromised. What kind of law would require notifying the owner or licensee of this incident?

- A. Consumer right disclosure
- B. Data breach disclosure
- C. Special circumstance disclosure
- D. Security incident disclosure

Suggested Answer: B

Community vote distribution

B (100%)

🗲️ 👤 **RamingoRoad** 1 month ago

Selected Answer: B

Answer is B.

upvoted 1 times

🗲️ 👤 **valec80** 2 months, 2 weeks ago

Selected Answer: B

Correct answer is B

upvoted 1 times

🗲️ 👤 **c1s0indepth** 5 months ago

Selected Answer: B

Security incident is any threat

Data breach is a specific event where sensitive data is accessed or stolen

upvoted 1 times

🗲️ 👤 **hwwgs** 1 year, 1 month ago

Answer is B. Data breach disclosure.

upvoted 1 times

Why is it vitally important that senior management endorse a security policy?

- A. So that employees will follow the policy directives.
- B. So that they can be held legally accountable.
- C. So that external bodies will recognize the organizations commitment to security.
- D. So that they will accept ownership for security within the organization.

Suggested Answer: D

Community vote distribution

D (80%)

A (20%)

🗳️ **valec80** 2 months, 2 weeks ago

Selected Answer: D

Answer is D. Ownership by the Executive is important.

upvoted 1 times

🗳️ **c1s0indepth** 5 months ago

Selected Answer: D

Top down buy-in is essential. "A" actually comes from "D" where ELT or ITLT buys in on the policy so that the employees follow it.

upvoted 1 times

🗳️ **Emporeo** 1 year, 3 months ago

Selected Answer: D

D is correct. business leader ownership. Also a policy is the voice of management. a clear statement of manegement intention

upvoted 2 times

🗳️ **Kentish** 2 years, 2 months ago

The wording can be misleading to suggest that management own security instead of being accountable for it, as many teams 'own' aspects of security.

upvoted 1 times

🗳️ **Jaya_1975** 2 years, 5 months ago

The answer D is correct. You have to go back to definition, a Policy is mandatory directive, regardless of who set it. Employees are still required to abide by the policy. So A is not the best answer, though most cases it is Senior management who approve it.

upvoted 1 times

🗳️ **letsdoitnow** 2 years, 6 months ago

Senior management owns the security responsibility of the organization.

upvoted 1 times

🗳️ **hwwgs** 2 years, 7 months ago

Answer is D. Ownership by the Executive is important.

upvoted 1 times

🗳️ **qais005** 2 years, 10 months ago

Selected Answer: A

I think you need the senior management support to enforce the policies

upvoted 1 times

Which of the following is of MOST importance when security leaders of an organization are required to align security to influence the culture of an organization?

- A. Understand the business goals of the organization
- B. Poses a strong technical background
- C. Poses a strong auditing background
- D. Understand all regulations affecting the organization

Suggested Answer: A

Community vote distribution

A (100%)

🗲️ 👤 **RamingoRoad** 1 month ago

Selected Answer: A

Answer is A

upvoted 1 times

🗲️ 👤 **valec80** 2 months, 2 weeks ago

Selected Answer: A

A. Understand the business goals of the organization

upvoted 1 times

🗲️ 👤 **LArchitecte** 9 months, 3 weeks ago

Selected Answer: A

I do agree. A CISO needs to understand the business objectives as s/he is there protect the business and ensuring the business meet its objectives by protecting the business from cyber attacks.

upvoted 1 times

🗲️ 👤 **bobby_kl** 1 year, 6 months ago

Selected Answer: A

A. Understand the business goals of the organization

upvoted 1 times

🗲️ 👤 **hwwgs** 2 years, 1 month ago

Answer is A. Business goals of the organization must be aligned with Security program.

upvoted 1 times

The PRIMARY objective of security awareness is to:

- A. Encourage security-conscious employee behavior
- B. Put employees on notice in case follow-up action for noncompliance is necessary
- C. Ensure that security policies are read
- D. Meet legal and regulatory requirements

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **LArchitecte** 9 months, 3 weeks ago

Selected Answer: A

We need to have employees who are security conscient. This will help to reduce attacks through the weakest security link, employees
upvoted 1 times

🗳️ 👤 **kanishkar** 1 year, 1 month ago

Selected Answer: A

Answer is A.
upvoted 2 times

🗳️ 👤 **hwwgs** 2 years, 7 months ago

Answer is A. Awareness helps employee's behavior.
upvoted 1 times

Which of the following is MOST likely to be discretionary?

- A. Policies
- B. Procedures
- C. Guidelines
- D. Standards

Suggested Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **adiru** 1 year ago

Selected Answer: C

Guidelines provide general direction or recommendations without specify a requirement.

upvoted 1 times

🗳️ 👤 **musagul** 1 year, 4 months ago

Policies and Procedures are must from compliance. Standards are regulatories from Organization's business flow. Guidelines are optional

Correct answer is C

upvoted 3 times

🗳️ 👤 **AJRuff** 2 years, 7 months ago

I disagree the answer is Procedures

upvoted 2 times

🗳️ 👤 **hwwgs** 2 years, 7 months ago

Answer is C. Guidelines.

upvoted 2 times

Which of the following has the GREATEST impact on the implementation of an information security governance model?

- A. Complexity of organizational structure
- B. Distance between physical locations
- C. Organizational budget
- D. Number of employees

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **LArchitecte** 9 months, 3 weeks ago

Selected Answer: A

Even with budget, if the org structure is complex, it can affect the security program. So having the right governance is the very important to the success of a security program.

upvoted 1 times

🗳️ 👤 **Ludikraut** 1 year, 6 months ago

I would agree that organizational complexity influences everything however structural complexity does not. Answer A is not the best answer as written, IMO.

upvoted 1 times

🗳️ 👤 **hwwgs** 2 years, 1 month ago

Complexity influences everything.

Answer is A.

upvoted 1 times

🗳️ 👤 **mmus** 2 years, 7 months ago

Question talk about governance model it should be Org structure.

upvoted 1 times

🗳️ 👤 **letsdoitnow** 3 years, 6 months ago

I see your point, however, the complexity of the org supersede budget. Budget will be driven by the complexity of the organization. Simple things usually have simple cost while complex things usually have high cost.

upvoted 1 times

🗳️ 👤 **Prosecco** 3 years, 12 months ago

I understand that org complexity can have an impact, but isnt budget equally if not more important? Without it, doesnt matter how complex the org is.

upvoted 1 times

When dealing with Security Incident Response procedures, which of the following steps come FIRST when reacting to an incident?

- A. Eradication
- B. Escalation
- C. Containment
- D. Recovery

Suggested Answer: C

🗨️ 👤 **musagul** 1 year, 4 months ago

This philosophy comes from Medicine. First you have to contain it like Pandemic. Close it -> fix the problem. Correct answer is C
upvoted 2 times

🗨️ 👤 **hwwgs** 2 years, 7 months ago

Containment. Answer is C.
upvoted 1 times

🗨️ 👤 **mmus** 3 years, 1 month ago

C Correct
upvoted 1 times

What is the relationship between information protection and regulatory compliance?

- A. That all information in an organization must be protected equally.
- B. The information required to be protected by regulatory mandate does not have to be identified in the organizations data classification policy.
- C. There is no relationship between the two.
- D. That the protection of some information such as National ID information is mandated by regulation and other information such as trade secrets are protected based on business need.

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **musagul** 1 year, 4 months ago

Selected Answer: D

D is the Correct Answer.

upvoted 2 times

🗳️ 👤 **hwwgs** 2 years, 7 months ago

Answer is D.

upvoted 1 times

Who in the organization determines access to information?

- A. Compliance officer
- B. Legal department
- C. Data Owner
- D. Information security officer

Suggested Answer: C

🗨️ 👤 **MURY23** 1 year, 3 months ago

The Question should be expanded to explain what type of Information.

upvoted 1 times

🗨️ 👤 **hwwgs** 1 year, 7 months ago



Data owner decides on access. Answer is C.

upvoted 1 times

When managing an Information Security Program, which of the following is of MOST importance in order to influence the culture of an organization?

- A. Compliance with local privacy regulations
- B. An independent Governance, Risk and Compliance organization
- C. Support Legal and HR teams
- D. Alignment of security goals with business goals

Suggested Answer: *D*

  **hwwgs** 1 year, 1 month ago

Answer is D.

upvoted 2 times

The FIRST step in establishing a security governance program is to?

- A. Obtain senior level sponsorship
- B. Conduct a workshop for all end users.
- C. Conduct a risk assessment.
- D. Prepare a security budget.

Suggested Answer: A

🗨️ 👤 **arifbhatkar** 1 year, 6 months ago

Option C will be correct option

upvoted 1 times

🗨️ 👤 **Electric43** 11 months, 2 weeks ago


First, you need money to run any program. Answer is A

upvoted 1 times

When an organization claims it is secure because it is PCI-DSS certified, what is a good first question to ask towards assessing the effectiveness of their security program?

- A. How many credit records are stored?
- B. What is the value of the assets at risk?
- C. What is the scope of the certification?
- D. How many servers do you have?

Suggested Answer: C

  **JeBaCas** 1 year, 4 months ago

Scope may be just an Application/system, or even an outsourced service independently of the #transacins and #records. leaving the rest of operations activities out of such an scope

upvoted 3 times

A security manager has created a risk program. Which of the following is a critical part of ensuring the program is successful?

- A. Ensuring developers include risk control comments in code
- B. Creating risk assessment templates based on specific threats
- C. Providing a risk program governance structure
- D. Allowing for the acceptance of risk for regulatory compliance requirements

Suggested Answer: C

Community vote distribution

C (100%)

  **RamingoRoad** 1 month ago

Selected Answer: C

Answer is C

upvoted 1 times

Ensuring that the actions of a set of people, applications and systems follow the organization's rules is BEST described as:

- A. Compliance management
- B. Security management
- C. Risk management
- D. Mitigation management

Suggested Answer: A

Community vote distribution

A (100%)

🗲️ 👤 **c1s0indepth** 5 months ago

Selected Answer: A

All other answers feed into Compliance

upvoted 1 times

🗲️ 👤 **LArchitecte** 9 months, 3 weeks ago

Selected Answer: A

It is about having people, application, and system to comply with the organizations rules (or policies)

upvoted 1 times

🗲️ 👤 **hwwgs** 1 year, 1 month ago

Answer is A.

upvoted 2 times

Which of the following international standards can be BEST used to define a Risk Management process in an organization?

- A. International Organization for Standardizations 27005 "€λ (ISO-27005)
- B. National Institute for Standards and Technology 800-50 (NIST 800-50)
- C. Payment Card Industry Data Security Standards (PCI-DSS)
- D. International Organization for Standardizations 27004 "€λ (ISO-27004)

Suggested Answer: A

Community vote distribution

A (100%)

🗉 👤 **RamingoRoad** 1 month ago

Selected Answer: A

A: ISO/IEC 27005:2018 : Information Security Risk Management Guidelines

upvoted 1 times

🗉 👤 **letsdoitnow** 1 year, 6 months ago

Agreed! Very good ISO summary list is found here <https://www.iso.org/management-system-standards-list.html>

upvoted 1 times

🗉 👤 **boyladdudeman** 1 year, 9 months ago

A is correct: ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management

upvoted 1 times

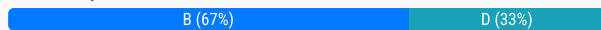
A security professional has been promoted to be the CISO of an organization. The first task is to create a security policy for this organization. The CISO creates and publishes the security policy.

This policy, however, is ignored and not enforced consistently. Which of the following is the MOST likely reason for the policy shortcomings?

- A. Lack of a formal risk management policy
- B. Lack of a formal security policy governance process
- C. Lack of formal definition of roles and responsibilities
- D. Lack of a formal security awareness program

Suggested Answer: B

Community vote distribution



🗳️ 👤 **RamingoRoad** 1 month ago

Selected Answer: D

Answer is D, Lack of a formal security awareness program.

upvoted 1 times

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

D D. Lack of a formal security awareness program. Without a security awareness program, employees may not fully understand the policy, its importance, or their role in enforcing it, leading to it being ignored or inconsistently applied.

upvoted 2 times

🗳️ 👤 **claudiosousa** 1 year, 11 months ago

Selected Answer: B

Lack of a formal security policy governance process: This is the most probable reason for the policy being ignored. Governance involves not just the creation of policies but also the mechanisms for enforcement, monitoring, and reviewing those policies. If there's no formal governance process, there's likely no mechanism to ensure that the policy is integrated into daily operations, no accountability for non-compliance, and no regular reviews or updates to the policy. All of these factors can lead to a policy being ignored or inconsistently enforced.

upvoted 3 times

🗳️ 👤 **RC2073** 2 years, 4 months ago

Selected Answer: B

B is correct. Refer to <https://vceguide.com/which-of-the-following-is-the-most-likely-reason-for-the-policy-shortcomings/>

upvoted 1 times

🗳️ 👤 **Kentish** 2 years, 8 months ago

B makes sense as a governance process would ensure the policies are rolled out and adopted. part of this would be defining the roles and responsibilities so also answer C

upvoted 1 times

🗳️ 👤 **tnagy** 2 years, 9 months ago

Selected Answer: D

Lack of Security Awareness Program

upvoted 1 times

Regulatory requirements typically force organizations to implement _____.

- A. Financial controls
- B. Mandatory controls
- C. Discretionary controls
- D. Optional controls

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **RamingoRoad** 1 month ago

Selected Answer: B

Answer is B. Regulatory is mandatory

upvoted 1 times

🗳️ 👤 **Perseus_68** 1 year, 4 months ago

Selected Answer: B

Financial could be a subset of mandatory controls, Thus B is comprehensive.

upvoted 1 times

🗳️ 👤 **ImranNY** 1 year, 4 months ago

A is a correct answer too. Regulatory requirements typically force organizations to implement financial controls as well e.g. the U.S Security and Exchange commission (SEC) mandates the financial related controls to the publicly traded companies.

upvoted 1 times

🗳️ 👤 **hwwgs** 2 years, 7 months ago

Answer is B.

upvoted 1 times

From an information security perspective, information that no longer supports the main purpose of the business should be:

- A. protected under the information classification policy
- B. analyzed under the data ownership policy
- C. assessed by a business impact analysis.
- D. analyzed under the retention policy.

Suggested Answer: D

Community vote distribution

D (100%)

🗨️ 👤 **RamingoRoad** 1 month ago

Selected Answer: D

Answer is D. Retention

upvoted 1 times

🗨️ 👤 **nshams** 1 year, 6 months ago

retention policy refers to the policy actions on a classified organizations data.

upvoted 2 times

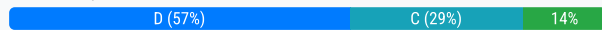
A global retail company is creating a new compliance management process.

Which of the following regulations is of MOST importance to be tracked and managed by this process?

- A. Information Technology Infrastructure Library (ITIL)
- B. National Institute for Standards and technology (NIST) standard
- C. International Organization for Standardization (ISO) standards
- D. Payment Card Industry Data Security Standards (PCI-DSS)

Suggested Answer: D

Community vote distribution



🗳️ 👤 **RamingoRoad** 1 month ago

Selected Answer: D

Answer D

upvoted 1 times

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

Selected Answer: C

Since C. and D, are non-mandatory standards, the wider one (ISO) should be the answer

upvoted 2 times

🗳️ 👤 **U_Rock** 1 year, 8 months ago

Keywords >> Retail. The only item tied specifically to "retail" is PCI DSS - as related to the protection of credit card payment transactions and the cardholder data.

upvoted 3 times

🗳️ 👤 **ats831** 1 year, 10 months ago

Selected Answer: D

D. Payment Card Industry Data Security Standards (PCI-DSS)

Here's why:

Option A: ITIL is a framework for IT service management, not a regulation. While it can be helpful in managing compliance processes, it doesn't directly dictate specific compliance requirements.

Option B: NIST standards are broad and encompass various areas, including cybersecurity. However, they are not specific to retail companies or payment card data security.

Option C: ISO standards also cover a wide range of areas, including some relevant to retail, like ISO 9001 for quality management. However, none directly address payment card data security like PCI-DSS does.

Option D: PCI-DSS is a set of security standards specifically designed to ensure the safe handling of cardholder data by organizations that accept, transmit, or store payment card information. This directly applies to most, if not all, global retail companies that process customer payments.

upvoted 3 times

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

PCI-DSS is the correct answer

upvoted 1 times

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

The quality of this question could be enhanced by indicating that this global retail company accepts Credit Card. It doesn't indicate anywhere in the question.

upvoted 1 times

🗳️ 👤 **Boats** 2 years, 7 months ago

PCI-DSS is not a regulation as tnagy says. NIST is US based. It is a global company. The best answer is ISO.



upvoted 1 times

🗳️ 👤 **tnagy** 2 years, 9 months ago

Selected Answer: B



NIST is enforced by regulations in the USA governmental bodies.

upvoted 1 times

  **boyladdudeman** 4 years, 9 months ago

D is Correct, it is the only mandatory while the other are optional.

upvoted 1 times

  **tnagy** 2 years, 9 months ago

PCI-DSS is not a regulation.

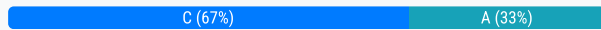
upvoted 2 times

One of the MAIN goals of a Business Continuity Plan is to_____.

- A. Ensure all infrastructure and applications are available in the event of a disaster
- B. Assign responsibilities to the technical teams responsible for the recovery of all data
- C. Provide step by step plans to recover business processes in the event of a disaster
- D. Allow all technical first-responders to understand their roles in the event of a disaster.

