EXAMTOPICS

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



CERTIFICATION TEST

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

Question #1 *Topic 1*

You work as a Network Auditor for Net Perfect Inc. The company has a Windows-based network. While auditing the company's network, you are facing problems in searching the faults and other entities that belong to it. Which of the following risks may occur due to the existence of these problems?

A. Residual risk

B. Secondary risk

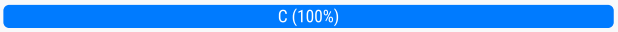
C. Detection risk

D. Inherent risk

Suggested Answer: *A*

Detection risks are the risks that an auditor will not be able to find what they are looking to detect. Hence, it becomes tedious to report negative results when material conditions (faults) actually exist. Detection risk includes two types of risk: Sampling risk: This risk occurs when an auditor falsely accepts or erroneously rejects an audit sample. Nonsampling risk: This risk occurs when an auditor fails to detect a condition because of not applying the appropriate event, a method or a (technical) process that, although being abreast with science, still conceives these dangers, even if all theoretically possible safety measures would be applied (scientifically conceivable measures). The formula to calculate residual risk is (inherent risk) x (control risk) where inherent risk is (threats auditing, is the risk that the account or section being audited is materially misstated without considering internal controls due to error or fraud. The assessment of incorrect. A secondary risk is a risk that arises as a straight consequence of implementing a risk response. The secondary risk is an outcome of dealing with the original risk. Secondary risks are not as rigorous or important as primary risks, but can turn out to be so if not estimated and planned properly.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

C. Detection risk: the risk that an audit will not detect an issue that can result in material error. https://www.accaglobal.com/gb/en/student/exam-support-resources/fundamentals-exams-study-resources/f8/technical-articles/audit-risk0.html Audit risk is defined as 'the risk that the auditor expresses an inappropriate audit opinion when the financial statements are materially misstated. Audit risk is a function of the risks of material misstatement and detection risk'. Hence, audit risk is made up of two components – risks of material misstatement and detection risk. ... Detection risk is defined as 'the risk that the procedures performed by the auditor to reduce audit risk to an acceptably low level will not detect a misstatement that exists and that could be material, either individually or when aggregated with other misstatements.'

upvoted 2 times

Question #2 *Topic 1*

The National Information Assurance Certification and Accreditation Process (NIACAP) is the minimum standard process for the certification and accreditation of computer and telecommunications systems that handle U.S. national security information. Which of the following participants are required in a NIACAP security assessment? Each correct answer represents a part of the solution. Choose all that apply.

A. Certification agent

B. Designated Approving Authority

C. IS program manager

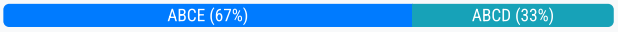
D. Information Assurance Manager

E. User representative

Suggested Answer: *D*

The NIACAP roles are nearly the same as the DITSCAP roles. Four minimum participants (roles) are required to perform a NIACAP security assessment: IS program manager: The IS program manager is the primary authorization advocate. He is responsible for the Information Systems (IS) throughout the life cycle of the system development. Designated Approving Authority (DAA): The Designated Approving Authority (DAA), in the United States Department of Defense, is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. Certification agent: The certification agent is also referred to as the certifier. He provides the technical expertise to conduct the certification throughout the system life cycle. User representative: The user representative focuses on system availability, access, integrity, functionality, performance, and confidentiality in a Certification and Accreditation (C&A)

Community vote distribution



FrolickingDalish Most Recent 1 year, 8 months ago

On page 3 section 3, it list all the participants required for NIACAP security assessment: https://www.fismacenter.com/nstissi_1000.pdf So the answer is ABCE

upvoted 2 times

74gjd_37 1 year, 10 months ago

The following participants are required in a NIACAP security assessment: A. Certification agent B. Designated Approving Authority C. IS program manager D. Information Assurance Manager Therefore, options A, B, C and D are correct answers. Option E is not applicable to a NIACAP security assessment from a CSSLP perspective as it pertains more towards user involvement or representation rather than actual security assessment roles and responsibilities.

upvoted 1 times

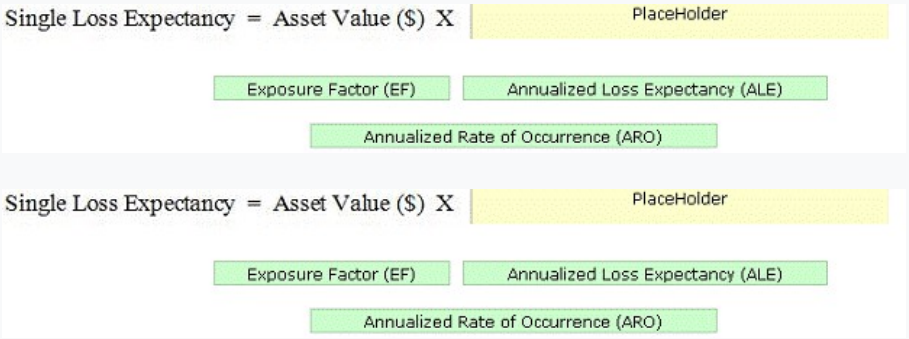
Question #3 *Topic 1*

DRAG DROP -

Drop the appropriate value to complete the formula.

Select and Place:

Suggested Answer:



A Single Loss Expectancy (SLE) is the value in dollar ($) that is assigned to a single event. The SLE can be calculated by the following formula: SLE = Asset Value ($) X Exposure Factor (EF) The Exposure Factor (EF) represents the % of assets loss caused by a threat. The EF is required to calculate the Single Loss Expectancy (SLE). The Annualized Loss Expectancy (ALE) can be calculated by multiplying the Single Loss Expectancy (SLE) with the Annualized Rate of Occurrence (ARO). Annualized Loss Expectancy (ALE) = Single Loss Expectancy (SLE) X Annualized Rate of Occurrence (ARO) Annualized Rate of Occurrence (ARO) is a number that represents the estimated frequency in which a threat is expected to occur. It is calculated based upon the probability of the event occurring and the number of employees that could make that event occur.

74gjd_37 Most Recent 1 year, 10 months ago

SLE = asset value × exposure factor Single loss expectancy (SLE): Loss in monetary (e.g., dollars) terms associated with occurrence of a single event. Eric Cole, in Advanced Persistent Threat, 2013 Calculating Risk In calculating risk, there are two general formulas that are used: SLE (single loss expectancy) and ALE (annualized loss expectancy). SLE is the starting point to determine the single loss that would occur if a specific item occurred. The formula for the SLE is: SLE=assetvalue×exposurefactor. While the SLE is a valuable starting point it only represents the single loss an organization would suffer. From: HCISPP Study Guide, 2015

upvoted 1 times

Shriyanka 2 years, 3 months ago

why are the question and answers not updated properly?

upvoted 2 times

4e3rv21rq3vq2q 3 years, 1 month ago

correct

upvoted 1 times

Question #4 *Topic 1*

Which of the following penetration testing techniques automatically tests every phone line in an exchange and tries to locate modems that are attached to the network?

A. Demon dialing

B. Sniffing

C. Social engineering

D. Dumpster diving

Suggested Answer: *B, A*

The demon dialing technique automatically tests every phone line in an exchange and tries to locate modems that are attached to the network. most commonly used technique of all, getting information (like passwords) just by asking for them.

Community vote distribution

A (100%)

74gjd_37 Most Recent 1 year, 10 months ago

Demon dialing can refer to both the technique of repeatedly dialing a number to gain access immediately after another user had hung up and the automated technique used to test every phone line in an exchange and locate modems attached to the network. In terms of cybersecurity, demon dialing is typically used as part of penetration testing to identify vulnerabilities in a system's security by discovering accessible modems or potentially exploitable telephone lines on a target network. "Demon dialing" was popularized by the movie WarGames, which demonstrates the hacking technique (the technique eventually evolves into a technique called phreaking). After giving the program an area code and 3 digit prefix, the program then serially dialed every phone number in that prefix in order, recording which phone numbers were answered by a computer modem. Soon after, most likely because it was popularized by the movie, serial dialing was outlawed. Hackers got around this by simply randomizing the order the program dialed all the numbers. Later the terms "demon dialing" and "war dialing" became synonymous.

upvoted 1 times

Question #5 *Topic 1*

Which of the following roles is also known as the accreditor?

A. Data owner

B. Chief Risk Officer

C. Chief Information Officer

D. Designated Approving Authority

Suggested Answer: *D, A*

B is incorrect. A Chief Risk Officer (CRO) is also known as Chief Risk Management Officer (CRMO). The Chief Risk Officer or Chief Risk Management Officer of a corporation is the executive accountable for enabling the efficient and effective governance of significant risks, and related opportunities, to a business and its various segments. Risks are commonly categorized as strategic, reputational, operational, financial, or compliance-related. CRO's are accountable to the Executive Committee and The Board for enabling the business to balance risk and reward. In more complex organizations, they are generally responsible for Technology (IT) director, is a job title commonly given to the most senior executive in an enterprise responsible for the information technology and computer systems that support enterprise goals. The CIO plays the role of a leader and reports to the chief executive officer, chief operations officer, or chief financial officer. In military organizations, they report to the commanding officer.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

The correct answer is D. Designated Approving Authority (DAA) is also known as the accreditor in most compliance frameworks that utilize this role. The DAA provides authorization for a system or application to operate based on an evaluation of its security posture and risks. http://www.fismapedia.org/index.php/Term:Designated_Approving_Authority NSTISSI 1000 Designated Approving Authority (DAA) (Accreditor)-Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designed accrediting authority and delegated accrediting authority.

upvoted 1 times

Ecyor 2 years, 1 month ago

D. Designated Approving Authoritydid you take the exam, are these in it

upvoted 1 times

Ecyor 2 years, 1 month ago

Selected Answer: D

D. Designated Approving Authority

upvoted 1 times

4vv 2 years ago

did you take the exam, are these in it

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

correct

upvoted 2 times

Question #6 *Topic 1*

DoD 8500.2 establishes IA controls for information systems according to the Mission Assurance Categories (MAC) and confidentiality levels. Which of the following MAC levels requires high integrity and medium availability?

A. MAC III

B. MAC IV

C. MAC I

D. MAC II

Suggested Answer: *D*

The various MAC levels are as follows: MAC I: It states that the systems have high availability and high integrity. MAC II: It states that the systems have high integrity and medium availability. MAC III: It states that the systems have basic integrity and availability.

Community vote distribution

D (100%)

arunraj90hr Most Recent 11 months, 1 week ago

Integrity Availability MAC I High High MAC II High Medium MAC III Basic / Low Basic / Low

upvoted 1 times

74gjd_37 1 year, 10 months ago

D. "MAC II" is the answer. Source: https://acqnotes.com/acqnote/careerfields/mission-assurance-category MAC I has High, MAC II has Medium and MAC III has Basic availability. There is no MAC IV, as there are only 3 levels from MAC I through MAC III. See also https://en.wikipedia.org/wiki/Mission_assurance

upvoted 2 times

4e3rv21rq3vq2q 3 years, 1 month ago

correct

upvoted 2 times

Question #7 *Topic 1*

Microsoft software security expert Michael Howard defines some heuristics for determining code review in "A Process for Performing Security Code Reviews".
Which of the following heuristics increase the application's attack surface? Each correct answer represents a complete solution. Choose all that apply.

A. Code written in C/C++/assembly language

B. Code listening on a globally accessible network interface

C. Code that changes frequently

D. Anonymously accessible code

E. Code that runs by default

F. Code that runs in elevated context

Suggested Answer: *B, D, E, F*
Microsoft software security expert Michael Howard defines the following heuristics for determining code review in "A Process for Performing Security Code Reviews": Old code: Newer code provides better understanding of software security and has lesser number of vulnerabilities. Older code must be checked deeply. Code that runs by default: It must have high quality, and must be checked deeply than code that does not execute by default. Code that runs by default increases the application's attack surface. Code that runs in elevated context: It must have higher quality. Code that runs in elevated privileges must be checked deeply and increases the application's attack surface. Anonymously accessible code: It must be checked deeply than code that only authorized users and administrators can access, and it increases the application's attack surface. Code listening on a globally accessible network interface: It must be checked deeply for security vulnerabilities and increases the application's attack surface. Code written in C/C++/assembly language: It is prone to security vulnerabilities, for example, buffer overruns. Code with a history of security vulnerabilities: It includes additional vulnerabilities except concerted efforts that are required for removing them. Code that handles sensitive data: It must be checked deeply to ensure that data is protected from unintentional disclosure. Complex code: It includes undiscovered errors because it is more difficult to analyze complex code manually and programmatically. Code that changes frequently: It has more security vulnerabilities than code that does not change frequently.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago
The article by Michael Howard lists the following heuristics to determine code review priority: Old code Code that runs by default Code that runs in elevated context Anonymously accessible code Code listening on a globally accessible network interface Code written in C/C++/assembly language Code with a history of vulnerabilities Code that handles sensitive data Complex code Code that changes frequently Therefore, all options have to be checked (ABCDEF). The option BDEF is incorrect as it does not include A and C mentioned in the article.
upvoted 2 times

4e3rv21rq3vq2q 3 years, 1 month ago
seems to be correct
upvoted 1 times

Question #8 *Topic 1*

Which of the following cryptographic system services ensures that information will not be disclosed to any unauthorized person on a local network?

A. Authentication

B. Integrity

C. Non-repudiation

D. Confidentiality

Suggested Answer: *D*

The confidentiality service of a cryptographic system ensures that information will not be disclosed to any unauthorized person on a local network.

Community vote distribution

D (100%)

c08c27b Most Recent 2 years ago

D confidentiality

upvoted 1 times

74gjd_37 2 years, 4 months ago

Confidentialy (D)

upvoted 1 times

4e3rv21rq3vq2q 3 years, 7 months ago

correct

upvoted 1 times

Question #9 *Topic 1*

What are the various activities performed in the planning phase of the Software Assurance Acquisition process? Each correct answer represents a complete solution. Choose all that apply.

A. Develop software requirements.

B. Implement change control procedures.

C. Develop evaluation criteria and evaluation plan.

D. Create acquisition strategy.

Suggested Answer: *B*

The various activities performed in the planning phase of the Software Assurance Acquisition process are as follows: Determine software product or service requirements. Identify associated risks. Develop software requirements. Create acquisition strategy. Develop evaluation criteria and evaluation plan. Software Assurance acquisition process.

Community vote distribution

ACD (100%)

74gjd_37 1 year, 10 months ago

There is A Reference Guide for Security-Enhanced Software Acquisition and Outsourcing called "Software Assurance in Acquisition: Mitigating Risks to the Enterprise" by Information Resources Management College of National Defense University https://apps.dtic.mil/sti/pdfs/ADA495389.pdf It defines the folloiwng phases: - planning - contracting - monitoring and acceptance - follow-on The planning phase (quote) "begins with (1) needs determination for acquiring software services or products, identifying potential alternative software approaches, and identifying risks associated with those alternatives. This set of activities is followed by (2) developing software requirements to be included in work statements; (3) creating an acquisition strategy and/or plan that includes identifying risks associated with various software acquisition strategies; and (4) developing evaluation criteria and an evaluation plan. SwA considerations are discussed for each of the major activities. In the last part of this section (2.5), the development and use of SwA due diligence questionnaires are discussed.In the Planning Phase, there are several activities undertaken to ensure that Software Assurance in Acquisition is thoroughly considered before moving on to subsequent phases of development. Developing comprehensive software requirements helps identify which factors must be present in acquired or outsourced products or services for them to meet all functional and security-based specifications appropriately. Creating an evaluation plan and associated criteria allows project stakeholders to decide what aspects will be covered when examining potential vendors' proposals, work products, or services offered during the contracting phase adequately. Finally, outlining a clear acquisition strategy enables procuring organizations (including government institutions) to stay aware of relevant mandates/regulations potentially impeding progress related to acquiring security-enhanced software development

upvoted 2 times

74gjd_37 1 year, 10 months ago

Selected Answer: ACD

There is A Reference Guide for Security-Enhanced Software Acquisition and Outsourcing called "Software Assurance in Acquisition: Mitigating Risks to the Enterprise" by Information Resources Management College of National Defense University

https://apps.dtic.mil/sti/pdfs/ADA495389.pdf

It defines the folloiwng phases: - planning - contracting - monitoring and acceptance - follow-on

The planning phase (quote) "begins with (1) needs determination for acquiring software services or products, identifying potential alternative software approaches, and identifying risks associated with those alternatives. This set of activities is followed by (2) developing software requirements to be included in work statements; (3) creating an acquisition strategy and/or plan that includes identifying risks associated with various software acquisition strategies; and (4) developing evaluation criteria and an evaluation plan. SwA considerations are discussed for each of the major activities. In the last part of this section (2.5), the development and use of SwA due diligence questionnaires are discussed.

upvoted 2 times

74gjd_37 Most Recent 1 year, 10 months ago

In the Planning Phase, there are several activities undertaken to ensure that Software Assurance in Acquisition is thoroughly considered before moving on to subsequent phases of development. Developing comprehensive software requirements helps identify which factors must be present in acquired or outsourced products or services for them to meet all functional and security-based specifications appropriately. Creating an evaluation

plan and associated criteria allows project stakeholders to decide what aspects will be covered when examining potential vendors' proposals, work products, or services offered during the contracting phase adequately. Finally, outlining a clear acquisition strategy enables procuring organizations (including government institutions) to stay aware of relevant mandates/regulations potentially impeding progress related to acquiring security-enhanced software development activities while developing a thorough course of action for mitigating any issues encountered during this stage effectively.

upvoted 1 times

74gjd_37 1 year, 10 months ago

Implementing change (or configuration) control procedures is a part of Monitoring and Acceptance Phase, not of a Planning Phase. Therefore, the correct answer is ACD.

upvoted 1 times

74gjd_37 1 year, 10 months ago

Implementing change control procedures typically occurs during the monitoring & acceptance phase when overlooking potential issues after deployment consequently creating deviations from intended outcomes or previous stages' goals within this life cycle model used as a reference guide by Information Resources Management College (IRMC) at National Defense University (NDU). Therefore it is not included in the planning phase's set of activities described above since it does not directly deal with designing new SwA measures but enforcing those previously established earlier while ensuring that their implementation matches original plans accordingly throughout runtime modifications performed when needed forming part of production maintenance.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

This set of activities is followed by (2) developing software requirements to be included in work statements; (3) creating an acquisition strategy and/or plan that includes identifying risks associated with various software acquisition strategies; and (4) developing evaluation criteria and an evaluation plan. SwA considerations are discussed for each of the major activities.

upvoted 1 times

Question #10 *Topic 1*

You work as a project manager for BlueWell Inc. You are working on a project and the management wants a rapid and cost-effective means for establishing priorities for planning risk responses in your project. Which risk management process can satisfy management's objective for your project?

A. Qualitative risk analysis

B. Historical information

C. Rolling wave planning

D. Quantitative analysis

Suggested Answer: *B*

Qualitative risk analysis is the best answer as it is a fast and low-cost approach to analyze the risk impact and its effect. It can promote certain risks onto risk response planning. Qualitative Risk Analysis uses the likelihood and impact of the identified risks in a fast and cost-effective manner. Qualitative Risk Analysis establishes a basis for a focused quantitative analysis or Risk Response Plan by evaluating the precedence of risks with a concern to impact on the project's scope, cost, schedule, and quality objectives. The qualitative risk analysis is conducted at any point in a project life cycle. The primary goal of qualitative risk analysis is to determine proportion of effect and theoretical response. The inputs to the Qualitative Risk Analysis process are: Organizational process assets

Community vote distribution



74gjd_37 1 year, 10 months ago

Qualitative Risk Analysis (Option A) technique prioritizes risks based on their probability of occurrence, impact on project objectives, and other subjective factors such as stakeholder perception. It also uses expert judgment to evaluate and rank risks using techniques like SWOT analysis or risk scoring matrices. The output of qualitative risk analysis helps project managers identify which risks require further action and what type of response is required to mitigate them effectively while balancing costs and benefits. Overall, this process provides management with valuable information necessary to make informed decisions about how best to respond to potential risks within the project budget constraints.B. Historical information: This option may be useful in identifying risks that were encountered in past projects, but these risks may not be similar to the ones faced by the current project. They also may not reflect new or updated industry-specific knowledge. C. Rolling wave planning: This option is a process of progressive elaboration where work is planned incrementally over time, reflecting data from completed activities to inform future tasks; it doesn't really address prioritizing risks nor give initial insights about how important each potential risk might be. D. Quantitative analysis: While this involves numerical modeling techniques such as Monte Carlo simulations for assessing probability and impact of identified risks, it can take more time and resources to complete than qualitative analysis because many factors must be considered beforehand so basically, being too detailed will slow down decision-making processes which goes against our original objectives indicated by management.

upvoted 1 times

74gjd_37 1 year, 10 months ago

Selected Answer: A

Qualitative Risk Analysis (Option A) technique prioritizes risks based on their probability of occurrence, impact on project objectives, and other subjective factors such as stakeholder perception. It also uses expert judgment to evaluate and rank risks using techniques like SWOT analysis or risk scoring matrices. The output of qualitative risk analysis helps project managers identify which risks require further action and what type of response is required to mitigate them effectively while balancing costs and benefits. Overall, this process provides management with valuable information necessary to make informed decisions about how best to respond to potential risks within the project budget constraints.

upvoted 1 times

74gjd_37 Most Recent 1 year, 10 months ago

B. Historical information: This option may be useful in identifying risks that were encountered in past projects, but these risks may not be similar to the ones faced by the current project. They also may not reflect new or updated industry-specific knowledge. C. Rolling wave planning: This option is a process of progressive elaboration where work is planned incrementally over time, reflecting data from completed activities to inform future tasks; it doesn't really address prioritizing risks nor give initial insights about how important each potential risk might be. D. Quantitative analysis: While this involves numerical modeling techniques such as Monte Carlo simulations for assessing probability and impact of identified risks, it can take more time and resources to complete than qualitative analysis because many factors must be considered beforehand so basically, being too detailed will slow down decision-making processes which goes against our original objectives indicated by management.

upvoted 1 times

Question #11 *Topic 1*

Which of the following models uses a directed graph to specify the rights that a subject can transfer to an object or that a subject can take from another subject?

A. Take-Grant Protection Model

B. Biba Integrity Model

C. Bell-LaPadula Model

D. Access Matrix

Suggested Answer: *D, A*

The take-grant protection model is a formal model used in the field of computer security to establish or disprove the safety of a given computer system that follows specific rules. It shows that for specific systems the question of safety is decidable in linear time, which is in general undecidable. The model represents a system as directed graph, where vertices are either subjects or objects. The edges between them are labeled and the label indicates the rights that the source of the edge has over the destination. Two rights occur in every instance of the model: take and grant. They play a special role in the graph rewriting address additional integrity requirements.

Community vote distribution

A (100%)

74gjd_37 1 year, 10 months ago

Option A: Take-grant protection model https://en.wikipedia.org/wiki/Take-grant_protection_model The model represents a system as directed graph, where vertices are either subjects or objects. The edges between them are labeled, and the label indicates the rights that the source of the edge has over the destination. Two rights occur in every instance of the model: take and grant. They play a special role in the graph rewriting rules describing admissible changes of the graph. There are a total of four such rules: take rule allows a subject to take rights of another object (add an edge originating at the subject) grant rule allows a subject to grant own rights to another object (add an edge terminating at the subject) create rule allows a subject to create new objects (add a vertex and an edge from the subject to the new vertex) remove rule allows a subject to remove rights it has over on another object (remove an edge originating at the subject)- The Biba Integrity Model focuses on the protection of data integrity and prevents unauthorized modification of information by enforcing a hierarchy of integrity levels. - The Bell-LaPadula Model specifies access control policies based on confidentiality requirements in a multilevel security environment, where subjects are assigned clearance levels representing their authorizations to access certain levels of sensitive information. - The Access Matrix is used to describe the permissions associated with specific objects and subjects in a system, providing an overview of who can access what resources under which conditions. Therefore, since none of these models use directed graphs to specify rights that can be transferred or taken away, options B, C and D are incorrect.

upvoted 2 times

74gjd_37 1 year, 10 months ago

Selected Answer: A

Option A: Take-grant protection model

https://en.wikipedia.org/wiki/Take-grant_protection_model

The model represents a system as directed graph, where vertices are either subjects or objects. The edges between them are labeled, and the label indicates the rights that the source of the edge has over the destination. Two rights occur in every instance of the model: take and grant. They play a special role in the graph rewriting rules describing admissible changes of the graph.

There are a total of four such rules:

take rule allows a subject to take rights of another object (add an edge originating at the subject) grant rule allows a subject to grant own rights to another object (add an edge terminating at the subject) create rule allows a subject to create new objects (add a vertex and an edge from the subject to the new vertex) remove rule allows a subject to remove rights it has over on another object (remove an edge originating at the subject)

upvoted 2 times

74gjd_37 Most Recent 1 year, 10 months ago

- The Biba Integrity Model focuses on the protection of data integrity and prevents unauthorized modification of information by enforcing a hierarchy of integrity levels. - The Bell-LaPadula Model specifies access control policies based on confidentiality requirements in a multilevel security

environment, where subjects are assigned clearance levels representing their authorizations to access certain levels of sensitive information. - The Access Matrix is used to describe the permissions associated with specific objects and subjects in a system, providing an overview of who can access what resources under which conditions. Therefore, since none of these models use directed graphs to specify rights that can be transferred or taken away, options B, C and D are incorrect.

upvoted 1 times

Etester 3 years, 3 months ago

take and Grant protection model

upvoted 1 times

Question #12 *Topic 1*

You are the project manager for GHY Project and are working to create a risk response for a negative risk. You and the project team have identified the risk that the project may not complete on time, as required by the management, due to the creation of the user guide for the software you're creating. You have elected to hire an external writer in order to satisfy the requirements and to alleviate the risk event. What type of risk response have you elected to use in this instance?

A. Transference

B. Exploiting

C. Avoidance

D. Sharing

Suggested Answer: *A*

This is an example of transference as you have transferred the risk to a third party. Transference almost always is done with a negative risk event and it usually requires a contractual relationship.

Community vote distribution



CertMaster Most Recent 1 year, 11 months ago

C . Avoidance: This involves taking action to eliminate the risk entirely. In your case, hiring an external writer to create the user guide completely eliminates the risk of not completing the project on time due to the user guide creation.

upvoted 1 times

74gjd_37 2 years, 10 months ago

Option A: Transferance is correct. Transference alone doesn't eliminate the risk entirely, but rather it transfers ownership of the identified risk to another party who has more capacity or expertise in managing that particular type of risk than you do. In this case, by hiring an external writer, you have transferred some of the responsibilities and accountability related to writing user guides to them. However, it's crucial to note that not all risks can be effectively transferred, as there is always the potential for something preventing effective transference from happening. Therefore when employing a transference strategy as your preferred risk response plan; You need to ensure that suitable contracts are in place with proper agreements that hold both parties responsible and accountable for meeting agreed-upon deadlines and outcomes based on specified metrics set during inception planning previously undertaken between stakeholders.Avoidance aims to eliminate the risk event by eliminating the cause of the identified threat. In this project scenario, creating a user manual for the software is essential and mandatory; avoiding it altogether would halt or significantly delay product development, which is not feasible nor desirable. As such, hiring an external writer to complete a user guide ensures that you are taking specific actions and mitigations to minimize any adverse impact on time schedules due to delays in completing this necessary requirement. This response strategy acknowledges that there will be risks involved but seeks ways to manage those risks rather than avoid them entirely. Hence, choosing transference as your risk response plan makes more sense in managing potential challenges related to writing professional documents and minimizing negative outcomes' impacts on GHY Project's objectives within defined budgets and deadlines.Risk sharing occurs when you allocate a portion of the risk to another party who will also be adversely affected by the same or

upvoted 2 times

74gjd_37 2 years, 10 months ago

Selected Answer: A

Option A: Transferance is correct.