Suggested Answer: C

Community vote distribution



🗲️ 👤 **RamingoRoad** 1 month ago

Selected Answer: C

Answer is C. BCP activities consist of steps to implement formal plans and procedures to restore or maintain operations.

upvoted 1 times

🗲️ 👤 **GVJohn** 5 months, 1 week ago

Selected Answer: C

All infra & applications are Not expected to be available soon after a disaster. The main goal of a BCM is to get the system up and running in a phased manner - all critical ones first & then the remaining.

upvoted 1 times

🗲️ 👤 **Tobbyceaser** 1 year ago

Selected Answer: C

There is a difference between a DRP and a BCP, Moreso, not all infrastructure is required for operations to continue, the critical ones are given preference based on the BIA. Hence the answer is C

upvoted 2 times

🗲️ 👤 **perritoFaldero** 1 year, 4 months ago

Selected Answer: A

the main goal of a BCP is to ensure the continuity of the operations, no matter how it is done. So the correct answer should be A

upvoted 2 times

An organization's Information Security Policy is of MOST importance because_____.

- A. It defines a process to meet compliance requirements
- B. It establishes a framework to protect confidential information
- C. It communicates management's commitment to protecting information resources
- D. It is formally acknowledged by all employees and vendors

Suggested Answer: C

Community vote distribution

C (100%)

🗉 👤 **RamingoRoad** 1 month ago

Selected Answer: C

Answer is C, because management's commitment

upvoted 1 times

🗉 👤 **mmus** 1 year, 2 months ago

C, its management commitment

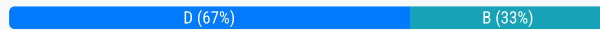
upvoted 1 times

The alerting, monitoring and life-cycle management of security-related events is typically handled by the_____.

- A. risk management process
- B. risk assessment process
- C. governance, risk, and compliance tools
- D. security threat and vulnerability management process

Suggested Answer: *D*

Community vote distribution



RamingoRoad 1 month ago

Selected Answer: D

Answer D, threats regard alerting and monitoring
upvoted 1 times

c1s0indepth 5 months ago

Selected Answer: D

Alerting and monitoring = SOC and TVM
upvoted 1 times

GVJohn 5 months, 1 week ago

Selected Answer: B

I cannot completely agree that D is the correct answer. Among the other choices Risk assessment process could be a more better answer
upvoted 1 times

A Security Operations Centre (SOC) manager is informed that a database containing highly sensitive corporate strategy information is under attack. Information has been stolen, and the database server was disconnected.

Who must be informed of this incident?

- A. Internal audit
- B. The data owner
- C. All executive staff
- D. Government regulators

Suggested Answer: B

Community vote distribution

B (83%)

C (17%)

🗳️ 👤 **RamingoRoad** 1 month ago

Selected Answer: B

Answer is B. The data owner is the controller so responsible and decision making for response
upvoted 1 times

🗳️ 👤 **Naida** 5 months, 2 weeks ago

Selected Answer: B

Data accountability lies with the data owner. During a security event, the data owner is the key person responsible for decision-making and response
upvoted 1 times

🗳️ 👤 **johnndoe69** 1 year, 5 months ago

Selected Answer: B

B. The data owner

The data owner is responsible for the data and is the primary stakeholder in terms of understanding the sensitivity and importance of the data. Informing the data owner promptly allows them to take appropriate actions, such as initiating an incident response, assessing the impact, and making decisions regarding further notifications and mitigation steps. The data owner can then coordinate with other relevant parties, such as internal audit, executive staff, and government regulators, if necessary.
upvoted 3 times

🗳️ 👤 **Emporeo** 1 year, 9 months ago

Selected Answer: C

for me a major incident and a data breach, i would certainly get executive staff onboard
upvoted 1 times

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

If we do not pick "All executive staff" it will compromise the question integrity.
upvoted 1 times

🗳️ 👤 **Radoi40** 2 years, 6 months ago

Who is being notified about such breach must be defined in the security inc. man process. Stolen DB information implies a security breach meaning inc can be treated as major. Exec team must get notification for all major inc. especially for the security ones
upvoted 2 times

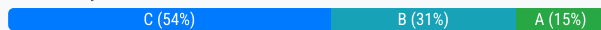
An organization has defined a set of standard security controls. This organization has also defined the circumstances and conditions in which they must be applied.

What is the NEXT logical step in applying the controls in the organization?

- A. Determine the risk tolerance
- B. Perform an asset classification
- C. Analyze existing controls on systems
- D. Create an architecture gap analysis

Suggested Answer: C

Community vote distribution



🗳️ 👤 **shiko81** 6 months ago

Selected Answer: B

Asset classification is 1st in order to understand how these controls should be applied. Once classified, conduct gap analysis for required additional controls

upvoted 1 times

🗳️ 👤 **shiko81** 6 months ago

Selected Answer: A

Asset classification is 1st in order to understand how these controls should be applied. Once classified, conduct gap analysis for required additional controls

upvoted 1 times

🗳️ 👤 **LArchitecte** 9 months, 3 weeks ago

Selected Answer: A

It is just logical to analyze after all that

upvoted 1 times

🗳️ 👤 **JeBaCas** 1 year, 4 months ago

Asset classification is 1st in order to understand how these controls should be applied. Once classified, we are ready to explore the controls in place and identify gaps Vs defined applicable controls

upvoted 2 times

🗳️ 👤 **johndoe69** 1 year, 5 months ago

Selected Answer: C

After defining the standard security controls and the conditions for their application, the next step is to analyze the existing controls on the systems to identify any gaps or overlaps. This analysis helps in understanding how well the current controls align with the new standards and where adjustments or enhancements are needed. By doing this, the organization can ensure that the new controls are effectively integrated and that all systems comply with the updated security requirements.

upvoted 2 times

🗳️ 👤 **nshams** 1 year, 5 months ago

Asset classification is the first step

upvoted 1 times

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

Selected Answer: C

analyze existing controls. asset classification must be in place already. how to apply the correct controls if you do not know the asset classification?

upvoted 2 times

🗳️ 👤 **Perseus_68** 1 year, 10 months ago

That was my first thought. But the question does not state a program has been implemented and it is being reviewed. Our only info is the company has some documentation on controls, not that any have been applied, so the first step in Risk management is to categorize the Asset or System, pg 71 CCISO guide.

upvoted 2 times

🗨️ 👤 **Emporeo** 1 year, 9 months ago

Maybe the question is not 100% clear for me, i was rather thinking about Control Lifecycle Management . The steps are select, validate, catalog, implement. So if in first step a control has been selected/defined...next to validate (which i thought also analyse existing ones...) upvoted 1 times

🗨️ 👤 **Perseus_68** 1 year, 10 months ago

Selected Answer: B

What happens before you apply controls, you need to know your assets and what level of protection they need based on the standards. upvoted 3 times

🗨️ 👤 **38eefed** 1 year, 10 months ago

Selected Answer: C

Since the organization has already defined its security controls and their application conditions, the next step is to analyze the existing controls on systems (Option C). This will help the organization understand where these standard controls need to be applied or where existing controls may need to be updated. upvoted 3 times

🗨️ 👤 **arkb103** 1 year, 8 months ago

How do you define new set of controls without first analyzing the exisiting controls to determine their effectiveness or otherwise. You can only come up with the standard controls and their applicability after thorough understanding of existing controls not the other way round. Answer C is incorrect. upvoted 1 times


The single most important consideration to make when developing your security program, policies, and processes is:

- A. Alignment with the business
- B. Budgeting for unforeseen data compromises
- C. Establishing your authority as the Security Executive
- D. Streaming for efficiency

Suggested Answer: A

Community vote distribution

A (100%)

 **LArchitecte** 9 months, 3 weeks ago

Selected Answer: A

Security activities must align with the business objectives and goal. There should never be any misalignment between the security objectives and business/organization objectives

upvoted 1 times

In accordance with best practices and international standards, how often is security awareness training provided to employees of an organization?

- A. Every 18 months
- B. Every 12 months
- C. High risk environments 6 months, low-risk environments 12 months
- D. Every 6 months

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is a MAJOR consideration when an organization retains sensitive customer data and uses this data to better target the organization's products and services?

- A. Strong authentication technologies
- B. Financial reporting regulations
- C. Credit card compliance and regulations
- D. Local privacy laws

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

If your organization operates under a model of "assumption of breach", you should:

- A. Establish active firewall monitoring protocols
- B. Purchase insurance for your compliance liability
- C. Focus your security efforts on high value assets
- D. Protect all information resource assets equally

Suggested Answer: C

Community vote distribution

C (67%)

B (33%)

🗳️ 👤 **Alex19741974** 1 year, 2 months ago

Selected Answer: B

Assumption of breach, means the event is post asset protection and controls, how to handle breach, assurance, investigation and incident retainers are the ways to handle assume breach.

upvoted 1 times

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

Selected Answer: C

Under Assumption of breach not a single insurance company will sing a contract

upvoted 1 times

🗳️ 👤 **john doe69** 1 year, 5 months ago

Selected Answer: C

The "assumption of breach" model operates on the premise that breaches are inevitable. Therefore, it's crucial to prioritize and focus security efforts on protecting high-value assets, as these are the most critical and potentially damaging if compromised. This approach helps in allocating resources efficiently to areas that matter the most, ensuring that the organization's most valuable and sensitive information is adequately protected.

upvoted 3 times

🗳️ 👤 **Emporeo** 1 year, 9 months ago

i honestly would pick none of the answers. Focus on most critical assets can't be the right answer, that would leave other assets vulnerable.

Transferring risk to an insurance company? that might compensate some costs, but will NOT protect your company getting hit by a severe attack...and fines in case of regulations. My thoughts here are to harden the incident response process, implement a stronger process and tech, implement network segregation and strong IAM to limit the damage and potential lateral movement. Thats the theory everyone gets a victim of an attack..the difference is the severity and capability to stop bleeding..

upvoted 1 times

🗳️ 👤 **ab1523e** 1 year, 9 months ago

Selected Answer: B

the "assumption of a breach" require an insurance for the compliance liability

upvoted 1 times

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

Selected Answer: B

We should be thinking quantitatively, we know that there is or will be a breach. Insurance is a must for us. However, we do not know which assets. Correct one is B

upvoted 1 times

🗳️ 👤 **7926e67** 1 year, 11 months ago

Selected Answer: C

If there is a breach, the organization will prioritize the security efforts on high value assets. It is too late to have insurance and you may not have enough resource to put on all assets as well.

upvoted 1 times

🗳️ 👤 **Malik2165** 2 years, 1 month ago

It is about assumption that we have already a breach, at this point we need to remediate the risk of Regulatory or compliance fines and paneties. Hence Answer B is correct.

upvoted 1 times

🗨️ 👤 **RC2073** 2 years, 4 months ago

Selected Answer: B

B is correct, I checked on two other websites

upvoted 1 times

🗨️ 👤 **arifbhatkar** 2 years, 6 months ago

Answer is C. Focus your security efforts on high value assets

upvoted 1 times

🗨️ 👤 **Pika26** 2 years, 9 months ago

Answer is C.

upvoted 1 times

🗨️ 👤 **tnagy** 2 years, 9 months ago

Selected Answer: C

Focus your security efforts on high value assets

upvoted 3 times

When dealing with a risk management process, asset classification is important because it will impact the overall:

- A. Threat identification
- B. Risk treatment
- C. Risk monitoring
- D. Risk tolerance

Suggested Answer: A

Community vote distribution

A (67%)

B (33%)

🗳️ 👤 **Abodi000** 12 months ago

Selected Answer: B

Asset classification involves categorizing assets based on their importance, value, sensitivity, and the impact of their loss or compromise. Proper classification helps in determining the level of protection required for each asset. This is crucial because it directly impacts how the organization treats (or responds to) various risks, including the selection of security controls, risk mitigation strategies, and the prioritization of resources.

Why not the other options?

A. Threat identification: While asset classification helps to prioritize which assets may be more attractive to attackers, it doesn't directly affect the identification of threats. Threat identification is more focused on understanding potential adversaries and attack vectors.

upvoted 2 times

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

Selected Answer: A

The asset determine the threats it is subject to. That is the very first step

upvoted 2 times

🗳️ 👤 **JeBaCas** 1 year, 4 months ago

Asst classification or categorization determines the CIA needs. Risk Treatment will be affected by it due to controls should be aligned to these needs, however is more important for threat identification since these are the once that will determine if risk is be treated or accepted (criteria). Besides, treatment can have other options than mitigation, where CIA needs are not relevant

upvoted 2 times

🗳️ 👤 **Pika26** 2 years, 9 months ago

B is correct, because Asset classification is important in the risk management process because it will impact the overall risk treatment. Asset classification involves identifying and categorizing assets based on their value, criticality, sensitivity, and other relevant factors. This classification helps determine the appropriate level of protection and resources that should be allocated to each asset. Based on the classification of assets, the organization can determine the appropriate risk treatment strategy, which may include risk avoidance, risk mitigation, risk transfer, or risk acceptance.

upvoted 4 times

🗳️ 👤 **tnagy** 2 years, 9 months ago

Selected Answer: A

Assets must be classified to identify potential threats not to prepare for a remediation plan.

upvoted 2 times

You have a system with 2 identified risks. You determine the probability of one risk occurring is higher than the

- A. Relative likelihood of event
- B. Controlled mitigation effort
- C. Risk impact comparison
- D. Comparative threat analysis

Suggested Answer: A

Community vote distribution



A (100%)

  **Perseus_68** 1 year, 4 months ago

Selected Answer: A

voting for A apprehensively, only because the question is comparing one characteristic vs another, the first states probability so a comparative term would be likelihood.

upvoted 1 times

  **LARdT** 3 years, 2 months ago

To make sense it should end in "than the other"

upvoted 1 times

Which of the following is a benefit of information security governance?

- A. Direct involvement of senior management in developing control processes
- B. Reduction of the potential for civil and legal liability
- C. Questioning the trust in vendor relationships
- D. Increasing the risk of decisions based on incomplete management information

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Developing effective security controls is a balance between:

- A. Technology and Vendor Management
- B. Operations and Regulations
- C. Risk Management and Operations
- D. Corporate Culture and Job Expectations

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

The framework that helps to define a minimum standard of protection that business stakeholders must attempt to achieve is referred to as a standard of:

- A. Due Compromise
- B. Due process
- C. Due Care
- D. Due Protection

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is considered the MOST effective tool against social engineering?

- A. Effective Security Vulnerability Management Program
- B. Anti-malware tools
- C. Effective Security awareness program
- D. Anti-phishing tools

Suggested Answer: C

Currently there are no comments in this discussion, be the first to comment!

When managing the security architecture for your company you must consider:

- A. Budget
- B. Security and IT Staff size
- C. Company values
- D. All of the above

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

The PRIMARY objective for information security program development should be:

- A. Reducing the impact of the risk to the business.
- B. Establishing incident response programs.
- C. Establishing strategic alignment with business continuity requirements.
- D. Identifying and implementing the best security solutions.

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

After a risk assessment is performed, a particular risk is considered to have the potential of costing the organization 1.2 Million USD. This is an example of_____.

- A. Qualitative risk analysis
- B. Risk Appetite
- C. Quantitative risk analysis
- D. Risk Tolerance



Suggested Answer: C

Currently there are no comments in this discussion, be the first to comment!

Quantitative Risk Assessments have the following advantages over qualitative risk assessments:

- A. They are subjective and can be completed more quickly
- B. They are objective and express risk / cost in approximates
- C. They are subjective and can express risk / cost in real numbers
- D. They are objective and can express risk / cost in real numbers

Suggested Answer: *D*

  **mmus** 1 year, 2 months ago

D Quantitative Risk Objective, Real Value

upvoted 2 times

Which of the following most commonly falls within the scope of an information security governance steering committee?

- A. Vetting information security policies
- B. Approving access to critical financial systems
- C. Interviewing candidates for information security specialist positions
- D. Developing content for security awareness programs

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

A company wants to fill a Chief Information Security Officer position in the organization. They need to define and implement a more holistic security program.

Which of the following qualifications and experience would be MOST desirable to find in a candidate?

- A. Industry certifications, technical knowledge and program management skills
- B. Multiple references, strong background check and industry certifications
- C. Multiple certifications, strong technical capabilities and lengthy resume
- D. College degree, audit capabilities and complex project management

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following intellectual Property components is focused on maintaining brand recognition?

- A. Trademark
- B. Research Logs
- C. Copyright
- D. Patent

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

Credit card information, medical data, and government records are all examples of:

- A. None
- B. Communications Information
- C. Bodily Information
- D. Confidential/Protected Information
- E. Territorial Information

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

You have implemented a new security control. Which of the following risk strategy options have you engaged in?

- A. Risk Transfer
- B. Risk Mitigation
- C. Risk Avoidance
- D. Risk Acceptance

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

What is a difference from the list below between quantitative and qualitative Risk Assessment?

- A. Quantitative risk assessments result in an exact number (in monetary terms)
- B. Quantitative risk assessments result in a quantitative assessment (high, medium, low, red, yellow, green)
- C. Qualitative risk assessments map to business objectives
- D. Qualitative risk assessments result in a quantitative assessment (high, medium, low, red, yellow, green)

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

You have purchased a new insurance policy as part of your risk strategy. Which of the following risk strategy options have you engaged in?

- A. Risk Mitigation
- B. Risk Acceptance
- C. Risk Avoidance
- D. Risk Transfer

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

What is the definition of Risk in Information Security?

- A. Risk = Probability x Impact
- B. Risk = Impact x Threat
- C. Risk = Threat x Probability
- D. Risk = Financial Impact x Probability

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **nshams** 1 year, 5 months ago

chance of occurring an incident like earthquake and outcome of it which is the impact combines total risk
upvoted 1 times

🗳️ 👤 **Mr_Magoo1518** 2 years, 1 month ago

How is risk calculated in security?

Risk is the combination of the probability of an event and its consequence. In general, this can be explained as: Risk = Likelihood × Impact. In particular, IT risk is the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.
upvoted 2 times

🗳️ 👤 **arifbhatkar** 2 years, 6 months ago

Answer should be C: Risk = Threat x Probability
upvoted 1 times

🗳️ 👤 **Boats** 2 years, 7 months ago

Selected Answer: A

Risk is the combination of the probability of an event and its consequence. In general, this can be explained as: Risk = Likelihood × Impact.
upvoted 1 times

🗳️ 👤 **Pika26** 2 years, 9 months ago

Answer is C. C. In Information Security, the definition of Risk is: Risk = Threat x Probability.

Risk refers to the potential for harm or loss resulting from a threat exploiting a vulnerability. A threat is any potential danger that could harm or compromise the confidentiality, integrity, or availability of an organization's information assets. Probability refers to the likelihood of a threat exploiting a vulnerability, while vulnerability is a weakness or gap in an organization's security defenses that could be exploited by a threat.

By multiplying the likelihood of a threat exploiting a vulnerability (i.e., probability) by the potential impact of a successful attack (i.e., threat), organizations can determine the level of risk associated with a particular information asset or system. This formula allows organizations to quantify and prioritize risks and determine appropriate risk treatment strategies.

upvoted 2 times

🗳️ 👤 **boyladdudemane** 4 years, 9 months ago

A is correct

upvoted 1 times

A business unit within your organization intends to deploy a new technology in a manner that places it in violation of existing information security standards.



What immediate action should the information security manager take?

- A. Enforce the existing security standards and do not allow the deployment of the new technology.
- B. If the risks associated with that technology are not already identified, perform a risk analysis to quantify the risk, and allow the business unit to proceed based on the identified risk level.
- C. Amend the standard to permit the deployment.
- D. Permit a 90-day window to see if an issue occurs and then amend the standard if there are no issues.

Suggested Answer: B

  **Ludikraut** 2 years, 6 months ago



As written A is the best answer. B would be the best if it mentioned documenting an exception to the standard based on the risk assessment.
upvoted 3 times

  **LArchitecte** 9 months, 3 weeks ago

in general policies should have exception. Again, security objectives must align with business objectives, and it must be balanced between the risk and business objectives.

In A, security would have completely stopped or delayed the achievement of business objectives. However, with B, there is a second chance- the chance of implementing the technology if the risk is within the tolerance level.

upvoted 1 times

  **adv87** 1 year, 4 months ago

Agreed. Policy and security standards are not subjective, they are to be followed. If exceptions are to be made, it must go through an approval process rather than allowed to proceed and management catches up to the problem. Allowing a precedent to happen opens the doors to other departments performing the same action causing disorganized management

upvoted 2 times

The establishment of a formal risk management framework and system authorization program is essential.

The LAST step of the system authorization process is:

- A. Getting authority to operate the system from executive management
- B. Contacting the Internet Service Provider for an IP scope
- C. Changing the default passwords
- D. Conducting a final scan of the live system and mitigating all high and medium level vulnerabilities

Suggested Answer: A

  **boyladdudeman** 1 year, 3 months ago


A is correct

upvoted 1 times

An organization's firewall technology needs replaced. A specific technology has been selected that is less costly than others and lacking in some important capabilities. The security officer has voiced concerns about sensitive data breaches but the decision is made to purchase. What does this selection indicate?

- A. A high threat environment
- B. A low vulnerability environment
- C. A high risk tolerance environment
- D. A low risk tolerance environment

Suggested Answer: *C*

  **BigMomma4752** 1 year, 2 months ago

Answer C is correct.

upvoted 1 times

Which of the following is MOST important when dealing with an Information Security Steering committee?

- A. Ensure that security policies and procedures have been vetted and approved.
- B. Review all past audit and compliance reports.
- C. Include a mix of members from different departments and staff levels.
- D. Be briefed about new trends and products at each meeting by a vendor.

Suggested Answer: B

Community vote distribution

C (50%)

A (50%)

🗳️ 👤 **Sean_P** 4 months, 3 weeks ago

Selected Answer: C

Including a mix of members from different departments and staff levels ensures that the Information Security Steering Committee has diverse perspectives. This diversity leads to more informed, balanced, and business-aligned security decisions that reflect the needs of the entire organization.

upvoted 1 times

🗳️ 👤 **shiko81** 5 months, 4 weeks ago

Selected Answer: A

This question appears twice here. Answer is A

upvoted 1 times

🗳️ 👤 **Aboodi000** 12 months ago

Selected Answer: C

The correct answer is:

C. Include a mix of members from different departments and staff levels.

Explanation:

An Information Security Steering Committee plays a crucial role in guiding the overall direction of an organization's information security program. It needs a diverse set of perspectives to ensure that security decisions align with the organization's broader business goals and that various aspects of the organization are represented.

upvoted 1 times

🗳️ 👤 **adv87** 1 year, 4 months ago

Selected Answer: A

This question appears twice here. Answer is A

upvoted 1 times

🗳️ 👤 **adv87** 1 year, 4 months ago

I'd like to correct myself. This is a slightly different question. C is plausible

upvoted 1 times

🗳️ 👤 **ONERAPTOR** 2 years, 1 month ago

The Correct Answer is C. This is crucial because the effectiveness of an Information Security Steering Committee hinges on its ability to understand and address security needs and concerns across the entire organization. The committee benefits from diverse perspectives and expertise by including members from various departments and staff levels. This diversity helps make more informed and comprehensive decisions about information security policies and strategies, ensuring that they align with the overall business objectives and the specific needs of different areas within the organization.

upvoted 3 times

🗳️ 👤 **arifbhatkar** 2 years, 6 months ago



A. Ensure that security policies and procedures have been vetted and approved.

upvoted 4 times

Risk that remains after risk mitigation is known as_____.

- A. Accepted risk
- B. Residual risk
- C. Non-tolerated risk
- D. Persistent risk

Suggested Answer: *B*

  **mmus** 1 year, 2 months ago

B. Residual risk

upvoted 1 times

An organization is looking for a framework to measure the efficiency and effectiveness of their Information Security Management System. Which of the following international standards can BEST assist this organization?

- A. Payment Card Industry Data Security Standards (PCI-DSS)
- B. International Organization for Standardizations 27005 "€λ (ISO-27005)
- C. International Organization for Standardizations 27004 "€λ (ISO-27004)
- D. Control Objectives for Information Technology (COBIT)

Suggested Answer: C

  **boyladdudeman** 1 year, 3 months ago

C is correct: ISO/IEC 27004 Information Technology - Security techniques - Information Security Management - Measurement.
upvoted 1 times

When would it be more desirable to develop a set of decentralized security policies and procedures within an enterprise environment?

- A. When there is a variety of technologies deployed in the infrastructure.
- B. When it results in an overall lower cost of operating the security program.
- C. When there is a need to develop a more unified incident response capability.
- D. When the enterprise is made up of many business units with diverse business activities, risks profiles and regulatory requirements.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Your IT auditor is reviewing significant events from the previous year and has identified some procedural oversights. Which of the following would be the MOST concerning?

- A. Failure to notify police of an attempted intrusion
- B. Lack of reporting of a successful denial of service attack on the network.
- C. Lack of periodic examination of access rights
- D. Lack of notification to the public of disclosure of confidential information

Suggested Answer: D

Community vote distribution

C (100%)

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

Selected Answer: C

D is not the correct Answer

upvoted 1 times

🗨️ 👤 **Electric43** 11 months, 2 weeks ago

D is correct. C is not While this indicates weak internal controls and could lead to unauthorised access, it is less immediately critical than failing to disclose a breach of confidential information, which carries immediate legal and regulatory risks

upvoted 1 times

Which of the following best represents a calculation for Annual Loss Expectancy (ALE)?

- A. Value of the asset multiplied by the loss expectancy
- B. Replacement cost multiplied by the single loss expectancy
- C. Single loss expectancy multiplied by the annual rate of occurrence
- D. Total loss expectancy multiplied by the total loss frequency

Suggested Answer: C

Community vote distribution

C (100%)

  **letsdoitnow** Highly Voted 3 years, 6 months ago

Agreed. Annual Loss Expectancy (ALE) = Single Loss Expectancy (SLE) x Annual Rate of Occurrence (ARO)
upvoted 5 times

  **bobby_kl** Most Recent 1 year, 5 months ago

Selected Answer: C

ALE = SLE x ARO
upvoted 2 times

  **boyladdudeman** 3 years, 9 months ago

C is correct
upvoted 2 times

The Information Security Management program MUST protect:

- A. Audit schedules and findings
- B. Intellectual property released into the public domain
- C. all organizational assets
- D. critical business processes and revenue streams

Suggested Answer: D

Community vote distribution

C (100%)

🗨️ 👤 **shiko81** 5 months, 4 weeks ago

Selected Answer: C

An Information Security Management (ISM) program is designed to protect all organizational assets
upvoted 1 times

🗨️ 👤 **ME79** 10 months, 1 week ago

Selected Answer: C

An Information Security Management (ISM) program is designed to protect all organizational assets, including:

Data assets (e.g., customer data, intellectual property, financial records)

Physical assets (e.g., servers, laptops, infrastructure)

Human assets (e.g., employees, contractors, security awareness)

Reputational assets (e.g., brand trust, compliance)

Since information security is a holistic approach, the ISM program should ensure all assets are classified, protected, and managed according to their sensitivity and business value.

upvoted 1 times

🗨️ 👤 **arifbhatkar** 1 year, 6 months ago

Right answer is C. all organizational assets

upvoted 3 times

Dataflow diagrams are used by IT auditors to:

- A. Graphically summarize data paths and storage processes.
- B. Order data hierarchically
- C. Highlight high-level data definitions
- D. Portray step-by-step details of data generation.

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

When measuring the effectiveness of an Information Security Management System which one of the following would be MOST LIKELY used as a metric framework?

- A. ISO 27001
- B. ISO 27004
- C. PRINCE2
- D. ITILv3

Suggested Answer: *B*

  **boyladdudeman** 1 year, 3 months ago

B is correct: ISO/IEC 27004 concerns measurements or measures needed for information security management: these are commonly known as 'security metrics' in the profession (if not within ISO/IEC JTC 1/SC 27!).

upvoted 2 times

The purpose of NIST SP 800-53 as part of the NIST System Certification and Accreditation Project is to establish a set of standardized, minimum security controls for IT systems addressing low, moderate, and high levels of concern for:

- A. Integrity and Availability
- B. Assurance, Compliance and Availability
- C. International Compliance
- D. Confidentiality, Integrity and Availability

Suggested Answer: *D*

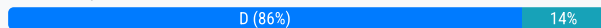
Currently there are no comments in this discussion, be the first to comment!

An organization is required to implement background checks on all employees with access to databases containing credit card information. This is considered a security_____.

- A. Technical control
- B. Management control
- C. Procedural control
- D. Administrative control

Suggested Answer: D

Community vote distribution



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

Selected Answer: D

Administrative controls are the policies, and formal procedures established by an organization to manage its security framework and enforce compliance with security regulations, internal governance goals, and cybersecurity standards. Administrative controls provide the governance needed to guide the behavior of individuals and the operation of systems within the organization. The primary purpose of administrative controls is to provide a framework for the organization's overall security strategy. They ensure that security measures are well-documented, communicated, and enforced throughout the organization.

upvoted 1 times

🗳️ 👤 **claudiosousa** 1 year, 11 months ago

Selected Answer: D

Background checks are a form of administrative control because they are part of the organization's policies and procedures regarding personnel security. These checks are aimed at ensuring that employees with access to sensitive information, such as credit card data, are reliable and do not pose a threat to the security of that information. Administrative controls typically involve methods implemented by the organization to manage and monitor business operations and employees, and background checks fall into this category.

upvoted 1 times

🗳️ 👤 **ONERAPTOR** 2 years, 1 month ago

C. Procedural control

Procedural controls refer to the policies and procedures to protect an organization's assets, including data. These controls are designed to ensure that the organization's processes and activities are conducted securely and controlled. Background checks are a procedural measure to ensure that individuals with access to sensitive information, such as credit card data, are reliable and do not pose a security risk. This type of control is more about the processes and procedures governing human actions rather than technical systems or management oversight.

upvoted 1 times

🗳️ 👤 **arifbhatkar** 2 years, 6 months ago

Answer is D. Administrative control, Administrative controls refer to the policies, procedures, and practices implemented by an organization to manage and mitigate risks. Background checks are typically considered an administrative control as they involve implementing specific measures and processes to verify the credentials and background of individuals before granting them access to sensitive information or systems.

upvoted 2 times

🗳️ 👤 **VOAKDO_cciso** 2 years, 7 months ago

Selected Answer: D

D,.., I made mistake in my previous vote, AD Control done by hr dept.

upvoted 1 times

🗳️ 👤 **VOAKDO_cciso** 2 years, 7 months ago

Selected Answer: B

B, this is Administrative Control done by HR dept.

upvoted 1 times

🗳️ 👤 **VOAKDO_cciso** 2 years, 7 months ago

mistake, I wanted to say D. Sorry!!

upvoted 1 times

🗨️ 👤 **Boats** 2 years, 7 months ago

Selected Answer: D

Administrative Control. If you have the CCISO book, it is located here, Domain 2 Page 72

upvoted 1 times

🗨️ 👤 **Pika26** 2 years, 9 months ago

Answer is D. Administrative control

The requirement to implement background checks on all employees with access to databases containing credit card information is an example of an administrative control. Administrative controls are policies, procedures, and guidelines that are put in place to manage and reduce risk, and typically involve management and administrative personnel.

upvoted 2 times

🗨️ 👤 **certguy0001** 3 years, 1 month ago

Background check is an administrative control

upvoted 2 times

🗨️ 👤 **mrsteve35** 3 years, 2 months ago

This is an administrative control

upvoted 2 times

🗨️ 👤 **bmaheux** 3 years, 2 months ago

Selected Answer: D

This is Administrative Control in CISSP for sure

upvoted 2 times

🗨️ 👤 **DinaBS** 3 years, 5 months ago

the answer is incorrect , security personnel is an operational control

upvoted 1 times

Information security policies should be reviewed _____.

- A. by the internal audit semiannually
- B. by the CISO when new systems are brought online
- C. by the Incident Response team after an audit
- D. by stakeholders at least annually

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Risk is defined as:

- A. Quantitative plus qualitative impact
- B. Asset loss times likelihood of event
- C. Advisory plus capability plus vulnerability
- D. Threat times vulnerability divided by control

Suggested Answer: B

Community vote distribution

B (75%)

D (25%)

🗳️ 👤 **BigMomma4752** 1 year, 2 months ago

B is the correct answer.

upvoted 1 times

🗳️ 👤 **JeBaCas** 1 year, 4 months ago

D response misses the consequences/impact part; then, is just a threat assessment formula

upvoted 1 times

🗳️ 👤 **claudiosousa** 1 year, 11 months ago

Selected Answer: B

This option aligns with the common definition of risk in the context of risk management, especially in information security and risk assessment frameworks. Risk is often quantified by considering the potential loss (or impact on assets) and the likelihood or probability of a particular event occurring. This approach helps in understanding, assessing, and prioritizing risks based on their potential impact and the likelihood of occurrence, enabling organizations to allocate resources and implement controls effectively.

upvoted 1 times

🗳️ 👤 **Rogue_Intel** 2 years, 2 months ago

Selected Answer: B

risk = likelihood x impact (or damage incurred by the event. If you put a dollar value on the impact, then you can value the risk and in a simple way compare one risk factor to another)

upvoted 1 times

🗳️ 👤 **arifbhatkar** 2 years, 6 months ago

The correct answer is B. "Asset loss times likelihood of event."

upvoted 1 times

🗳️ 👤 **Boats** 2 years, 7 months ago

Selected Answer: D

The formula is: risk = (threat x vulnerability x probability of occurrence x impact)/controls in place.

[https://stateofsecurity.com/formula-for-calculating-cyber-](https://stateofsecurity.com/formula-for-calculating-cyber-risk/#:~:text=The%20formula%20is%3A%20risk%20%3D%20(,impact)%2Fcontrols%20in%20place.)

[risk/#:~:text=The%20formula%20is%3A%20risk%20%3D%20\(,impact\)%2Fcontrols%20in%20place.](https://stateofsecurity.com/formula-for-calculating-cyber-risk/#:~:text=The%20formula%20is%3A%20risk%20%3D%20(,impact)%2Fcontrols%20in%20place.)

Risk = Likelihood × Impact

[https://www.isaca.org/resources/isaca-journal/past-issues/2014/an-enhanced-risk-formula-for-software-security-](https://www.isaca.org/resources/isaca-journal/past-issues/2014/an-enhanced-risk-formula-for-software-security-vulnerabilities#:~:text=Risk%20is%20the%20combination%20of,%3A%20Risk%20%3D%20Likelihood%20C3%97%20Impact.)

[vulnerabilities#:~:text=Risk%20is%20the%20combination%20of,%3A%20Risk%20%3D%20Likelihood%20C3%97%20Impact.](https://www.isaca.org/resources/isaca-journal/past-issues/2014/an-enhanced-risk-formula-for-software-security-vulnerabilities#:~:text=Risk%20is%20the%20combination%20of,%3A%20Risk%20%3D%20Likelihood%20C3%97%20Impact.)

Best answer is D

upvoted 1 times

🗳️ 👤 **CYNLEE** 2 years, 8 months ago

Selected Answer: B

Risk = Impact (i.e. Asset Cost Loss) X Likelihood of event (where likelihood is derived from Threat x Vulnerability / Control)


<https://stateofsecurity.com/formula-for-calculating-cyber-risk/>

upvoted 1 times

In which of the following cases, would an organization be more prone to risk acceptance vs. risk mitigation?

- A. The organization uses exclusively a qualitative process to measure risk
- B. The organization's risk tolerance is low
- C. The organization uses exclusively a quantitative process to measure risk
- D. The organization's risk tolerance is high

Suggested Answer: *D*

  **BigMomma4752** 1 year, 2 months ago

D is the correct answer.

upvoted 1 times

The regular review of a firewall ruleset is considered a _____.