Transference alone doesn't eliminate the risk entirely, but rather it transfers ownership of the identified risk to another party who has more capacity or expertise in managing that particular type of risk than you do. In this case, by hiring an external writer, you have transferred some of the responsibilities and accountability related to writing user guides to them.

However, it's crucial to note that not all risks can be effectively transferred, as there is always the potential for something preventing effective transference from happening. Therefore when employing a transference strategy as your preferred risk response plan; You need to ensure that suitable contracts are in place with proper agreements that hold both parties responsible and accountable for meeting agreed-upon deadlines and outcomes based on specified metrics set during inception planning previously undertaken between stakeholders.

upvoted 2 times

74gjd_37 2 years, 10 months ago

Avoidance aims to eliminate the risk event by eliminating the cause of the identified threat. In this project scenario, creating a user manual for the software is essential and mandatory; avoiding it altogether would halt or significantly delay product development, which is not feasible nor desirable. As such, hiring an external writer to complete a user guide ensures that you are taking specific actions and mitigations to minimize any adverse impact on time schedules due to delays in completing this necessary requirement. This response strategy acknowledges that there will be risks involved but seeks ways to manage those risks rather than avoid them entirely. Hence, choosing transference as your risk response plan makes more sense in managing potential challenges related to writing professional documents and minimizing negative outcomes' impacts on GHY Project's objectives within defined budgets and deadlines.

upvoted 1 times

74gjd_37 2 years, 10 months ago

Risk sharing occurs when you allocate a portion of the risk to another party who will also be adversely affected by the same or similar risks. Each party shares in both the likelihood and impact of loss associated with the risk event. In this scenario, if instead, you collaborated with another enterprise on creating user guides together, that would have been an example of risk sharing because each organization would share responsibility for ensuring timely completion of the task. However, hiring an external writer is a form of transference as it involves transferring part or all of the identified risks to a third-party provider responsible for completing specific tasks within specified timelines without burdening any other party involved in GHY project development.

upvoted 1 times

chronm 3 years, 1 month ago

Risk Transfer Avoidance always means that there is no risk anymore at all. By transfering the risk there is still a small risk (faulty contract or the external goes bancrupt)

upvoted 2 times

4e3rv21rq3vq2q 4 years, 1 month ago

Risk avoidance This technique usually involves developing an alternative strategy that is more likely to succeed, but is usually linked to a higher cost.

upvoted 3 times

Question #13 *Topic 1*

Which of the following organizations assists the President in overseeing the preparation of the federal budget and to supervise its administration in Executive
Branch agencies?

A. OMB

B. NIST

C. NSA/CSS

D. DCAA

Suggested Answer: *D, C, A*
The Office of Management and Budget (OMB) is a Cabinet-level office, and is the largest office within the Executive Office of the President (EOP) of the United States. The current OMB Director is Peter Orszag and was appointed by President Barack Obama. The OMB's predominant mission is to assist the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies. In helping to formulate the President's spending plans, the OMB evaluates the effectiveness of agency programs, policies, and procedures, assesses competing funding demands among agencies, and sets funding priorities. The OMB ensures that agency reports, rules, testimony, and proposed legislation are consistent with the President's Budget and with Administration policies. Central Security Service (NSA/CSS) is a crypto-logic intelligence agency of the United States government. It is administered as part of the United States Department of Defense. NSA is responsible for the collection and analysis of foreign communications and foreign signals intelligence, which involves cryptanalysis. NSA is also responsible for protecting U.S. government communications and information systems from similar agencies elsewhere, which involves cryptography. NSA is a key component of the U.S. Intelligence Community, which is headed by the Director of National Intelligence. The Central Security Service is a co-located agency created to coordinate intelligence activities and co-operation between NSA and U.S. military cryptanalysis agencies. NSA's work is limited Technology (NIST), known between 1901 and 1988 as the National Bureau of Standards (NBS), is a measurement standards laboratory which is a non-regulatory agency of the United States Department of Commerce. The institute's official mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life.

Community vote distribution



74gjd_37 1 year, 10 months ago

Selected Answer: A

A. OMB (Office of Management and Budget).

https://www.whitehouse.gov/omb/

The Office of Management and Budget oversees the implementation of the President’s vision across the Executive Branch. OMB carries out its mission through five main functions across executive departments and agencies:

- Budget development and execution; - Management, including oversight of agency performance, procurement, financial management, and information technology; - Coordination and review of all significant Federal regulations from executive agencies, privacy policy, information policy, and review and assessment of information collection requests; and - Clearance and coordination of legislative and other materials, including agency testimony, legislative proposals, and other communications with Congress, and coordination of other Presidential actions. - Clearance of Presidential Executive Orders and memoranda to agency heads prior to their issuance.

upvoted 1 times

74gjd_37 1 year, 10 months ago

A. OMB (Office of Management and Budget). https://www.whitehouse.gov/omb/ The Office of Management and Budget oversees the implementation of the President’s vision across the Executive Branch. OMB carries out its mission through five main functions across executive departments and agencies: - Budget development and execution; - Management, including oversight of agency performance, procurement, financial management, and information technology; - Coordination and review of all significant Federal regulations from executive agencies, privacy policy, information policy, and review and assessment of information collection requests; and - Clearance and coordination of legislative and other materials, including agency testimony, legislative proposals, and other communications with Congress, and coordination of other Presidential actions. - Clearance of Presidential

Executive Orders and memoranda to agency heads prior to their issuance.The other options are incorrect because: B. NIST (National Institute of Standards and Technology) is a non-regulatory agency that promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology. C. NSA/CSS (National Security Agency/Central Security Service) is the nation's cryptologic organization responsible for protecting national security information systems. D. DCAA (Defense Contract Audit Agency) provides audit and financial advisory services to Department of Defense (DoD) agencies in connection with procurement and contract administration activities.

upvoted 1 times

74gjd_37 Most Recent 1 year, 10 months ago

The other options are incorrect because: B. NIST (National Institute of Standards and Technology) is a non-regulatory agency that promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology. C. NSA/CSS (National Security Agency/Central Security Service) is the nation's cryptologic organization responsible for protecting national security information systems. D. DCAA (Defense Contract Audit Agency) provides audit and financial advisory services to Department of Defense (DoD) agencies in connection with procurement and contract administration activities.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

A. OMB

upvoted 1 times

Question #14 *Topic 1*

Part of your change management plan details what should happen in the change control system for your project. Theresa, a junior project manager, asks what the configuration management activities are for scope changes. You tell her that all of the following are valid configuration management activities except for which one?

A. Configuration Identification

B. Configuration Verification and Auditing

C. Configuration Status Accounting

D. Configuration Item Costing

Suggested Answer: *D*

Configuration item cost is not a valid activity for configuration management. Cost changes are managed by the cost change control system; configuration management is concerned with changes to the features and functions of the project deliverables.

Community vote distribution

D (100%)

74gjd_37 Most Recent 1 year, 10 months ago

D. Configuration Item Costing (is not a part of SCM), therefore should be selected.

upvoted 1 times

74gjd_37 1 year, 10 months ago

According to Wikipedia: The SCM process further defines the need to trace changes, and the ability to verify that the final delivered software has all of the planned enhancements that are supposed to be included in the release. It identifies four procedures that must be defined for each software project to ensure that a sound SCM process is implemented. They are: Configuration identification Configuration control Configuration status accounting Configuration audits

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

en.wikipedia.org/wiki/Configuration_management#Overview

upvoted 1 times

Question #15 *Topic 1*

Which of the following types of redundancy prevents attacks in which an attacker can get physical control of a machine, insert unauthorized software, and alter data?

A. Data redundancy

B. Hardware redundancy

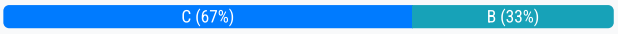
C. Process redundancy

D. Application redundancy

Suggested Answer: *C*

Process redundancy permits software to run simultaneously on multiple geographically distributed locations, with voting on results. It prevents attacks in which an attacker can get physical control of a machine, insert unauthorized software, and alter data.

Community vote distribution



c4310dc Most Recent 2 years, 1 month ago

Process redundancy involves running multiple instances of the same process, often on different systems. This provides protection against an attacker compromising a single machine, as the redundant processes on other systems would still be intact. Data redundancy (option A) primarily protects against data loss or corruption, but doesn't inherently prevent unauthorized software insertion or data alteration on a compromised machine. Hardware redundancy (option B) provides backup hardware components, but doesn't directly address software-based attacks or data alteration. Application redundancy (option D) is similar to process redundancy, but the question specifically mentions process redundancy as an option. Therefore, process redundancy (C) is the best answer, as running redundant processes on separate systems provides protection against an attacker compromising and altering data on a single physical machine.

upvoted 2 times

74gjd_37 2 years, 10 months ago

Selected Answer: B

Option B: Hardware Redundancy - should be the answer.

The key is the work "physical" in the question. This type of redundancy can prevent attacks on physical machines because even if an attacker gains physical control of a single machine and inserts unauthorized software in it; the redundant system remains unaffected and secure.

upvoted 2 times

74gjd_37 2 years, 10 months ago

Option B: Hardware Redundancy - should be the answer. The key is the work "physical" in the question. This type of redundancy can prevent attacks on physical machines because even if an attacker gains physical control of a single machine and inserts unauthorized software in it; the redundant system remains unaffected and secure.The other options, Data redundancy, Process redundancy and Application redundancy are incorrect because they do not specifically prevent attacks in which an attacker can get physical control of a machine. - Data redundancy refers to storing duplicate copies of the same data to ensure that it is always accessible but this does not address security issues arising from physical compromise. - Process redundancy involves having multiple identical processes set up as backups for each other so that if one fails the others can take over; again, this does not provide protection against attacks on physical machines. - Application Redundancy involves running multiple instances of the same application to ensure high availability and scalability. While this could reduce disruption caused by software failures or scheduled maintenance on applications systems it may have little impact on preventing physical breach induced attack vectors .

upvoted 2 times

74gjd_37 2 years, 10 months ago

The other options, Data redundancy, Process redundancy and Application redundancy are incorrect because they do not specifically prevent attacks in which an attacker can get physical control of a machine. - Data redundancy refers to storing duplicate copies of the same data to ensure that it is always accessible but this does not address security issues arising from physical compromise. - Process redundancy involves having multiple identical processes set up as backups for each other so that if one fails the others can take over; again, this does not provide protection against attacks on physical machines. - Application Redundancy involves running multiple instances of the same application to ensure high availability and scalability. While this could reduce disruption caused by software failures or scheduled maintenance on applications systems it may have little impact on preventing physical breach induced attack vectors .

upvoted 1 times

4e3rv21rq3vq2q 4 years, 1 month ago

C. Process redundancy

upvoted 2 times

Question #16 *Topic 1*

Which of the following individuals inspects whether the security policies, standards, guidelines, and procedures are efficiently performed in accordance with the company's stated security objectives?

A. Information system security professional

B. Data owner

C. Senior management

D. Information system auditor

Suggested Answer: *B, A*

An information system auditor is an individual who inspects whether the security policies, standards, guidelines, and procedures are efficiently performed in accordance with the company's stated security objectives. He is responsible for reporting the senior management about the value of security controls incorrect. An informational systems security professional is an individual who designs, implements, manages, and reviews the security policies, standards, senior management assigns overall responsibilities to other individuals.

Community vote distribution



01be656 Most Recent 1 year, 6 months ago

The correct answer is D. Information system auditor.

upvoted 1 times

CertMaster 1 year, 11 months ago

D. Information system auditor is the individual responsible for inspecting whether security policies, standards, guidelines, and procedures are being efficiently performed in accordance with the company's stated security objectives. Here's a breakdown of the other options: Information system security professional: While they are involved in security, their primary role is to implement and maintain security measures. Data owner: The data owner is responsible for the data itself, not the security measures. Senior management: Senior management is responsible for overall company strategy and direction, but they may not have the specific expertise to audit security practices.

upvoted 1 times

74gjd_37 2 years, 10 months ago

The question is about "efficiently" performed, not whether they are performed or not. Tjerefpre, the correct answer would be (Option A) Information system security professional, since they are responsible for ensuring that the security policies, standards, guidelines, and procedures are efficiently performed in accordance with the company's stated security objectives.- Data owners (Option B) are responsible for managing data within their purview and ensuring it is well classified and protected at all times. While they play an important role in security management, they may not specifically conduct inspections of security measures.- Information System Auditor (Option D) is not necessarily incorrect; However, the question specifically asks which individual inspects whether security objectives are efficiently performed. While auditing plays a pivotal role in evaluating overall performance on the said aspects; it does not inherently guarantee that efficient performance will follow-through consistently after audit delivery or understanding any risk mitigation recommendations shared by auditors. So while option D could be applicable here,it may have limited usefulness when compared to option A-Information System Security Professional who usually works collaboratively with all stakeholders across organization-wide projects for better Risk management optimization & practical implementation of set standards to achieve expected outcomes over time.- Senior management (Option C) has a critical responsibility of providing direction and support towards information security governance practices such as defining the risk appetite of an organization, providing resources and budget for implementing controls etc., however senior management might rely on audits or expert opinions internally before making any decisions.

upvoted 2 times

74gjd_37 2 years, 10 months ago

Selected Answer: A

The question is about "efficiently" performed, not whether they are performed or not. Tjerefpre, the correct answer would be (Option A) Information system security professional, since they are responsible for ensuring that the security policies, standards, guidelines, and procedures are efficiently performed in accordance with the company's stated security objectives.

upvoted 2 times

74gjd_37 2 years, 10 months ago

- Data owners (Option B) are responsible for managing data within their purview and ensuring it is well classified and protected at all times. While they play an important role in security management, they may not specifically conduct inspections of security measures.

upvoted 1 times

74gjd_37 2 years, 10 months ago

- Information System Auditor (Option D) is not necessarily incorrect; However, the question specifically asks which individual inspects whether security objectives are efficiently performed. While auditing plays a pivotal role in evaluating overall performance on the said aspects; it does not inherently guarantee that efficient performance will follow-through consistently after audit delivery or understanding any risk mitigation recommendations shared by auditors. So while option D could be applicable here,it may have limited usefulness when compared to option A- Information System Security Professional who usually works collaboratively with all stakeholders across organization-wide projects for better Risk management optimization & practical implementation of set standards to achieve expected outcomes over time.

upvoted 1 times

74gjd_37 2 years, 10 months ago

- Senior management (Option C) has a critical responsibility of providing direction and support towards information security governance practices such as defining the risk appetite of an organization, providing resources and budget for implementing controls etc., however senior management might rely on audits or expert opinions internally before making any decisions.

upvoted 2 times

4e3rv21rq3vq2q 4 years, 1 month ago

A. Information system security professional

upvoted 2 times

Question #17 *Topic 1*

Which of the following process areas does the SSE-CMM define in the 'Project and Organizational Practices' category? Each correct answer represents a complete solution. Choose all that apply.

A. Provide Ongoing Skills and Knowledge

B. Verify and Validate Security

C. Manage Project Risk

D. Improve Organization's System Engineering Process

Suggested Answer: *A, C, D*

Project and Organizational Practices include the following process areas: PA12: Ensure Quality PA13: Manage Configuration PA14: Manage Project Risk PA15: Monitor and Control Technical Effort PA16: Plan Technical Effort PA17: Define Organization's System Engineering Process PA18: Improve Organization's System Engineering Process PA19: Manage Product Line Evolution PA20: Manage Systems Engineering Support Environment PA21: Provide Ongoing Skills and Knowledge PA22: Coordinate with Suppliers

Community vote distribution

ACD (100%)

74gjd_37 1 year, 10 months ago

Selected Answer: ACD

The SSE-CMM also includes eleven process areas related to project and organizational practices. These process areas were adapted from the SE-CMM. These process areas and the base practices that define them are described in Annex B, and listed below: • PA12 - Ensure Quality; • PA13 - Manage Configuration; • PA14 - Manage Project Risk; (-- Option C --) • PA15 - Monitor and Control Technical Effort; • PA16 - Plan Technical Effort; • PA17 - Define Organization's Systems Engineering Process; • PA18 - Improve Organization's Systems Engineering Process; (-- Option D --) • PA19 - Manage Product Line Evolution; • PA20 - Manage Systems Engineering Support Environment; • PA21 - Provide Ongoing Skills and Knowledge; (-- Option A --) • PA22 - Coordinate with Suppliers

upvoted 1 times

74gjd_37 1 year, 10 months ago

The SSE-CMM also includes eleven process areas related to project and organizational practices. These process areas were adapted from the SE-CMM. These process areas and the base practices that define them are described in Annex B, and listed below: • PA12 - Ensure Quality; • PA13 - Manage Configuration; • PA14 - Manage Project Risk; (-- Option C --) • PA15 - Monitor and Control Technical Effort; • PA16 - Plan Technical Effort; • PA17 - Define Organization's Systems Engineering Process; • PA18 - Improve Organization's Systems Engineering Process; (-- Option D --) • PA19 - Manage Product Line Evolution; • PA20 - Manage Systems Engineering Support Environment; • PA21 - Provide Ongoing Skills and Knowledge; (-- Option A --) • PA22 - Coordinate with SuppliersThe "Verify and Validate Security" item is in the "systems security engineering process" section of the standard, therefore this option (B) should not be selected.

upvoted 1 times

74gjd_37 Most Recent 1 year, 10 months ago

The "Verify and Validate Security" item is in the "systems security engineering process" section of the standard, therefore this option (B) should not be selected.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

Correct Answer: ACD

upvoted 1 times

Question #18 *Topic 1*

The LeGrand Vulnerability-Oriented Risk Management method is based on vulnerability analysis and consists of four principle steps. Which of the following processes does the risk assessment step include? Each correct answer represents a part of the solution. Choose all that apply.

A. Remediation of a particular vulnerability

B. Cost-benefit examination of countermeasures

C. Identification of vulnerabilities

D. Assessment of attacks

Suggested Answer: *A*

Risk assessment includes identification of vulnerabilities, assessment of losses caused by threats materialized, cost-benefit examination of

Community vote distribution

BCD (100%)

74gjd_37 Most Recent 1 year, 10 months ago

The correct answers are B, C, and D. A is not a part of the risk assessment step, but rather a step that may come after the risk assessment step if a vulnerability is identified and needs to be addressed.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

Correct Answer: BCD

upvoted 1 times

Etester 3 years, 3 months ago

Remediation is a part of vulnerability management

upvoted 1 times

Question #19 *Topic 1*

You work as a Security Manager for Tech Perfect Inc. You have set up a SIEM server for the following purposes: Analyze the data from different log sources
Correlate the events among the log entries Identify and prioritize significant events Initiate responses to events if required One of your log monitoring staff wants to know the features of SIEM product that will help them in these purposes. What features will you recommend? Each correct answer represents a complete solution.
Choose all that apply.

A. Asset information storage and correlation

B. Transmission confidentiality protection

C. Incident tracking and reporting

D. Security knowledge base

E. Graphical user interface

Suggested Answer: *A, B*
The features of SIEM products are as follows: Graphical user interface (GUI): It is used in analysis for identifying potential problems and reviewing all available data that are associated with the problems. Security knowledge base: It includes information on known vulnerabilities, log messages, and other technical data. Incident tracking and hacking: It has robust workflow features to track and report incidents. Asset information storage and correlation: It gives higher priority

Community vote distribution
ACDE (100%)

4e3rv21rq3vq2q 3 years, 1 month ago
Selected Answer: ACDE
it's ACDE
upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago
it's ACDEWhy not B also? Transmission confidentiality protection feature ensures that the data being transmitted between different components of the SIEM system is kept confidential and secure. This is particularly important when the SIEM system is being used to collect and analyze sensitive data, such as network logs and security events.
upvoted 1 times

74gjd_37 Most Recent 1 year, 10 months ago
Why not B also? Transmission confidentiality protection feature ensures that the data being transmitted between different components of the SIEM system is kept confidential and secure. This is particularly important when the SIEM system is being used to collect and analyze sensitive data, such as network logs and security events.
upvoted 1 times

Question #20 *Topic 1*

According to U.S. Department of Defense (DoD) Instruction 8500.2, there are eight Information Assurance (IA) areas, and the controls are referred to as IA controls. Which of the following are among the eight areas of IA defined by DoD? Each correct answer represents a complete solution. Choose all that apply.

A. VI Vulnerability and Incident Management

B. Information systems acquisition, development, and maintenance

C. DC Security Design & Configuration

D. EC Enclave and Computing Environment

Suggested Answer: *B*

According to U.S. Department of Defense (DoD) Instruction 8500.2, there are eight Information Assurance (IA) areas, and the controls are referred to as IA controls. Following are the various U.S. Department of Defense information security standards: DC Security Design & Configuration IA Identification and Authentication EC Enclave and Computing Environment EB Enclave Boundary Defense PE Physical and Environmental PR Personnel CO Continuity VI

Community vote distribution

ACD (100%)

74gjd_37 Most Recent 1 year, 10 months ago

The areas are the following: - DC Security Design & Configuration - IA Identification and Authentication - EC Enclave and Computing Environment - EB Enclave Boundary Defense - PE Physical and Environmental - PR Personnel - CO Continuity - VI Vulnerability and Incident Management We didn't find option B (Information systems acquisition, development, and maintenance) in the list above, but found other options. Therefore, all options should be selected, except B.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

Correct Answer: ACD

upvoted 1 times

Question #21 *Topic 1*

The Information System Security Officer (ISSO) and Information System Security Engineer (ISSE) play the role of a supporter and advisor, respectively. Which of the following statements are true about ISSO and ISSE? Each correct answer represents a complete solution. Choose all that apply.

A. An ISSE manages the security of the information system that is slated for Certification & Accreditation (C&A).

B. An ISSE provides advice on the continuous monitoring of the information system.

C. An ISSO manages the security of the information system that is slated for Certification & Accreditation (C&A).

D. An ISSE provides advice on the impacts of system changes. E. An ISSO takes part in the development activities that are required to implement system

Suggested Answer: *B, C, D*

An Information System Security Officer (ISSO) plays the role of a supporter. The responsibilities of an Information System Security Officer (ISSO) are as follows: Manages the security of the information system that is slated for Certification & Accreditation (C&A). Insures the information systems configuration with the agency's information security policy. Supports the information system owner/information owner for the completion of security-related responsibilities. Takes part in the formal configuration management process. Prepares Certification & Accreditation (C&A) packages. An Information System Security Engineer (ISSE) plays the role of an advisor. The responsibilities of an Information System Security Engineer are as follows: Provides view on the continuous monitoring of the information system. Provides advice on the impacts of system changes. Takes part in the configuration management process. Takes part in the development activities that are required to implement system changes. Follows approved system changes.

Community vote distribution

BCD (100%)

4e3rv21rq3vq2q Most Recent 2 years, 1 month ago

Correct Answer: BCD

upvoted 1 times

Question #22 *Topic 1*

In which of the following types of tests are the disaster recovery checklists distributed to the members of disaster recovery team and asked to review the assigned checklist?

A. Parallel test

B. Simulation test

C. Full-interruption test

D. Checklist test

Suggested Answer: *B, A*

A checklist test is a test in which the disaster recovery checklists are distributed to the members of the disaster recovery team. All members are asked to review the assigned checklist. The checklist test is a simple test and it is easy to conduct this test. It allows to accomplish the following three goals: It ensures that the employees are aware of their responsibilities and they have the refreshed knowledge. It provides an individual with an opportunity to review the checklists for obsolete information and update any items that require modification during the changes in the organization. It ensures that the assigned members of operates just like a structured walk- through test. In the simulation test, the members of a disaster recovery team present with a disaster scenario and then, discuss on appropriate responses. These suggested responses are measured and some of them are taken by the team. The range of the simulation test should procedure, and relocates the employees to an alternate recovery site and implements site activation procedures. These employees present with their disaster recovery responsibilities as they would for an actual disaster. The disaster recovery sites have full responsibilities to conduct the day-to-day organization's the disaster recovery plan. It operates just like a parallel test. The full-interruption test is very expensive and difficult to arrange. Sometimes, it causes a major disruption of operations if the test fails.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

CISSP official study guide (9th Edition) on page 902-903 mentions that "Checklist tests are purely paperwork exercises", having no impact on business operations. On pages 899-900, checklist tests are referred to as a "read-through" tests. The purpose of this type of test is to review and verify the disaster recovery checklists to ensure that they are complete, accurate, and effective. The disaster recovery team members are typically given the checklists to review and provide feedback on any gaps or deficiencies in the plan before an actual disaster occurs. The correct answer is "D".

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

Correct Answer: D

upvoted 1 times

Question #23 *Topic 1*

SIMULATION -

Fill in the blank with an appropriate phrase. models address specifications, requirements, design, verification and validation, and maintenance activities.

Suggested Answer:

A life cycle model helps to provide an insight into the development process and emphasizes on the relationships among the different activities in this process. This model describes a structured approach to the development and adjustment process involved in producing and maintaining systems. The life cycle model addresses specifications, design, requirements, verification and validation, and maintenance activities.

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

Question #24 *Topic 1*

Which of the following security design patterns provides an alternative by requiring that a user's authentication credentials be verified by the database before providing access to that user's data?

A. Secure assertion

B. Authenticated session

C. Password propagation

D. Account lockout

Suggested Answer: *D, A*

Password propagation provides an alternative by requiring that a user's authentication credentials be verified by the database before providing specific sanity checks throughout the system.

Community vote distribution

C (100%)

74gjd_37 Most Recent 1 year, 10 months ago

There is a "Security Patterns Repository" by Darrell M. Kienzle, Matthew C. Elder, David Tyree, James Edwards-Hewitt at https://www.cse.msu.edu/~cse870/Homework/SS2005/HW5/Kienzle.pdf There is a secure design pattern called "Password Propagation" that means the following (quote): "Many Web applications rely on a single database account to store and manage all user data. If such an application is compromised, the attacker might have complete access to every user's data. The Password Propagation pattern provides an alternative by requiring that an individual user's authentication credentials be verified by the database before access is provided to that user's data."

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

Correct Answer: C

upvoted 1 times

Question #25 *Topic 1*

Which of the following is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in business continuity?