- A. Procedural control
- B. Organization control
- C. Management control
- D. Technical control

Suggested Answer: A

Community vote distribution

C (50%)

D (50%)

  **Riset** 9 months ago

Selected Answer: D

D. Technical control

Explanation:

A firewall ruleset review is classified as a technical control because it involves the direct configuration, maintenance, and auditing of a technical security mechanism (the firewall).

Key Reasons:

Technical controls are measures implemented through hardware, software, or firmware to enforce security policies.

Examples: Firewalls, IDS/IPS, encryption, access control lists (ACLs).

Firewall ruleset reviews require technical expertise to analyze:

Rule effectiveness (e.g., blocking unauthorized traffic).

Redundant or overly permissive rules.

Compliance with security policies.

upvoted 1 times

  **Abodi000** 12 months ago

Selected Answer: C

C. Management control

Explanation:

The regular review of a firewall ruleset is an example of a management control because it involves oversight and assessment of security practices to ensure that they are aligned with organizational policies and objectives. Management controls are typically focused on the direction, coordination, and evaluation of security processes, including reviewing, updating, and ensuring compliance with security configurations and policies.

upvoted 1 times

  **Rufus1** 1 year, 2 months ago

Just to complete

NIST SP.800-26, indicates 3 types of control categories

Management

Operational

Technical

upvoted 1 times

  **UNN_CCISO** 1 year, 3 months ago

NIST indicates 2 types of security controls - Management, Operational & Technical. However, since Management and Technical are not related and there is nothing called Orgn control, the remaining option is Procedural Control.

upvoted 1 times

The exposure factor of a threat to your organization is defined by?

- A. Annual loss expectancy minus current cost of controls
- B. Percentage of loss experienced due to a realized threat event
- C. Asset value times exposure factor
- D. Annual rate of occurrence

Suggested Answer: *B*

  **ImJohnC** 1 year, 4 months ago

Exposure factor describes the loss that will happen to the asset as a result of the threat (expressed as percentage value).

upvoted 1 times

The Information Security Governance program MUST:

- A. integrate with other organizational governance processes
- B. show a return on investment for the organization
- C. integrate with other organizational governance processes
- D. support user choice for Bring Your Own Device (BYOD)

Suggested Answer: C

Community vote distribution

A (100%)

🗳️ 👤 **peapres** Highly Voted 🏆 5 years, 7 months ago

A and C are the same
upvoted 8 times

🗳️ 👤 **alfaMegatron** Most Recent 🕒 1 year, 4 months ago

I cannot choose between A and C.
upvoted 2 times

🗳️ 👤 **ab1523e** 1 year, 9 months ago

Selected Answer: A
A and C are the same
upvoted 1 times

🗳️ 👤 **ImJohnC** 3 years, 4 months ago

A and C are still the same
upvoted 2 times

🗳️ 👤 **letsdoitnow** 4 years, 6 months ago

You are correct. The answer options need update
upvoted 2 times

You have recently drafted a revised information security policy. From whom should you seek endorsement in order to have the GREATEST chance for adoption and implementation throughout the entire organization?

- A. Chief Executive Officer
- B. Chief Information Officer
- C. Chief Information Security Officer
- D. Chief Information Officer

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following is a benefit of a risk-based approach to audit planning?

- A. Resources are allocated to the areas of the highest concern
- B. Scheduling may be performed months in advance
- C. Budgets are more likely to be met by the IT audit staff
- D. Staff will be exposed to a variety of technologies

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following are the MOST important factors for proactively determining system vulnerabilities?

- A. Subscribe to vendor mailing lists and distribute notifications of system requirements
- B. Configure firewall, perimeter router and Intrusion Prevention System (IPS)
- C. Conduct security testing, vulnerability scanning, and penetration testing
- D. Deploy Intrusion Detection System (IDS) and install anti-virus on systems

Suggested Answer: C

Currently there are no comments in this discussion, be the first to comment!

When choosing a risk mitigation method what is the MOST important factor?

- A. Approval from the board of directors
- B. Metrics of mitigation method success
- C. Cost of the mitigation is less than a risk
- D. Mitigation method complies with PCI regulations

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Payment Card Industry (PCI) compliance requirements are based on what criteria?

- A. The size of the organization processing credit card data
- B. The types of cardholder data retained
- C. The duration card holder data is retained
- D. The number of transactions performed per year by an organization

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

What role should the CISO play in properly scoping a PCI environment?

- A. Complete the self-assessment questionnaire and work with an Approved Scanning Vendor (ASV) to determine scope
- B. Work with a Qualified Security Assessor (QSA) to determine the scope of the PCI environment
- C. Validate the business units' suggestions as to what should be included in the scoping process
- D. Ensure internal scope validation is completed and that an assessment has been done to discover all credit card data

Suggested Answer: D

Community vote distribution

B (100%)

🗳️ 👤 **Abodi000** 12 months ago

Selected Answer: B

B. Work with a Qualified Security Assessor (QSA) to determine the scope of the PCI environment

Explanation:

The Chief Information Security Officer (CISO) plays a crucial role in ensuring that the organization properly scoping the PCI DSS (Payment Card Industry Data Security Standard) compliance process. While the CISO is responsible for overseeing security in the organization, when it comes to scoping a PCI environment, they should collaborate with a Qualified Security Assessor (QSA), who is a professional with the expertise to help define the scope of the environment, identify systems that process, store, or transmit cardholder data, and ensure proper security measures are implemented.

upvoted 1 times

🗳️ 👤 **Alex19741974** 1 year, 2 months ago

Selected Answer: B

Correct Answer : B. Work with a Qualified Security Assessor (QSA) to determine scope, D is wrong answer as of the wording of Credit Card Data Exist, that's trying to be compliant with PCI after the fact of implementing and process credit card

upvoted 1 times

🗳️ 👤 **arifbhatkar** 2 years, 6 months ago

Correct Answer : B. Work with a Qualified Security Assessor (QSA) to determine the scope of the PCI environment

upvoted 1 times

Which of the following reports should you as an IT auditor use to check on compliance with a Service Level Agreement (SLA) requirement for uptime?

- A. Systems logs
- B. Hardware error reports
- C. Availability reports
- D. Utilization reports

Suggested Answer: C

Currently there are no comments in this discussion, be the first to comment!

You work as a project manager for TYU project. You are planning for risk mitigation. You need to quickly identify high-level risks that will need a more in-depth analysis.

Which one of the following approaches would you use?

- A. Risk mitigation
- B. Estimate activity duration
- C. Quantitative analysis
- D. Qualitative analysis

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

A global health insurance company is concerned about protecting confidential information.

Which of the following is of MOST concern to this organization?

- A. Alignment with International Organization for Standardization (ISO) standards.
- B. Alignment with financial reporting regulations for each country where they operate.
- C. Compliance to the payment Card Industry (PCI) regulations.
- D. Compliance with patient data protection regulations for each country where they operate.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following represents the MOST negative impact resulting from an ineffective security governance program?

- A. Improper use of information resources
- B. Reduction of budget
- C. Decreased security awareness
- D. Fines for regulatory non-compliance

Suggested Answer: *D*

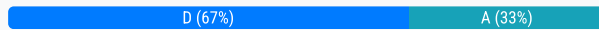
Currently there are no comments in this discussion, be the first to comment!

Within an organization's vulnerability management program, who has the responsibility to implement remediation actions?

- A. Data owner
- B. Data center manager
- C. Network architect
- D. System administrator

Suggested Answer: D

Community vote distribution



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

Selected Answer: D

The data Owner is accountable but not responsible. System admin. has the technical knowledge to implementation remediation.
upvoted 1 times

🗳️ 👤 **adv87** 1 year, 4 months ago

Selected Answer: D

Cannot be Data Owner. Anyone can be the owner of data (HR, Payroll, Marketing etc...). The best answer from options provided is D) Sys Admin, for the associated tasks mentioned in question
upvoted 1 times

🗳️ 👤 **JeBaCas** 1 year, 4 months ago

Syst Admin is the one managing the system, and Vuln management focuses on system and Apps vulns (no data vulns exist). On other side, DB owner is accountable for, whilst syst admin responsible for the action (RACI)
upvoted 1 times

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

Selected Answer: A

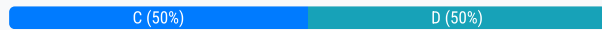
This is incorrect. According to the answers, the only possible one is Data Owner. What happens, when we are assessing a SaaS or PaaS platform for vulnerabilities? There is no infrastructure management, and there is no responsibility of System Administrator in some cases again for example Web Apps?
upvoted 1 times



The amount of risk an organization is willing to accept in pursuit of its mission is known as_____.

- A. risk transfer
- B. risk mitigation
- C. risk acceptance
- D. risk tolerance

Suggested Answer: D

Community vote distribution





  **Sean_P** 4 months, 2 weeks ago

Selected Answer: D

Risk tolerance refers to the specific level of risk an organization is willing to accept in pursuit of its objectives, essentially defining how much risk it is comfortable with.

upvoted 1 times

  **shiko81** 5 months, 1 week ago

Selected Answer: C

Risk tolerance is a deviation from risk appetite

upvoted 1 times

Which of the following is a critical operational component of an Incident Response Program (IRP)?

- A. Monthly program tests to ensure resource allocation is sufficient for supporting the needs of the organization.
- B. Weekly program budget reviews to ensure the percentage of program funding remains constant.
- C. Annual review of program charters, policies, procedures and organizational agreements.
- D. Daily monitoring of vulnerability advisories relating to your organization's deployed technologies.

Suggested Answer: D

Community vote distribution

C (100%)

🗳️ 👤 **Abodi000** 12 months ago

Selected Answer: C

C. Annual review of program charters, policies, procedures and organizational agreements.

Explanation:

A critical operational component of an Incident Response Program (IRP) is the annual review of program charters, policies, procedures, and organizational agreements. This ensures that the program stays up to date with the latest threat landscape, organizational changes, compliance requirements, and technological advancements. Regular reviews help in adapting the program to evolving risks and ensuring that all necessary stakeholders are aligned on the roles, responsibilities, and procedures in the event of a security incident.

upvoted 1 times

🗳️ 👤 **JeBaCas** 1 year, 4 months ago

monitoring of events is not an IR activity; event management performs that, and if not determined incident, IR team is not involved

upvoted 1 times

🗳️ 👤 **arifbhatkar** 2 years, 6 months ago

Correct Answer C. Annual review of program charters, policies, procedures and organizational agreements.

upvoted 2 times

What is the first thing that needs to be completed in order to create a security program for your organization?

- A. Security program budget
- B. Compliance and regulatory analysis
- C. Risk assessment
- D. Business continuity plan

Suggested Answer: C

🗨️ 👤 **JeBaCas** 1 year, 4 months ago

Risk Assessment includes identification of laws/regulatory requirements as well as contractual obligations (external Reqs)
upvoted 1 times

🗨️ 👤 **JeBaCas** 1 year, 4 months ago

as part of risk identification step
upvoted 1 times

As a new CISO at a large healthcare company you are told that everyone has to badge in to get in the building. Below your office window you notice a door that is normally propped open during the day for groups of people to take breaks outside. Upon looking closer, you see there is no badge reader.

What should you do?

- A. Post a guard at the door to maintain physical security
- B. Close and chain the door shut and send a company-wide memo banning the practice
- C. A physical risk assessment on the facility
- D. Nothing, this falls outside your area of influence

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

As the new CISO at the company you are reviewing the audit reporting process and notice that it includes only detailed technical diagrams. What else should be in the reporting process?

- A. Names and phone numbers of those who conducted the audit
- B. Executive summary
- C. Penetration test agreement
- D. Business charter

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following provides an audit framework?

- A. Control Objectives for IT (COBIT)
- B. International Organization Standard (ISO) 27002
- C. Payment Card Industry "Data Security Standard (PCI-DSS)
- D. National Institute of Standards and technology (NIST) SP 800-30

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following is used to establish and maintain a framework to provide assurance that information security strategies are aligned with organizational objectives?

- A. Governance
- B. Compliance
- C. Awareness
- D. Management

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following is the MOST important goal of risk management?

- A. Finding economic balance between the impact of the risk and the cost of the control
- B. Identifying the victim of any potential exploits
- C. Identifying the risk
- D. Assessing the impact of potential threats

Suggested Answer: A

  **JeBaCas** 1 year, 4 months ago

I thing is D: assessing threats and pot consequences is main goal of RM, to manage risk. balance impact and cost of controls is a CBA part of risk treatment decision.

upvoted 1 times

What is the SECOND step to creating a risk management methodology according to the National Institute of Standards and Technology (NIST) SP 800-30 standard?

- A. Mitigate risk
- B. Perform a risk assessment
- C. Determine appetite
- D. Evaluate risk avoidance criteria

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **velasco** Highly Voted 4 years, 7 months ago

The Correct Answer is B. Perform the risk Assessment (NIST Special Publication 800-30 which describes the process of assessing information security risk in support goal defined in SP 800-37 and SP 800-39 and include 4 Step: 1- Prepare for Assessment, 2- Conduct Assessment, 3- Communicate results and 4- Maintain Assessment)

upvoted 7 times

🗳️ 👤 **bobby_kl** Most Recent 1 year, 5 months ago

Selected Answer: B

B. Perform a risk assessment

upvoted 1 times

🗳️ 👤 **VOAKDO_cciso** 1 year, 7 months ago

Selected Answer: B

According to NIST 800-30: (<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>)

Risk management processes include: (i) framing risk; (ii) assessing risk; (iii) responding to risk; and (iv) monitoring risk.

B=assessing risk

upvoted 3 times

🗳️ 👤 **Pika26** 1 year, 9 months ago

Answer is B. The National Institute of Standards and Technology (NIST) SP 800-30 standard provides guidance on creating a risk management methodology. The second step in this process is to perform a risk assessment, which involves identifying and analyzing potential risks to the organization's assets, operations, and individuals. This step helps to determine the likelihood and potential impact of these risks and enables organizations to prioritize their risk management efforts.

upvoted 1 times

🗳️ 👤 **Rufus1** 3 years, 2 months ago

Hypothetically,

If question would have been "What is the SECOND step to creating a risk management methodology according to ISO-27005 ?"

The answer is B - Risk Assessment

upvoted 1 times

🗳️ 👤 **letsdoitnow** 3 years, 6 months ago

I agree with you. Mitigation should be part of maintaining risk assessment which is the 4th step.

upvoted 1 times

Which of the following tests is performed by an Information Systems (IS) auditor when a sample of programs is selected to determine if the source and object versions are the same?

- A. A substantive test of program library controls
- B. A compliance test of the program compiler controls
- C. A compliance test of program library controls
- D. A substantive test of the program compiler controls

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ 👤 **Perseus_68** 1 year, 4 months ago

Selected Answer: C

Compliance because it's versioning only. If it was the code itself and if it was built right or something happened in the compiling that created an issue, that would be substantive.

upvoted 1 times

🗨️ 👤 **ONERAPTOR** 1 year, 7 months ago

The correct answer is C. A compliance test of program library controls.

This type of test is conducted by an IS auditor to verify that the controls over the program library are effective. Specifically, by comparing the source and object versions of a sample of programs, the auditor can determine if the programs have been properly maintained and updated in the library. This helps ensure that the programs in use are the authorized and most current versions, which is a crucial aspect of maintaining the integrity and reliability of information systems. Compliance tests are focused on the effectiveness of the controls in place, rather than on the accuracy of the data, which is the focus of substantive tests.

upvoted 1 times

🗨️ 👤 **arifbhatkar** 2 years ago

Correct answer A. A substantive test of program library controls

when an IS auditor selects a sample of programs to determine if the source and object versions are the same, they would perform a substantive test of program library controls. This involves examining the controls and processes related to the program library, such as version control, change management, and documentation practices. The purpose of this test is to verify that the programs stored in the library are the correct and authorized versions, ensuring the integrity and reliability of the software used within the organization.

upvoted 1 times

When creating a vulnerability scan schedule, who is the MOST critical person to communicate with in order to ensure impact of the scan is minimized?

- A. The asset manager
- B. The project manager
- C. The asset owner
- D. The data custodian

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

What two methods are used to assess risk impact?

- A. Quantitative and qualitative
- B. Qualitative and percent of loss realized
- C. Subjective and Objective
- D. Cost and annual rate of expectance

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

An organization information security policy serves to_____.

- A. define security configurations for systems
- B. establish budgetary input in order to meet compliance requirements
- C. establish acceptable systems and user behavior
- D. define relationships with external law enforcement agencies
- E. None

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

An IT auditor has recently discovered that because of a shortage of skilled operations personnel, the security administrator has agreed to work one late night shift a week as the senior computer operator.

The most appropriate course of action for the IT auditor is to:

- A. Review the system log for each of the late night shifts to determine whether any irregular actions occurred.
- B. Inform senior management of the risk involved.
- C. Develop a computer-assisted audit technique to detect instances of abuses of the arrangement.
- D. Agree to work with the security officer on these shifts as a form of preventative control.

Suggested Answer: *B*

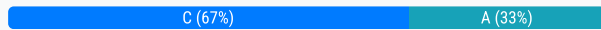
Currently there are no comments in this discussion, be the first to comment!

The patching and monitoring of systems on a consistent schedule is required by?

- A. Industry best practices
- B. Audit best practices
- C. Risk Management framework
- D. Local privacy laws

Suggested Answer: C

Community vote distribution



🗨️ **adv87** 1 year, 4 months ago

Selected Answer: C

"Best practice" is not a requirement, it's a guideline. A framework contains requirements in order to meet compliance under that framework
upvoted 2 times

🗨️ **kaibutsu** 2 years, 5 months ago

Is the answer C because it uses the phrase "required by?"
upvoted 2 times

🗨️ **bobby_kl** 2 years, 5 months ago

Selected Answer: A

A. Industry best practices
upvoted 1 times

🗨️ **arifbhatkar** 2 years, 6 months ago

Correct answer A. Industry best practices

The patching and monitoring of systems on a consistent schedule is required by industry best practices. Industry standards and guidelines, such as those provided by organizations like the National Institute of Standards and Technology (NIST), the Center for Internet Security (CIS), and the International Organization for Standardization (ISO), emphasize the importance of regular patching and monitoring as fundamental security practices
upvoted 2 times

IT control objectives are useful to IT auditors as they provide the basis for understanding the:

- A. The audit control checklist
- B. Technique for securing information
- C. Desired results or purpose of implementing specific control procedures.
- D. Security policy

Suggested Answer: *C*

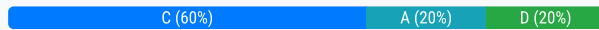
Currently there are no comments in this discussion, be the first to comment!

Which of the following activities results in change requests?

- A. Corrective actions
- B. Defect repair
- C. Preventive actions
- D. Inspection

Suggested Answer: C

Community vote distribution



ME79 10 months, 1 week ago

Selected Answer: D

Incorrectly worded question. Correct wording should be: Which of the following activities does NOT result in a change request?

D. Inspection (is the correct answer in this case.)

A change request is a formal proposal to make a change on the project, and per the PMBOK® Guide Sixth Edition "may be a corrective action, a preventive action, or a defect repair" (pg. 93).

Otherwise this question would be looking for A, B and C (but since this exam is single answer, it should be D.)

upvoted 1 times

musagul 1 year, 4 months ago

Selected Answer: C

You must create a change request when you are doing preventive action. Because the "preventive action" can prevent legal business processes. C is Correct.

upvoted 1 times

MJ_Sr 1 year, 6 months ago

This should actually be "B". A defect repair results in a change request ticket. Corrective actions would happen after and preventive actions happen before.

upvoted 1 times

RC2073 1 year, 10 months ago

Selected Answer: C

C is correct per other Q&A sites online

upvoted 1 times

kaibutsu 1 year, 11 months ago

I think we need more context. I can see A or C. If it said "Emergency Change" then I would say "Corrective."

upvoted 3 times

Jesse572 1 year, 12 months ago

Selected Answer: A

We know Inspection is not it for sure. Defect repair create work orders to repair / replace items. Preventive actions are already implemented and prevent users / systems from performing specific functions. I would have to state the answer is Corrective Actions.

upvoted 1 times

arifbhatkar 2 years ago

A. Corrective actions

Corrective actions involve addressing identified issues or problems within a system or process to prevent their recurrence. When corrective actions are implemented, they often require change requests to modify the existing system or process. These change requests capture the necessary modifications or updates needed to rectify the identified issues and improve the overall performance or functionality. Therefore, corrective actions typically lead to change requests as part of the process for implementing the necessary changes.

upvoted 2 times

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

Selected Answer: C

corrective=after a problem happens .

preventive=before a problem happens .

Here, it does not say when,....., it supposes before

upvoted 1 times

🗨️ 👤 **Examal** 2 years, 2 months ago

A, Preventive actions may not alter any changes or even may the require any reboots or resets.

upvoted 1 times

🗨️ 👤 **Pika26** 2 years, 3 months ago

Answer should be A, corrective actions. Corrective actions are activities taken to address identified problems, issues, or defects that have occurred during the project execution. These activities may result in change requests, which are formal proposals to modify any project document, deliverable, or baseline.

upvoted 3 times

What is the MAIN reason for conflicts between Information Technology and Information Security programs?

- A. The effective implementation of security controls can be viewed as an inhibitor to rapid Information technology implementations.
- B. Technology Governance is focused on process risks whereas Security Governance is focused on business risk.
- C. Technology governance defines technology policies and standards while security governance does not.
- D. Security governance defines technology best practices and Information Technology governance does not.

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following is the MOST important for a CISO to understand when identifying threats?

- A. How the security operations team will behave to reported incidents
- B. How vulnerabilities can potentially be exploited in systems that impact the organization
- C. How the firewall and other security devices are configured to prevent attacks
- D. How the incident management team prepares to handle an attack

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Who is responsible for securing networks during a security incident?

- A. Security Operations Center (SOC)
- B. Chief Information Security Officer (CISO)
- C. Disaster Recovery (DR) manager
- D. Incident response Team (IRT)

Suggested Answer: *D*

🗨️ 👤 **JeBaCas** 1 year, 4 months ago

Initially network config is addressed by Network team, as well as System config by IT team in close collaboration with IR team. IRT is not responsible for configuring net devices/systems even during an incident (usually)

upvoted 1 times

🗨️ 👤 **moodi5005** 1 year, 6 months ago

The correct Answer is C

upvoted 1 times

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

A disaster is not necessarily caused by a security incident.

upvoted 1 times

What is the BEST way to achieve on-going compliance monitoring in an organization?

- A. Outsource compliance to a 3 rd party vendor and let them manage the program.
- B. Have Compliance Direct Information Security to fix issues after the auditor's report.
- C. Only check compliance right before the auditors are scheduled to arrive onsite.
- D. Have Compliance and Information Security partner to correct issues as they arise.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

The success of the Chief Information Security Officer is MOST dependent upon:

- A. following the recommendations of consultants and contractors
- B. raising awareness of security issues with end users
- C. favorable audit findings
- D. development of relationships with organization executives

Suggested Answer: *D*

  **musagul** 1 year, 4 months ago

I can not say which one is MOST but i can say that developing relationship with organization executives is LESS than other choices.
upvoted 1 times

During the course of a risk analysis your IT auditor identified threats and potential impacts. Next, your IT auditor should:

- A. Identify and assess the risk assessment process used by management.
- B. Identify and evaluate existing controls.
- C. Identify information assets and the underlying systems.
- D. Disclose the threats and impacts to management.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is a fundamental component of an audit record?

- A. Originating IP-Address
- B. Date and time of the event
- C. Failure of the event
- D. Authentication type

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

What is the main purpose of the Incident Response Team?

- A. Communicate details of information security incidents
- B. Create effective policies detailing program activities
- C. Ensure efficient recovery and reinstate repaired systems
- D. Provide effective employee awareness programs

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Risk appetite directly affects what part of a vulnerability management program?

- A. Scope
- B. Schedule
- C. Staff
- D. Scan tools

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

Creating a secondary authentication process for network access would be an example of?

- A. An administrator with too much time on their hands
- B. Supporting the concept of layered security
- C. Network segmentation
- D. Putting undue time commitment on the system administrator

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

According to ISO 27001, of the steps for establishing an Information Security Governance program listed below, which comes first?

- A. Decide how to manage risk
- B. Define Information Security Policy
- C. Identify threats, risks, impacts and vulnerabilities
- D. Define the budget of the Information Security Management System

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following functions **MUST** your Information Security Governance program include for formal organizational reporting?

- A. Human Resources and Budget
- B. Audit and Legal
- C. Budget and Compliance
- D. Legal and Human Resources

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

The implementation of anti-malware and anti-phishing controls on centralized email servers is an example of what type of security control?

- A. Technical control
- B. Management control
- C. Procedural control
- D. Organization control

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following is a term related to risk management that represents the estimated frequency at which a threat is expected to transpire?

- A. Temporal Probability (TP)
- B. Annualized Rate of Occurrence (ARO)
- C. Single Loss Expectancy (SLE)
- D. Exposure Factor (EF)

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

A security officer wants to implement a vulnerability scanning program. The officer is uncertain of the state of vulnerability resiliency within the organization's large IT infrastructure.

What would be the BEST approach to minimize scan data output while retaining a realistic view of system vulnerability?

- A. Decrease the vulnerabilities within the scan tool settings
- B. Scan a representative sample of systems
- C. Filter the scan output so only pertinent data is analyzed
- D. Perform the scans only during off-business hours

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

What should an organization do to ensure that they have a sound Business Continuity (BC) Plan?

- A. Conduct a Disaster Recovery (DR) exercise every year to test the plan
- B. Conduct periodic tabletop exercises to refine the BC plan
- C. Test every three years to ensure that the BC plan is valid
- D. Define the Recovery Point Objective (RPO)

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ 👤 **Bettoxicity** 1 year ago

Selected Answer: B

Periodic reviews is better than annual or long time reviews.

upvoted 1 times

🗨️ 👤 **Bto881** 1 year, 3 months ago

A should be correct.

upvoted 1 times

According to the National Institute of Standards and Technology (NIST) SP 800-40, which of the following considerations are MOST important when creating a vulnerability management program?

- A. Susceptibility to attack, expected duration of attack, and mitigation availability
- B. Attack vectors, controls cost, and investigation staffing needs
- C. Susceptibility to attack, mitigation response time, and cost
- D. Vulnerability exploitation, attack recovery, and mean time to repair

Suggested Answer: C

Currently there are no comments in this discussion, be the first to comment!

When deploying an Intrusion Prevention System (IPS), the BEST way to get maximum protection from the system is to deploy it_____

- A. In-line and turn on alert mode to stop malicious traffic.
- B. In promiscuous mode and block malicious traffic.
- C. In promiscuous mode and only detect malicious traffic.
- D. In-line and turn on blocking mode to stop malicious traffic in-line.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is a weakness of an asset or group of assets that can be exploited by one or more threats?

- A. Vulnerability
- B. Threat
- C. Exploitation
- D. Attack vector

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

How often should an environment be monitored for cyber threats, risks, and exposures?

- A. Weekly
- B. Daily
- C. Monthly
- D. Quarterly

Suggested Answer: *B*

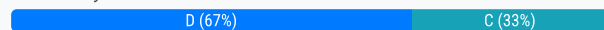
Currently there are no comments in this discussion, be the first to comment!

Many times a CISO may have to speak to the Board of Directors (BOD) about their cyber security posture. What would be the BEST choice of security metrics to present to the BOD?

- A. All vulnerabilities found on servers and desktops
- B. Only critical and high vulnerabilities servers
- C. Only critical and high vulnerabilities on servers and desktops
- D. All vulnerabilities that impact important production servers

Suggested Answer: B

Community vote distribution



🗨️ 👤 **Bettoxicity** 1 year ago

Selected Answer: C

Why not B?: Only critical and high vulnerabilities on servers: While focusing on servers is important, desktops can also present significant risks, especially with a remote workforce. Excluding desktops would present an incomplete picture.

upvoted 1 times

🗨️ 👤 **e8ab9ae** 1 year, 1 month ago

Selected Answer: D

all vulnerabilities that impact, means high, no ??

upvoted 2 times

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

This question and answers are poorly written.

upvoted 1 times

Creating a secondary authentication process for network access would be an example of?

- A. Defense in depth cost enumerated costs
- B. Nonlinearities in physical security performance metrics
- C. System hardening and patching requirements
- D. Anti-virus for mobile devices

Suggested Answer: A

Community vote distribution

A (83%)

C (17%)

  **ME79** 10 months, 1 week ago

Selected Answer: C

Implementing a secondary authentication process (such as multi-factor authentication (MFA)) enhances security by adding another layer of protection to network access. This falls under system hardening, which refers to implementing security measures to reduce vulnerabilities in IT systems.

Key aspects of system hardening include:

- Enforcing strong authentication mechanisms (e.g., MFA, biometrics, smart cards).
- Applying security patches and updates to mitigate vulnerabilities.
- Disabling unnecessary services and protocols to reduce the attack surface.
- Implementing least privilege access control to limit user permissions.

This aligns with NIST SP 800-53 (AC-17, IA-2) and ISO 27001 Annex A.9 (Access Control), which emphasize securing network access through authentication and system hardening practices.

upvoted 1 times

  **nshams** 1 year, 5 months ago

Selected Answer: A

sec authentication is an added sec feature underlying defense in depth concept

upvoted 1 times

  **johndoe69** 1 year, 7 months ago

Selected Answer: A

A. Defense in depth cost enumerated costs

Defense in depth is a cybersecurity strategy that employs multiple layers of security controls (defenses) to protect information and resources. Implementing a secondary authentication process is a classic example of adding an additional layer of security, enhancing the overall security posture by requiring multiple factors to authenticate users. This approach ensures that even if one layer of defense (e.g., primary authentication) is compromised, other layers (e.g., secondary authentication) provide additional protection.

upvoted 1 times

  **musagul** 1 year, 10 months ago

Selected Answer: A

Correct answer is A

upvoted 1 times

  **Otto_Aulicino** 4 years ago

Selected Answer: A

Each letter here seem to have more than one answer. This is either layered security or MFA or similar.

upvoted 2 times

  **shay5** 4 years, 10 months ago

This is layered security.

upvoted 1 times

In MOST organizations which group periodically reviews network intrusion detection system logs for all systems as part of their daily tasks?

- A. Internal Audit
- B. Information Security
- C. Compliance
- D. Database Administration



Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following BEST describes an international standard framework that is based on the security model Information Technology-Code of Practice for Information Security Management?

- A. National Institute of Standards and technology Special Publication SP 800-12
- B. Request for Comment 2196
- C. International Organization for Standardization 27001
- D. National Institute of Standards and technology Special Publication SP 800-26

Suggested Answer: C

  **tnagy** 1 year, 3 months ago

The answer is partially correct. It should be ISO 27002 not 27001.

upvoted 1 times

The BEST organization to provide a comprehensive, independent and certifiable perspective on established security controls in an environment is _____.

- A. External Audit
- B. Forensic experts
- C. Internal Audit
- D. Penetration testers

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

When a critical vulnerability has been discovered on production systems and needs to be fixed immediately, what is the BEST approach for a CISO to mitigate the vulnerability under tight budget constraints?

- A. Schedule an emergency meeting and request the finding to fix the issue
- B. Take the system off line until budget is available
- C. Transfer financial resources from other critical programs
- D. Deploy countermeasures and compensation controls until the budget is available

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

The executive board has requested that the CISO of an organization define and Key Performance Indicators (KPI) to measure the effectiveness of the security awareness program provided to call center employees.

Which of the following can be used as a KPI?

- A. Number of successful social engineering attempts on the call center
- B. Number of callers who abandon the call before speaking with a representative
- C. Number of callers who report a lack of customer service from the call center
- D. Number of callers who report security issues.

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

The effectiveness of social engineering penetration testing using phishing can be used as a Key Performance Indicator (KPI) for the effectiveness of an organization's

- A. Risk Management Program
- B. Anti-Spam controls
- C. Identity and Access Management Program
- D. Security Awareness Program

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is the MOST effective way to measure the effectiveness of security controls on a perimeter network?

- A. Perform a vulnerability scan of the network
- B. Internal Firewall ruleset reviews
- C. Implement network intrusion prevention systems
- D. External penetration testing by a qualified third party

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

The CIO of an organization has decided to assign the responsibility of internal IT audit to the IT team. This is considering a bad practice MAINLY because_____.

- A. The IT team is not familiar in IT audit practices
- B. This represents a bad implementation of the Least Privilege principle
- C. The IT team is not certified to perform audits
- D. This represents a conflict of interest

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following activities is the MAIN purpose of the risk assessment process?

- A. Creating an inventory of information assets
- B. Calculating the risks to which assets are exposed in their current setting
- C. Classifying and organizing information assets into meaningful groups
- D. Assigning value to each information asset

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

You are the Chief Information Security Officer of a large, multinational bank and you suspect there is a flaw in a two factor authentication token management process.

Which of the following represents your BEST course of action?

- A. Determine program ownership to implement compensating controls
- B. Send a report to executive peers and business unit owners detailing your suspicions
- C. Validate that security awareness program content includes information about the potential vulnerability
- D. Conduct a throughout risk assessment against the current implementation to determine system functions

Suggested Answer: *D*

  **Billsss** 1 year, 1 month ago

Correct answer should say "Conduct a thorough risk assessment against the current implementation to determine system functions"
upvoted 2 times

Which of the following is considered to be an IT governance framework and a supporting toolset that allows for managers to bridge the gap between control requirements, technical issues, and business risks?

- A. Information technology Infrastructure Library (ITIL)
- B. Committee of Sponsoring Organizations (COSO)
- C. Control Objective for Information Technology (COBIT)
- D. Payment Card Industry (PCI)

Suggested Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which is the BEST solution to monitor, measure, and report changes to critical data in a system?

- A. SNMP traps
- B. Syslog
- C. File integrity monitoring
- D. Application logs

Suggested Answer: C

Community vote distribution

D (100%)

  **never64738** 9 months, 2 weeks ago

Selected Answer: D

File Integrity Monitoring (FIM) use hashing on file that shouldn't change frequently. Using this technique on data results in frequent false-positive alerts (alert fatigue).

Application logs monitoring ("D") seems to be the best choice.

upvoted 1 times

Which of the following represents the BEST reason for an organization to use the Control Objectives for Information and Related Technology (COBIT) as an Information Technology (IT) framework?

- A. Information Security (IS) procedures often require augmentation with other standards
- B. Implementation of it eases an organization's auditing and compliance burden
- C. It provides for a consistent and repeatable staffing model for technology organizations
- D. It allows executives to more effectively monitor IT implementation costs

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

The mean time to patch, number of virus outbreaks prevented, and number of vulnerabilities mitigated are examples of what type of performance metrics?

- A. Risk metrics
- B. Operational metrics
- C. Compliance metrics
- D. Management metrics

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

When should IT security project management be outsourced?

- A. On projects not forecasted in the yearly budget
- B. When organizational resources are limited
- C. When the benefits of outsourcing outweigh the inherent risks of outsourcing
- D. On new, enterprise-wide security initiatives

Suggested Answer: C

Currently there are no comments in this discussion, be the first to comment!

Assigning the role and responsibility of Information Assurance to a dedicated and independent security group is an example of:

- A. Detective Controls
- B. Proactive Controls
- C. Organizational Controls
- D. Preemptive Controls

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

An international organization is planning a project to implement encryption technologies to protect company confidential information. This organization has data centers on three continents.

Which of the following would be considered a MAJOR constraint for the project?