A. RTO

B. RTA

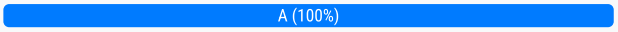
C. RPO

D. RCO

Suggested Answer: *B*

The Recovery Time Objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster or disruption in order to avoid unacceptable consequences associated with a break in business continuity. It includes the time for trying to fix the problem without a recovery, the recovery itself, tests and the communication to the users. Decision time for user representative is not included. The business continuity timeline usually runs parallel with an incident management timeline and may start at the same, or different, points. In accepted business continuity planning methodology, the RTO is established during the Business Impact Analysis (BIA) by the owner of a process (usually in conjunction with the Business Continuity planner). The RTOs are then presented to senior management for acceptance. The RTO attaches to the business process and not the resources required to support the methodology the technology support team develops. This is the time frame the technology support takes to deliver the recovered infrastructure to the business. Objective (RPO) describes the acceptable amount of data loss measured in time. It is the point in time to which data must be recovered as defined by the organization. The RPO is generally a definition of what an organization determines is an "acceptable loss" in a disaster situation. If the RPO of a company is 2 hours and the time it takes to get the data back into production is 5 hours, the RPO is still 2 hours. Based on this RPO the data must be restored to within 2 hours of the disaster.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

The correct answer is A. RTO (Recovery Time Objective) is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in business continuity

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

Correct Answer: A

upvoted 1 times

Question #26 *Topic 1*

Which of the following processes culminates in an agreement between key players that a system in its current configuration and operation provides adequate protection controls?

A. Information Assurance (IA)

B. Information systems security engineering (ISSE)

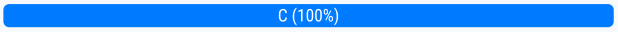
C. Certification and accreditation (C&A)

D. Risk Management

Suggested Answer: *D, A*

Certification and accreditation (C&A) is a set of processes that culminate in an agreement between key players that a system in its current configuration and operation provides adequate protection controls. Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. The C&A process is used extensively in the U.S. Federal Government. Some C&A processes include FISMA, NIACAP, DIACAP, and DCID 6/3. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the information-related risks. It ensures that only the approved users have access to the approved information at the approved time. IA practitioners seek to protect and defend information and information systems by ensuring confidentiality, integrity, authentication, availability, and non-repudiation. These objectives are and solutions used during all phases of a system's life cycle to meet the system's information protection needs.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

Certification is typically the result of an audit or evaluation process and not an agreement. However, accreditation does involve an agreement between key players, such as the system owner, accrediting authority, and other stakeholders, about the level of risk that is acceptable for the system and the controls that are in place to manage that risk. The accreditation decision is based on a review of the system's certification report and other relevant information, and it represents an official endorsement that the system meets the established security requirements and can be operated in its current state.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

Correct Answer: C

upvoted 1 times

Question #27 *Topic 1*

Adam works as a Computer Hacking Forensic Investigator for a garment company in the United States. A project has been assigned to him to investigate a case of a disloyal employee who is suspected of stealing design of the garments, which belongs to the company and selling those garments of the same design under different brand name. Adam investigated that the company does not have any policy related to the copy of design of the garments. He also investigated that the trademark under which the employee is selling the garments is almost identical to the original trademark of the company. On the grounds of which of the following laws can the employee be prosecuted?

A. Espionage law

B. Trademark law

C. Cyber law

D. Copyright law

Suggested Answer: *A, D*

The Trademark law is a piece of legislation that contains the federal statutes of trademark law in the United States. The Act prohibits a number of activities, including trademark infringement, trademark dilution, and false advertising. Trademarks were traditionally protected in the United States only under State common law, growing out of the tort of unfair competition. Trademark law in the United States is almost entirely enforced through private lawsuits. The exception is in the case of criminal counterfeiting of goods. Otherwise, the responsibility is entirely on the mark owner to file suit in either state or federal civil court in order to United States governs the legally enforceable rights of creative and artistic works under the laws of the United States. Copyright law in the United States is part of federal law, and is authorized by the U.S. Constitution. The power to enact copyright law is granted in Article I, Section 8, Clause 8, also known as the Copyright Clause. This clause forms the basis for U.S. copyright law ("Science", "Authors", "Writings") and patent law ("useful Arts", "Inventors", "Discoveries"), and includes the limited terms (or durations) allowed for copyrights and patents ("limited Times"), as well as the items they may protect. In the U.S., registrations of claims of copyright, recordation of copyright transfers, and other administrative aspects of copyright are the responsibility of the United States Copyright Office, a part of the 1917, which made it a crime for a person: To convey information with intent to interfere with the operation or success of the armed forces of the United States or to promote the success of its enemies. This was punishable by death or by imprisonment for not more than 30 years. To convey false reports or false statements with intent to interfere with the operation or success of the military or naval forces of the United States or to promote the success of its enemies and whoever when the United States is at war, to cause or attempt to cause insubordination, disloyalty, mutiny, refusal of duty, in the military or naval forces of the United States, or to related to the use of communicative, transactional and distributive aspect of networked information device and technologies. It is commonly known as INTERNET LAW. These Laws are important to apply as Internet does not tend to make any geographical and jurisdictional boundaries clear; this is the reason why Cyber law is not very efficient. A single transaction may involve the laws of at least three jurisdictions, which are as follows: 1.The laws of the state/nation in which the user resides 2.The laws of the state/nation that apply where the server hosting the transaction is located 3.The laws of the state/nation, which apply to the person or business with whom the transaction takes place

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

B. Trademark law. The Espionage law is unlikely to apply in this case. Espionage involves the theft of government secrets or classified information that could harm national security. It is not typically used in cases of intellectual property theft or trademark infringement. While the employee's actions are certainly unethical and possibly illegal, they do not involve the theft of national secrets or classified information. Therefore, the Espionage law is not applicable to this case.

upvoted 1 times

anuradha1306 2 years, 2 months ago

B. Trademark law Trademark law protects the rights of a company or individual to use and protect their unique brand names, logos, and other distinctive marks associated with their goods or services. In this case, the employee is suspected of selling garments under a different brand name that is almost identical to the original trademark of the company. This can be considered as trademark infringement, as the employee is using a confusingly similar mark to deceive customers and profit from the company's reputation and designs. It's important to note that other laws, such as copyright law, may also be applicable depending on the specifics of the case, such as the originality and copyright protection of the garment designs. However, based on the information provided, the most relevant law for prosecuting the employee would be trademark law.

upvoted 1 times

Question #28 *Topic 1*

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. In order to do so, he performs the following steps of the pre-attack phase successfully: Information gathering Determination of network range Identification of active systems Location of open ports and applications Now, which of the following tasks should he perform next?

A. Perform OS fingerprinting on the We-are-secure network.

B. Map the network of We-are-secure Inc.

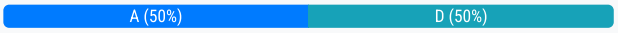
C. Install a backdoor to log in remotely on the We-are-secure server.

D. Fingerprint the services running on the we-are-secure network.

Suggested Answer: *D, B*

John will perform OS fingerprinting on the We-are-secure network. Fingerprinting is the easiest way to detect the Operating System (OS) of a remote system. OS detection is important because, after knowing the target system's OS, it becomes easier to hack into the system. The comparison of data packets that are sent by the target system is done by fingerprinting. The analysis of data packets gives the attacker a hint as to which operating system is being used by the remote system. There are two types of fingerprinting techniques as follows: 1.Active fingerprinting 2.Passive fingerprinting In active fingerprinting ICMP messages are sent to the target system and the response message of the target system shows which OS is being used by the remote system. In passive fingerprinting the identify which services are running on the network since there are many services that run only on a specific operating system. After performing OS fingerprinting, John install a backdoor.

Community vote distribution



anuradha1306 Most Recent 1 year, 8 months ago

D. Fingerprint the services running on the we-are-secure network. After gathering information, determining the network range, identifying active systems, and locating open ports and applications, the next logical step is to fingerprint the services running on the network. Service fingerprinting involves analyzing the network services and applications to determine their specific versions, configurations, and vulnerabilities. By fingerprinting the services, John can gain a better understanding of the target system's software and potentially identify any known vulnerabilities associated with those services. This information will be crucial for the subsequent steps in the ethical hacking process, such as vulnerability scanning and exploitation.

upvoted 1 times

4e3rv21rq3vq2q 2 years, 7 months ago

Correct Answer: A

upvoted 1 times

Question #29 *Topic 1*

Which of the following DITSCAP C&A phases takes place between the signing of the initial version of the SSAA and the formal accreditation of the system?

A. Phase 4

B. Phase 3

C. Phase 1

D. Phase 2

Suggested Answer: *C, B, A*

The Phase 2 of DITSCAP C&A is known as Verification. The goal of this phase is to obtain a fully integrated system for certification testing and accreditation. This phase takes place between the signing of the initial version of the SSAA and the formal accreditation of the system. This phase verifies security SSAA and the formal accreditation of the system.

Community vote distribution

D (100%)

74gjd_37 Most Recent 1 year, 10 months ago

There are four DITSCAP phases: 1. Definition 2. Verification 3. Validation 4. Post accreditation

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

it's D

upvoted 1 times

Question #30 *Topic 1*

In which of the following testing methodologies do assessors use all available documentation and work under no constraints, and attempt to circumvent the security features of an information system?

A. Full operational test

B. Penetration test

C. Paper test

D. Walk-through test

Suggested Answer: *A, C*

A penetration testing is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution. The intent of a penetration test is to determine feasibility of an attack complex test in the disaster recovery and business continuity testing approaches. In this test, the BCP/DRP plan documents are distributed to the appropriate managers and BCP/DRP team members for review, markup, and comment. This approach helps the auditor to ensure that the plan is complete and that all team continuity and disaster recovery process. In this testing methodology, appropriate managers and BCP/DRP team members discuss and walk through procedures members and participants in the disaster recovery and business continuity process. This full operation test involves the mobilization of personnel. It restores operations in the same manner as an outage or disaster would. The full operational test extends the preparedness test by including actual notification, mobilization of resources, processing of data, and utilization of backup media for restoration.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

A walk-through test is not typically used to circumvent security features of an information system. Rather, it is a type of static testing that is used to review the design and code of a system to identify any potential issues such as syntax errors, logical errors, or other issues that may arise. A walk-through test is used to identify and correct problems before the system is deployed or tested. In contrast, a penetration test is a type of dynamic testing where the tester attempts to exploit vulnerabilities and circumvent security features of an information system. The goal of a penetration test is to simulate an attack on a system to identify potential security weaknesses.

upvoted 1 times

anuradha1306 2 years, 2 months ago

The testing methodology in which assessors use all available documentation, work under no constraints, and attempt to circumvent the security features of an information system is: B. Penetration test Penetration testing, also known as ethical hacking, involves simulating real-world attacks on an information system to identify vulnerabilities and assess its security posture. In this testing methodology, assessors have access to all available documentation, work without constraints, and attempt to exploit security weaknesses in the system.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

B. Penetration test

upvoted 1 times

Question #31 *Topic 1*

You work as a systems engineer for BlueWell Inc. Which of the following tools will you use to look outside your own organization to examine how others achieve their performance levels, and what processes they use to reach those levels?

A. Benchmarking

B. Six Sigma

C. ISO 9001:2000

D. SEI-CMM

Suggested Answer: *C*





Benchmarking is the tool used by system assessment process to provide a point of reference by which performance measurements can be reviewed with respect to other organizations. Benchmarking is also recognized as Best Practice Benchmarking or Process Benchmarking. It is a process used in management and mostly useful for strategic management. It is the process of comparing the business processes and performance metrics including cost, cycle time, productivity, or quality to another that is widely considered to be an industry standard benchmark or best practice. It allows organizations to develop plans on how to implement best practice with the aim of increasing some aspect of performance. Benchmarking might be a one-time event, although it is frequently treated as a continual process in which organizations continually seek out to challenge their practices. It allows organizations to develop plans on how to make standard combines the three standards 9001, 9002, and 9003 into one, called 9001. Design and development procedures are required only if a company does in fact engage in the creation of new products. The 2000 version sought to make a radical change in thinking by actually placing the concept of process management front and center ("Process management" was the monitoring and optimizing of a company's tasks and activities, instead of just inspecting the final product). The ISO 9001:2000 version also demands involvement by upper executives, in order to integrate quality into the business system and avoid delegation of quality functions to junior administrators. Another goal is to improve effectiveness via process performance metrics numerical measurement of the effectiveness of tasks business management strategy, initially implemented by Motorola. As of 2009 it enjoys widespread application in many sectors of industry, although its application is not without controversy. Six Sigma seeks to improve the quality of process outputs by identifying and removing the causes of defects and variability in manufacturing and business processes. It uses a set of quality management methods, including statistical methods, and creates a special infrastructure of people within the organization ("Black Belts", "Green Belts", etc.) who are experts in these methods. Each Six Sigma project carried out within an organization follows a defined sequence of steps and has quantified financial targets (cost reduction or profit increase). The often used Six Sigma symbol is as follows: organizational development is a process improvement approach that provides organizations with the essential elements for effective process improvement. It can be used to guide process improvement across a project, a division, or an entire organization. CMMI can help integrate traditionally separate organizational functions, set process improvement goals and priorities, provide guidance for quality processes, and provide a point of reference for appraising current processes. CMMI is now the de facto standard for measuring the maturity of any process. Organizations can be assessed against the CMMI model using Standard CMMI Appraisal Method for Process Improvement (SCAMPI).

Community vote distribution

A (100%)

74gjd_37 Most Recent 1 year, 10 months ago

Benchmarking allow to identify how other organizations in your industry are securing their software development lifecycle and what best practices they are implementing. This can help you assess your organization's performance and identify areas for improvement. Six Sigma and ISO 9001:2000

are more general quality management methodologies, while SEI-CMM is a model specifically for assessing the maturity of software development processes.

upvoted 1 times

anuradha1306 2 years, 2 months ago

Correct Answer: A Explanation/Reference: Explanation: Benchmarking is the tool used by system assessment process to provide a point of reference by which performance measurements can be reviewed with respect to other organizations. Benchmarking is also recognized as Best Practice Benchmarking or Process Benchmarking. It is a process used in management and mostly useful for strategic management.

upvoted 2 times

Question #32 *Topic 1*

Which of the following methods determines the principle name of the current user and returns the jav a.security.Principal object in the HttpServletRequest interface?

A. getUserPrincipal()

B. isUserInRole()

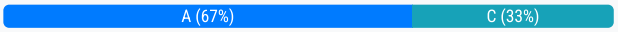
C. getRemoteUser()

D. getCallerPrincipal()

Suggested Answer: *C*

The getUserPrincipal() method determines the principle name of the current user and returns the java.security.Principal object. The incorrect. The getRemoteUser() method returns the user name that is used for the client authentication. The value of the getRemoteUser() method returns null if method is used to identify a caller using a java.security.Principal object. It is not used in the HttpServletRequest interface.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

https://docs.oracle.com/javaee/7/api/javax/servlet/http/HttpServletRequest.html#getUserPrincipal-- Principal getUserPrincipal() Returns a java.security.Principal object containing the name of the current authenticated user. If the user has not been authenticated, the method returns null.

upvoted 1 times

chronm 2 years, 1 month ago

https://tomcat.apache.org/tomcat-10.0-doc/servletapi/jakarta/servlet/http/HttpServletRequest.html#getUserPrincipal()

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

C. getRemoteUser()

upvoted 1 times

Question #33 *Topic 1*

The NIST Information Security and Privacy Advisory Board (ISPAB) paper "Perspectives on Cloud Computing and Standards" specifies potential advantages and disdvantages of virtualization. Which of the following disadvantages does it include? Each correct answer represents a complete solution. Choose all that apply.

A. It increases capabilities for fault tolerant computing using rollback and snapshot features.

B. It increases intrusion detection through introspection.

C. It initiates the risk that malicious software is targeting the VM environment.

D. It increases overall security risk shared resources.

E. It creates the possibility that remote attestation may not work.

F. It involves new protection mechanisms for preventing VM escape, VM detection, and VM-VM interference.

G. It increases configuration effort because of complexity and composite system.

Suggested Answer: *A, B*

The potential security disadvantages of virtualization are as follows: It increases configuration effort because of complexity and composite system. It initiates the problem of how to prevent overlap while mapping VM storage onto host files. It introduces the problem of virtualizing the TPM. It creates the possibility that remote attestation may not work. It initiates the problem of detecting VM covert channels. It involves new protection mechanisms for preventing VM escape, VM detection, and VM-VM interference. It initiates the possibility of virtual networking configuration errors. It initiates the risk that malicious software is targeting the VM environment. incorrect. These are not the disadvantages of virtualization, as described in the NIST Information Security and Privacy Advisory Board (ISPAB) paper "Perspectives on Cloud Computing and Standards".

Community vote distribution

CDEFG (100%)

74gjd_37 Most Recent 1 year, 10 months ago

The possible disadvantages of virtualization included in the NIST ISPAB paper are: C. It initiates the risk that malicious software is targeting the VM environment. D. It increases overall security risk shared resources. E. It creates the possibility that remote attestation may not work. F. It involves new protection mechanisms for preventing VM escape, VM detection, and VM-VM interference. G. It increases configuration effort because of complexity and composite system. The correct answers are: C, D, E, F, G.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

Correct Answer: CDEFG csrc.nist.gov/CSRC/media/Events/ISPAB-DECEMBER-2008-MEETING/documents/vmsec_ISPAB_L-Badger.pdf

upvoted 1 times

Question #34 *Topic 1*

Which of the following are the types of access controls? Each correct answer represents a complete solution. Choose three.

A. Physical

B. Technical

C. Administrative

D. Automatic

Suggested Answer: *D*

Security guards, locks on the gates, and alarms come under physical access control. Policies and procedures implemented by an organization come incorrect. There is no such type of access control as automatic control.

Community vote distribution

ABC (100%)

74gjd_37 Most Recent 1 year, 10 months ago

Option D is not a recognized type of access control in information security practice.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

it's ABC

upvoted 1 times

Question #35 *Topic 1*

What are the subordinate tasks of the Initiate and Plan IA C&A phase of the DIACAP process? Each correct answer represents a complete solution. Choose all that apply.

A. Initiate IA implementation plan

B. Develop DIACAP strategy

C. Assign IA controls.

D. Assemble DIACAP team

E. Register system with DoD Component IA Program.

F. Conduct validation activity.

Suggested Answer: *F*

The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is a process defined by the United States Department of Defense (DoD) for managing risk. The subordinate tasks of the Initiate and Plan IA C&A phase are as follows: Register system with DoD Component IA Program. Assign IA controls. Assemble DIACAP process, i.e., Implement and Validate Assigned IA Controls.

Community vote distribution

ABDE (100%)

74gjd_37 1 year, 10 months ago

The correct answers are: A. Initiate IA implementation plan B. Develop DIACAP strategy D. Assemble DIACAP team E. Register system with DoD Component IA Program. These are the subordinate tasks of the Initiate and Plan IA C&A phase of the DIACAP process. Assigning IA controls and conducting validation activity are part of later phases in the process (Implement and Validate), not the initial planning phase."IA" stands for Information Assurance, "C&A" stands for Certification and Accreditation, and "DIACAP" is an acronym for Defense Information Assurance Certification and Accreditation Process. Therefore, the full expansion of "Initiate and Plan IA C&A phase of the DIACAP" would be: The stage in the process where information assurance activities are initiated to certify that a defense information system meets security standards set by DoD along with developing plans to achieve accreditation. These activities include associated procedures like defining architecture baseline initiatives, controlling access points of vulnerabilities or potential threats during system lifecycle acquisition design; confirming necessary IT infrastructure requirements needed as dictated through consistently updated Compliance Risk Management (CRM) measures which adhere guidelines established in National Institute Standards Technology (NIST).

upvoted 1 times

74gjd_37 1 year, 10 months ago

Selected Answer: ABDE

The correct answers are:

A. Initiate IA implementation plan B. Develop DIACAP strategy D. Assemble DIACAP team E. Register system with DoD Component IA Program.

These are the subordinate tasks of the Initiate and Plan IA C&A phase of the DIACAP process. Assigning IA controls and conducting validation activity are part of later phases in the process (Implement and Validate), not the initial planning phase.

upvoted 1 times

74gjd_37 Most Recent 1 year, 10 months ago

"IA" stands for Information Assurance, "C&A" stands for Certification and Accreditation, and "DIACAP" is an acronym for Defense Information Assurance Certification and Accreditation Process. Therefore, the full expansion of "Initiate and Plan IA C&A phase of the DIACAP" would be: The stage in the process where information assurance activities are initiated to certify that a defense information system meets security standards set by DoD along with developing plans to achieve accreditation. These activities include associated procedures like defining architecture baseline initiatives, controlling access points of vulnerabilities or potential threats during system lifecycle acquisition design; confirming necessary IT infrastructure requirements needed as dictated through consistently updated Compliance Risk Management (CRM) measures which adhere guidelines established in National Institute Standards Technology (NIST).

upvoted 1 times

Question #36 *Topic 1*

Which of the following attacks causes software to fail and prevents the intended users from accessing software?

A. Enabling attack

B. Reconnaissance attack

C. Sabotage attack

D. Disclosure attack

Suggested Answer: *A, B*

A sabotage attack is an attack that causes software to fail. It also prevents the intended users from accessing software. A sabotage attack is referred attack delivers an easy path for other attacks.

Community vote distribution

C (100%)

74gjd_37 Most Recent 1 year, 10 months ago

A sabotage attack is a deliberate action aimed at disrupting, damaging or destroying computer systems, networks, and infrastructure. In the context of software security, sabotaging an application involves injecting malicious code into its source code or corrupting its data to impair its proper functioning. Sabotage attacks can lead to loss of critical data, downtime of essential services and applications which leads to business disruption and financial losses. It can also impact the reputation of an organization that relies on technology for operation if such incidents result in breach of confidentiality or integrity violations.

upvoted 1 times

Question #37 *Topic 1*

FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. Which of the following FITSAF levels shows that the procedures and controls have been implemented?

A. Level 2

B. Level 3

C. Level 5

D. Level 1

E. Level 4

Suggested Answer: *B*

The following are the five levels of FITSAF based on SEI's Capability Maturity Model (CMM): Level 1: The first level reflects that an asset has documented a security policy. Level 2: The second level shows that the asset has documented procedures and controls to implement the policy. Level 3: The third level indicates that these procedures and controls have been implemented. Level 4: The fourth level shows that the procedures and controls are tested and reviewed. Level 5: The fifth level is the final level and shows that the asset has procedures and controls fully integrated into a comprehensive program.

Community vote distribution

B (100%)

74gjd_37 Most Recent 1 year, 10 months ago

Selected Answer: B

https://csrc.nist.gov/files/pubs/other/2000/11/28/federal-information-technology-security-assessment/final/docs/federal-it-saf-2000.pdf

Level 1 Documented Policy Level 2 Documented Procedures Level 3 Implemented Procedures and Controls Level 4 Tested and Reviewed Procedures and Controls Level 5 Fully Integrated Procedures and Controls

The correct answer is B. Level 3, which indicates that the procedures and controls have been implemented and their effectiveness is being tested or validated.

upvoted 2 times

74gjd_37 1 year, 10 months ago

https://csrc.nist.gov/files/pubs/other/2000/11/28/federal-information-technology-security-assessment/final/docs/federal-it-saf-2000.pdf Level 1 Documented Policy Level 2 Documented Procedures Level 3 Implemented Procedures and Controls Level 4 Tested and Reviewed Procedures and Controls Level 5 Fully Integrated Procedures and Controls The correct answer is B. Level 3, which indicates that the procedures and controls have been implemented and their effectiveness is being tested or validated.

upvoted 2 times

4e3rv21rq3vq2q 3 years, 1 month ago

Correct Answer: B

upvoted 1 times

Question #38 *Topic 1*

Which of the following is a name, symbol, or slogan with which a product is identified?

A. Trademark

B. Copyright

C. Trade secret

D. Patent

Suggested Answer: *C, A*

A trademark is a name, symbol, or slogan with which a product is identified. Its uniqueness makes the product noticeable among the same type of products. For example, Pentium and Athlon are brand names of the CPUs that are manufactured by Intel and AMD, respectively. The trademark law protects a company's trademark by making it illegal for other companies to use it without taking prior permission of the trademark owner. A trademark is registered so that information which is not generally known. It helps a business to obtain an economic advantage over its competitors or customers. In some jurisdictions, such holder the exclusive right to produce copies of his or her works of original expression, such as a literary work, movie, musical work or sound recording, painting, photograph, computer program, or industrial design, for a defined, yet extendable, period of time. It does not cover ideas or facts. Copyright laws protect useful machine, process, composition of matter, etc. A patent enables the inventor to legally enforce his right to exclude others from using his invention.

Community vote distribution

A (100%)

74gjd_37 Most Recent 1 year, 10 months ago

A trademark is a recognizable sign, design, or expression which identifies products or services of a particular source and distinguishes them from those of others.

upvoted 1 times

Question #39 *Topic 1*

Della work as a project manager for BlueWell Inc. A threat with a dollar value of $250,000 is expected to happen in her project and the frequency of threat occurrence per year is 0.01. What will be the annualized loss expectancy in her project?

A. $2,000

B. $2,500

C. $3,510

D. $3,500

Suggested Answer: *D, C, A*

The annualized loss expectancy in her project will be $2,500. Annualized loss expectancy (ALE) is the annually expected financial loss to an organization from a threat. The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). It is mathematically expressed as follows: ALE = Single Loss Expectancy (SLE) * Annualized Rate of Occurrence (ARO) Here, it is as follows:

ALE = SLE * ARO - = 250,000 * 0.01 = 2,500

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

Question #40 *Topic 1*

Which of the following coding practices are helpful in simplifying code? Each correct answer represents a complete solution. Choose all that apply.

A. Programmers should use multiple small and simple functions rather than a single complex function.

B. Software should avoid ambiguities and hidden assumptions, recursions, and GoTo statements.

C. Programmers should implement high-consequence functions in minimum required lines of code and follow proper coding standards.

D. Processes should have multiple entry and exit points.

Suggested Answer: *D*

The various coding practices that are helpful in simplifying the code are as follows: Programmers should implement high-consequence functions in minimum required lines of code and follow the proper coding standards. Software should implement the functions that are defined in the software specification. Software should avoid ambiguities and hidden assumptions, recursion, and GoTo statements. Programmers should use multiple small and simple functions rather than a complex function. The processes should have only one entry point and minimum exit points. Interdependencies should be minimum so that a process module or component can be disabled when it is not needed, or replaced when it is found insecure or a better alternative is available, without disturbing the software operations. Programmers should use object-oriented techniques to keep the code simple and small. Some of the object-oriented techniques are object

Community vote distribution

ABC (100%)

74gjd_37 Most Recent 1 year, 10 months ago

High-consequence functions are those software functions that could significantly impact the confidentiality, integrity or availability of a system and its data. These include: Authentication mechanisms: Functions handling user authentication are considered high-consequence as they control access to critical data. Encryption/decryption algorithms: Functions used for encryption and decryption play an important role in protecting sensitive information from unauthorized access. Input validation routines: Functions that validate inputs provided by users can prevent malicious input from causing security vulnerabilities. Authorization controls: Functions responsible for determining what actions individual users may carry out within the system need to be carefully designed to ensure that only authorized actions are permitted. Audit logging functions: Logging activity is essential for maintaining accountability, detecting suspicious activity and maintaining compliance with legal requirements.

upvoted 1 times

Question #41 *Topic 1*

Which of the following methods does the Java Servlet Specification v2.4 define in the HttpServletRequest interface that control programmatic security? Each correct answer represents a complete solution. Choose all that apply.