- A. Compliance to local hiring laws
- B. Encryption import/export regulations
- C. Local customer privacy laws
- D. Time zone differences

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

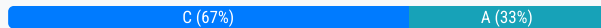
A new CISO just started with a company and on the CISO's desk is the last complete Information Security Management audit report. The audit report is over two years old.

After reading it, what should be your first priority?

- A. Review the recommendations and follow up to see if audit implemented the changes
- B. Meet with audit team to determine a timeline for corrections
- C. Have internal audit conduct another audit to see what has changed.
- D. Contract with an external audit company to conduct an unbiased audit

Suggested Answer: A

Community vote distribution



🗲️ 👤 **Betotoxicity** 1 year ago

Selected Answer: C

Why not A: While reviewing recommendations is valuable, it doesn't provide insights into new risks or changes that have occurred since the last audit.
upvoted 1 times

🗲️ 👤 **alfaMegatron** 1 year, 4 months ago

Selected Answer: C

Audit does not implement changes
upvoted 1 times

🗲️ 👤 **Emporeo** 1 year, 10 months ago

C audit does not implement changes
upvoted 1 times

🗲️ 👤 **RC2073** 2 years, 3 months ago

Selected Answer: A

A is correct. I confirmed the same answer on another website.
upvoted 1 times

🗲️ 👤 **Kentish** 2 years, 9 months ago

Audit wouldn't be implementing the changes, it should be reviewing the actions with the internal team to see what they have implemented.
upvoted 2 times

🗲️ 👤 **jaaf** 3 years ago

It should be C
upvoted 4 times

The risk found after a control has been fully implemented is called:

- A. Total Risk
- B. Transferred Risk
- C. Residual Risk
- D. Post Implementation Risk

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Which of the following set of processes is considered to be one of the cornerstone cycles of the International Organization for Standardization (ISO) 27001 standard?

- A. Plan-Check-Do-Act
- B. Plan-Select-Implement-Evaluate
- C. Plan-Do-Check-Act
- D. SCORE (Security Consensus Operational Readiness Evaluation)

Suggested Answer: *C*

  **Emporeo** 1 year, 3 months ago

doubled correct answer

upvoted 1 times

A recent audit has identified a few control exceptions and is recommending the implementation of technology and processes to address the finding.

Which of the following is the MOST likely reason for the organization to reject the implementation of the recommended technology and processes?

- A. The organization has purchased cyber insurance
- B. The risk tolerance of the organization permits this risk
- C. The CIO of the organization disagrees with the finding
- D. The auditors have not followed proper auditing processes

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

When you develop your audit remediation plan what is the MOST important criteria?

- A. To validate the remediation process with the auditor.
- B. To validate that the cost of the remediation is less than risk of the finding.
- C. To remediate half of the findings before the next audit.
- D. To remediate all of the findings before the next audit.

Suggested Answer: B

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

You is referred as CISO. The correct answer is B.
upvoted 1 times

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

Auditor will not be going through the remediation process, may guide though, but cares whether the risk is taken care of.
upvoted 1 times

🗨️ 👤 **Ludikraut** 2 years, 5 months ago

Within this context, I disagree that B is the best answer. Audit is often tied to regulatory or legal compliance, in which case cost is not the primary consideration and answer A would be better IMO.
upvoted 1 times

To have accurate and effective information security policies how often should the CISO review the organization policies?

- A. Before an audit
- B. At least once a year
- C. Quarterly
- D. Every 6 months

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

When a CISO considers delaying or not remediating system vulnerabilities which of the following are MOST important to take into account?

- A. Threat Level, Risk of Compromise, and Consequences of Compromise
- B. Risk Avoidance, Threat Level, and Consequences of Compromise
- C. Reputational Impact, Financial impact, and Risk of Compromise
- D. Risk transfer, reputational Impact, and Consequences of Compromise

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

When managing the critical path of an IT security project, which of the following is MOST important?

- A. Knowing all the stakeholders.
- B. Knowing the milestones and timelines of deliverables.
- C. Knowing the people on the data center team.
- D. Knowing the threats to the organization.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Creating good security metrics is essential for a CISO. What would be the BEST sources for creating security metrics for baseline defenses coverage?

- A. Servers, routers, switches, modem
- B. Firewall, anti-virus console, IDS, syslog
- C. Firewall, exchange, web server, intrusion detection system (IDS)
- D. IDS, syslog, router, switches

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

A Chief Information Security Officer received a list of high, medium, and low impact audit findings.


Which of the following represents the BEST course of action?

- A. If the findings do not impact regulatory compliance, remediate only the high and medium risk findings.
- B. If the findings do not impact regulatory compliance, review current security controls.
- C. If the findings impact regulatory compliance, try to apply remediation that will address the most findings for the least cost.
- D. If the findings impact regulatory compliance, remediate the high findings as quickly as possible.

Suggested Answer: D

Community vote distribution

C (100%)

 **ME79** 10 months, 1 week ago

Selected Answer: C

As a Chief Information Security Officer (CISO), the best course of action is to prioritize risk remediation based on compliance, impact, and cost-effectiveness. If the audit findings impact regulatory compliance, the organization must address them to avoid legal, financial, and reputational consequences.

A risk-based approach means:

- Prioritizing remediation to meet compliance requirements.
- Optimizing resources by implementing solutions that address multiple findings at once.
- Ensuring cost-effective security improvements that align with business objectives.

By applying remediation strategies that cover multiple findings efficiently, the CISO ensures regulatory compliance, risk reduction, and resource optimization.

This aligns with NIST Risk Management Framework (RMF) and ISO 27001 Annex A.12 (Security Operations), which emphasize cost-effective risk mitigation while ensuring compliance.

upvoted 1 times

At which point should the identity access management team be notified of the termination of an employee?

- A. Immediately so the employee account(s) can be disabled
- B. During the monthly review cycle
- C. At the end of the day once the employee is off site
- D. Before an audit

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

Providing oversight of a comprehensive information security program for the entire organization is the primary responsibility of which group under the InfoSec governance framework?

- A. Office of the General Counsel
- B. Office of the Auditor
- C. Senior Executives
- D. All employees and users

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Which International Organization for Standardization (ISO) below BEST describes the performance of risk management, and includes a five-stage risk management methodology.

- A. ISO 27005
- B. ISO 27004
- C. ISO 27002
- D. ISO 27001

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

With respect to the audit management process, management response serves what function?

- A. revealing the "root cause" of the process failure and mitigating for all internal and external units
- B. adding controls to ensure that proper oversight is achieved by management
- C. determining whether or not resources will be allocated to remediate a finding
- D. placing underperforming units on notice for failing to meet standards

Suggested Answer: C

Currently there are no comments in this discussion, be the first to comment!

The remediation of a specific audit finding is deemed too expensive and will not be implemented.
Which of the following is a TRUE statement?

- A. The audit findings is incorrect
- B. The asset is more expensive than the remediation
- C. The asset being protected is less valuable than the remediation costs
- D. The remediation costs are irrelevant; it must be implemented regardless of cost.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Which of the following organizations is typically in charge of validating the implementation and effectiveness of security controls?

- A. Security Operations
- B. Internal/External Audit
- C. Risk Management
- D. Security Administrators

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

An information security department is required to remediate system vulnerabilities when they are discovered. Please select the three primary remediation methods that can be used on an affected system.

- A. Install software patch, configuration adjustment, software removal
- B. Install software patch, operate system, maintain system
- C. Discover software, remove affected software, apply software patch
- D. Software removal, install software patch, maintain system

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ 👤 **kenCISSP** 1 year, 1 month ago

Selected Answer: A

vulnerability is caused by two major reasons, first one is the product weakness (so you need to patch or upgrade), the second one is wrong configuration (that's why you need to disable the unnecessary service/port and change the default password setting).

upvoted 1 times

🗨️ 👤 **Examal** 2 years, 2 months ago

A, operation is not remediation

upvoted 1 times

🗨️ 👤 **ironman_86** 2 years, 4 months ago

I think it should be B not A.

upvoted 1 times

Which of the following best describes the purpose of the International Organization for Standardization (ISO) 27002 standard?

- A. To provide effective security management practice and to provide confidence in interorganizational dealings
- B. To establish guidelines and general principles for initiating, implementing, maintaining and improving information security management within an organization
- C. To give information security management recommendations to those who are responsible for initiating, implementing, or maintaining security in their organization.
- D. To provide a common basis for developing organizational security standards

Suggested Answer: B

Currently there are no comments in this discussion, be the first to comment!

Which represents PROPER separation of duties in the corporate environment?

- A. Information Security and Network teams perform two distinct functions
- B. Information Security and Identity Access Management teams perform two distinct functions
- C. Finance has access to Human Resources data
- D. Developers and Network teams both have admin rights on servers

Suggested Answer: B

Community vote distribution

B (100%)

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

Selected Answer: B

Both A and B looks correct. But B is more realistic given the context.

upvoted 1 times

🗨️ 👤 **johndoe69** 1 year, 5 months ago

Selected Answer: B

Proper Separation of Duties: Separation of duties (SoD) is a key principle in internal controls that ensures no single individual has control over all aspects of any critical function or process. This principle helps prevent fraud, errors, and conflicts of interest.

Information Security and Identity Access Management (IAM): These two teams perform distinct functions. Information Security is responsible for the overall security posture, policies, and incident response, while IAM focuses specifically on managing user identities and access privileges. Separating these duties helps ensure that no single team has too much control over both the security policies and the access to critical systems.

upvoted 2 times

🗨️ 👤 **nshams** 1 year, 5 months ago

B is correct

upvoted 1 times

🗨️ 👤 **arifbhatkar** 2 years, 6 months ago

The correct answer is B. Information Security and Identity Access Management teams perform two distinct functions.

Proper separation of duties is an important principle in the corporate environment to ensure accountability, prevent conflicts of interest, and reduce the risk of fraud or unauthorized activities. The separation of duties involves dividing responsibilities among different individuals or teams to create checks and balances. By separating the responsibilities of Information Security and Identity Access Management teams, it ensures that there is a clear distinction between the functions related to securing information and managing user access

Option A is not a complete separation as both Information Security and Network teams may have overlapping responsibilities and access to sensitive information

upvoted 1 times

When working in the Payment Card Industry (PCI), how often should security logs be review to comply with the standards?

- A. Monthly
- B. Hourly
- C. Weekly
- D. Daily

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

The MOST common method to get an unbiased measurement of the effectiveness of an Information Security Management System (ISMS) is to_____.

- A. assign the responsibility to the information security team
- B. assign the responsibility to the team responsible for the management of the controls
- C. perform an independent audit of the security controls
- D. create operational reports on the effectiveness of the controls.

Suggested Answer: C

Currently there are no comments in this discussion, be the first to comment!

The ultimate goal of an IT security projects is:

- A. Support business requirements
- B. Implement information security policies
- C. Increase stock value
- D. Complete security

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

An organization has implemented a change management process for all changes to the IT production environment. This change management process follows best practices and is expected to help stabilize the availability and integrity of the organization's IT environment. Which of the following can be used to measure the effectiveness of this newly implemented process?

- A. Number and length of planned outages
- B. Number of change orders processed
- C. Number of change orders rejected
- D. Number of unplanned outages

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

You have implemented the new controls. What is the next step?

- A. Perform a risk assessment
- B. Monitor the effectiveness of the controls
- C. Document the process for the stakeholders
- D. Update the audit findings report

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Step-by-step procedures to regain normalcy in the event of a major earthquake is PRIMARILY covered by which of the following plans?

- A. Damage control plan
- B. Disaster recovery plan
- C. Business Continuity plan
- D. Incident response plan

Suggested Answer: B

🗨️ 👤 **Kentish** 1 year, 2 months ago

It isn't a very clear question, but typically DR is for technical recovery and BCP for business processes including technical DR. I would say the correct answer is C

upvoted 1 times

🗨️ 👤 **CYNLEE** 1 year, 3 months ago

BCP covers resume minimal business operations under disaster, but not necessary refer to back to normal.

upvoted 1 times

🗨️ 👤 **CYNLEE** 1 year, 3 months ago

Answer is B

upvoted 1 times

🗨️ 👤 **Avinash75** 1 year, 11 months ago

The key word here is return to normalcy. DRP ensures return to normalcy. BCP Would be mainly concerned about continuing business operations of critical functions at reduced operational capacity.

upvoted 2 times

🗨️ 👤 **Rufus1** 2 years, 8 months ago

I would say the same, Correct answer C

upvoted 2 times

🗨️ 👤 **UNN_CCISO** 2 years, 9 months ago

The question does not state the word "technical" and hence is there a reason why Business Continuity Plan is not the correct answer? DR comes under BCP.

upvoted 3 times

An employee successfully avoids becoming a victim of a sophisticated spear phishing attack due to knowledge gained through the corporate information security awareness program.

What type of control has been effectively utilized?

- A. Technical Control
- B. Management Control
- C. Operational Control
- D. Training Control

Suggested Answer: C

Community vote distribution

C (100%)

🗲️ 👤 **tnagy** 2 years, 2 months ago

Selected Answer: C

Operational Control as per official material and NIST SP 800-26
upvoted 1 times

🗲️ 👤 **Pika26** 2 years, 3 months ago

Answer should be training control.
upvoted 3 times

🗲️ 👤 **Emporeo** 1 year, 3 months ago

A training control does not exist
upvoted 2 times

A system was hardened at the Operating System level and placed into the production environment. Months later an audit was performed and it identified insecure configuration different from the original hardened state.

Which of the following security issues is the MOST likely reason leading to the audit findings?

- A. Lack of asset management processes
- B. Lack of hardening standards
- C. Lack of proper access controls
- D. Lack of change management processes

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

When is an application security development project complete?

- A. When the application turned over to production.
- B. After one year
- C. When the application reaches the maintenance phase.
- D. When the application is retired.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

An audit was conducted and many critical applications were found to have no disaster recovery plans in place. You conduct a Business Impact Analysis (BIA) to determine impact to the company for each application.

What should be the NEXT step?

- A. Create technology recovery plans
- B. Determine the annual loss expectancy (ALE)
- C. Build a secondary hot site
- D. Create a crisis management plan

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following activities must be completed BEFORE you can calculate risk?

- A. Assigning a value to each information asset
- B. Assessing the relative risk facing the organization's information assets
- C. Determining the likelihood that vulnerable systems will be attacked by specific threats
- D. Calculating the risks to which assets are exposed in their current setting

Suggested Answer: A

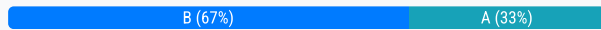
Currently there are no comments in this discussion, be the first to comment!

Which of the following are primary concerns for management with regard to assessing internal control objectives?

- A. Confidentiality, Availability, Integrity
- B. Compliance, Effectiveness, Efficiency
- C. Communication, Reliability, Cost
- D. Confidentiality, Compliance, Cost

Suggested Answer: B

Community vote distribution



RC2073 1 year, 3 months ago

Selected Answer: B

B is correct, confirmed on another website for the same question
upvoted 1 times

VOAKDO_cciso 1 year, 7 months ago

Selected Answer: B

Here is talking about INTERNAL CONTROL OBJECTIVES, regarding the achievement of objectives: 1.1.4 COSO PDC Defense-in-Depth Model (just after CIA triad).
upvoted 1 times

Nickknock 1 year, 7 months ago

Answer is B:

COSO framework defines internal control as a process regarding the achievement of objectives in the following categories: effectiveness and efficiency of operations, reliability of financial reporting, compliance with applicable laws and regulations.
upvoted 2 times

tnagy 1 year, 9 months ago

Selected Answer: A

It must be the CIA Triangle; Confidentiality, Integrity, and Availability.
upvoted 1 times

The effectiveness of an audit is measured by?

- A. The number of security controls the company has in use
- B. How it exposes the risk tolerance of the company
- C. The number of actionable items in the recommendations
- D. How the recommendations directly support the goals of the company

Suggested Answer: D

Community vote distribution

C (100%)

  **Bettoxicity** 1 year ago

Selected Answer: C

Why not D: While alignment with company goals is desirable, it's not the sole determinant of an effective audit. The focus should be on identifying and addressing risks.

upvoted 1 times

Which of the following is the MOST important reason to measure the effectiveness of an Information Security Management System (ISMS)?

- A. Better understand the threats and vulnerabilities affecting the environment
- B. Better understand strengths and weakness of the program
- C. Meet regulatory compliance requirements
- D. Meet legal requirements

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!



Control Objectives for Information and Related Technology (COBIT) is which of the following?

- A. An audit guideline for certifying secure systems and controls
- B. An information Security audit standard
- C. A framework for Information Technology management and governance
- D. A set of international regulations for Information Technology governance

Suggested Answer: C

Community vote distribution

C (100%)

  **tnagy** 1 year, 3 months ago

Selected Answer: C

You cannot be certified against COBIT.

upvoted 1 times

Which of the following are not stakeholders of IT security projects?

- A. Board of directors
- B. Help Desk
- C. Third party vendors
- D. CISO

Suggested Answer: C

🗨️ 👤 **Valen2259** 1 year, 3 months ago

B. Help Desk (answer)

While the Help Desk plays an essential role in IT operations and may be involved in implementing security measures, they are generally not considered primary stakeholders in the governance or strategic oversight of IT security projects.

The key here is vendor, clearly they are developing for the business, the CEO and BoD involved naturally, the help desk is the help desk, they would have varying input unless the project is about the help desk.

A very vague one-dimensional question
upvoted 2 times

🗨️ 👤 **Kentish** 2 years, 9 months ago

Third party vendors could be important stakeholders depending on the project. Perhaps the person writing the question envisaged they would be a simple supplier but often in IT these days vendors are in partnership to provide critical services so could be an important stakeholder.

upvoted 3 times

Which of the following illustrates an operational control process:

- A. Classifying an information system as part of a risk assessment
- B. Conducting an audit of the configuration management process
- C. Installing an appropriate fire suppression system in the data center
- D. Establishing procurement standards for cloud vendors

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

A person in your security team calls you at night and informs you that one of your web applications is potentially under attack from a cross-site scripting vulnerability.