A. getCallerIdentity()

B. isUserInRole()

C. getUserPrincipal()

D. getRemoteUser()

Suggested Answer: *A*

The various methods of the HttpServletRequest interface are as follows: getRemoteUser(): It returns the user name that is used for the client authentication. The value of the getRemoteUser() method returns null if no user is authenticated. isUserInRole(): It determines whether the remote user is granted a specified user role. The value of the isUserInRole() method returns true if the remote user is granted the specified user role; otherwise it returns false. getUserPrincipal(): It determines the principle name of the current user and returns the java.security.Principal object. The java.security.Principal object contains HttpServletRequest interface. The getCallerIdentity() method is used to obtain the java.security.Identity of the caller.

Community vote distribution

BCD (100%)

74gjd_37 Most Recent 1 year, 10 months ago

getCallerIdentity() is not a method defined in the HttpServletRequest interface of the Java Servlet Specification v2.4 however, it is used in AWS SDK for Java to retrieve the details about the current IAM identity establishing an HTTP connection with Amazon Web Services (AWS) services.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

Correct Answer: BCD

upvoted 1 times

Question #42 *Topic 1*

You are the project manager of the CUL project in your organization. You and the project team are assessing the risk events and creating a probability and impact matrix for the identified risks. Which one of the following statements best describes the requirements for the data type used in qualitative risk analysis?

A. A qualitative risk analysis encourages biased data to reveal risk tolerances.

B. A qualitative risk analysis required unbiased stakeholders with biased risk tolerances.

C. A qualitative risk analysis requires accurate and unbiased data if it is to be credible.

D. A qualitative risk analysis requires fast and simple data to complete the analysis.

Suggested Answer: *D*

Official Answer: Explanation: Of all the choices only this answer is accurate. The PMBOK clearly states that the data must be accurate and unbiased to be credible. Answer: D is

Community vote distribution

C (100%)

influence777 Most Recent 1 year, 10 months ago

ANswer is C

upvoted 1 times

Question #43 *Topic 1*

FIPS 199 defines the three levels of potential impact on organizations. Which of the following potential impact levels shows limited adverse effects on organizational operations, organizational assets, or individuals?

A. Moderate

B. Low

C. Medium

D. High

Suggested Answer: *C, A*

The potential impact is called low if the loss of confidentiality, integrity, or availability is expected to have a limited adverse effect on organizational impact is known to be moderate if the loss of confidentiality, integrity, or availability is expected to have a serious adverse effect on organizational operations, have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Community vote distribution

B (100%)

74gjd_37 Most Recent 1 year, 10 months ago

The answer is B. Low. FIPS 199 defines three levels of potential impact on organizations, which are low, moderate and high. The low level indicates limited adverse effects on organizational operations, assets or individuals; the moderate level indicates serious impacts but ones which can be resolved; and the high level indicates severe impacts that could adversely affect an organization's missions or reputation or national interests.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

B. Low

upvoted 1 times

Question #44 *Topic 1*

You work as the senior project manager in SoftTech Inc. You are working on a software project using configuration management. Through configuration management you are decomposing the verification system into identifiable, understandable, manageable, traceable units that are known as Configuration Items
(CIs). According to you, which of the following processes is known as the decomposition process of a verification system into Configuration Items?

A. Configuration status accounting

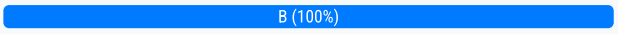
B. Configuration identification

C. Configuration auditing

D. Configuration control

Suggested Answer: *D, A*
Configuration identification is known as the decomposition process of a verification system into Configuration Items. Configuration identification is the process of identifying the attributes that define every aspect of a configuration item. A configuration item is a product (hardware and/or software) that has an end- user purpose. These attributes are recorded in configuration documentation and baselined. Baselining an attribute forces formal configuration change control management. Configuration control is a set of processes and approval stages required to change a configuration item's attributes and to re-baseline them. It supports the change of the functional and physical attributes of software at various points in time, and performs systematic control of changes to the identified attributes. Configuration control is a means of ensuring that system changes are approved before being implemented. Only the proposed and approved changes and report on the configuration baselines associated with each configuration item at any moment of time. It supports the functional and physical attributes of software at various points in time, and performs systematic control of accounting to the identified attributes for the purpose of maintaining software integrity and management. It is occupied in the process of periodic checks to establish the consistency and completeness of accounting information and to validate that all configuration management policies are being followed. Configuration audits are broken into functional and physical configuration audits. They occur either at delivery or at the moment of effecting the change. A functional configuration audit ensures that functional and performance attributes of a configuration item are achieved, while a physical configuration audit ensures that a configuration item is installed in accordance with the requirements of its detailed design documentation.

Community vote distribution



influence777 Most Recent 1 year, 10 months ago
Configuration Identification is the process in the realm of configuration management where components of the verification system (software, hardware, or both) are identified and defined as Configuration Items (CIs). This step involves determining the specific subsets of the system's components that need to be managed and controlled throughout the project lifecycle to ensure integrity and traceability. It's the foundational process that makes it possible to manage changes, perform audits, and maintain the historical record of system states through configuration status accounting.
upvoted 1 times

anuradha1306 2 years, 8 months ago
Configuration identification is known as the decomposition process of a verification system into Configuration Items. Configuration identification is the process of identifying the attributes that define every aspect of a configuration item. A configuration item is a product (hardware and/or software) that has an end-user purpose. These attributes are recorded in configuration documentation and baselined. Baselining an attribute forces formal configuration change control processes to be effected in the event that these attributes are changed.
upvoted 2 times

Question #45 *Topic 1*

Bill is the project manager of the JKH Project. He and the project team have identified a risk event in the project with a high probability of occurrence and the risk event has a high cost impact on the project. Bill discusses the risk event with Virginia, the primary project customer, and she decides that the requirements surrounding the risk event should be removed from the project. The removal of the requirements does affect the project scope, but it can release the project from the high risk exposure. What risk response has been enacted in this project?

A. Mitigation

B. Transference

C. Acceptance

D. Avoidance

Suggested Answer: *C*

This is an example of the avoidance risk response. Because the project plan has been changed to avoid the risk event, so it is considered the avoidance risk response. Risk avoidance is a technique used for threats. It creates changes to the project management plan that are meant to either eliminate the risk completely or to protect the project objectives from its impact. Risk avoidance removes the risk event entirely either by adding additional steps to avoid the event or reducing the project scope requirements. It may seem the answer to all possible risks, but avoiding risks also means losing out on the potential gains that the event could happen and could have an impact on the project. Acceptance is usually used for risk events that have low risk exposure or risk events in which the incorrect. Transference is when the risk is still within the project, but the ownership and management of the risk event is transferred to a third party - usually for a fee.

Community vote distribution

D (100%)

influence777 Most Recent 1 year, 10 months ago

Avoidance involves changing the project plan to eliminate the risk or to protect the project objectives from its impact. It might include altering the scope, specifications, or even the project schedule to avoid the risk entirely. In the scenario described, by removing the requirements surrounding the high-risk event, Bill and Virginia have effectively changed the project's scope to avoid the risk, making "Avoidance" the correct response.

upvoted 1 times

anuradha1306 2 years, 8 months ago

This is an example of the avoidance risk response. Because the project plan has been changed to avoid the risk event, so it is considered the avoidance risk response. Risk avoidance is a technique used for threats. It creates changes to the project management plan that are meant to either eliminate the risk completely or to protect the project objectives from its impact. Risk avoidance removes the risk event entirely either by adding additional steps to avoid the event or reducing the project scope requirements. It may seem the answer to all possible risks, but avoiding risks also means losing out on the potential gains that accepting (retaining) the risk might have allowed

upvoted 2 times

4e3rv21rq3vq2q 3 years, 7 months ago

D. Avoidance

upvoted 1 times

Question #46 *Topic 1*

Martha registers a domain named Microsoft.in. She tries to sell it to Microsoft Corporation. The infringement of which of the following has she made?

A. Copyright

B. Trademark

C. Patent

D. Intellectual property

Suggested Answer: *B*

According to the Lanham Act, domain names fall under trademarks law. A new section 43(d) of the Trademark Act (Lanham Act) states that anyone who in bad faith registers, traffics in, or uses a domain name that infringes or dilutes another's trademark has committed trademark infringement. Factors involved in assessing bad faith focus on activities typically associated with cyberpiracy or cybersquatting, such as whether the registrant has offered to sell the domain name to the trademark holder for financial gain without having used or intended to use it for a bona fide business; whether the domain-name registrant registered multiple domain names that are confusingly similar to the trademarks of others; and whether the trademark incorporated in the domain name is distinctive and famous. Other factors are whether the domain name consists of the legal name or common handle of the domain-name registrant and whether the domain-name registrant previously used the mark in connection with a bona fide business.

Community vote distribution

B (100%)

4e3rv21rq3vq2q Most Recent 2 years, 1 month ago

Correct Answer: B

upvoted 2 times

Question #47 *Topic 1*

Which of the following is a variant with regard to Configuration Management?

A. A CI that has the same name as another CI but shares no relationship.

B. A CI that particularly refers to a software version.

C. A CI that has the same essential functionality as another CI but a bit different in some small manner.

D. A CI that particularly refers to a hardware specification.

Suggested Answer: *B, D, A*

A CI that has the same essential functionality as another CI but a bit different in some small manner, and therefore, might be required to be analyzed along with its generic group. A Configuration item (CI) is an IT asset or a combination of IT assets that may depend and have relationships with other IT processes. A CI will have attributes which may be hierarchical and relationships that will be assigned by the configuration manager in the CM database. The Configuration Item (CI) attributes are as follows: 1.Technical: It is data that describes the CI's capabilities which include software version and model numbers, hardware and manufacturer specifications, and other technical details like networking speeds, and data storage size. Keyboards, mice and cables are considered consumables. 2.Ownership: It is part of financial asset management, ownership attributes, warranty, location, and responsible person for the CI. 3.Relationship: It Configuration Management.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

the correct answer is C

upvoted 1 times

74gjd_37 1 year, 10 months ago

Variant: A variant of a resource (configuration item) is a version that may exist at the same time as one or more other variants, and is identified by a specific set of characteristics, features, or capabilities that distinguish it from other variants of the same resource. For example, the Coupe Si, Sedan Si, and Hybrid may be variants of a vehicle product. From the point of view of configuration management, a variant may be treated in the same manner as time-based versions, just differing along other non-time-based dimensions.

upvoted 1 times

74gjd_37 1 year, 10 months ago

Variant: A variant of a resource (configuration item) is a version that may exist at the same time as one or more other variants, and is identified by a specific set of characteristics, features, or capabilities that distinguish it from other variants of the same resource. For example, the Coupe Si, Sedan Si, and Hybrid may be variants of a vehicle product. From the point of view of configuration management, a variant may be treated in the same manner as time-based versions, just differing along other non-time-based dimensions.Sorry, the correct answer is C, not A.

upvoted 1 times

74gjd_37 1 year, 10 months ago

Sorry, the correct answer is C, not A.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

Correct Answer: C

upvoted 1 times

Question #48 *Topic 1*

The organization level is the Tier 1 and it addresses risks from an organizational perspective. What are the various Tier 1 activities? Each correct answer represents a complete solution. Choose all that apply.

A. The organization plans to use the degree and type of oversight, to ensure that the risk management strategy is being effectively carried out.

B. The level of risk tolerance.

C. The techniques and methodologies an organization plans to employ, to evaluate information system-related security risks.

D. The RMF primarily operates at Tier 1.

Suggested Answer: *D*

The Organization Level is the Tier 1, and it addresses risks from an organizational perspective. It includes the following points: The techniques and methodologies an organization plans to employ, to evaluate information system-related security risks. During risk assessment, the methods and procedures the organization plans to use, to evaluate the significance of the risks identified. The types and extent of risk mitigation measures the organization plans to employ, to address identified risks. The level of risk tolerance. According to the environment of operation, how the organization plans to monitor risks on an ongoing basis, given the inevitable changes to organizational information system. incorrect. The RMF primarily operates at Tier 3.

Community vote distribution

ABC (100%)

anuradha1306 Most Recent 1 year, 8 months ago

The organization plans to use the degree and type of oversight, in order to ensure that the risk management strategy is being effectively carried out.Answer: D is The Organization Level is the Tier 1, and it addresses risks from an organizational perspective. It includes the following points: The techniques and methodologies an organization plans to employ, to evaluate information system-related security risks. During risk assessment, the methods and procedures the organization plans to use, to evaluate the significance of the risks identified. The types and extent of risk mitigation measures the organization plans to employ, to address identified risks. The level of risk tolerance. According to the environment of operation, how the organization plans to monitor risks on an ongoing basis, given the inevitable changes to organizational information system. incorrect. The RMF primarily operates at Tier 3.

upvoted 1 times

Question #49 *Topic 1*

An asset with a value of $600,000 is subject to a successful malicious attack threat twice a year. The asset has an exposure of 30 percent to the threat. What will be the annualized loss expectancy?

A. $360,000

B. $180,000

C. $280,000

D. $540,000

Suggested Answer: *C, B, D*

The annualized loss expectancy will be $360,000. Annualized loss expectancy (ALE) is the annually expected financial loss to an organization from a threat. The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). It is mathematically expressed as follows: ALE = Single Loss Expectancy (SLE) * Annualized Rate of Occurrence (ARO) Here, it is as follows: SLE = Asset value * EF (Exposure factor) = 600,000 * (30/100) = 600,000 * 0.30 = 180,000

ALE = SLE * ARO - = 180,000 * 2 = 360,000

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

Question #50 *Topic 1*

Which of the following are the common roles with regard to data in an information classification program? Each correct answer represents a complete solution.
Choose all that apply.

A. Editor

B. Custodian

C. Owner

D. User

E. Security auditor

Suggested Answer: *B, C, D, E*
The following are the common roles with regard to data in an information classification program: Owner Custodian User Security auditor The following are the responsibilities of the owner with regard to data in an information classification program: Determining what level of classification the information requires. Reviewing the classification assignments at regular time intervals and making changes as the business needs change. Delegating the responsibility of the data protection duties to the custodian. The following are the responsibilities of the custodian with regard to data in an information classification program: Running regular backups and routinely testing the validity of the backup data Performing data restoration from the backups when necessary Controlling access, adding and removing privileges for individual users The users must comply with the requirements laid out in policies and procedures. They must also exercise due care. A security auditor examines an organization's security procedures and mechanisms.

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

Question #51 *Topic 1*

Which of the following life cycle modeling activities establishes service relationships and message exchange paths?

A. Service-oriented logical design modeling

B. Service-oriented conceptual architecture modeling

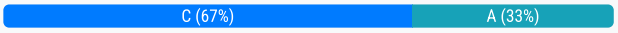
C. Service-oriented discovery and analysis modeling

D. Service-oriented business integration modeling

Suggested Answer: *A*

The service-oriented logical design modeling establishes service relationships and message exchange paths. It also addresses service visibility and crafts service logical compositions.

Community vote distribution



influence777 Most Recent 1 year, 10 months ago

A. Service-oriented logical design modeling

upvoted 1 times

74gjd_37 2 years, 4 months ago

Option C. Service-oriented discovery and analysis modeling is the life cycle modeling activity that establishes service relationships and message exchange paths. This activity is performed during the analysis phase of the Service-Oriented Architecture (SOA) life cycle, where the requirements and business goals of the organization are identified, and the services that will be provided to meet those requirements are defined. During this activity, the relationships between services are identified, and the message exchange paths between them are established, which are essential for the successful implementation of SOA.

upvoted 2 times

Question #52 *Topic 1*

You have a storage media with some data and you make efforts to remove this data. After performing this, you analyze that the data remains present on the media. Which of the following refers to the above mentioned condition?

A. Object reuse

B. Degaussing

C. Residual

D. Data remanence

Suggested Answer: *C, B, A*

Data remanence refers to the data that remains even after the efforts have been made for removing or erasing the data. This event occurs because of data being left intact by an insignificant file deletion operation, by storage media reformatting, or through physical properties of the storage medium. Data remanence can make unintentional disclosure of sensitive information possible. So, it is required that the storage media is released into an uncontrolled storage media that has one or more objects.

Community vote distribution

D (100%)

74gjd_37 Most Recent 1 year, 10 months ago

D. Data remanence refers to the condition where data remains present on a storage media even after attempts have been made to erase or remove it. This can occur due to various factors such as object reuse, magnetic fields, or residual information remaining on the media. Degaussing is a method of erasing data from magnetic media by applying a strong magnetic field, but even with this method there may still be some residual information left which could result in data remanence.

upvoted 1 times

Question #53 *Topic 1*

Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. Which of the following statements are true about Certification and Accreditation? Each correct answer represents a complete solution. Choose two.

A. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system.

B. Accreditation is a comprehensive assessment of the management, operational, and technical security controls in an information system.

C. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system.

D. Certification is the official management decision given by a senior agency official to authorize operation of an information system.

Suggested Answer: *A, C*

Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. The C&A process is used extensively in the U.S. Federal Government. Some C&A processes include FISMA, NIACAP, DIACAP, and DCID 6/3. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

A. Certification is a process that assesses the technical and non-technical security controls of an information system. It evaluates whether these controls are implemented correctly, operating as intended, and producing the desired outcomes. C. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system based on its certification status and residual risk. Accreditation confirms that the system meets security requirements, and it provides authorization to operate for a specific period, subject to ongoing periodic assessments.

upvoted 1 times

Question #54 *Topic 1*

The Phase 1 of DITSCAP C&A is known as Definition Phase. The goal of this phase is to define the C&A level of effort, identify the main C&A roles and responsibilities, and create an agreement on the method for implementing the security requirements. What are the process activities of this phase? Each correct answer represents a complete solution. Choose all that apply.

A. Negotiation

B. Registration

C. Document mission need

D. Initial Certification Analysis

Suggested Answer: *D, A*

The Phase 1 of DITSCAP C&A is known as Definition Phase. The goal of this phase is to define the C&A level of effort, identify the main C&A roles and responsibilities, and create an agreement on the method for implementing the security requirements. The Phase 1 starts with the input of the mission need. activity.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

During the Definition Phase (Phase 1) of DITSCAP C&A, negotiations between the organization and various stakeholders take place to identify the extent of security measures that will be implemented in a given system. Similarly, documenting mission needs is necessary during this phase to clearly define system requirements based on stated objectives and planned use. Registration process activity is not part of the Definition Phase since it deals with registering information systems for assessment during Phase 2 (Verification). The Initial Certification Analysis process activity also isn't part of this phase because it occurs later in Phase 3 (Validation).

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

Correct Answer: ABC

upvoted 1 times

Question #55 *Topic 1*

Which of the following NIST Special Publication documents provides a guideline on network security testing?

A. NIST SP 800-42

B. NIST SP 800-53A

C. NIST SP 800-60

D. NIST SP 800-53

E. NIST SP 800-37

F. NIST SP 800-59

Suggested Answer: *A, E, D, B, F, C*

for conducting Certification & Accreditation (C&A). These documents are as follows: NIST Special Publication 800-37: This document is a guide for the security certification and accreditation of Federal Information Systems. NIST Special Publication 800-53: This document provides a guideline for security controls for Federal Information Systems. NIST Special Publication 800-53A. This document consists of techniques and procedures for verifying the effectiveness of security controls in Federal Information System. NIST Special Publication 800-59: This document is a guideline for identifying an information system as a National Security System. NIST Special Publication 800-60: This document is a guide for mapping types of information and information systems to security objectives and risk levels.

Community vote distribution

A (100%)

74gjd_37 Most Recent 1 year, 10 months ago

A. NIST SP 800-42 "Guideline on Network Security Testing" (Withdrawn on September 30, 2008. Superseded by SP 800-115)

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

A. NIST SP 800-42

upvoted 1 times

Question #56 *Topic 1*

Which of the following tools is used to attack the Digital Watermarking?

A. Steg-Only Attack

B. Active Attacks

C. 2Mosaic

D. Gifshuffle

Suggested Answer: *A, D*

2Mosaic is a tool used for watermark breaking. It is an attack against a digital watermarking system. In this type of attack, an image is chopped into small pieces and then placed together. When this image is embedded into a web page, the web browser renders the small pieces into one image. This image Gifshuffle is used to hide message or information inside GIF images. It is done by shuffling the colormap. This tool also provides compression and encryption.

Community vote distribution

C (100%)

74gjd_37 Most Recent 1 year, 10 months ago

2Mosaic by Fabien Petitcolas employs a so-called "presentation attack" primarily against images on a Website. 2Mosaic attacks a digital watermarking system by chopping an image into smaller subimages. On the Website, the series of small images are positioned next to each other and appear the same as the original large image (Petitcolas 2003). https://www.garykessler.net/library/fsc_stego.html

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

C. 2Mosaic

upvoted 1 times

Question #57 *Topic 1*

You and your project team have identified the project risks and now are analyzing the probability and impact of the risks. What type of analysis of the risks provides a quick and high-level review of each identified risk event?

A. Quantitative risk analysis

B. Qualitative risk analysis

C. Seven risk responses

D. A risk probability-impact matrix

Suggested Answer: *B*

Qualitative risk analysis is a high-level, fast review of the risk event. Qualitative risk analysis qualifies the risk events for additional analysis.

Community vote distribution

B (100%)

74gjd_37 Most Recent 1 year, 10 months ago

B. Qualitative risk analysis. This type of analysis prioritizes risks according to their likelihood and potential impact on the project objectives, without quantifying them numerically. It provides an opportunity for subjective judgments from stakeholders to inform the process and help frame subsequent steps in risk response planning. A quantitative risk analysis involves numerical estimates, simulations or modeling techniques for a more rigorous examination of project risks; while a probability-impact matrix considers both probability (likelihood) and impact (consequence), typically using a four-quadrant chart that makes it easy to visualize and prioritize risks. The seven-risk responses are associated with the process of dealing with risks once they have been analyzed as part of a broader Risk Management Plan.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

B. Qualitative risk analysis

upvoted 1 times

Question #58 *Topic 1*

What component of the change management system is responsible for evaluating, testing, and documenting changes created to the project scope?

A. Project Management Information System

B. Integrated Change Control

C. Configuration Management System

D. Scope Verification

Suggested Answer: *C*

The change management system is comprised of several components that guide the change request through the process. When a change request is made that will affect the project scope. The Configuration Management System evaluates the change request and documents the features and functions of the change on the project scope.

Community vote distribution

B (100%)

74gjd_37 Most Recent 1 year, 10 months ago

Integrated change control is the process of reviewing all change requests within a project, analyzing those requests and implementing approved changes. Through integrated change control, project managers may have a more organized structure for changing a project. They can also determine the effects of a proposed change before implementation, allowing them to make better decisions for the project. https://www.indeed.com/career-advice/career-development/integrated-change-control Integrated Change Control ensures that all proposed changes are evaluated based on their impact to overall project objectives and that appropriate approvals are obtained before the changes can be implemented. This helps to ensure that the security posture of a system does not degrade as a result of any change in project scope.

upvoted 1 times

Question #59 *Topic 1*

You work as a project manager for BlueWell Inc. You with your team are using a method or a (technical) process that conceives the risks even if all theoretically possible safety measures would be applied. One of your team member wants to know that what is a residual risk. What will you reply to your team member?

A. It is a risk that remains because no risk response is taken.

B. It is a risk that can not be addressed by a risk response.

C. It is a risk that will remain no matter what type of risk response is offered.

D. It is a risk that remains after planned risk responses are taken.

Suggested Answer: *B, A*

Residual risks are generally smaller risks that remain in the project after larger risks have been addressed. The residual risk is the risk or danger of an action or an event, a method or a (technical) process that still conceives these dangers even if all theoretically possible safety measures would be applied. The risks.

Community vote distribution

D (100%)

4e3rv21rq3vq2q Most Recent 2 years, 1 month ago

D. It is a risk that remains after planned risk responses are taken.

upvoted 1 times

Question #60 *Topic 1*

You are the project manager of the NNN project for your company. You and the project team are working together to plan the risk responses for the project. You feel that the team has successfully completed the risk response planning and now you must initiate what risk process it is. Which of the following risk processes is repeated after the plan risk responses to determine if the overall project risk has been satisfactorily decreased?

A. Quantitative risk analysis

B. Risk identification

C. Risk response implementation

D. Qualitative risk analysis

Suggested Answer: *D, B*

The quantitative risk analysis process is repeated after the plan risk responses to determine if the overall project risk has been satisfactorily

Community vote distribution

A (100%)

74gjd_37 Most Recent 1 year, 10 months ago

The correct answer is A. Quantitative risk analysis. After the plan risk responses process, the project team should perform a quantitative risk analysis to determine if the overall project risk has been satisfactorily decreased. This process involves using numerical techniques to assess the probability and impact of each identified risk and determining if the planned risk responses have not been effective in reducing the overall project risk. If the risk responses have not been effective, the project team may need to re-evaluate the risks and develop new risk response strategies.

upvoted 1 times

Question #61 *Topic 1*

Which of the following statements is true about residual risks?

A. It is the probabilistic risk after implementing all security measures.

B. It can be considered as an indicator of threats coupled with vulnerability.

C. It is a weakness or lack of safeguard that can be exploited by a threat.

D. It is the probabilistic risk before implementing all security measures.

Suggested Answer: *B*

The residual risk is the risk or danger of an action or an event, a method or a (technical) process that still conceives these dangers even if all theoretically possible safety measures would be applied. The formula to calculate residual risk is (inherent risk) x (control risk) where inherent risk is (threats security risk is a probabilistic function of a given threat agent exercising a particular vulnerability and the impact of that risk on the organization. Security risks can be exploited by a threat, thus causing harm to the information systems or networks. It can exist in hardware , operating systems, firmware, applications, and configuration files. Vulnerability has been variously defined in the current context as follows: 1.A security weakness in a Target of Evaluation due to failures in analysis, design, implementation, or operation and such. 2.Weakness in an information system or components (e.g. system security procedures, hardware design, or internal controls that could be exploited to produce an information-related misfortune.) 3.The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the system, network, application, or protocol involved.

Community vote distribution

A (100%)

74gjd_37 Most Recent 1 year, 10 months ago

the correct answer is A. Residual risk is the risk that remains after all planned risk responses have been implemented. It is the risk that is left over even after all security measures have been taken. The residual risk can be assessed by conducting a risk assessment after the planned risk responses have been implemented. The residual risk assessment helps to determine if the planned risk responses were effective in reducing the overall risk to an acceptable level.

upvoted 1 times

Question #62 *Topic 1*

To help review or design security controls, they can be classified by several criteria . One of these criteria is based on their nature. According to this criterion, which of the following controls consists of incident response processes, management oversight, security awareness, and training?

A. Compliance control

B. Physical control

C. Procedural control

D. Technical control

Suggested Answer: *B*

Official Answer: Explanation: Procedural controls include incident response processes, management oversight, security awareness, and training. Answer: B is incorrect. Physical

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

The controls consisting of incident response processes, management oversight, security awareness, and training are categorized as procedural controls. Therefore, the correct answer is C.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

C. Procedural control

upvoted 2 times

Question #63 *Topic 1*

A Web-based credit card company had collected financial and personal details of Mark before issuing him a credit card. The company has now provided Mark's financial and personal details to another company. Which of the following Internet laws has the credit card issuing company violated?

A. Trademark law

B. Security law

C. Privacy law

D. Copyright law

Suggested Answer: *A, B*

The credit card issuing company has violated the Privacy law. According to the Internet Privacy law, a company cannot provide their customer's dramatic, musical, artistic, and certain other intellectual works.

Community vote distribution

C (100%)

74gjd_37 Most Recent 1 year, 10 months ago

C. Privacy law The credit card issuing company has violated privacy law by sharing Mark's financial and personal details with another company without his consent.

upvoted 1 times

Question #64 *Topic 1*

There are seven risks responses that a project manager can choose from. Which risk response is appropriate for both positive and negative risk events?

A. Acceptance

B. Transference

C. Sharing

D. Mitigation

Suggested Answer: *C, A*

Only acceptance is appropriate for both positive and negative risk events. Often sharing is used for low probability and low impact risk events regardless of the positive or negative effects the risk event may bring the project. Acceptance response is a part of Risk Response planning process. Acceptance response delineates that the project plan will not be changed to deal with the risk. Management may develop a contingency plan if the risk does occur. Acceptance response to a risk event is a strategy that can be used for risks that pose either threats or opportunities. Acceptance response can be of two types: Passive acceptance: It is a strategy in which no plans are made to try or avoid or mitigate the risk. Active acceptance: Such responses include developing seeks to lower the probability and/or impact of a risk event.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

The risk response that is appropriate for both positive and negative risk events is "A. Acceptance." Acceptance involves acknowledging the risk event, but choosing not to take any action to prevent or mitigate it. This response is suitable for both positive and negative risk events because sometimes the best course of action is to allow the risk to occur and take advantage of the positive outcome or to simply tolerate the negative impact if the risk does occur.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

A. Acceptance

upvoted 2 times

Question #65 *Topic 1*

You work as a Security Manager for Tech Perfect Inc. In the organization, Syslog is used for computer system management and security auditing, as well as for generalized informational, analysis, and debugging messages. You want to prevent a denial of service (DoS) for the Syslog server and the loss of Syslog messages from other sources. What will you do to accomplish the task?

A. Use a different message format other than Syslog in order to accept data.

B. Enable the storage of log entries in both traditional Syslog files and a database.

C. Limit the number of Syslog messages or TCP connections from a specific source for a certain time period.

D. Encrypt rotated log files automatically using third-party or OS mechanisms.

Suggested Answer: *A, D*

In order to accomplish the task, you should limit the number of Syslog messages or TCP connections from a specific source for a certain time period. entries in both traditional Syslog files and a database for creating a database storage for logs.

Community vote distribution

C (100%)

74gjd_37 Most Recent 1 year, 10 months ago

C. Limit the number of Syslog messages or TCP connections from a specific source for a certain time period would be the best option to prevent a DoS attack on the Syslog server and the loss of Syslog messages from other sources. This will help to prevent an overwhelming number of messages from a single source and allow other sources to send their messages to the Syslog server. Additionally, it is important to ensure that the Syslog server has sufficient resources to handle the number of messages it receives and to regularly monitor the server for any potential security vulnerabilities.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

C. Limit the number of Syslog messages or TCP connections from a specific source for a certain time period.

upvoted 2 times

Question #66 *Topic 1*

You work as a project manager for a company. The company has started a new security software project. The software configuration management will be used throughout the lifecycle of the project. You are tasked to modify the functional features and the basic logic of the software and then make them compatible to the initial design of the project. Which of the following procedures of the configuration management will you follow to accomplish the task?

A. Configuration status accounting

B. Configuration control

C. Configuration audits

D. Configuration identification

Suggested Answer: *C*

Configuration control is a procedure of the Configuration management. Configuration control is a set of processes and approval stages required to change a configuration item's attributes and to re-baseline them. It supports the change of the functional and physical attributes of software at various points in identification for a configured item is accurate, complete, and will meet specified program needs. Configuration audits are broken into functional and physical configuration audits. They occur either at delivery or at the moment of effecting the change. A functional configuration audit ensures that functional and performance attributes of a configuration item are achieved, while a physical configuration audit ensures that a configuration item is installed in accordance with every aspect of a configuration item. A configuration item is a product (hardware and/or software) that has an end-user purpose. These attributes are recorded in configuration documentation and baselined. Baselining an attribute forces formal configuration change control processes to be effected in the event that these associated with each configuration item at any moment of time. It supports the functional and physical attributes of software at various points in time, and performs systematic control of accounting to the identified attributes for the purpose of maintaining software integrity and traceability throughout the software development life cycle.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

The procedure of the configuration management that you should follow to modify the functional features and the basic logic of the software and make them compatible with the initial design of the project is Configuration Control. Configuration Control is the process of identifying, evaluating, approving or disapproving, and implementing changes to the configuration items throughout the life cycle of the project. This process ensures that any changes made to the software are properly reviewed and approved by the appropriate stakeholders before being implemented. It also ensures that the software remains consistent with the initial design of the project.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

B. Configuration control

upvoted 1 times

Question #67 *Topic 1*

Which of the following areas of information system, as separated by Information Assurance Framework, is a collection of local computing devices, regardless of physical location, that are interconnected via local area networks (LANs) and governed by a single security policy?

A. Local Computing Environments

B. Networks and Infrastructures

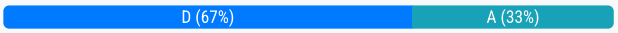
C. Supporting Infrastructures

D. Enclave Boundaries

Suggested Answer: *D*

The areas of information system, as separated by Information Assurance Framework, are as follows: Local Computing Environments: This area includes servers, client workstations, operating system, and applications. Enclave Boundaries: This area consists of collection of local computing devices, regardless of physical location, that are interconnected via local area networks (LANs) and governed by a single security policy. Networks and Infrastructures: This area provides the network connectivity between enclaves. It includes operational area networks (OANs), metropolitan area networks (MANs), and campus area networks (CANs). Supporting Infrastructures: This area provides security services for networks, client workstations, Web servers, operating systems, applications, files, and single-use infrastructure machines

Community vote distribution



influence777 Most Recent 1 year, 10 months ago

Enclave Boundaries refer to a security domain that is defined by the implementation of a uniform security policy and security posture. These enclaves can encompass local computing devices and are often managed as a single entity, despite the physical location of its components, to ensure cohesive security practices and controls are applied across the board.

upvoted 2 times

74gjd_37 2 years, 4 months ago

A. Local Computing Environments refer to a collection of local computing devices, regardless of physical location, that are interconnected via local area networks (LANs) and governed by a single security policy. These environments can include desktop computers, laptops, servers, printers, and other computing devices that are connected to each other through a LAN. Local computing environments are typically managed by a local system administrator and are subject to a set of security policies that are designed to protect the confidentiality, integrity, and availability of the information processed and stored within the environment. Examples of local computing environments include small business networks, home networks, and branch office networks.

upvoted 1 times

Question #68 *Topic 1*

Which of the following is a signature-based intrusion detection system (IDS) ?

A. RealSecure

B. StealthWatch

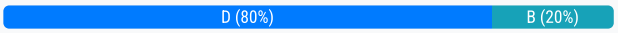
C. Tripwire

D. Snort

Suggested Answer: *A, B*

Snort is a signature-based intrusion detection system. Snort is an open source network intrusion prevention and detection system that operates as a network sniffer. It logs activities of the network that is matched with the predefined signatures. Signatures can be designed for a wide range of traffic, including Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP). The three main modes in which Snort can be configured are as follows: Sniffer mode: It reads the packets of the network and displays them in a continuous stream on the console. Packet logger mode: It logs the packets to the disk. Network intrusion detection mode: It is the most complex and configurable configuration, allowing incorrect. Tripwire is a file integrity checker for UNIX/Linux that can be used for host-based intrusion detection.

Community vote distribution



influence777 Most Recent 1 year, 10 months ago

D. Snort Snort is a widely recognized signature-based intrusion detection system (IDS) that uses a rule-driven language to detect and alert on network intrusion attempts. It compares network traffic against a database of known threat signatures to identify malicious activity, making it an effective tool for real-time traffic analysis and packet logging.

upvoted 2 times

74gjd_37 2 years, 4 months ago

"People are using signature based IDS's. Snort is mostly used signature based IDS because of it is open source software. " source: Signature Based Intrusion Detection System Using SNORT, November 2012, International Journal of Computer Applications & Information Technology 1(3):7

upvoted 1 times

4e3rv21rq3vq2q 3 years, 7 months ago

D. Snort

upvoted 2 times

Question #69 *Topic 1*

Which of the following statements about the availability concept of Information security management is true?

A. It ensures that modifications are not made to data by unauthorized personnel or processes.

B. It determines actions and behaviors of a single individual within a system.

C. It ensures reliable and timely access to resources.

D. It ensures that unauthorized modifications are not made to data by authorized personnel or processes.

Suggested Answer: *A, D*

The concept of availability ensures reliable and timely access to data or resources. In other words, availability ensures that the systems are up and ensures that modifications are not made to data by unauthorized personnel or processes. It also ensures that unauthorized modifications are not made to data by particular individual. Audit trails and logs support accountability.

Community vote distribution

C (100%)

74gjd_37 Most Recent 1 year, 10 months ago

The statement that is true about the availability concept of Information security management is C. It ensures reliable and timely access to resources. The availability concept of information security management ensures that authorized personnel have reliable and timely access to resources, such as data, systems, and networks, when needed. This involves preventing disruptions, downtime, and other forms of interference that could prevent access or limit functionality. The other statements are not accurate descriptions of the availability concept.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

C. It ensures reliable and timely access to resources.

upvoted 1 times

Question #70 *Topic 1*

A security policy is an overall general statement produced by senior management that dictates what role security plays within the organization. Which of the following are required to be addressed in a well designed policy? Each correct answer represents a part of the solution. Choose all that apply.

A. What is being secured?

B. Where is the vulnerability, threat, or risk?

C. Who is expected to exploit the vulnerability?

D. Who is expected to comply with the policy?

Suggested Answer: *A, B, D*

A security policy is an overall general statement produced by senior management (or a selected policy board or committee) that dictates what role security plays within the organization. A well designed policy addresses the following: What is being secured? - Typically an asset. Who is expected to comply with the policy? - Typically employees. Where is the vulnerability, threat, or risk? - Typically an issue of integrity or responsibility.

Community vote distribution



influence777 Most Recent 1 year, 10 months ago

A, B, D A well-designed security policy should clearly address: - **What is being secured** (A): Identifying the assets that require protection. - **Where is the vulnerability, threat, or risk** (B): Outlining the potential security concerns that the policy aims to mitigate. - **Who is expected to comply with the policy** (D): Specifying the individuals or groups that must follow the policy guidelines. While understanding potential adversaries is crucial for security strategies, specific identification of who might exploit vulnerabilities is usually not a direct component of a general security policy.

upvoted 1 times

74gjd_37 2 years, 4 months ago

All of the options A, B, C, and D are required to be addressed in a well-designed security policy. A. What is being secured? The policy should clearly define the assets that need to be protected and the level of protection that is required for them. B. Where is the vulnerability, threat, or risk? The policy should identify the potential vulnerabilities, threats, and risks that the organization faces and the measures that need to be taken to mitigate them. C. Who is expected to exploit the vulnerability? The policy should identify the potential threat actors who may exploit vulnerabilities in the organization's assets and systems. D. Who is expected to comply with the policy? The policy should clearly define the roles and responsibilities of both employees and management in ensuring the security of the organization's assets and information. It should also outline the consequences of non-compliance with the policy.

upvoted 1 times

Question #71 *Topic 1*

The Phase 4 of DITSCAP C&A is known as Post Accreditation. This phase starts after the system has been accredited in Phase 3. What are the process activities of this phase? Each correct answer represents a complete solution. Choose all that apply.

A. Security operations

B. Maintenance of the SSAA

C. Compliance validation

D. Change management

E. System operations

F. Continue to review and refine the SSAA

Suggested Answer: *F, A*

The Phase 4 of DITSCAP C&A is known as Post Accreditation. This phase starts after the system has been accredited in the Phase 3. The goal of this phase is to continue to operate and manage the system and to ensure that it will maintain an acceptable level of residual risk. The process activities of this Phase 3 activity.

Community vote distribution

BCDE (100%)

HaveToLearnALot Most Recent 2 years, 1 month ago

Post-accreditation activities include ongoing maintenance of the SSAA system operations change management compliance validation

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

Correct Answer: BCDE

upvoted 1 times

Question #72 *Topic 1*

You work as a security engineer for BlueWell Inc. Which of the following documents will you use as a guide for the security certification and accreditation of
Federal Information Systems?

A. NIST Special Publication 800-60

B. NIST Special Publication 800-53

C. NIST Special Publication 800-37

D. NIST Special Publication 800-59

Suggested Answer: *C*

NIST has developed a suite of documents for conducting Certification & Accreditation (C&A). These documents are as follows: NIST Special Publication 800-37: This document is a guide for the security certification and accreditation of Federal Information Systems. NIST Special Publication 800-53: This document provides a guideline for security controls for Federal Information Systems. NIST Special Publication 800-53A. This document consists of techniques and procedures for verifying the effectiveness of security controls in Federal Information System. NIST Special Publication 800-59: This document is a guideline for identifying an information system as a National Security System. NIST Special Publication 800-60: This document is a guide for mapping types of information and information systems to security objectives and risk levels.

Community vote distribution

C (100%)

74gjd_37 Most Recent 1 year, 10 months ago

The correct answer is C. NIST Special Publication 800-37. This document provides guidelines and requirements for the security certification and accreditation of federal information systems. NIST Special Publication 800-60 provides guidance for information security program development, while NIST Special Publication 800-53 provides security and privacy controls for federal information systems and organizations. NIST Special Publication 800-59 provides guidance for identifying an information system as a national security system.

upvoted 1 times

Question #73 *Topic 1*

Which of the following is an example of over-the-air (OTA) provisioning in digital rights management?

A. Use of shared secrets to initiate or rebuild trust.

B. Use of software to meet the deployment goals.

C. Use of concealment to avoid tampering attacks.

D. Use of device properties for unique identification.

Suggested Answer: *A, D, C*

Over- the- air provisioning is a mechanism to deploy MIDlet suites over a network. It is a method of distributing MIDlet suites. MIDlet suite providers install their MIDlet suites on Web servers and provide a hypertext link for downloading. A user can use this link to download the MIDlet suite either through the Internet microbrowser or through WAP on his device. Over-the-air provisioning is required for end-to-end encryption or other security purposes in order to deliver properties for unique identification and the use of concealment to avoid tampering attacks are the security challenges in digital rights management (DRM).

Community vote distribution



influence777 Most Recent 1 year, 10 months ago

A. Use of shared secrets to initiate or rebuild trust.

upvoted 1 times

74gjd_37 2 years, 4 months ago

The correct answer is B. Use of software to meet the deployment goals is an example of over-the-air (OTA) provisioning in digital rights management. This refers to the delivery of digital content or services to devices over a wireless network using software and other security measures to ensure that the content or service is only delivered to authorized devices and users. Option A, use of shared secrets to initiate or rebuild trust, refers to a security mechanism used to establish or reestablish trust between two parties. It is not an example of OTA provisioning in digital rights management. Option C, use of concealment to avoid tampering attacks, refers to a security technique used to protect digital content or services from tampering or modification by unauthorized parties. It is not an example of OTA provisioning in digital rights management. Option D, use of device properties for unique identification, refers to the use of device characteristics to identify and authenticate a device. It is not an example of OTA provisioning in digital rights management.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 7 months ago

A. Use of shared secrets to initiate or rebuild trust.

upvoted 1 times

Question #74 *Topic 1*

The service-oriented modeling framework (SOMF) provides a common modeling notation to address alignment between business and IT organizations. Which of the following principles does the SOMF concentrate on? Each correct answer represents a part of the solution. Choose all that apply.

A. Architectural components abstraction

B. SOA value proposition

C. Business traceability

D. Disaster recovery planning

E. Software assets reuse

Suggested Answer: *D*

The service-oriented modeling framework (SOMF) concentrates on the following principles: Business traceability Architectural best-practices traceability Technological traceability SOA value proposition Software assets reuse SOA integration strategies Technological abstraction and generalization

Community vote distribution

ABCE (100%)

4e3rv21rq3vq2q Most Recent 2 years, 1 month ago

Correct Answer: ABCE

upvoted 1 times

Question #75 *Topic 1*

Which of the following DoD directives is referred to as the Defense Automation Resources Management Manual?

A. DoD 8910.1

B. DoD 7950.1-M

C. DoDD 8000.1

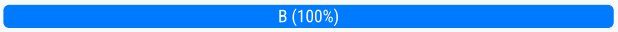
D. DoD 5200.22-M

E. DoD 5200.1-R

Suggested Answer: *B*

The various DoD directives are as follows: DoD 5200.1-R: This DoD directive refers to the 'Information Security Program Regulation'. DoD 5200.22-M: This DoD directive refers the 'National Industrial Security Program Operating Manual'. DoD 7950.1-M: This DoD directive refers to the 'Defense Automation Resources Management Manual'. DoDD 8000.1: This DoD directive refers to the 'Defense Information Management (IM) Program'. DoD 8910.1: This DoD directive refers to the 'Management and Control of Information Requirements'.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

Answer: B. DoD 7950.1-M is known as the Defense Automation Resources Management Manual, which provides guidance and procedures for managing Department of Defense (DoD) Information Technology (IT) resources in accordance with policies set forth by DoD Directive 5144.02, "Defense Information System for Security (DISS). Therefore, it is commonly referred to as the "Defense Automation Resources Management Manual."

upvoted 1 times

Question #76 *Topic 1*

Which of the following access control models are used in the commercial sector? Each correct answer represents a complete solution. Choose two.

A. Biba model

B. Clark-Biba model

C. Clark-Wilson model

D. Bell-LaPadula model

Suggested Answer: *A, D*

The Biba and Clark-Wilson access control models are used in the commercial sector. The Biba model is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. Data and subjects are grouped into ordered levels of integrity. The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject. The

Community vote distribution

AC (100%)

4e3rv21rq3vq2q Most Recent 2 years, 1 month ago

Correct Answer: AC

upvoted 1 times

Question #77 *Topic 1*

Which of the following testing methods verifies the interfaces between components against a software design?

A. Regression testing

B. Integration testing

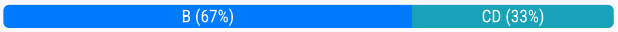
C. Black-box testing

D. Unit testing

Suggested Answer: *A*

Integration testing is a software testing that seeks to verify the interfaces between components against a software design. Software components may be integrated in an iterative way or all together ("big bang"). Normally the former is considered a better practice since it allows interface issues to be localized more quickly and fixed. Integration testing works to expose defects in the interfaces and interaction between the integrated components (modules). Progressively larger groups of tested software components corresponding to elements of the architectural design are integrated and tested until the software works as a system. regressions, or old bugs that have come back. Such regressions occur whenever software functionality that was previously working correctly stops working as intended. Typically, regressions occur as an unintended consequence of program changes, when the newly developed part of the software collides with the an object-oriented environment, this is usually at the class level, and the minimal unit tests include the constructors and destructors. These types of tests are usually written by developers as they work on code (white-box style), to ensure that the specific function is working as expected. One function might have multiple tests, to catch corner cases or other branches in the code. Unit testing alone cannot verify the functionality of a piece of software, but rather is used to assure that including specifications, requirements, and design to derive test cases. These tests can be functional or non-functional, though usually functional. The test designer selects valid and invalid inputs and determines the correct output. There is no knowledge of the test object's internal structure. This method of test design is applicable to all levels of software testing: unit, integration, functional testing, system and acceptance. The higher the level, and hence the bigger and more complex the box, the more one is forced to use black box testing to simplify. While this method can uncover unimplemented parts of the specification, one cannot be sure that all existent paths are tested.

Community vote distribution



influence777 Most Recent 1 year, 10 months ago

B. Integration testing

upvoted 1 times

74gjd_37 2 years, 4 months ago

C. Clark-Wilson model and D. Bell-LaPadula model are used in the commercial sector Access Control Models. The Biba model and Clark-Biba model are used in the government sector to ensure confidentiality, integrity, and availability of sensitive information. These models are not commonly used in the commercial sector. The Clark-Wilson model and Bell-LaPadula model have been adopted by many commercial organizations worldwide to control access to data and ensure their security from external or internal threats.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 7 months ago

B. Integration testing

upvoted 1 times

Question #78 *Topic 1*

Which of the following statements best describes the difference between the role of a data owner and the role of a data custodian?

A. The custodian makes the initial information classification assignments, and the operations manager implements the scheme.

B. The data owner implements the information classification scheme after the initial assignment by the custodian.

C. The custodian implements the information classification scheme after the initial assignment by the operations manager.

D. The data custodian implements the information classification scheme after the initial assignment by the data owner.

Suggested Answer: *B, A, C*

The data owner is responsible for ensuring that the appropriate security controls are in place, for assigning the initial classification to the data to be protected, for approving access requests from other parts of the organization, and for periodically reviewing the data classifications and access rights. Data owners are primarily responsible for determining the data's sensitivity or classification levels, whereas the data custodian has the responsibility for backup, answers.

Community vote distribution

D (100%)

74gjd_37 Most Recent 1 year, 10 months ago

D. The data custodian implements the information classification scheme after the initial assignment by the data owner is the statement that best describes the difference between the role of a data owner and a data custodian. The data owner is responsible for classifying information based on its sensitivity, value, and criticality to an organization. Once this task is done, they define access rights and control policies for each classification level (e.g., Public, Confidential, Private). In contrast, a data custodian has operational responsibility for protecting classified assets or sensitive information according to rules established by owners while ensuring compliance with industry regulations. Custodians implement technical controls such as firewalls or anti-virus software; manage user access permissions/revoking; and maintain confidentiality/integrity as part of day-to-day business operations activities.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

Correct Answer: D

upvoted 1 times

Question #79 *Topic 1*

Della works as a security engineer for BlueWell Inc. She wants to establish configuration management and control procedures that will document proposed or actual changes to the information system. Which of the following phases of NIST SP 800-37 C&A methodology will define the above task?

A. Initiation

B. Security Certification

C. Continuous Monitoring

D. Security Accreditation

Suggested Answer: *C*

The various phases of NIST SP 800-37 C&A are as follows: Phase 1: Initiation- This phase includes preparation, notification and resource identification. It performs the security plan analysis, update, and acceptance. Phase 2: Security Certification- The Security certification phase evaluates the controls and documentation. Phase 3: Security Accreditation- The security accreditation phase examines the residual risk for acceptability, and prepares the final security accreditation package. Phase 4: Continuous Monitoring-This phase monitors the configuration management and control, ongoing security control verification, and status reporting and documentation.

Community vote distribution

C (100%)

74gjd_37 Most Recent 1 year, 10 months ago

C. The phase of NIST SP 800-37 C&A methodology that defines the task mentioned is Continuous Monitoring. In this phase, configuration management and control procedures are established to document proposed or actual changes to the information system on an ongoing basis through assessments, audits, and reviews. This ensures that security controls remain effective over time and any changes made do not introduce new vulnerabilities or weaken existing safeguards.

upvoted 1 times

Question #80 *Topic 1*

Which of the following secure coding principles and practices defines the appearance of code listing so that a code reviewer and maintainer who have not written that code can easily understand it?

A. Make code forward and backward traceable

B. Review code during and after coding

C. Use a consistent coding style

D. Keep code simple and small

Suggested Answer: *D, A*

Use a consistent coding style is one of the principles and practices that contribute to defensive coding. This principle defines the appearance of code listing so that a code reviewer and maintainer who have not written that code can easily understand it. For this purpose, all programmers of a team must follow the defines that code must be examined in order to identify coding errors in modules.

Community vote distribution

C (100%)

74gjd_37 Most Recent 1 year, 10 months ago

C. The secure coding principle and practice that defines the appearance of code listing so that a code reviewer and maintainer who have not written the code can easily understand it is "Use a consistent coding style." Therefore, option C is the correct answer. Using a consistent coding style ensures that different parts of the system are written in a similar manner for ease of use as well as allowing other developers to maintain or extend existing functionality with minimal training requirements. This also facilitates proper documentation since individuals trained on one part should be able to easily navigate another area within an application.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

C. Use a consistent coding style

upvoted 2 times

Question #81 *Topic 1*

Which of the following software review processes increases the software security by removing the common vulnerabilities, such as format string exploits, race conditions, memory leaks, and buffer overflows?

A. Management review

B. Code review

C. Peer review

D. Software audit review

Suggested Answer: *C, A*

A code review is a systematic examination of computer source code, which searches and resolves issues occurred in the initial development phase. It increases the software security by removing common vulnerabilities, such as format string exploits, race conditions, memory leaks, and buffer overflows. A code process in which author and one or more colleagues examine a work product, such as document, code, etc., and evaluate technical content and quality. According to the Capability Maturity Model, peer review offers a systematic engineering practice in order to detect and resolve issues occurring in the software artifacts, and examination of a software product, software process, or a set of software processes for assessing compliance with specifications, standards, contractual agreements, or other specifications.

Community vote distribution

B (100%)

74gjd_37 Most Recent 1 year, 10 months ago

B. Code Review. While Peer Review can also provide valuable insights towards improving security, it is not specifically designed to eliminate common vulnerabilities identified in the question. The primary goal of peer review is to ensure that code adheres to coding standards and team conventions while meeting functional requirements. Peer reviews are typically performed by members of the same development team who collaborate on projects. Peers may catch errors that went unnoticed during programming or testing phases, but they may not be familiar with all current security best practices or up-to-date threats/targets. Code reviews for security purposes require specialized knowledge regarding known vulnerabilities and how attackers might exploit them, which a peer reviewer might not have. Therefore, peer reviews complement (but do not replace) other software review processes such as management review, code review, and software audit review that address commonly-known cybersecurity concerns like format string exploits, race conditions, memory leaks, and buffer overflows by focusing explicitly on eliminating these types of weaknesses from within source codebases.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

B. Code review

upvoted 1 times

Question #82 *Topic 1*

Which of the following governance bodies directs and coordinates implementations of the information security program?

A. Chief Information Security Officer

B. Information Security Steering Committee

C. Business Unit Manager

D. Senior Management

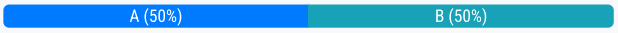
Suggested Answer: *A*

Governance Body	Membership	Responsibilities
Information Security Steering Commitee	CFO, CEO, COO, CTO, VP Business units chaired by CISO	It establishes and supports security programs
Senior Management	C-level, unit VPs and senior VPs	It provides management, operational and technical controls to satisfy security requirements.
Chief Information Security Officer	CISO and staff	It directs and coordinates implementations of information security program.
Business Unit Managers	Department heads and supervisors	They Classify and establish requirements for safeguarding information assets.