What do you do?

- A. tell him to shut down the server
- B. tell him to call the police
- C. tell him to invoke the incident response process
- D. tell him to analyze the problem, preserve the evidence and provide a full analysis and report.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Which of the following are necessary to formulate responses to external audit findings?

- A. Technical Staff, Budget Authority, Management
- B. Technical Staff, Internal Audit, Budget Authority
- C. Internal Audit, Budget Authority, Management
- D. Internal Audit, management, and Technical Staff

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following is the PRIMARY purpose of International Organization for Standardization (ISO) 27001?

- A. Implementation of business-enabling information security
- B. Use within an organization to ensure compliance with laws and regulations
- C. To enable organizations that adopt it to obtain certifications
- D. Use within an organization to formulate security requirements and objectives

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

A missing/ineffective security control is identified.

Which of the following should be the NEXT step?

- A. Perform an audit to measure the control formally
- B. Escalate the issue to the IT organization
- C. Perform a risk assessment to measure risk
- D. Establish Key Risk Indicators

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Acme Inc. has engaged a third party vendor to provide 99.999% up-time for their online web presence and had them contractually agree to this service level agreement.

What type of risk tolerance is Acme exhibiting?

- A. medium-high risk-tolerance
- B. low risk-tolerance
- C. high risk-tolerance
- D. moderate risk-tolerance

Suggested Answer: *B*

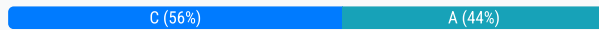
Currently there are no comments in this discussion, be the first to comment!

Your incident response plan should include which of the following?

- A. Procedures for classification
- B. Procedures for charge-back
- C. Procedures for reclamation
- D. Procedures for litigation

Suggested Answer: C

Community vote distribution



Bettoxicity 1 year ago

Selected Answer: A

Why not C: Reclamation refers to the process of recovering data or systems after an incident. While important, it's a later stage in the incident response lifecycle.

upvoted 1 times

johnndoe69 1 year, 5 months ago

Selected Answer: A

Procedures for Classification: Proper classification of incidents is crucial in an incident response plan. It helps in determining the severity and priority of incidents, guiding the appropriate response actions. Classification procedures ensure that incidents are categorized consistently, allowing for an efficient and effective response. Example incident classification: Critical, Major, Minor.

upvoted 3 times

nshams 1 year, 5 months ago

Selected Answer: C

reclamation is mitigation and it should be part of IRP

upvoted 2 times

Perseus_68 1 year, 10 months ago

Selected Answer: C

IR defined in CCISO book pg 263 - prepare, Identify, Contain, Eradicate, RECOVER, lessons learned - then repeat

upvoted 3 times


To get an Information Security project back on schedule, which of the following will provide the MOST help?

- A. Upper management support
- B. More frequent project milestone meetings
- C. Stakeholder support
- D. None
- E. Extend work hours

Suggested Answer: A

Community vote distribution

E (100%)

  **mknick131223223** 1 year ago

Selected Answer: E

I fail to see how upper management can speed up a project to get it back on schedule vs simply crashing a project via extended work hours. Either we catch up, or we don't.

upvoted 1 times

You currently cannot provide for 24/7 coverage of your security monitoring and incident response duties and your company is resistant to the idea of adding more full-time employees to the payroll.

Which combination of solutions would help to provide the coverage needed without the addition of more dedicated staff?

- A. Employ an assumption of breach protocol and defend only essential information resources.
- B. Deploy a SEIM solution and have your staff review incidents first thing in the morning
- C. Configure your syslog to send SMS messages to current staff when target events are triggered.
- D. Engage a managed security provider and have current staff on call for incident response

Suggested Answer: *D*

  **ImranNY** 1 year, 5 months ago

Why the assumption here is that the Third-Party vendor would be cheaper than internal staff?

upvoted 1 times

A department within your company has proposed a third party vendor solution to address an urgent, critical business need. As the CISO you have been asked to accelerate screening of their security control claims.

Which of the following vendor provided documents is BEST to make your decision?

- A. Vendor provided reference from an existing reputable client detailing their implementation
- B. Vendor's client list of reputable organizations currently using their solution
- C. Vendor provided internal risk assessment and security control documentation
- D. Vendor provided attestation of the detailed security controls from a reputable accounting firm

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

A severe security threat has been detected on your corporate network. As CISO you quickly assemble key members of the Information Technology team and business operations to determine a modification to security controls in response to the threat.

This is an example of:

- A. Change management
- B. Thought leadership
- C. Business continuity planning
- D. Security Incident Response

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following represents the best method of ensuring business unit alignment with security program requirements?

- A. Create collaborative risk management approaches within the organization
- B. Perform increased audits of security processes and procedures
- C. Provide clear communication of security requirements throughout the organization
- D. Demonstrate executive support with written mandates for security policy adherence

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

When operating under severe budget constraints a CISO will have to be creative to maintain a strong security organization. Which example below is the MOST creative way to maintain a strong security posture during these difficult times?

- A. Download security tools from a trusted source and deploy to production network
- B. Download open source security tools from a trusted site, test, and then deploy on production network
- C. Download trial versions of commercially available security tools and deploy on your production network
- D. Download open source security tools and deploy them on your production network

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

How often should the SSAE16 report of your vendors be reviewed?

- A. Quarterly
- B. Semi-annually
- C. Bi-annually
- D. Annually

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following will be MOST helpful for getting an Information Security project that is behind schedule back on schedule?

- A. More frequent project milestone meetings
- B. Involve internal audit
- C. Upper management support
- D. More training of staff members

Suggested Answer: C

Currently there are no comments in this discussion, be the first to comment!

The organization does not have the time to remediate the vulnerability; however it is critical to release the application. Which of the following needs to be further evaluated to help mitigate the risks?

- A. Provide security testing tools
- B. Provide developer security training
- C. Deploy Intrusion Detection Systems
- D. Implement Compensating Controls

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Your company has a `no right to privacy` notice on all logon screens for your information systems and users sign an Acceptable Use Policy informing them of this condition. A peer group member and friend comes to you and requests access to one of her employee's email account. What should you do?

- A. Deny the request citing national privacy laws
- B. None
- C. Grant her access, the employee has been adequately warned through the AUP.
- D. Assist her with the request, but only after her supervisor signs off on the action.
- E. Reset the employee's password and give it to the supervisor.

Suggested Answer: D

Community vote distribution

C (67%)

A (33%)

  **BiteSize** 10 months, 3 weeks ago

Selected Answer: C



Answer is C

your peer, as a CISO, is an executive level. Asking for the supervisor signature is dumb,
upvoted 1 times

  **Bettoxicity** 1 year ago



Selected Answer: A

Why not C: is incorrect. Granting access based solely on an AUP is not sufficient justification and could have legal and ethical consequences.
upvoted 1 times

  **nshams** 1 year, 5 months ago

Selected Answer: C

AUP is accepted , so grant access to management team
upvoted 1 times

  **mlestyk** 2 years, 4 months ago

The request should be denied citing possible state privacy laws.
upvoted 2 times

Which one of the following BEST describes which member of the management team is accountable for the day-to-day operation of the information security program?

- A. Security managers
- B. Security analysts
- C. Security technicians
- D. Security administrators

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following is a major benefit of applying risk levels?

- A. Resources are not wasted on risks that are already managed to an acceptable level
- B. Risk appetite increase within the organization once the levels are understood
- C. Risk budgets are more easily managed due to fewer due to fewer identified risks as a result of using a methodology
- D. Risk management governance becomes easier since most risks remain low once mitigated

Suggested Answer: A

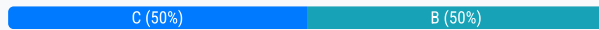
Currently there are no comments in this discussion, be the first to comment!

Which business stakeholder is accountable for the integrity of a new information system?

- A. Compliance Officer
- B. CISO
- C. Project manager
- D. Board of directors

Suggested Answer: B

Community vote distribution



🗨️ 👤 **Sean_P** 4 months, 2 weeks ago

Selected Answer: C

Project Manager → Has project-level accountability for delivering the system according to its requirements, including ensuring the controls and processes are in place to protect integrity within that specific system. The PM coordinates all stakeholders (including the CISO or security team) and is the single point of accountability for the project's outcome.

upvoted 1 times

🗨️ 👤 **johnndoe69** 1 year ago

Selected Answer: B

The business stakeholder accountable for the integrity of a new information system is typically the Chief Information Security Officer (CISO). The CISO is responsible for ensuring that the information security measures, including controls and processes, are adequately implemented to protect the integrity, confidentiality, and availability of the system. This includes overseeing the development, implementation, and maintenance of security policies and procedures, conducting risk assessments, and ensuring compliance with relevant standards and regulations.

According to NIST Special Publication 800-53, the CISO plays a crucial role in managing the security and privacy controls for information systems and ensuring these controls are effective throughout the system development life cycle. The CISO's responsibilities encompass the establishment and maintenance of an organization's overall security posture, which directly includes the integrity of new information systems.

upvoted 1 times

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

I would have thought the system owner would be accountable, the CISO's role is to advise the business owner, but the business owners are accountable for taking the action to protect the system and it is their choice to release it.

upvoted 3 times

A CISO decides to analyze the IT infrastructure to ensure security solutions adhere to the concepts of how hardware and software is implemented and managed within the organization.

Which of the following principles does this best demonstrate?

- A. Proper budget management
- B. Effective use of existing technologies
- C. Alignment with the business
- D. Leveraging existing implementations

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Which of the following functions evaluates risk present in IT initiatives and/or systems when implementing an information security program?

- A. Risk Assessment
- B. Risk Management
- C. Vulnerability Assessment
- D. System Testing

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following information may be found in table top exercises for incident response?

- A. Real-time to remediate
- B. Process improvements
- C. Security budget augmentation
- D. Security control selection

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

When gathering security requirements for an automated business process improvement program, which of the following is MOST important?

- A. Type of data contained in the process/system
- B. Type of encryption required for the data once it is at rest
- C. Type of computer the data is processed on
- D. Type of connection/protocol used to transfer the data

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

You manage a newly created Security Operations Center (SOC), your team is being inundated with security alerts and don't know what to do. What is the BEST approach to handle this situation?

- A. Tune the sensors to help reduce false positives so the team can react better
- B. Request additional resources to handle the workload
- C. Tell the team to do their best and respond to each alert
- D. Tell the team to only respond to the critical and high alerts

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

In order for a CISO to have true situational awareness there is a need to deploy technology that can give a real-time view of security events across the enterprise.

Which of the following tools represents the BEST choice to achieve this awareness?

- A. Intrusion Detection System (IDS), firewall, switch, syslog
- B. Security Incident Event Management (SIEM), IDS, router, syslog
- C. VMware, router, switch, firewall, syslog, vulnerability management system (VMS)
- D. SIEM, IDS, firewall, VMS

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Information Security is often considered an excessive, after-the-fact cost when a project or initiative is completed.

What can be done to ensure that security is addressed cost effectively?

- A. Launch an internal awareness campaign
- B. Installation of new firewalls and intrusion detection systems
- C. Integrate security requirements into project inception
- D. User awareness training for all employees

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is the BEST indicator of a successful project?

- A. it comes in at or below the expenditures planned for in the baseline budget
- B. it meets most of the specifications as outlined in the approved project definition
- C. it is completed on time or early as compared to the baseline project plan
- D. the deliverables are accepted by the key stakeholders

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is the MOST important component of any change management process?

- A. Outage planning
- B. Scheduling
- C. Approval tracking
- D. Back-out procedures

Suggested Answer: A

Community vote distribution

C (67%)

A (33%)

🗳️ 👤 **Valen2259** 1 year, 3 months ago

D.

It has to be; whilst outage planning maybe at the behest of the system/operational window. You need a plan should that update go wrong. You will not get Management approval unless you have a roll-back plan.

Back-out procedures are essential because, no matter how well a change is planned, there is always a risk of failure or unintended consequences. A well-documented and tested back-out procedure allows for a quick and controlled response, minimizing risks and maintaining system stability.

upvoted 1 times

🗳️ 👤 **nshams** 1 year, 5 months ago

Selected Answer: C

Approvals

upvoted 1 times

🗳️ 👤 **johndoe69** 1 year, 7 months ago

Selected Answer: C

C. ITIL (Information Technology Infrastructure Library): ITIL emphasizes the importance of a structured change management process, including approval tracking to manage risks and ensure changes are beneficial.

upvoted 1 times

🗳️ 👤 **Perseus_68** 1 year, 10 months ago

Selected Answer: A

I would have pick approval process if it was a choice, since it is not and tracking was an answer, taking a critical system or application off line to update could have a massive impact to a business.

upvoted 1 times

🗳️ 👤 **ONERAPTOR** 2 years, 1 month ago

Answer is C

This is key to ensuring that all changes are reviewed, authorized, and documented before implementation. Approval tracking ensures accountability and oversight, which are critical for managing risks associated with changes. It helps in ensuring that changes align with the organization's policies, compliance requirements, and business objectives.

upvoted 1 times

🗳️ 👤 **Kentish** 2 years, 9 months ago



I would argue back out procedures are equally important with the best will in the world in today's complex systems it is impossible to predict all the effects of changes so being able to back-out a change quickly and smoothly is a vital safety net.

upvoted 3 times

When selecting a security solution with reoccurring maintenance costs after the first year

- A. Implement the solution and ask for the increased operating cost budget when it is time
- B. Communicate future operating costs to the CIO/CFO and seek commitment from them to ensure the new solution's continued use
- C. Defer selection until the market improves and cash flow is positive
- D. The CISO should cut other essential programs to ensure the new solution's continued use

Suggested Answer: *B*

  **Malik2165** 1 year, 5 months ago

it is important to convey the budgetary requirement and expectations in advance for multi-year projects
upvoted 2 times

What oversight should the information security team have in the change management process for application security?

- A. Information security should be aware of any significant application security changes and work with developer to test for vulnerabilities before changes are deployed in production
- B. Information security should be aware of all application changes and work with developers before changes and deployed in production
- C. Information security should be informed of changes to applications only
- D. Development team should tell the information security team about any application security flaws

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

An application vulnerability assessment has identified a security flaw in an application. This is a flaw that was previously identified and remediated on a prior release of the application.

Which of the following is MOST likely the reason for this recurring issue?

- A. Lack of version/source controls
- B. Lack of change management controls
- C. Ineffective configuration management controls
- D. High turnover in the application development department

Suggested Answer: A

Community vote distribution

A (100%)

🗲️ 👤 **nshams** 1 year, 5 months ago

Selected Answer: A

version control

upvoted 1 times

🗲️ 👤 **musagul** 1 year, 10 months ago

Selected Answer: A

In this condition, there is no version management we can see.

upvoted 1 times

🗲️ 👤 **arifbhatkar** 2 years, 6 months ago

The most likely reason for the recurring security flaw in the application, even after it was previously identified and remediated, is option B: Lack of change management controls.

Change management controls refer to processes and procedures in place to manage and control changes to an application or system. These controls ensure that proper documentation, testing, and approval processes are followed before implementing changes. In this scenario, the recurring security flaw suggests that there may be a lack of effective change management controls in place.

upvoted 3 times

In effort to save your company money which of the following methods of training results in the lowest cost for the organization?

- A. One-One Training
- B. Self-Study (noncomputerized)
- C. Distance learning/Web seminars
- D. Formal Class

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

When entering into a third party vendor agreement for security services, at what point in the process is it BEST to understand and validate the security posture and compliance level of the vendor?

- A. Prior to signing the agreement and before any security services are being performed
- B. Once the agreement has been signed and the security vendor states that they will need access to the network
- C. Once the vendor is on premise and before they perform security services
- D. At the time the security services are being performed and the vendor needs access to the network

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following represents the BEST method for obtaining business unit acceptance of security controls within an organization?

- A. Allow the business units to decide which controls apply to their systems, such as the encryption of sensitive data
- B. Ensure business units are involved in the creation of controls and defining conditions under which they must be applied
- C. Provide the business units with control mandates and schedules of audits for compliance validation
- D. Create separate controls for the business based on the types of business and functions they perform

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Risk appetite is typically determined by which of the following organizational functions?

- A. Business units
- B. Board of Directors
- C. Audit and compliance
- D. Security

Suggested Answer: A

Community vote distribution

B (67%)

A (33%)

 **Dzidzorli** Highly Voted 5 years, 6 months ago

I think this should be the Board of Directors. I think they must determine the Risk Appetite of the business and NOT the Business Units. The Business Units could be compensating?
upvoted 7 times

 **nshams** Most Recent 1 year, 5 months ago

Selected Answer: B

BOD determine
upvoted 1 times

 **john doe69** 1 year, 7 months ago

Selected Answer: B

B. NIST Special Publication 800-39 (Managing Information Security Risk): This publication underscores the importance of senior leadership, including the Board, in setting the organization's risk appetite.
upvoted 1 times

 **Perseus_68** 1 year, 10 months ago

Selected Answer: A

accountable, business units, hence they determine appetite. Responsible, Board of Directors and senior leadership, They accept or reject the recommendation.
upvoted 1 times


 **Ludikraut** 2 years, 5 months ago

Poorly phrased question, IMO. I agree with @Rufus1. It also depends on the size and type of organization.
upvoted 1 times


 **arifbhatkar** 2 years, 6 months ago

The risk appetite is typically determined by the Board of Directors, making option B the correct answer.

The Board of Directors holds the overall responsibility for setting the strategic direction and objectives of an organization, including its risk management approach. The risk appetite represents the level of risk that an organization is willing to accept in pursuit of its objectives. It reflects the organization's tolerance for risk and guides decision-making processes regarding risk management.
upvoted 1 times

 **Pika26** 2 years, 9 months ago

Answer is B. The risk appetite of an organization refers to the level of risk that an organization is willing to accept to achieve its objectives. This decision is typically made by senior management or the board of directors, as they are responsible for setting the overall strategic direction and risk tolerance of the organization. Business units, audit and compliance, and security may provide input into the risk appetite decision-making process, but they do not typically have the authority to make the final decision.
upvoted 3 times

 **MURY23** 2 years, 10 months ago



Business Unit may not have the knowledge of Risk, CISO is expected to present it to Board of Directors for approval.
upvoted 3 times

 **Rufus1** 4 years, 2 months ago

"Determined"...


Can be Business Units to determine, and Board to approve. Very debating choices...

upvoted 4 times

  **mat333** 5 years ago

B Board of directors

upvoted 3 times

  **Mrimbert** 5 years, 1 month ago

Board of directors

upvoted 3 times

How often should the Statements of Standards for Attestation Engagements-16 (SSAE16)/International Standard on Assurance Engagements 3402 (ISAE3402) report of your vendors be reviewed?

- A. Annually
- B. Quarterly
- C. Bi-annually
- D. Semi-annually

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

The Security Operations Center (SOC) just purchased a new intrusion prevention system (IPS) that needs to be deployed in-line for best defense. The IT group is concerned about putting the new IPS in-line because it might negatively impact network availability. What would be the BEST approach for the CISO to reassure the IT group?

- A. Explain to the IT group that this is a business need and the IPS will fail open however, if there is a network failure the CISO will accept responsibility
- B. Work with the IT group and tell them to put IPS in-line and say it won't cause any network impact
- C. Explain to the IT group that the IPS will fail open once in-line however it will be deployed in monitor mode for a set period of time to ensure that it doesn't block any legitimate traffic
- D. Explain to the IT group that the IPS won't cause any network impact because it will fail open

Suggested Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following represents the BEST method of ensuring security program alignment to business needs?

- A. Ensure the organization has strong executive-level security representation through clear sponsorship or the creation of a CISO role
- B. Create a comprehensive security awareness program and provide success metrics to business units
- C. Create security consortiums, such as strategic security planning groups, that include business unit participation
- D. Ensure security implementations include business unit testing and functional validation prior to production rollout

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

A stakeholder is a person or group:

- A. Vested in the success and/or failure of a project or initiative regardless of budget implications.
- B. That will ultimately use the system.
- C. That has budget authority.
- D. Vested in the success and/or failure of a project or initiative and is tied to the project budget.

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following is considered one of the most frequent failures in project management?

- A. Overly restrictive management
- B. Insufficient resources
- C. Excessive personnel on project
- D. Failure to meet project deadlines

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

A recommended method to document the respective roles of groups and individuals for a given process is to:

- A. Develop a detailed internal organization chart
- B. Develop an isolinear response matrix with cost benefit analysis projections
- C. Develop a Responsible, Accountable, Consulted, Informed (RACI) chart
- D. Develop a telephone call tree for emergency response

Suggested Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following refers to the quantity or quality of project deliverables expanding from the original project plan?

- A. Scope creep
- B. Deadline extension
- C. Deliverable expansion
- D. Scope modification

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

You are the CISO of a commercial social media organization. The leadership wants to rapidly create new methods of sharing customer data through creative linkages with mobile devices. You have voiced concern about privacy regulations but the velocity of the business is given priority. Which of the following BEST describes this organization?

- A. Risk conditional
- B. Risk minimal
- C. Risk tolerant
- D. Risk averse

Suggested Answer: *C*


Currently there are no comments in this discussion, be the first to comment!

The security team has investigated the theft/loss of several unencrypted laptop computers containing sensitive corporate information. To prevent the loss of any additional corporate data, it is unilaterally decided by the CISO that all existing and future laptop computers will be encrypted. The help desk is then flooded with complaints about the slow performance of the laptops and users are upset.

Which of the following best describes what the CISO did wrong?

- A. Failed to identify all stakeholders and their needs
- B. Deployed the encryption solution in an inadequate manner
- C. Used 1024 bit encryption when 256 bit would have sufficed
- D. Used hardware encryption instead of software encryption

Suggested Answer: A

  **Kentish** 1 year, 2 months ago

It could be argued that B incorporates A as well as insufficient testing.

upvoted 1 times

An example of professional unethical behavior is:

- A. Sharing copyrighted material with other members of a professional organization where all members have legitimate access to the material
- B. Copying documents from an employer's server which you assert that you have an intellectual property claim to possess, but the company disputes
- C. Storing client lists and other sensitive corporate internal documents on a removable thumb drive
- D. Gaining access to an affiliated employee's work email account as part of an officially sanctioned internal investigation

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

When considering using a vendor to help support your security devices remotely, what is the BEST choice for allowing access?

- A. Vendor uses their own laptop and logins using two factor authentication with their own unique credentials
- B. Vendor uses a company supplied laptop and logins using two factor authentication wit same admin credentials your security team uses
- C. Vendor uses a company supplied laptop and logins using two factor authentication with their own unique credentials
- D. Vendors uses their own laptop and logins with same admin credentials your security team uses

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is critical in creating a security program aligned with an organization's goals?

- A. Develop a culture in which users, managers and IT professionals all make good decisions about information risk
- B. Provide clear communication of security program support requirements and audit schedules
- C. Create security awareness programs that include clear definition of security program goals and charters
- D. Ensure security budgets enable technical acquisition and resource allocation based in internal compliance requirements

Suggested Answer: A



Currently there are no comments in this discussion, be the first to comment!

An organization has a stated requirement to block certain traffic on networks. The implementation of controls will disrupt a manufacturing process and cause unacceptable delays, resulting in severe revenue disruptions.

Which of the following is MOST likely to be responsible for accepting the risk until mitigating controls can be implemented?

- A. Audit and Compliance
- B. The CFO
- C. The CISO
- D. The business owner

Suggested Answer: D

  **Kentish** 1 year, 2 months ago

I think this should be "severe revenue disruption" instead of server?

upvoted 1 times

A newly appointed security officer finds data leakage software licenses that had never been used. The officer decides to implement a project to ensure it gets installed, but the project gets a great deal of resistance across the organization.

Which of the following represents the MOST likely reason for this situation?

- A. The project was initiated without an effort to get support from impacted business units in the organization
- B. The security officer should allow time for the organization to get accustomed to her presence before initiating security projects
- C. The software is out of date and does not provide for a scalable solution across the enterprise
- D. The software license expiration is probably out of synchronization with other software licenses

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

The company decides to release the application without remediating the high-risk vulnerabilities.

Which of the following is the MOST likely reason for the company to release the application?

- A. The company does not believe the security vulnerabilities to be real
- B. The company lacks the tools to perform a vulnerability assessment
- C. The company lacks a risk management process
- D. The company has a high risk tolerance

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following best summarizes the primary goal of a security program?

- A. Provide security reporting to all levels of an organization
- B. Manage risk within the organization
- C. Create effective security awareness to employees
- D. Assure regulatory compliance

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is a strong post designed to stop a car?

- A. Fence
- B. Bollard
- C. Reinforced rebar
- D. Gate

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following items of a computer system will an anti-virus program scan for viruses?

- A. Boot Sector
- B. Password Protected Files
- C. Windows Process List
- D. Deleted Files

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

A CISO has recently joined an organization with a poorly implemented security program. The desire is to base the security program on a risk management approach.

Which of the following is a foundational requirement in order to initiate this type of program?

- A. A complete inventory of Information technology assets including infrastructure, networks, applications and data
- B. A security organization that is adequately staffed to apply required mitigation strategies and regulatory compliance solutions
- C. A clear set of security policies and procedures that are more concept-based than controls-based than controls-based
- D. A clearly identified executive sponsor who will champion the effort to ensure organizational buy-in

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is considered a project versus a managed process?

- A. ongoing risk assessment of routine operations
- B. continuous vulnerability assessment and vulnerability repair
- C. monitoring external and internal environment during incident response
- D. installation of a new firewall system

Suggested Answer: *D*

  **Malik2165** 1 year, 6 months ago

The managed process is an ongoing activity, Project is a one-time task, hence the answer is correct.

upvoted 1 times

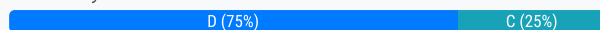
A CISO implements smart cards for credential management, and as a result has reduced costs associated with help desk operations supporting password resets.

This demonstrates which of the following principles?

- A. Increased security program presence
- B. Regulatory compliance effectiveness
- C. Security organizational policy enforcement
- D. Proper organizational policy enforcement

Suggested Answer: D

Community vote distribution



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

Selected Answer: D

proper policy enforcement

upvoted 1 times

🗳️ 👤 **nshams** 1 year, 5 months ago

Selected Answer: D

proper policy enforcement

upvoted 1 times

🗳️ 👤 **johnndoe69** 1 year, 7 months ago

Selected Answer: D

Proper organizational policy enforcement: This option highlights adherence to policies that improve operational efficiency and security. Given that the scenario specifies reduced costs, which implies an effective and efficient implementation of security controls according to organizational policies, this is a strong contender.

upvoted 1 times

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

Selected Answer: C

To mark this as Proper organizational policy enforcement, we must have valid datas from other policy enforcement processes (maybe from other departments, etc.). What we saw from the text is C) Security Organizational Policy Enforcement. Answer is correct.

upvoted 1 times

🗳️ 👤 **arifbhatkar** 2 years, 6 months ago

D. Proper organizational policy enforcement.

The implementation of smart cards for credential management, resulting in reduced costs associated with help desk operations supporting password resets, demonstrates the principle of proper organizational policy enforcement. By implementing smart cards, the CISO is enforcing the organizational policy of using strong authentication mechanisms and reducing reliance on password-based authentication. This action aligns with the security policy and demonstrates the proper implementation and enforcement of organizational policies.

Option C, security organizational policy enforcement, is similar to the correct answer but is not as comprehensive. The implementation of smart cards is a specific instance of enforcing a security organizational policy, rather than encompassing the broader concept of policy enforcement in general.

Therefore, the most appropriate answer is D. Proper organizational policy enforcement.

upvoted 1 times

Which of the following methodologies references the recommended industry standard that all project managers should follow?

- A. The Security Systems Development Life Cycle
- B. Project Management System Methodology
- C. Project Management Body of Knowledge
- D. The Security Project and Management Methodology

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Which of the following can the company implement in order to avoid this type of security issue in the future?

- A. Network based intrusion detection systems
- B. An audit management process
- C. A security training program for developers
- D. A risk management process

Suggested Answer: C

Community vote distribution

C (100%)


  **hchurn** Highly Voted 4 years, 7 months ago

Incomplete question? what type of security issue?
upvoted 7 times



  **john doe69** Most Recent 1 year ago

Selected Answer: C

Implementing a security training program for developers is the most effective measure to avoid similar security issues in the future. This approach addresses the root cause by equipping developers with the knowledge and skills necessary to write secure code, thereby preventing vulnerabilities from being introduced during the development process.
upvoted 2 times

  **Emporeo** 1 year, 3 months ago

incomplete question
upvoted 1 times

  **kaibutsu** 1 year, 11 months ago

Can someone at ExamTopics please review this question? It is incomplete.
upvoted 1 times

  **UNN_CCISO** 3 years, 9 months ago

C is a more preventive action, and hence is more appropriate compared to other answers which do not help to "avoid" any security issue
upvoted 1 times

  **letsdoitnow** 4 years ago

Agreed! It appeared to be incomplete question.
upvoted 2 times

Knowing the potential financial loss an organization is willing to suffer if a system fails is a determination of which of the following?

- A. Cost benefit
- B. Risk appetite
- C. Business continuity
- D. Likelihood of impact

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following methods are used to define contractual obligations that force a vendor to meet customer expectations?


- A. Terms and Conditions
- B. Statements of Work
- C. Service Level Agreements (SLA)
- D. Key Performance Indicators (KPI)

Suggested Answer: C

Community vote distribution

C (50%)

A (50%)

 **shiko81** 5 months, 1 week ago

Selected Answer: A

Contractual obligations should be terms and conditions(the contract clauses), SLA is ensure the availability and quality of delivery
upvoted 1 times

 **johnndoe69** 1 year ago

Selected Answer: C

Service Level Agreements (SLA) are the most appropriate method for defining contractual obligations that ensure a vendor meets customer expectations. They provide a structured and enforceable framework for service delivery and performance measurement.
upvoted 1 times

 **arifbhatkar** 1 year, 12 months ago

This is suppose to be multiple answer option, so The methods used to define contractual obligations that force a vendor to meet customer expectations are:

- A. Terms and Conditions
 - B. Statements of Work
 - C. Service Level Agreements (SLA)
- upvoted 1 times

 **Malik2165** 3 years, 5 months ago

SLA is a service level agreement, which goes with ongoing maintenance, service contract, on the other Hand SOW Statement of Work define how the will commence.
upvoted 1 times

A CISO sees abnormally high volumes of exceptions to security requirements and constant pressure from business units to change security processes.

Which of the following represents the MOST LIKELY cause of this situation?

- A. Poor audit support for the security program
- B. Poor alignment of the security program to business needs
- C. This is normal since business units typically resist security requirements
- D. A lack of executive presence within the security program

Suggested Answer: *B*

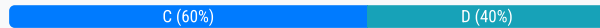
Currently there are no comments in this discussion, be the first to comment!

Which of the following functions evaluates patches used to close software vulnerabilities and perform validation of new systems to assure compliance with security?

- A. Incident response
- B. Risk management
- C. System security administration
- D. System testing

Suggested Answer: C

Community vote distribution



🗨️ **Bettoxicity** 12 months ago

Selected Answer: C

Why not D: System testing primarily focuses on verifying the functionality and performance of software systems.
upvoted 1 times

🗨️ **alfaMegatron** 1 year, 4 months ago

Selected Answer: D

looks best in this context
upvoted 1 times

🗨️ **nshams** 1 year, 5 months ago

Selected Answer: C

sys sec administration
upvoted 1 times

🗨️ **johndoe69** 1 year, 7 months ago

Selected Answer: C

System security administration is the function best suited for evaluating patches to close software vulnerabilities and validating new systems to assure compliance with security requirements. This role ensures that patches are effectively managed and systems are secure and compliant before being deployed.
upvoted 1 times

🗨️ **Perseus_68** 1 year, 10 months ago

Selected Answer: D

which function EVALUATES patches, not approves, recommends, installs or manages. The testing group has to do V&V to make sure the patch doesn't negatively impact the system.
upvoted 1 times

🗨️ **ONERAPTOR** 2 years, 1 month ago

Answer is C

This function is directly responsible for maintaining the security of systems. It includes tasks such as applying patches to fix vulnerabilities, configuring systems securely, and validating new systems for compliance with security standards. This is the most relevant function for the activities described in your question.
upvoted 1 times

Which of the following functions implements and oversees the use of controls to reduce risk when creating an information security program?

- A. Risk Assessment
- B. Risk Management
- C. Incident Response
- D. Network Security administration

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is MOST beneficial in determining an appropriate balance between uncontrolled innovation and excessive caution in an organization?

- A. Collaborate security projects
- B. Review project charters
- C. Define the risk appetite
- D. Determine budget constraints

Suggested Answer: C

Currently there are no comments in this discussion, be the first to comment!

As the CISO for your company you are accountable for the protection of information resources commensurate with:

- A. Risk of exposure
- B. Cost and time to replace
- C. Insurability tables
- D. Customer demand

Suggested Answer: A

Currently there are no comments in this discussion, be the first to comment!

The process of identifying and classifying assets is typically included in the_____.

- A. Threat analysis process
- B. Business Impact Analysis
- C. Asset configuration management process
- D. Disaster Recovery plan

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

File Integrity Monitoring (FIM) is considered a_____.

- A. Network-based security preventative control
- B. Software segmentation control
- C. User segmentation control
- D. Security detective control

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

What are the primary reasons for the development of a business case for a security project?

- A. To forecast usage and cost per software licensing
- B. To understand the attack vectors and attack sources
- C. To communicate risk and forecast resource needs
- D. To estimate risk and negate liability to the company

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

John is the project manager for a large project in his organization. A new change request has been proposed that will affect several areas of the project. One area of the project change impact is on work that a vendor has already completed. The vendor is refusing to make the changes as they've already completed the project work they were contracted to do.

What can John do in this instance?

- A. Withhold the vendor's payments until the issue is resolved.
- B. refer to the contract agreement for direction.
- C. Refer the vendor to the Service Level Agreement (SLA) and insist that they make the changes.
- D. Review the Request for proposal (RFP) for guidance.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

One of your executives needs to send an important and confidential email. You want to ensure that the message cannot be read by anyone but the recipient.

Which of the following keys should be used to encrypt the message?

- A. Certificate authority key
- B. The recipient's private key
- C. The recipient's public key
- D. Your public key

Suggested Answer: C

Community vote distribution

C (100%)

  **johndoe69** 1 year ago

Selected Answer: C

Encryption Basics: To ensure that an important and confidential email can only be read by the recipient, you should use the recipient's public key to encrypt the message. The recipient will then use their private key to decrypt it.

upvoted 1 times

  **VOAKDO_cciso** 2 years, 1 month ago

I got my CEH only months ago, and there are 2 ways to use PKI:

1.-CONFIDENTIAL:When encrypting, you use recipient's public key to write a message and recipient use their private key to read itTHEREFORE C IS OK

2.-NON-REPUDIATION-When signing, you use your private key to write message's signature, and recipient's use your public key to check if it's really yours

upvoted 1 times

  **UNN_CCISO** 3 years, 9 months ago

Using Recipients public key will ensure that only the recipient can decrypt using his/her private key. If sender's private key is used, anyone will be able to decrypt using the senders public key & will only help in "non-repudiation"...of course practically it is a combination of recipients public key and senders private key

upvoted 1 times

  **ChrisZo** 4 years ago

Should the answer be sender's private key?

upvoted 1 times

  **Malik2165** 3 years, 5 months ago

No, If we encrypt with Sender's private key then anyone having senders public key, will be able to read the message.

upvoted 1 times