Governance Body	Membership	Responsibilities
Information Security Steering Commitee	CFO, CEO, COO, CTO, VP Business units chaired by CISO	It establishes and supports security programs
Senior Management	C-level, unit VPs and senior VPs	It provides management, operational and technical controls to satisfy security requirements.
Chief Information Security Officer	CISO and staff	It directs and coordinates implementations of information security program.
Business Unit Managers	Department heads and supervisors	They Classify and establish requirements for safeguarding information assets.

Chief Information Security Officer directs and coordinates implementations of the information security program. The governance roles and responsibilities are mentioned below in the table:

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

B. The Chief Information Security Officer (CISO) is an executive role responsible for managing the organization's overall information security program. They are primarily responsible for implementing and enforcing policies, procedures, and standards to protect the confidentiality, integrity, and availability of sensitive data or critical systems. However, while CISOs do play a vital role in directing information security activities within their organizations, they typically do not work alone in this regard. The role of the Information Security Steering Committee is to ensure that information security risks are managed consistently across all business units within an organization. The committee helps define organizational policies and priorities related to cybersecurity issues. It coordinates efforts between different departments involved in implementing these policies across multiple business lines or geographies.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

A. Chief Information Security Officer

upvoted 1 times

Question #83 *Topic 1*

In which of the following alternative processing sites is the backup facility maintained in a constant order, with a full complement of servers, workstations, and communication links ready to assume the primary operations responsibility?

A. Cold Site

B. Hot Site

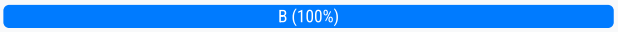
C. Warm Site

D. Mobile Site

Suggested Answer: *A*

A hot site is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data. It provides the backup facility, which is maintained in a constant order, with a full complement of servers, workstations, and communication links ready to assume the primary operations responsibility. A hot site is a backup site in case disaster has taken place in a data center. A hot site is located off site and provides the best protection. It is an exact replica of the current data center. In case a disaster struck to the data center, administrators just need to take the backup of recent data in hot site and the data center is back online in a very short time. It is very expensive to create and maintain the hot site. There are lots of third party companies that provide disaster recovery expensive disaster recovery solution, usually having only a single room with no equipment. All equipment is brought to the site after the disaster. It can be on site hot and cold sites. Warm sites will have hardware and connectivity already established, though on a smaller scale than the original production site or even a hot site. These sites will have backups on hand, but they may not be complete and may be between several days and a week old. An example would be backup tapes sent to the warm site by courier.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

The answer is B. Hot Site. A hot site is an alternative processing site that maintains a backup facility in a constant state of readiness, with a full complement of servers, workstations, and communication links ready to assume the primary operations responsibility. In case of disruption or disaster affecting the primary data center or production facility, operations can be transferred immediately to the hot site with minimal downtime and little to no loss of data. Other types of alternate processing sites include: - Cold Site: This type of site has all physical infrastructure like power supply connectivity and building but does not have IT equipment. - Warm Site: It's similar in concept to a cold site; however, it already has some functional components such as hardware/software installed on its servers but may still need configuration before activation. - Mobile Site: It represents transportation vehicles outfitted with various computing devices in which data storage capacity could be limited at times due primarily to space constraints.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

B. Hot Site

upvoted 1 times

Question #84 *Topic 1*

Which of the following methods offers a number of modeling practices and disciplines that contribute to a successful service-oriented life cycle management and modeling?

A. Service-oriented modeling framework (SOMF)

B. Service-oriented architecture (SOA)

C. Sherwood Applied Business Security Architecture (SABSA)

D. Service-oriented modeling and architecture (SOMA)

Suggested Answer: *B, A*

The service-oriented modeling framework (SOMF) has been proposed by author Michael Bell as a service-oriented modeling language for software development that employs disciplines and a holistic language to provide strategic solutions to enterprise problems. The service-oriented modeling framework (SOMF) is a service-oriented development life cycle methodology. It offers a number of modeling practices and disciplines that contribute to a successful service- oriented life cycle management and modeling. The service-oriented modeling framework illustrates the major elements that identify the "what to do" aspects of a incorrect. SABSA (Sherwood Applied Business Security Architecture) is a framework and methodology for Enterprise Security Architecture and Service Management. It is a model and a methodology for developing risk-driven enterprise information security architectures and for delivering security infrastructure solutions that support critical business initiatives.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

The answer is A. Service-oriented modeling framework (SOMF). Service-oriented modeling and architecture (SOMA) is a method that provides guidance on how to model, design, and implement services in service-oriented architecture (SOA). However, it is not related to service lifecycle management. On the other hand, the service-oriented modeling framework (SOMF) offers various practices and disciplines that contribute to a successful service-oriented lifecycle management and modeling. SOMF provides detailed guidance through different phases of a system development cycle with numerous critical success factors such as governance issues or value chain analysis. It covers areas like business process redesigning around services orientation, governance mechanisms for SOA adoption/fosterage based upon defined contracts between entities down and across enterprise layers.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

A. Service-oriented modeling framework (SOMF)

upvoted 1 times

Question #85 *Topic 1*

Which of the following phases of DITSCAP includes the activities that are necessary for the continuing operation of an accredited IT system in its computing environment and for addressing the changing threats that a system faces throughout its life cycle?

A. Phase 3, Validation

B. Phase 1, Definition

C. Phase 2, Verification

D. Phase 4, Post Accreditation Phase

Suggested Answer: *A, B*

Phase 4, Post Accreditation Phase of the DITSCAP includes the activities, which are necessary for the continuing operation of an accredited IT Definition, focuses on understanding the mission, the environment, and the architecture in order to determine the security requirements and level of effort information stated in the SSAA.

Community vote distribution

D (100%)

74gjd_37 Most Recent 1 year, 10 months ago

The answer is D. Phase 4, Post Accreditation Phase. DITSCAP (Department of Defense Information Technology Security Certification and Accreditation Process) is a standard information assurance process for the Department of Defense (DoD). It comprises five distinct phases to ensure that an IT system meets specific security requirements before it can be put into operation within the DoD's computing environment. Phase 4, known as the Post Accreditation Phase, includes activities that are necessary for maintaining operational security controls continually throughout a system's life cycle under changing threats or operational conditions. During this phase, ongoing monitoring takes place to identify any new vulnerabilities in the IT system or changes in its operating environment that could affect its accreditation status.

upvoted 1 times

4e3rv21rq3vq2q 3 years, 1 month ago

D. Phase 4, Post Accreditation Phase

upvoted 1 times

Question #86 *Topic 1*

Joseph works as a Software Developer for WebTech Inc. He wants to protect the algorithms and the techniques of programming that he uses in developing an application. Which of the following laws are used to protect a part of software?

A. Code Security law

B. Patent laws

C. Trademark laws

D. Copyright laws

Suggested Answer: *A, D*

Patent laws are used to protect the duplication of software. Software patents cover the algorithms and techniques that are used in creating the software. It does not cover the entire program of the software. Patents give the author the right to make and sell his product. The time of the patent of a product is works or creations of authorship including literary, dramatic, musical, artistic, and certain other intellectual works.

74gjd_37 Most Recent 1 year, 10 months ago

D. Copyright laws Patent laws can indeed be used to protect algorithms if they meet specific requirements established by patent offices. However, obtaining software patents for algorithms and techniques of programming is often a challenging task since the majority of countries require that an algorithm or programming technique meets stringent standards like novelty and non-obviousness. In addition, there is considerable uncertainty as to whether algorithms can even fall under subject matter eligible for patent protection in some jurisdictions like Europe (European Patent Convention-Art 52) whereas in the US many court cases establish this right to protect intellectual property using patterns/algorithms through inventiveness demonstrated when innovations occur during innovation fits within statutory guidelines involving sufficiently defined parameters.

upvoted 1 times

Question #87 *Topic 1*

Which of the following types of signatures is used in an Intrusion Detection System to trigger on attacks that attempt to reduce the level of a resource or system, or to cause it to crash?

A. Access

B. Benign

C. DoS

D. Reconnaissance

Suggested Answer: *C*

Following are the basic categories of signatures: Informational (benign): These types of signatures trigger on normal network activity. For example: ICMP echo requests The opening or closing of TCP or UDP connections Reconnaissance: These types of signatures trigger on attacks that uncover resources and hosts that are reachable, as well as any possible vulnerabilities that they might contain. For example: Reconnaissance attacks include ping sweeps DNS queries Port scanning Access: These types of signatures trigger on access attacks, which include unauthorized access, unauthorized escalation of privileges, and access to protected or sensitive data. For example: Back Orifice A Unicode attack against the Microsoft IIS NetBus DoS: These types of signatures trigger on attacks that attempt to reduce the level of a resource or system, or to cause it to crash. For example: TCP SYN floods The Ping of Death Smurf Fraggle Trinoo Tribe Flood Network

Community vote distribution

C (100%)

74gjd_37 Most Recent 1 year, 10 months ago

The type of signature used in an Intrusion Detection System to trigger on attacks that attempt to reduce the level of a resource or system, or to cause it to crash is C. DoS, which stands for Denial-of-Service.

upvoted 1 times

Question #88 *Topic 1*

Which of the following is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention?

A. Copyright

B. Snooping

C. Utility model

D. Patent

Suggested Answer: *A*

A patent is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an of original expression, such as a literary work, movie, musical work or sound recording, painting, photograph, computer program, or industrial design, for a incorrect. Snooping is an activity of observing the content that appears on a computer monitor or watching what a user is typing. Snooping also occurs by using software programs to remotely monitor activity on a computer or network device. Hackers or attackers use snooping techniques and equipment such as keyloggers to monitor keystrokes, capture passwords and login information, and to intercept e-mail and other private communications. Sometimes, organizations intellectual property right to protect inventions.

Community vote distribution

D (100%)

74gjd_37 Most Recent 1 year, 10 months ago

D. Patent Patenting an invention helps to protect it against infringement by competitors who may attempt to copy or steal intellectual property. Patents indicate exclusive rights over a particular technology for a fixed period of time in exchange for public disclosure of its workings. Therefore, information related to new inventions within organizations is kept confidential so that appropriate measures can be taken if there are any vulnerabilities that were exploited while developing core technology. This results in tight regulation and management required for such kind of information which requires legal protection through patents.

upvoted 1 times

Question #89 *Topic 1*

Which of the following actions does the Data Loss Prevention (DLP) technology take when an agent detects a policy violation for data of all states? Each correct answer represents a complete solution. Choose all that apply.

A. It creates an alert.

B. It quarantines the file to a secure location.

C. It reconstructs the session.

D. It blocks the transmission of content.

Suggested Answer: *C*

When an agent detects a policy violation for data of all states, the Data Loss prevention (DLP) technology takes one of the following actions: It creates an alert. It notifies an administrator of a violation. It quarantines the file to a secure location. It encrypts the file. It blocks the transmission of content.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

D. While creating an alert is useful to notify concerned parties about potential violations and help in investigating incidents, it does not solve the issue at hand - which is to prevent any further potential violations from occurring. Similarly, quarantining files or reconstructing sessions may not be necessary or effective solutions for every instance of policy violation. Blocking transmission can minimize risks associated with confidential data leaks and unauthorized disclosures when policies governing those types of data are violated.

upvoted 1 times

Question #90 *Topic 1*

In which of the following processes are experienced personnel and software tools used to investigate, resolve, and handle process deviation, malformed data, infrastructure, or connectivity issues?

A. Risk Management

B. Exception management

C. Configuration Management

D. Change Management

Suggested Answer: *C*

Exception management is a process in which experienced personnel and software tools are used to investigate, resolve, and handle process deviation, malformed Configuration Management (CM) is an Information Technology Infrastructure Library (ITIL) IT Service Management (ITSM) process. It tracks all of the individual Configuration Items (CI) in an IT system, which may be as simple as a single server, or as complex as the entire IT department. In large organizations a control risks. It includes analyzing the value of assets to the business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats. Risk Management is part of Service Design and the owner of the Risk Management is the Risk Manager. Risks are addressed within several processes in ITIL V3; however, there is no dedicated Risk Management process. ITIL V3 calls for "coordinated risk assessment exercises", so at IT Process Maps we decided used for efficient handling of all changes. A change is "an event that results in a new status of one or more configuration items (CI's)" approved by management, cost effective, enhances business process changes (fixes) - with a minimum risk to IT infrastructure. The main aims of Change Management are as follows: Minimal disruption of services Reduction in back-out activities Economic utilization of resources involved in the change

Community vote distribution

B (100%)

74gjd_37 Most Recent 1 year, 10 months ago

B. Exception management is the process of identifying and resolving issues that deviate from the standard operating procedures or exceptional events that occur during normal operation. When a deviation occurs, experienced personnel and software tools are used to investigate, resolve, and handle the issue promptly before it affects system performance. Therefore, exception management involves investigating and handling both process deviations and infrastructure/connectivity issues in real-time. Risk Management deals with managing unknown risks in advance by identifying vulnerabilities along with their likelihoods of occurrence; Configuration Management manages changes to hardware configuration items (CIs); Change Management facilitates controlled modifications to IT environments without change-related disruptions on services generally but not specifically for handling exceptions or deviations.

upvoted 1 times

Question #91 *Topic 1*

Which of the following rated systems of the Orange book has mandatory protection of the TCB?

A. A-rated

B. B-rated

C. D-rated

D. C-rated

Suggested Answer: *B*

A B-rated system of the orange book has mandatory protection of the trusted computing base (TCB). Trusted computing base (TCB) refers to hardware, software, controls, and processes that cause a computer system or network to be devoid of malicious software or hardware. Maintaining the trusted computing base (TCB) is essential for security policy to be implemented successfully.

Community vote distribution

D (100%)

74gjd_37 1 year, 10 months ago

D. C-rated. The Orange Book refers to the Trusted Computer System Evaluation Criteria (TCSEC), which was developed by the United States Department of Defense in 1983 to evaluate computer systems' security effectiveness. The TCSEC was later replaced by the Common Criteria for Information Technology Security Evaluation (CC). The C-rating applied to a system signifies that it is intended for use with non-sensitive data and requires discretionary protection of classified information. Mandatory protection of the trusted computing base (TCB), including identification and authentication mechanisms and reference validation mechanisms, must be enforced in this rated system category. Therefore, option D is correct as mandatory protection of TCB is required in a C-rated system.The Trusted Computing Base (TCB) is a component of a computer system that implements the necessary security mechanisms to enforce the system's overall security policy. It includes all hardware, software, and firmware components that are critical to enforcing security policies. The TCB ensures that information processed by the system remains protected, making it one of the essential parts of secure systems. In context with this question about Orange Book ratings, mandatory protection for TCB refers to the fact that certain levels of rated systems require strict enforcement measures in place for maintaining hardware and software integrity. In particular, C-rated systems must have mechanisms in place such as identification/authentication and reference validation mechanism within their TCB configurations.The TCSEC was developed by the United States Department of Defense to evaluate computer systems' security effectiveness. Each rating level represents a different level of security protection provided by a particular computing system: A-rated: Designated for systems containing highly sensitive information that require mandatory protection mechanisms. B-rated: Designated for systems where users share access to

upvoted 1 times

74gjd_37 1 year, 10 months ago

Selected Answer: D

D. C-rated.

The Orange Book refers to the Trusted Computer System Evaluation Criteria (TCSEC), which was developed by the United States Department of Defense in 1983 to evaluate computer systems' security effectiveness. The TCSEC was later replaced by the Common Criteria for Information Technology Security Evaluation (CC).

The C-rating applied to a system signifies that it is intended for use with non-sensitive data and requires discretionary protection of classified information. Mandatory protection of the trusted computing base (TCB), including identification and authentication mechanisms and reference validation mechanisms, must be enforced in this rated system category. Therefore, option D is correct as mandatory protection of TCB is required in a C-rated system.

upvoted 1 times

74gjd_37 Most Recent 1 year, 10 months ago

The Trusted Computing Base (TCB) is a component of a computer system that implements the necessary security mechanisms to enforce the system's overall security policy. It includes all hardware, software, and firmware components that are critical to enforcing security policies. The TCB ensures that information processed by the system remains protected, making it one of the essential parts of secure systems. In context with this question about Orange Book ratings, mandatory protection for TCB refers to the fact that certain levels of rated systems require strict enforcement measures in place for maintaining hardware and software integrity. In particular, C-rated systems must have mechanisms in place such as identification/authentication and reference validation mechanism within their TCB configurations.

upvoted 1 times

74gjd_37 1 year, 10 months ago

The TCSEC was developed by the United States Department of Defense to evaluate computer systems' security effectiveness. Each rating level represents a different level of security protection provided by a particular computing system: A-rated: Designated for systems containing highly sensitive information that require mandatory protection mechanisms. B-rated: Designated for systems where users share access to data but can be restricted from certain resources granted only at those user's discretion C-rated: Designed for general-purpose computer systems in which discretionary-based access is permitted avoiding any accidental or incidental loss or destruction of hardware or software components D-rated: Represents minimal-security assurance, and it applies to standalone computers and other low-end communication devices.

upvoted 1 times

Question #92 *Topic 1*

Which of the following is designed to detect unwanted attempts at accessing, manipulating, and disabling of computer systems through the Internet?

A. DAS

B. IPsec

C. IDS

D. ACL

Suggested Answer: *D*

An Intrusion detection system (IDS) is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer systems, mainly through a network, such as the Internet. These attempts may take the form of attacks, as examples, by crackers, malware and/or disgruntled employees. An IDS cannot directly detect attacks within properly encrypted traffic. An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (viruses, trojan horses, whether routed packets are forwarded or blocked at the router's interfaces. According to the criteria specified within the access lists, router determines whether the packets to be forwarded or dropped. Access control list criteria could be the source or destination address of the traffic or other information. The types of Cisco using encryption and digital signing. It enhances the security of data as if an IPSec packet is captured, its contents cannot be read. IPSec also provides sender is directly attached to a server or workstation, without using a storage network.

Community vote distribution

C (100%)

74gjd_37 Most Recent 1 year, 10 months ago

C. IDS

upvoted 1 times

Question #93 *Topic 1*

Which of the following ensures that a party to a dispute cannot deny the authenticity of their signature on a document or the sending of a message that they originated?

A. Confidentiality

B. OS fingerprinting

C. Reconnaissance

D. Non-repudiation

Suggested Answer: *A*

Non-repudiation is a term that refers to the ability to ensure that a party to a dispute cannot deny the authenticity of their signature on a document or the sending of a message that they originated. Non-repudiation is the concept of ensuring that a party in a dispute cannot refuse to acknowledge, or refute the validity of a statement or contract. As a service, it provides proof of the integrity and origin of data. Although this concept can be applied to any transmission, mechanism that ensures that only the intended and authorized recipients are able to read data. The data is so encrypted that even if an unauthorized user gets the organization, employees, network, and systems before an attack is performed efficiently. It is the first step in the process of intrusion and involves unauthorized discovery and mapping of systems, services, or vulnerabilities. These discovery and mapping techniques are commonly known as scanning and enumeration. Common tools, commands, and utilities used for scanning and enumeration include ping, telnet, nslookup, rpcinfo, File Explorer, finger, etc. Reconnaissance activities take place before performing a malicious attack. These activities are used to increase the probability of successful operation against the target, and to external network interface of a computer to determine the computer's operating system. It is one of the primary steps taken by hackers in preparing an attack.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

D. Non-repudiation

upvoted 1 times

Question #94 *Topic 1*

Which of the following are examples of the application programming interface (API)? Each correct answer represents a complete solution. Choose three.

A. HTML

B. PHP

C. .NET

D. Perl

Suggested Answer: *A*

Perl, .NET, and PHP are examples of the application programming interface (API). API is a set of routines, protocols, and tools that users can use to work with a component, application, or operating system. It consists of one or more DLLs that provide specific functionality. API helps in reducing the development time of applications by reducing application code. Most operating environments, such as MS-Windows, provide an API so that programmers can write applications create Web pages and define formatting specifications. The markup tells the Web browser how to display the content of the Web page.

Community vote distribution

BCD (100%)

74gjd_37 Most Recent 1 year, 10 months ago

The correct answers are B. PHP, C. .NET, and D. Perl. HTML is a markup language and not an API.

upvoted 1 times

Question #95 *Topic 1*

In which of the following cryptographic attacking techniques does an attacker obtain encrypted messages that have been encrypted using the same encryption algorithm?

A. Chosen plaintext attack

B. Chosen ciphertext attack

C. Ciphertext only attack

D. Known plaintext attack

Suggested Answer: *C*

In a ciphertext only attack, an attacker obtains encrypted messages that have been encrypted using the same encryption algorithm.

Community vote distribution

D (100%)

74gjd_37 Most Recent 1 year, 10 months ago

The attack where an attacker obtains encrypted messages that have been encrypted using the same encryption algorithm is called a "known plaintext attack". So, the correct option is D.

upvoted 1 times

Question #96 *Topic 1*

The IAM/CA makes certification accreditation recommendations to the DAA. The DAA issues accreditation determinations. Which of the following are the accreditation determinations issued by the DAA? Each correct answer represents a complete solution. Choose all that apply.

A. IATT

B. IATO

C. DATO

D. ATO

E. ATT

Suggested Answer: *E*

The DAA issues one of the following four accreditation determinations: Approval to Operate (ATO): It is an authorization of a DoD information system to process, store, or transmit information. Interim Approval to Operate (IATO): It is a temporary approval to operate based on an assessment of the implementation status of the assigned IA Controls. Interim Approval to Test (IATT): It is a temporary approval to conduct system testing based on an assessment of the implementation status of the assigned IA Controls. Denial of Approval to Operate (DATO): It is a determination that a DoD information system cannot operate

Community vote distribution

BD (100%)

74gjd_37 1 year, 10 months ago

The accreditation determinations issued by the DAA are IATO and ATO. Therefore, options B and D are correct. Option A (IATT), option C (DATO), and option E (ATT) are not relevant to CSSLP accreditation.A Designated Accreditation Authority (DAA) is an individual or group responsible for making formal accreditation determinations regarding a given system, network, application or organization. The DAA ensures that critical data-related assets such as networks and applications meet stringent regulatory security controls established by government bodies. This person has full authority over decision-making relating to information security and operational risk management and oversee periodic reviews and assessments of systems/applications to ensure continued compliance with established standards.IATO stands for Interim Authorization to Operate. It is an accreditation determination issued by the Designated Accreditation Authority (DAA) that allows a system or application to operate on an interim basis while a full assessment of its security controls and risks is being conducted. This determination may be given when there is an urgent need for the system/application to become operational, but a full Assessment and Authorization (A&A) process has not yet been completed. An IATO typically remains in effect until the A&A process can be fully completed, which involves conducting comprehensive testing and evaluation of all relevant security controls and documenting their effectiveness in mitigating identified risks.ATO stands for Authorization to Operate and is a formal determination issued by the Designated Accreditation Authority (DAA) stating that a particular system or application has been assessed, evaluated, and found to have an acceptable level of security controls in place. An ATO indicates that the organization responsible for the system/application has completed all necessary steps in adhering to established guidelines, policies, and regulations. An ATO includes documen

upvoted 1 times

74gjd_37 1 year, 10 months ago

Selected Answer: BD

The accreditation determinations issued by the DAA are IATO and ATO. Therefore, options B and D are correct. Option A (IATT), option C (DATO), and option E (ATT) are not relevant to CSSLP accreditation.

upvoted 1 times

74gjd_37 Most Recent 1 year, 10 months ago

A Designated Accreditation Authority (DAA) is an individual or group responsible for making formal accreditation determinations regarding a given system, network, application or organization. The DAA ensures that critical data-related assets such as networks and applications meet stringent regulatory security controls established by government bodies. This person has full authority over decision-making relating to information security and operational risk management and oversee periodic reviews and assessments of systems/applications to ensure continued compliance with established standards.

upvoted 1 times

74gjd_37 1 year, 10 months ago

IATO stands for Interim Authorization to Operate. It is an accreditation determination issued by the Designated Accreditation Authority (DAA) that allows a system or application to operate on an interim basis while a full assessment of its security controls and risks is being conducted. This determination may be given when there is an urgent need for the system/application to become operational, but a full Assessment and Authorization

(A&A) process has not yet been completed. An IATO typically remains in effect until the A&A process can be fully completed, which involves conducting comprehensive testing and evaluation of all relevant security controls and documenting their effectiveness in mitigating identified risks.

upvoted 1 times

74gjd_37 1 year, 10 months ago

ATO stands for Authorization to Operate and is a formal determination issued by the Designated Accreditation Authority (DAA) stating that a particular system or application has been assessed, evaluated, and found to have an acceptable level of security controls in place. An ATO indicates that the organization responsible for the system/application has completed all necessary steps in adhering to established guidelines, policies, and regulations. An ATO includes documentation indicating compliance with federal standards such as CNSSI 1253, NIST SP 800-53 Rev4 requirements. The authorization process involves conducting comprehensive testing and evaluation of all relevant security controls based on the information gathered during earlier stages. Organizational leadership will determine if this risk is acceptable before issuing an ATO.

upvoted 1 times

Question #1 *Topic 2*

Which of the following strategies is used to minimize the effects of a disruptive event on a company, and is created to prevent interruptions to normal business activity?

A. Continuity of Operations Plan

B. Contingency Plan

C. Disaster Recovery Plan

D. Business Continuity Plan

Suggested Answer: *A, B*

BCP is a strategy to minimize the consequence of the instability and to allow for the continuation of business processes. The goal of BCP is to minimize the effects of a disruptive event on a company, and is formed to avoid interruptions to normal business activity. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a plan devised for a specific situation when things could go wrong. Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen. Contingency plans include specific strategies and actions to deal with specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also include a monitoring process and "triggers" for initiating planned actions. They are required to help recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking), and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication, and reputation protection, and should refer to the disaster recovery plan (DRP) for IT-related infrastructure government, providing survival of federal government operations in the case of catastrophic events. It provides procedures and capabilities to sustain an organization's essential. COOP is the procedure documented to ensure persistent critical operations throughout any period where normal operations are unattainable.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

Selected Answer: D

The correct answer is D. Business Continuity Plan. A business continuity plan (BCP) is created to minimize the effects of a disruptive event on a company and ensure that critical business functions can continue uninterrupted. BCPs typically involve procedures for disaster recovery, contingency planning, emergency response communication, and resource management in case of an adverse event or threat.

upvoted 1 times

74gjd_37 1 year, 10 months ago

The correct answer is D. Business Continuity Plan. A business continuity plan (BCP) is created to minimize the effects of a disruptive event on a company and ensure that critical business functions can continue uninterrupted. BCPs typically involve procedures for disaster recovery, contingency planning, emergency response communication, and resource management in case of an adverse event or threat.While a disaster recovery plan (DRP) may sound similar to a business continuity plan (BCP), they serve different purposes. A disaster recovery plan focuses on recovering from an event that has already occurred, such as restoring data and IT infrastructure systems after an interruption or outage. A DRP typically includes procedures for assessing damage, identifying resources required for recovery, and executing the technical steps needed to restore critical IT systems. In contrast, a business continuity plan is designed to prevent disruptions in the first place

upvoted 1 times

74gjd_37 1 year, 10 months ago

While a disaster recovery plan (DRP) may sound similar to a business continuity plan (BCP), they serve different purposes. A disaster recovery plan focuses on recovering from an event that has already occurred, such as restoring data and IT infrastructure systems after an interruption or outage. A DRP typically includes procedures for assessing damage, identifying resources required for recovery, and executing the technical steps needed to restore critical IT systems. In contrast, a business continuity plan is designed to prevent disruptions in the first place

upvoted 1 times

Question #2 *Topic 2*

Which of the following ISO standards provides guidelines for accreditation of an organization that is concerned with certification and registration related to ISMS?

A. ISO 27006

B. ISO 27005

C. ISO 27003

D. ISO 27004

Suggested Answer: *C*

ISO 27006 is an information security standard developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is entitled as "Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems". The ISO 27006 standard provides guidelines for accreditation of an organization which is concerned with certification and registration related to ISMS. The ISO 27006 standard contains the following elements: Scope Normative references Terms and definitions Principles General requirements Structural requirements Resource requirements Information requirements Process requirements Management system requirements for certification bodies Information security risk communication Information security risk monitoring and review Annex A. Defining the scope of process Annex B. Asset valuation and impact assessment Annex C. Examples of typical threats Annex D. Vulnerabilities and vulnerability assessment methods Annex E. Information security risk provides guidelines for information security risk management.

Community vote distribution

A (100%)

74gjd_37 Most Recent 1 year, 10 months ago

The correct answer is A. ISO 27006 provides guidelines for the accreditation of organizations that provide certification and registration of Information Security Management Systems (ISMS) based on the ISO 27001 standard.

upvoted 1 times

Question #3 *Topic 2*

You are advising a school district on disaster recovery plans. In case a disaster affects the main IT centers for the district they will need to be able to work from an alternate location. However, budget is an issue. Which of the following is most appropriate for this client?

A. Cold site

B. Off site

C. Warm site

D. Hot site

Suggested Answer: *A, D*

A cold site provides an office space, and in some cases basic equipment. However, you will need to restore your data to that equipment in order to make disaster recovery much faster, but will also be more expensive. And a school district can afford to be down for several hours before resuming IT operations, backup site terminology.

Community vote distribution

C (100%)

74gjd_37 Most Recent 1 year, 10 months ago

C. Given the budget concerns, the most appropriate option for this school district would be a warm site. A warm site is a location that has infrastructure and equipment in place but is not actively running. The district can quickly move their data and systems to the warm site in case of an IT center disaster, but it will require some additional time and effort to get everything up and running smoothly. This option is less expensive than a hot site (which provides immediate backup capabilities) or off-site storage (which requires constant maintenance). A cold site would also be less ideal as it lacks any existing infrastructure or equipment, meaning more resources would have to be spent on setting it up before use.

upvoted 1 times

Question #4 *Topic 2*

Which of the following authentication methods is used to access public areas of a Web site?

A. Anonymous authentication

B. Biometrics authentication

C. Mutual authentication

D. Multi-factor authentication

Suggested Answer: *A, D*

Anonymous authentication is an authentication method used for Internet communication. It provides limited access to specific public folders and directory information or public areas of a Web site. It is supported by all clients and is used to access unsecured content in public folders. An administrator must methods of authentication. For example, an authentication method that uses smart cards as well as usernames and passwords can be referred to as multi-factor before performing any application function. The client and server identities can be verified through a trusted third party and use shared secrets as in the case of Kerberos v5. The MS-CHAP v2 and EAP-TLS authentication methods support mutual authentication. to identify a user.

Community vote distribution

A (100%)

74gjd_37 Most Recent 1 year, 10 months ago

The authentication method used to access public areas of a website is anonymous authentication. Answer: A.

upvoted 1 times

Question #5 *Topic 2*

Stella works as a system engineer for BlueWell Inc. She wants to identify the performance thresholds of each build. Which of the following tests will help Stella to achieve her task?

A. Reliability test

B. Performance test

C. Regression test

D. Functional test

Suggested Answer: *B*

The various types of internal tests performed on builds are as follows: Regression tests: It is also known as the verification testing. These tests are developed to confirm that capabilities in earlier builds continue to work correctly in the subsequent builds. Functional test: These tests emphasizes on verifying that the build meets its functional and data requirements and correctly generates each expected display and report. Performance tests: These tests are used to identify the performance thresholds of each build. Reliability tests: These tests are used to identify the reliability thresholds of each build.

Community vote distribution



74gjd_37 1 year, 10 months ago

The best test for Stella to identify the performance thresholds of each build would be a Performance test. Therefore, option B is correct.A Performance Test is a type of testing that measures the speed, responsiveness, stability, and scalability of a system or application under specific conditions. The goal of performance testing is to identify the maximum number of users or transactions that can be supported by the system without compromising its functionality, security, and reliability. It involves simulating real-world scenarios and measuring various system parameters such as response time, throughput rate, CPU usage, memory consumption, network latency/throughput. The purpose of performance testing is not only to test whether the application responds correctly but also whether it does so quickly enough under varying loads to meet user expectations and business requirements. This type of testing enables developers and testers to detect any bottlenecks in the system's architecture or code early in development or before deployment into production environments which may cause poor performance on customer end-users thereby causing dissatisfaction with product/services which affects revenue negatively over time.

upvoted 1 times

74gjd_37 1 year, 10 months ago

Selected Answer: B

The best test for Stella to identify the performance thresholds of each build would be a Performance test. Therefore, option B is correct.

upvoted 1 times

74gjd_37 Most Recent 1 year, 10 months ago

A Performance Test is a type of testing that measures the speed, responsiveness, stability, and scalability of a system or application under specific conditions. The goal of performance testing is to identify the maximum number of users or transactions that can be supported by the system without compromising its functionality, security, and reliability. It involves simulating real-world scenarios and measuring various system parameters such as response time, throughput rate, CPU usage, memory consumption, network latency/throughput. The purpose of performance testing is not only to test whether the application responds correctly but also whether it does so quickly enough under varying loads to meet user expectations and business requirements. This type of testing enables developers and testers to detect any bottlenecks in the system's architecture or code early in development or before deployment into production environments which may cause poor performance on customer end-users thereby causing dissatisfaction with product/services which affects revenue negatively over time.

upvoted 1 times

Question #6 *Topic 2*

Continuous Monitoring is the fourth phase of the security certification and accreditation process. What activities are performed in the Continuous Monitoring process? Each correct answer represents a complete solution. Choose all that apply.

A. Security accreditation decision

B. Security control monitoring and impact analyses of changes to the information system

C. Security accreditation documentation

D. Configuration management and control

E. Status reporting and documentation

Suggested Answer: *A, C*

Continuous Monitoring is the fourth phase of the security certification and accreditation process. The Continuous Monitoring process consists of the following three main activities: Configuration management and control Security control monitoring and impact analyses of changes to the information system Status reporting and documentation The objective of these tasks is to observe and evaluate the information system security controls during the system life cycle. decision and security accreditation documentation are the two tasks of the security accreditation phase.

Community vote distribution

BDE (100%)

74gjd_37 Most Recent 1 year, 10 months ago

From an ISC2 CSSLP perspective, the activities performed in the Continuous Monitoring process include: B. Security control monitoring and impact analyses of changes to the information system D. Configuration management and control E. Status reporting and documentation Therefore, options B, D, and E are correct answers.

upvoted 1 times

Question #7 *Topic 2*

Which of the following terms ensures that no intentional or unintentional unauthorized modification is made to data?

A. Non-repudiation

B. Integrity

C. Authentication

D. Confidentiality

Suggested Answer: *D*

host.

Community vote distribution

B (100%)

74gjd_37 Most Recent 1 year, 10 months ago

B. Integrity

upvoted 1 times

Question #8 *Topic 2*

Which of the following provides an easy way to programmers for writing lower-risk applications and retrofitting security into an existing application?

A. Watermarking

B. ESAPI

C. Encryption wrapper

D. Code obfuscation

Suggested Answer: *A*

ESAPI (Enterprise Security API) is a group of classes that encapsulate the key security operations, needed by most of the applications. It is a free, open source, Web application security control library. ESAPI provides an easy way to programmers for writing lower-risk applications and retrofitting security into

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

Selected Answer: B

From an ISC2 CISSP perspective, ESAPI (Enterprise Security Application Programming Interface) provides an easy way for programmers to write lower-risk applications and retrofit security into existing ones. Therefore, option B is the correct answer.

ESAPI offers a set of libraries that includes functionality such as user authentication and input validation, which significantly reduces the risk of common web application vulnerabilities like SQL injection and cross-site scripting. It simplifies coding by incorporating standardized security practices into existing applications rather than requiring extensive changes to be made manually.

Watermarking, encryption wrappers, and code obfuscation are not specifically designed for adding security features to applications but have other uses in different contexts related to software development.

upvoted 1 times

74gjd_37 1 year, 10 months ago

From an ISC2 CISSP perspective, ESAPI (Enterprise Security Application Programming Interface) provides an easy way for programmers to write lower-risk applications and retrofit security into existing ones. Therefore, option B is the correct answer. ESAPI offers a set of libraries that includes functionality such as user authentication and input validation, which significantly reduces the risk of common web application vulnerabilities like SQL injection and cross-site scripting. It simplifies coding by incorporating standardized security practices into existing applications rather than requiring extensive changes to be made manually. Watermarking, encryption wrappers, and code obfuscation are not specifically designed for adding security features to applications but have other uses in different contexts related to software development.ESAPI is an open-source library developed by the Open Web Application Security Project (OWASP) community. It provides standard security functions for software developers to easily implement into their applications, aiming to reduce common web application vulnerabilities. The core team consists of experienced professionals who have been working on software security and testing projects for several years. ESAPI includes input validation, output encoding, access control, cryptographic functionalities and audit logging components ready for implementation. Due to its adaptability across various languages like Java, PHP & Python it has become well-supported when implementing secure web-based infrastructures.

upvoted 1 times

74gjd_37 1 year, 10 months ago

ESAPI is an open-source library developed by the Open Web Application Security Project (OWASP) community. It provides standard security functions for software developers to easily implement into their applications, aiming to reduce common web application vulnerabilities. The core team consists of experienced professionals who have been working on software security and testing projects for several years. ESAPI includes input validation, output encoding, access control, cryptographic functionalities and audit logging components ready for implementation. Due to its adaptability across various languages like Java, PHP & Python it has become well-supported when implementing secure web-based infrastructures.

upvoted 1 times

Question #9 *Topic 2*

Which of the following testing methods tests the system efficiency by systematically selecting the suitable and minimum set of tests that are required to effectively cover the affected changes?

A. Unit testing

B. Integration testing

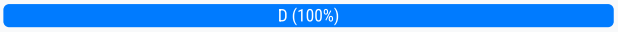
C. Acceptance testing

D. Regression testing

Suggested Answer: *A*

Regression testing focuses on finding defects after a major code change has occurred. Specifically, it seeks to uncover software regressions, or old bugs that have come back. Such regressions occur whenever software functionality that was previously working correctly stops working as intended. Typically, regressions occur as an unintended consequence of program changes, when the newly developed part of the software collides with the previously existing code. Regression testing tests the system efficiency by systematically selecting the suitable and minimum set of tests that are required to effectively cover the affected developer takes the smallest unit of an application, isolates it from the rest of the application code, and tests it to determine whether it works as expected. Unit testing is performed before integrating these independent units into modules. The most common approach to unit testing requires drivers and stubs to be written. the application before its implementation into the production environment. It is done either by a client or an application specialist to ensure that the software meets against a software design. Software components may be integrated in an iterative way or all together ("big bang"). Normally the former is considered a better practice since it allows interface issues to be localized more quickly and fixed. Integration testing works to expose defects in the interfaces and interaction between the integrated components (modules). Progressively larger groups of tested software components corresponding to elements of the architectural design are integrated and tested until the software works as a system.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

The testing method that tests system efficiency by systematically selecting a suitable and minimum set of tests required to effectively cover affected changes is regression testing. Regression testing focuses on retesting previously tested functionality after changes or new features have been introduced into the software, helping ensure that existing functionality performs as expected. Regression testing can be very efficient because it uses automated tools to select specific test cases from a large pool of possible scenarios, minimizing costs associated with running unnecessary tests while prioritizing those most likely to identify issues. To maintain effective security measures and control risks around their systems, organizations must implement comprehensive Software Development Life Cycle (SDLC) practices. Implementing regression testing as an essential part of SDLC continuous integration allows developers to quickly identify potential issues before moving code into production environments.

upvoted 1 times

Question #10 *Topic 2*

Which of the following specifies access privileges to a collection of resources by using the URL mapping?

A. Code Access Security

B. Security constraint

C. Configuration Management

D. Access Management

Suggested Answer: *A*

Security constraint is a type of declarative security, which specifies the protection of web content. It also specifies access privileges to a collection of resources by using the URL mapping. A deployment descriptor is used to define the security constraint. Security constraint includes the following elements: Web Microsoft's solution to prevent untrusted code from performing privileged actions. When the CLR (common language runtime) loads an assembly it will obtain evidence for the assembly and use this to identify the code group that the assembly belongs to. A code group contains a permission set (one or more permissions). Code that performs a privileged action will perform a code access demand, which will cause the CLR to walk up the call stack and examine the permission set granted to the assembly of each method in the call stack. The code groups and permission sets are determined by the administrator of the machine to non- authorized users. The Access Management process essentially executes policies defined in IT Security Management. It is sometimes also referred to as Rights Management or Identity Management. It is part of Service Operation and the owner of Access Management is the Access Manager. Access Management is added as a new process to ITIL V3. The sub-processes of Access Management are as follows: Maintain Catalogue of User Roles and Access Profiles Manage (ITSM) process. It tracks all of the individual Configuration Items (CI) in an IT system, which may be as simple as a single server, or as complex as the entire IT department. In large organizations a configuration manager may be appointed to oversee and manage the CM process.

Community vote distribution

B (100%)

74gjd_37 Most Recent 1 year, 10 months ago

B. Security constraints specify access privileges to a collection of resources by using URL mapping in order to ensure confidentiality, integrity and availability. Code Access Security refers to .NET framework's security system. Configuration Management aims at maintaining consistent performance across an organization over time while Access Management deals with controlling access to resources based on individual user's role or level of need-to-know information.

upvoted 1 times

Question #11 *Topic 2*

You are the project manager of QSL project for your organization. You are working with your project team and several key stakeholders to create a diagram that shows how various elements of a system interrelate and the mechanism of causation within the system. What diagramming technique are you using as a part of the risk identification process?

A. Cause and effect diagrams

B. Influence diagrams

C. Predecessor and successor diagramming

D. System or process flowcharts

Suggested Answer: *A*

In this example you are using a system or process flowchart. These can help identify risks within the process flow, such as bottlenecks or C is incorrect. Predecessor and successor diagramming is not a valid risk identification term.

Community vote distribution

A (100%)

74gjd_37 Most Recent 1 year, 10 months ago

A. Cause and effect diagrams, also known as fishbone or Ishikawa diagrams, are commonly used in risk identification processes to show how different factors may contribute to a problem or potential risk. This technique helps identify the root cause of a problem by exploring its many possible causes and visualizing how they relate to each other.

upvoted 1 times

Question #12 *Topic 2*

Which of the following security models characterizes the rights of each subject with respect to every object in the computer system?

A. Clark-Wilson model

B. Bell-LaPadula model

C. Biba model

D. Access matrix

Suggested Answer: *A, B*

The access matrix or access control matrix is an abstract, formal security model of protection state in computer systems that characterizes the rights of each subject with respect to every object in the system. It was first introduced by Butler W. Lampson in 1971. According to the access matrix model, the protection state of a computer system can be abstracted as a set of objects 'O', that is the set of entities that needs to be protected (e.g. processes, files, memory pages) and a set of subjects 'S' that consists of all active entities (e.g. users, processes). Further there exists a set of rights 'R' of the form r(s,o), where s S, o O is a state machine model used for enforcing access control in government and military applications. The model is a formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and clearances for subjects. Security labels range from the most sensitive (e.g.,"Top Secret"), down to the least sensitive (e.g., "Unclassified" or "Public"). The Bell-La Padula model focuses on data confidentiality and controlled Wilson model provides a foundation for specifying and analyzing an integrity policy for a computing system. The model is primarily concerned with formalizing the notion of information integrity. Information integrity is maintained by preventing corruption of data items in a system due to either error or malicious intent. The model's enforcement and certification rules define data items and processes that provide the basis for an integrity policy. The core of the model is based on the rules designed to ensure data integrity. Data and subjects are grouped into ordered levels of integrity. The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject.

Community vote distribution

D (100%)

74gjd_37 Most Recent 1 year, 10 months ago

D. Access matrix characterizes the rights of each subject with respect to every object in the computer system.

upvoted 1 times

Question #13 *Topic 2*

Penetration testing (also called pen testing) is the practice of testing a computer system, network, or Web application to find vulnerabilities that an attacker could exploit. Which of the following areas can be exploited in a penetration test? Each correct answer represents a complete solution. Choose all that apply.

A. Kernel flaws

B. Information system architectures

C. Race conditions

D. File and directory permissions

E. Buffer overflows

F. Trojan horses

G. Social engineering

Suggested Answer: *A, C, D, E, F, G*
Penetration testing (also called pen testing) is the practice of testing a computer system, network, or Web application to find vulnerabilities that an attacker could exploit. Following are the areas that can be exploited in a penetration test: Kernel flaws: Kernel flaws refer to the exploitation of kernel code flaws in the operating system. Buffer overflows: Buffer overflows refer to the exploitation of a software failure to properly check for the length of input data. This overflow can cause malicious behavior on the system. Race conditions: A race condition is a situation in which an attacker can gain access to a system as a privileged user. File and directory permissions: In this area, an attacker exploits weak permissions restrictions to gain unauthorized access of documents. Trojan horses: These are malicious programs that can exploit an information system by attaching themselves in valid programs and files. Social engineering: In this technique, an attacker uses his social skills and persuasion to acquire valuable information that can be used to conduct an attack against a system.

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

Question #14 *Topic 2*

Which of the following types of activities can be audited for security? Each correct answer represents a complete solution. Choose three.

A. File and object access

B. Data downloading from the Internet

C. Printer access

D. Network logons and logoffs

Suggested Answer: *B*

The following types of activities can be audited: Network logons and logoffs File access Printer access Remote access service Application usage Network services Auditing is used to track user accounts for file and object access, logon attempts, system shutdown, etc. This enhances the security of the network. Before enabling security auditing, the type of event to be audited should be specified in the audit policy. Auditing is an essential component to maintain the security of deployed systems. Security auditing depends on the criticality of the environment and on the company's security policy. The security system should

Community vote distribution

ACD (100%)

74gjd_37 Most Recent 1 year, 10 months ago

Answer: ACD. While both printer access and data downloading from the internet can potentially represent a security threat, auditing printer access is typically considered more important because it relates directly to physical document security. If an unauthorized user gained access to a printer or printed confidential information that they were not authorized to view, this could cause serious problems such as loss of intellectual property, theft of sensitive data, or even legal liability if sensitive client information was involved. By auditing printer usage logs and determining who accessed which printers and when, organizations can help ensure the physical security of documents and prevent unauthorized access or misuse. In contrast, while downloading data from the internet represents its own potential risks (such as downloading malware), it may not always be necessary to audit this activity for every organization. The need for auditing internet downloads would largely depend on each individual organization's specific needs and risk profile - some companies may have more stringent policies around limiting employee web browsing than others depending on their industry or compliance requirements.

upvoted 1 times

Question #15 *Topic 2*

Which of the following federal agencies has the objective to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life?

A. National Security Agency (NSA)

B. National Institute of Standards and Technology (NIST)

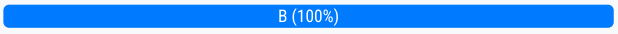
C. United States Congress

D. Committee on National Security Systems (CNSS)

Suggested Answer: *D, A*

The National Institute of Standards and Technology (NIST), known between 1901 and 1988 as the National Bureau of Standards (NBS), is a measurement standards laboratory which is a non-regulatory agency of the United States Department of Commerce. The institute's official mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and policy for the security of the US security systems. The CNSS holds discussions of policy issues, sets national policy, directions, operational procedures, and guidance for the information systems operated by the U.S. Government, its contractors, or agents that contain classified information, involve intelligence activities, The National Security Agency/Central Security Service (NSA/CSS) is a crypto-logic intelligence agency of the United States government. It is administered as part of the United States Department of Defense. NSA is responsible for the collection and analysis of foreign communications and foreign signals intelligence, which involves cryptanalysis. NSA is also responsible for protecting U.S. government communications and information systems from similar agencies elsewhere, which involves cryptography. NSA is a key component of the U.S. Intelligence Community, which is headed by the Director of National Intelligence. The Central Security Service is a co-located agency created to coordinate intelligence activities and co-operation between NSA and U.S. military cryptanalysis agencies. NSA's work is bicameral legislature of the federal government of the United States of America. It consists of the Senate and the House of Representatives. The Congress meets in the United States Capitol in Washington, D.C. Both senators and representatives are chosen through direct election. Each of the 435 members of the House of Representatives represents a district and serves a two-year term. House seats are apportioned among the states by population. The 100 Senators serve staggered six-year terms. Each state has two senators, regardless of population. Every two years, approximately one-third of the Senate is elected at a time. The United States Congress main function is to make laws. The Office of the Law Revision Counsel organizes and publishes the United States Code (USC). It is a consolidation and codification by subject matter of the general and permanent laws of the United States.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

The federal agency with the objective to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life is B. National Institute of Standards and Technology (NIST).

upvoted 1 times

Question #16 *Topic 2*

Which of the following SDLC phases consists of the given security controls: Misuse Case Modeling Security Design and Architecture Review Threat and Risk
Modeling Security Requirements and Test Cases Generation?

A. Deployment

B. Requirements Gathering

C. Maintenance

D. Design

Suggested Answer: *D*
The various security controls in the SDLC design phase are as follows: Misuse Case Modeling: It is important that the inverse of the misuse cases be modeled to understand and address the security aspects of the software. The requirements traceability matrix can be used to track the misuse cases to the functionality of the software. Security Design and Architecture Review: This control can be introduced when the teams are engaged in the "functional" design and architecture review of the software. Threat and Risk Modeling: Threat modeling determines the attack surface of the software by examining its functionality for trust boundaries, data flow, entry points, and exit points. Risk modeling is performed by ranking the threats as they pertain to the users organization's business objectives, compliance and regulatory requirements and security exposures. Security Requirements and Test Cases Generation: All the above three security controls, i.e., Misuse Case Modeling, Security Design and Architecture Review, and Threat and Risk Modeling are used to produce the security requirements.

Community vote distribution
D (100%)

74gjd_37 1 year, 10 months ago

Selected Answer: D

The given security controls - Misuse Case Modeling, Security Design and Architecture Review, Threat and Risk Modeling, Security Requirements and Test Cases Generation – are part of the "Design" phase of the SDLC (Software Development Life Cycle), so the answer is D.

upvoted 1 times

74gjd_37 1 year, 10 months ago

The given security controls - Misuse Case Modeling, Security Design and Architecture Review, Threat and Risk Modeling, Security Requirements and Test Cases Generation – are part of the "Design" phase of the SDLC (Software Development Life Cycle), so the answer is D.The SDLC is a framework used to guide the development of software applications. Its different phases include planning, requirements gathering, design, implementation, and maintenance. The security controls provided in this question - Misuse Case Modeling, Security Design and Architecture Review, Threat and Risk Modeling, Security Requirements and Test Cases Generation – belong to the "Design" phase. During this stage of development, system designers use threat modeling techniques such as misuse case modeling and threat and risk modeling to identify potential vulnerabilities within their designs before writing any code. Additionally designing secure architectures are also taken into considerations along with generating security requirements that can be tested before proceeding further. Overall these practices ensure that all required security features will be included in the final product. Thus it becomes important for developers or those responsible for application security to understand how these controls fit into each SDLC phase while developing robust applications.While planning and requirements gathering are important phases in the SDLC, their focus is mainly on defining the project scope, developing a mitigation plan for potential risks, identifying stakeholders' requirements, and establishing priorities. Threat modeling techniques such as Misuse Case Modeling or Risk & threat assessments often require more insights into design or system architecture to effectively identify vulnerabilities in intended scenarios. In contrast with Planning and Requirements Gathering stages that primarily deal with business reasoning behind development, Design is where actual architectural solutions of Applications fall

upvoted 1 times

74gjd_37 1 year, 10 months ago

The SDLC is a framework used to guide the development of software applications. Its different phases include planning, requirements gathering, design, implementation, and maintenance. The security controls provided in this question - Misuse Case Modeling, Security Design and Architecture Review, Threat and Risk Modeling, Security Requirements and Test Cases Generation – belong to the "Design" phase. During this stage of development, system designers use threat modeling techniques such as misuse case modeling and threat and risk modeling to identify potential vulnerabilities within their designs before writing any code. Additionally designing secure architectures are also taken into considerations along with generating security requirements that can be tested before proceeding further. Overall these practices ensure that all required security features will

be included in the final product. Thus it becomes important for developers or those responsible for application security to understand how these controls fit into each SDLC phase while developing robust applications.

upvoted 1 times

74gjd_37 Most Recent 1 year, 10 months ago

While planning and requirements gathering are important phases in the SDLC, their focus is mainly on defining the project scope, developing a mitigation plan for potential risks, identifying stakeholders' requirements, and establishing priorities. Threat modeling techniques such as Misuse Case Modeling or Risk & threat assessments often require more insights into design or system architecture to effectively identify vulnerabilities in intended scenarios. In contrast with Planning and Requirements Gathering stages that primarily deal with business reasoning behind development, Design is where actual architectural solutions of Applications fall into place while building up comprehensive security controls around it. Thus the Security Design process flows from early Development Phases but separate enough to understand detailed critical aspects of a systems Architecture driven largely by its Functionalities.

upvoted 1 times

Question #17 *Topic 2*

Which of the following are the initial steps required to perform a risk analysis process? Each correct answer represents a part of the solution. Choose three.

A. Valuations of the critical assets in hard costs.

B. Evaluate potential threats to the assets.

C. Estimate the potential losses to assets by determining their value.

D. Establish the threats likelihood and regularity.

Suggested Answer: *A*

The main steps of performing risk analysis are as follows: Estimate the potential losses to the assets by determining their value. Evaluate the final steps taken after performing the risk analysis.

Community vote distribution

BCD (100%)

74gjd_37 1 year, 10 months ago

Selected Answer: BCD

The correct answers are:

B. Evaluate potential threats to the assets. C. Estimate the potential losses to assets by determining their value. D. Establish the threats likelihood and regularity.

Valuations of critical assets in hard costs may be needed, but it is not an initial step required for performing a risk analysis process from an ISC2 CSSLP perspective.

upvoted 1 times

74gjd_37 1 year, 10 months ago

The correct answers are: B. Evaluate potential threats to the assets. C. Estimate the potential losses to assets by determining their value. D. Establish the threats likelihood and regularity. Valuations of critical assets in hard costs may be needed, but it is not an initial step required for performing a risk analysis process from an ISC2 CSSLP perspective.The initial steps required to perform a risk analysis process involve evaluating potential threats, estimating potential losses, and establishing the likelihood and regularity of these threats. These steps help identify areas where security measures need to be implemented or improved in order to mitigate risks. Threat evaluation involves identifying different types of threats that could potentially harm critical assets within an organization's systems. Estimating potential losses requires determining the value of each asset and assessing the financial impact if it were lost or compromised. Threat likelihood and regularity must also be established by examining how often incidents occur and how likely they are to happen again. By going through these initial steps, organizations can develop better-informed risk management strategies that enable them to prioritize investment in effective security controls based on which assets are more valuable or at higher risk for particular threat sources or motives.

upvoted 1 times

74gjd_37 Most Recent 1 year, 10 months ago

The initial steps required to perform a risk analysis process involve evaluating potential threats, estimating potential losses, and establishing the likelihood and regularity of these threats. These steps help identify areas where security measures need to be implemented or improved in order to mitigate risks. Threat evaluation involves identifying different types of threats that could potentially harm critical assets within an organization's systems. Estimating potential losses requires determining the value of each asset and assessing the financial impact if it were lost or compromised. Threat likelihood and regularity must also be established by examining how often incidents occur and how likely they are to happen again. By going through these initial steps, organizations can develop better-informed risk management strategies that enable them to prioritize investment in effective security controls based on which assets are more valuable or at higher risk for particular threat sources or motives.

upvoted 1 times

Question #18 *Topic 2*

Which of the following technologies is used by hardware manufacturers, publishers, copyright holders and individuals to impose limitations on the usage of digital content and devices?

A. Hypervisor

B. Grid computing

C. Code signing

D. Digital rights management

Suggested Answer: *C*

Digital rights management (DRM) is an access control technology used by hardware manufacturers, publishers, copyright holders and individuals to impose limitations on the usage of digital content and devices. It describes the technology that prevents the uses of digital content that were not desired or foreseen by the content provider. DRM does not refer to other forms of copy protection which can be circumvented without modifying the file or device, such as process of digitally signing executables and scripts in order to confirm the software author, and guarantee that the code has not been altered or corrupted since it concurrently on a host computer. It is also called the virtual machine monitor (VMM). The hypervisor provides a virtual operating platform to the guest operating Grid computing refers to the combination of computer resources from multiple administrative domains to achieve a common goal.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

D. Digital rights management

upvoted 1 times

Question #19 *Topic 2*

Which of the following processes provides a standard set of activities, general tasks, and a management structure to certify and accredit systems, which maintain the information assurance and the security posture of a system or site?

A. NSA-IAM

B. NIACAP

C. ASSET

D. DITSCAP

Suggested Answer: *A, D*

NIACAP is a process, which provides a standard set of activities, general tasks, and a management structure to certify and accredit systems that process, a set of activities, general task descriptions, and a management structure to certify and accredit the IT systems that will maintain the required security through the use of the questionnaire in NIST.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

The correct answer is B. NIACAP (National Information Assurance Certification and Accreditation Process) provides a standard set of activities, general tasks, and a management structure to certify and accredit systems, which maintain the information assurance and security posture of a system or site. DITSCAP (Department of Defense Information Technology Security Certification and Accreditation Process) was the predecessor to NIACAP for U.S. Department of Defense systems. NSA-IAM (Information Assurance Methodology) is used by the National Security Agency for certifying government IT systems. ASSET (Automated Security Self-Evaluation Tool) is an automated tool used to assess the security posture of computer networks for risk assessment purposes but does not provide standard processes for certification and accreditation like NIACAP does.NIACAP (National Information Assurance Certification and Accreditation Process) is a U.S. government standard for certifying and accrediting information systems to ensure their security posture meets defined requirements. It provides a structured framework of activities, tasks, roles and responsibilities for the certification and accreditation process. The NIACAP process includes four phases: initiation & planning; certification; accreditation; and maintenance. During each phase, various stakeholders participate in different stages of the process to evaluate system design, construction, testing and operations against established criteria. These criteria include technical controls such as access control mechanisms or encryption standards alongside non-technical considerations like policies or procedures implementing best practices.

upvoted 1 times

74gjd_37 1 year, 10 months ago

Selected Answer: B

The correct answer is B. NIACAP (National Information Assurance Certification and Accreditation Process) provides a standard set of activities, general tasks, and a management structure to certify and accredit systems, which maintain the information assurance and security posture of a system or site. DITSCAP (Department of Defense Information Technology Security Certification and Accreditation Process) was the predecessor to NIACAP for U.S. Department of Defense systems. NSA-IAM (Information Assurance Methodology) is used by the National Security Agency for certifying government IT systems. ASSET (Automated Security Self-Evaluation Tool) is an automated tool used to assess the security posture of computer networks for risk assessment purposes but does not provide standard processes for certification and accreditation like NIACAP does.

upvoted 1 times

74gjd_37 1 year, 10 months ago

NIACAP (National Information Assurance Certification and Accreditation Process) is a U.S. government standard for certifying and accrediting information systems to ensure their security posture meets defined requirements. It provides a structured framework of activities, tasks, roles and responsibilities for the certification and accreditation process. The NIACAP process includes four phases: initiation & planning; certification; accreditation; and maintenance. During each phase, various stakeholders participate in different stages of the process to evaluate system design, construction, testing and operations against established criteria. These criteria include technical controls such as access control mechanisms or encryption standards alongside non-technical considerations like policies or procedures implementing best practices.

upvoted 1 times

Question #20 *Topic 2*

Which of the following security issues does the Bell-La Padula model focus on?

A. Authorization

B. Confidentiality

C. Integrity

D. Authentication

Suggested Answer: *B*

The Bell-La Padula model is a state machine model used for enforcing access control in large organizations. It focuses on data confidentiality and access to classified information, in contrast to the Biba Integrity model, which describes rules for the protection of data integrity. In the Bell-La Padula model, the entities in an information system are divided into subjects and objects. The Bell-La Padula model is built on the concept of a state machine with a set of allowable states in a computer network system. The transition from one state to another state is defined by transition functions. The model defines two mandatory access control (MAC) rules and one discretionary access control (DAC) rule with three security properties: 1.The Simple Security Property: A subject at a given security level may not read an object at a higher security level (no read-up). 2.The *-property (star-property): A subject at a given security level must not write to any object at a lower security level (no write-down). The *-property is also known as the Confinement property. 3.The Discretionary Security Property: It uses an access matrix to specify the discretionary access control.

Community vote distribution

B (100%)

74gjd_37 Most Recent 1 year, 10 months ago

Selected Answer: B

The Bell-La Padula model focuses on maintaining confidentiality in information systems by controlling access to classified information. Therefore, the correct answer is B. Confidentiality.

upvoted 1 times

74gjd_37 1 year, 10 months ago

The Bell-La Padula model focuses on maintaining confidentiality in information systems by controlling access to classified information. Therefore, the correct answer is B. Confidentiality.The Bell-La Padula model is a security model designed to protect the confidentiality of information in computer systems. It was developed by David Bell and Len La Padula in 1973, primarily for use by the United States Department of Defense. The model consists of three elements: subjects, objects, and labels. Subjects are entities that can access objects, such as users or processes. Objects are data resources that need to be protected from unauthorized access or modification, such as files or databases. Labels define the security levels assigned to both subjects and objects. In the Bell-La Padula model, each user is assigned a clearance level based on their job requirements and responsibilities. Each object also has a classification level based on its sensitivity or importance.The model operates under two primary rules: The Simple Security Property - This rule ensures that no subject at one security level should read data from an object at a higher security level. The *-Property (Star Property) - This rule specifies that no subject should be able to write data with lower classification into an object with higher classification. Overall, the Bell-La Padula model seeks to maintain confidentiality by preventing unauthorized disclosure of sensitive information within IT systems while allowing authorized access only if deemed necessary according to predefined policies defined in terms of classifications like top secret/confidential/secret etc., clearances bestowed upon different individual actors/entities involved in handling any type/classification/specific piece(s)of information/data/equipment/systems/components/etc

upvoted 1 times

74gjd_37 1 year, 10 months ago

The Bell-La Padula model is a security model designed to protect the confidentiality of information in computer systems. It was developed by David Bell and Len La Padula in 1973, primarily for use by the United States Department of Defense. The model consists of three elements: subjects, objects, and labels. Subjects are entities that can access objects, such as users or processes. Objects are data resources that need to be protected from unauthorized access or modification, such as files or databases. Labels define the security levels assigned to both subjects and objects. In the Bell-La Padula model, each user is assigned a clearance level based on their job requirements and responsibilities. Each object also has a classification level based on its sensitivity or importance.The model operates under two primary rules: The Simple Security Property - This rule ensures that no subject at one security level should read data from an object at a higher security level. The *-Property (Star Property) - This rule specifies that no subject should be able to write data with lower classification into an object with higher classification. Overall, the Bell-La Padula model seeks to maintain confidentiality by preventing unauthorized disclosure of sensitive information within IT systems while allowing authorized

access only if deemed necessary according to predefined policies defined in terms of classifications like top secret/confidential/secret etc., clearances bestowed upon different individual actors/entities involved in handling any type/classification/specific piece(s)of information/data/equipment/systems/components/etc

upvoted 1 times

74gjd_37 1 year, 10 months ago

The Bell-La Padula model is a security model designed to protect the confidentiality of information in computer systems. It was developed by David Bell and Len La Padula in 1973, primarily for use by the United States Department of Defense.

The model consists of three elements: subjects, objects, and labels. Subjects are entities that can access objects, such as users or processes. Objects are data resources that need to be protected from unauthorized access or modification, such as files or databases. Labels define the security levels assigned to both subjects and objects.

In the Bell-La Padula model, each user is assigned a clearance level based on their job requirements and responsibilities. Each object also has a classification level based on its sensitivity or importance.

upvoted 1 times

74gjd_37 1 year, 10 months ago

The model operates under two primary rules: The Simple Security Property - This rule ensures that no subject at one security level should read data from an object at a higher security level. The *-Property (Star Property) - This rule specifies that no subject should be able to write data with lower classification into an object with higher classification. Overall, the Bell-La Padula model seeks to maintain confidentiality by preventing unauthorized disclosure of sensitive information within IT systems while allowing authorized access only if deemed necessary according to predefined policies defined in terms of classifications like top secret/confidential/secret etc., clearances bestowed upon different individual actors/entities involved in handling any type/classification/specific piece(s)of information/data/equipment/systems/components/etc

upvoted 1 times

Question #21 *Topic 2*

Which of the following phases of the DITSCAP C&A process is used to define the C&A level of effort, to identify the main C&A roles and responsibilities, and to create an agreement on the method for implementing the security requirements?

A. Phase 1

B. Phase 4

C. Phase 2

D. Phase 3

Suggested Answer: *C, A*

The Phase 1 of the DITSCAP C&A process is known as Definition Phase. The goal of this phase is to define the C&A level of effort, identify the main incorrect. The Phase 4 of the DITSCAP C&A process is known as Post Accreditation.

Community vote distribution

A (100%)

74gjd_37 1 year, 10 months ago

In the DITSCAP C&A process, Phase 1 (Definition) is used to define the system and its security requirements. Phase 2 (Verification) involves testing and evaluating the system's security controls. Phase 3 (Validation) verifies that all security controls are implemented correctly. Phase 4 (Post Accreditation) involves ongoing monitoring and maintenance of the system. So based on the options provided in your question, it appears that "Phase 1" would be the correct answer as it relates to defining roles & responsibilities for implementation of security requirements.The DITSCAP (Department of Defense Information Technology Security Certification and Accreditation Process) is a risk management process developed by the US Department of Defense (DoD) to provide a standard process for certifying and accrediting information systems that handle sensitive or classified information. This includes systems such as military command-and-control, logistics, finance, personnel, and intelligence systems.The purpose of the DITSCAP C&A process is to ensure that these information systems meet defined security requirements before they are put into operation. It involves six phases: Definition - define the system and its security requirements Verification - test and evaluate the system's security controls Validation - verify that all security controls are implemented correctly Post Accreditation - ongoing monitoring and maintenance of the system Reaccreditation - periodic review to ensure continued compliance with security requirements Decommissioning phase

upvoted 1 times

74gjd_37 1 year, 10 months ago

Selected Answer: A

In the DITSCAP C&A process, Phase 1 (Definition) is used to define the system and its security requirements. Phase 2 (Verification) involves testing and evaluating the system's security controls. Phase 3 (Validation) verifies that all security controls are implemented correctly. Phase 4 (Post Accreditation) involves ongoing monitoring and maintenance of the system.

So based on the options provided in your question, it appears that "Phase 1" would be the correct answer as it relates to defining roles & responsibilities for implementation of security requirements.

upvoted 1 times

74gjd_37 Most Recent 1 year, 10 months ago

The DITSCAP (Department of Defense Information Technology Security Certification and Accreditation Process) is a risk management process developed by the US Department of Defense (DoD) to provide a standard process for certifying and accrediting information systems that handle sensitive or classified information. This includes systems such as military command-and-control, logistics, finance, personnel, and intelligence systems.

upvoted 1 times

74gjd_37 1 year, 10 months ago

The DITSCAP (Department of Defense Information Technology Security Certification and Accreditation Process) is a risk management process developed by the US Department of Defense (DoD) to provide a standard process for certifying and accrediting information systems that handle sensitive or classified information. This includes systems such as military command-and-control, logistics, finance, personnel, and intelligence systems.The purpose of the DITSCAP C&A process is to ensure that these information systems meet defined security requirements before they are put into operation. It involves six phases: Definition - define the system and its security requirements Verification - test and evaluate the system's security controls Validation - verify that all security controls are implemented correctly Post Accreditation - ongoing monitoring and maintenance of the system Reaccreditation - periodic review to ensure continued compliance with security requirements Decommissioning phase

upvoted 1 times

74gjd_37 1 year, 10 months ago

The purpose of the DITSCAP C&A process is to ensure that these information systems meet defined security requirements before they are put into operation. It involves six phases: Definition - define the system and its security requirements Verification - test and evaluate the system's security controls Validation - verify that all security controls are implemented correctly Post Accreditation - ongoing monitoring and maintenance of the system Reaccreditation - periodic review to ensure continued compliance with security requirements Decommissioning phase

upvoted 1 times

Question #22 *Topic 2*

Which of the following types of obfuscation transformation increases the difficulty for a de-obfuscation tool so that it cannot extract the true application from the obfuscated version?

A. Preventive transformation

B. Data obfuscation

C. Control obfuscation

D. Layout obfuscation

Suggested Answer: *A*

Preventive transformation increases the difficulty for a de-obfuscation tool so that it cannot extract the true application from the obfuscated version.

Community vote distribution

A (100%)

74gjd_37 Most Recent 1 year, 10 months ago

A. The main goal of preventive transformations is not to obscure the program to a human reader, but to make known automatic deobfuscation techniques more difficult or to exploit known problems in current deobfuscators or decompilers . Such transformations are known as inherent and targeted, respectively. An example of an inherent preventive transformation is reordering a for-loop to run backward. Such reordering is possible if the loop has no loop-carried data dependencies. A deobfuscator could perform the same analysis and reorder the loop to forward execution. However, if a bogus data dependency is added to the reversed loop, the identification of the loop and its reordering would be prevented. Source: https://patents.google.com/patent/WO1999001815A1/en

upvoted 1 times

Question #23 *Topic 2*

Which of the following techniques is used when a system performs the penetration testing with the objective of accessing unauthorized information residing inside a computer?

A. Biometrician

B. Van Eck Phreaking

C. Port scanning

D. Phreaking

Suggested Answer: *D, A*

Port scanning identifies open doors to a computer. Hackers and crackers use this technique to obtain unauthorized information. Port scanning is the first basic step to get the details of open ports on the target system. Port scanning is used to find a hackable server with a hole or vulnerability. A port is a medium of communication between two computers. Every service on a host is identified by a unique 16-bit number called a port. A port scanner is a piece of software designed to search a network host for open ports. This is often used by administrators to check the security of their networks and by hackers to identify running services on a host with the view to compromising it. Port scanning is used to find the open ports, so that it is possible to search exploits related to distance calls. As telephone networks have become computerized, phreaking has become closely linked with computer hacking. This is sometimes called the H/P equipments are used to pick up the telecommunication signals or data within a computer device.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

C. Port scanning Phreaking is a form of hacking that targets the telephone system. Port scanning is a technique used to detect which ports are open on a target system. By identifying which ports are open on the system, pentesters can determine potential vulnerabilities that may be exploited by attackers seeking unauthorized access. They can also assess whether any services running on those ports are correctly configured and secured appropriately. The purpose of port scanning in penetration testing is not to gain unauthorized access but rather to identify potential attack surfaces so they can be mitigated before an actual attack occurs.

upvoted 1 times

Question #24 *Topic 2*

Which of the following types of attacks is targeting a Web server with multiple compromised computers that are simultaneously sending hundreds of FIN packets with spoofed IP source IP addresses?

A. DDoS attack

B. Evasion attack

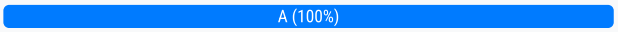
C. Insertion attack

D. Dictionary attack

Suggested Answer: *A, D*

A distributed denial of service (DDoS) attack targets a Web server with multiple compromised computers that are simultaneously sending hundreds of FIN packets with spoofed IP source IP addresses. DDoS attack occurs when multiple compromised systems flood the bandwidth or resources of a targeted system, usually one or more Web servers. These systems are compromised by attackers using a variety of methods. It is an attempt to make a computer resource unavailable to its intended users. This type of attack can cause the following to occur: Saturate network resources. Disrupt connections between two computers, guessing attack. This type of attack uses a dictionary of common words to find out the password of a user. It can also use common words in either upper or lower attack, an IDS accepts a packet and assumes that the host computer will also accept it. But in reality, when a host system rejects the packet, the IDS accepts the evasion attack is one in which an IDS rejects a malicious packet but the host computer accepts it. Since an IDS has rejected it, it does not check the contents of the packet. Hence, using this technique, an attacker can exploit the host computer. In many cases, it is quite simple for an attacker to send such data packets that can easily perform evasion attacks on an IDSs.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

The correct answer is A. DDoS attack. A Distributed Denial of Service (DDoS) attack involves multiple compromised computers, often referred to as a botnet or zombie army, that target a single server with an overwhelming number of requests or traffic to disrupt normal operation and deny service to legitimate users. The use of spoofed IP source addresses is a common technique used in DDoS attacks to make it difficult for the targeted server to distinguish between legitimate and malicious traffic and effectively defend against the attack.

upvoted 1 times

Question #25 *Topic 2*

Which of the following programming languages are compiled into machine code and directly executed by the CPU of a computer system? Each correct answer represents a complete solution. Choose two.

A. C

B. Microosft.NET

C. Java EE

D. C++

Suggested Answer: *C, B*

C and C++ programming languages are unmanaged code. Unmanaged code is compiled into machine code and directly executed by the CPU of a

Community vote distribution

AD (100%)

74gjd_37 Most Recent 1 year, 10 months ago

A. C D. C++

upvoted 1 times

gordzilla8968 2 years, 7 months ago

c,c++ is right answer

upvoted 1 times

Question #26 *Topic 2*

Which of the following is a standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system?

A. FITSAF

B. FIPS

C. TCSEC

D. SSAA

Suggested Answer: *D*

Trusted Computer System Evaluation Criteria (TCSEC) is a United States Government Department of Defense (DoD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system. TCSEC was used to evaluate, classify, and select computer systems being considered for the processing, storage, and retrieval of sensitive or classified information. It was replaced with the development of the Common Criteria international standard originally published in 2005. The TCSEC, frequently referred to as the Orange Book, is the centerpiece of the DoD States Department of Defense (DoD) to describe and accredit networks and systems. The SSAA is part of the Department of Defense Information Technology Security Certification and Accreditation Process, or DITSCAP (superseded by DIACAP). The DoD instruction (issues in December 1997, that describes DITSCAP and provides an outline for the SSAA document is DODI 5200.40. The DITSCAP application manual (DoD 8510.1- M), published in July 2000, provides additional of information systems. It provides an approach for federal agencies. It determines how federal agencies are meeting existing policy and establish goals. The main advantage of FITSAF is that it addresses the requirements of Office of Management and Budget (OMB). It also addresses the guidelines provided by the National developed by the United States federal government for use by all non-military government agencies and by government contractors. Many FIPS standards are modified versions of standards used in the wider community (ANSI, IEEE, ISO, etc.). Some FIPS standards were originally developed by the U.S. government. For instance, standards for encoding data (e.g., country codes), but more significantly some encryption standards, such as the Data Encryption Standard (FIPS 46-3) and the Advanced Encryption Standard (FIPS 197). In 1994, NOAA (Noaa) began broadcasting coded signals called FIPS (Federal Information Processing System) codes along with their standard weather broadcasts from local stations. These codes identify the type of emergency and the specific geographic area (such as a county) affected by the emergency.

Community vote distribution



74gjd_37 1 year, 10 months ago

The correct answer is C. TCSEC (Trusted Computer System Evaluation Criteria) is a standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system. FITSAF (Federal IT Security Assessment Framework), FIPS (Federal Information Processing Standards), and SSAA (System Security Authorization Agreement) are all related to information security but do not specifically address assessment of security controls in computer systems.Trusted Computer System Evaluation Criteria (TCSEC) is a US Department of Defense computer security standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system. The TCSEC establishes four primary levels, from lowest to highest: D, C, B, and A. These levels are based on increasing assurance criteria such as accountability, integrity, confidentiality and auditability. Knowledge of TCSEC is essential in understanding how to evaluate the trustworthiness of different categories of systems with varying degrees of security needs for organizations. It also provides insight into government policies related specifically to information systems relating primarily to access control models used for administration. The evaluation process established by TCSEC can serve as a framework used internally in risk assessments or certification and accreditation processes under various regulatory regimes like FedRAMP (Federal Risk Authorization Management Program).

upvoted 1 times

74gjd_37 1 year, 10 months ago

Selected Answer: C

The correct answer is C. TCSEC (Trusted Computer System Evaluation Criteria) is a standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system. FITSAF (Federal IT Security Assessment Framework), FIPS (Federal Information Processing Standards), and SSAA (System Security Authorization Agreement) are all related to information security but do not specifically address assessment of security controls in computer systems.

upvoted 1 times

74gjd_37 Most Recent 1 year, 10 months ago

Trusted Computer System Evaluation Criteria (TCSEC) is a US Department of Defense computer security standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system. The TCSEC establishes four primary levels, from lowest to highest: D, C, B, and A. These levels are based on increasing assurance criteria such as accountability, integrity, confidentiality and auditability. Knowledge of TCSEC is essential in understanding how to evaluate the trustworthiness of different categories of systems with varying degrees of security needs for organizations. It also provides insight into government policies related specifically to information systems relating primarily to access control models used for administration. The evaluation process established by TCSEC can serve as a framework used internally in risk assessments or certification and accreditation processes under various regulatory regimes like FedRAMP (Federal Risk Authorization Management Program).

upvoted 1 times

Question #27 *Topic 2*

Which of the following elements of BCP process includes the areas of plan implementation, plan testing, and ongoing plan maintenance, and also involves defining and documenting the continuity strategy?

A. Business continuity plan development

B. Business impact assessment

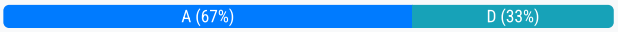
C. Scope and plan initiation

D. Plan approval and implementation

Suggested Answer: *C*

The business continuity plan development refers to the utilization of the information collected in the Business Impact Analysis (BIA) for the creation of the recovery strategy plan to support the critical business functions. The information gathered from the BIA is mapped out to make a strategy for creating a continuity plan. The business continuity plan development process includes the areas of plan implementation, plan testing, and ongoing plan maintenance. This beginning of the BCP process. It emphasizes on creating the scope and the additional elements required to define the parameters of the plan. The scope and plan initiation phase embodies a check of the company's operations and support services. The scope activities include creating a detailed account of the work required, used to facilitate business units to understand the impact of a disruptive event. This phase includes the execution of a vulnerability assessment. This process makes out the mission-critical areas and business processes that are important for the survival of business. It is similar to the risk assessment process. The function of a business impact assessment process is to create a document, which is used to help and understand what impact a disruptive event would have on senior management signoff, and implementing a maintenance procedure for updating the plan as required.

Community vote distribution



01be656 Most Recent 1 year, 5 months ago

The correct answer is A. Business continuity plan development. This element of the Business Continuity Planning (BCP) process encompasses plan implementation, plan testing, ongoing plan maintenance, and the definition and documentation of the continuity strategy

upvoted 2 times

74gjd_37 1 year, 10 months ago

The correct answer is D. Plan approval and implementation.

upvoted 1 times

Question #28 *Topic 2*

Which of the following refers to a process that is used for implementing information security?

A. Classic information security model

B. Five Pillars model

C. Certification and Accreditation (C&A)

D. Information Assurance (IA)

Suggested Answer: *D*

Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. The C&A process is used extensively in the U.S. Federal Government. Some C&A processes include FISMA, NIACAP, DIACAP, and DCID 6/3. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. data and the systems and processes used for those purposes. While focused dominantly on information in digital form, the full range of IA encompasses not only digital but also analog or physical form. Information assurance as a field has grown from the practice of information security, which in turn grew out of practices and procedures of computer security. information security model, also called the CIA Triad, addresses three attributes of information and information systems, confidentiality, integrity, and availability. This C-I-A model is extremely useful for teaching introductory and basic concepts of information security and assurance; the initials are an easy mnemonic to The Five Pillars model is used in the practice of Information Assurance (IA) to define assurance requirements. It was promulgated by the U.S. Department of Defense (DoD) in a variety of publications, beginning with the National Information Assurance Glossary, Committee on National Security Systems Instruction CNSSI-4009. Here is the definition from that publication: "Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." The Five Pillars model is sometimes criticized because authentication and non-repudiation are not attributes of information or systems; rather, they are procedures or methods useful to assure the integrity and authenticity of information, and to protect the confidentiality of the same.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

Information Assurance (IA) refers to the process of protecting and managing information systems by ensuring their confidentiality, integrity, availability, authentication, and non-repudiation. In other words, it's a comprehensive approach to securing sensitive information by mitigating risks associated with technology infrastructure. The IA process involves identifying potential risks and vulnerabilities in an organization's IT environment; assessing the likelihood of those threats being exploited or causing damage; developing strategies to reduce or eliminate those risks through policies, procedures, tools and technologies; monitoring performance and effectiveness regularly; and responding quickly if breaches occur.

upvoted 1 times

Question #29 *Topic 2*

The Web resource collection is a security constraint element summarized in the Java Servlet Specification v2.4. Which of the following elements does it include?
Each correct answer represents a complete solution. Choose two.

A. HTTP methods

B. Role names

C. Transport guarantees

D. URL patterns

Suggested Answer: *B*
Web resource collection is a set of URL patterns and HTTP operations that define all resources required to be protected. It is a security constraint

Community vote distribution
BD (100%)

74gjd_37 Most Recent 1 year, 10 months ago
B. Role names D. URL patterns
upvoted 1 times

Question #30 *Topic 2*

Which of the following activities are performed by the 'Do' cycle component of PDCA (plan-do-check-act)? Each correct answer represents a complete solution.
Choose all that apply.

A. It detects and responds to incidents properly.

B. It determines controls and their objectives.

C. It manages resources that are required to achieve a goal.

D. It performs security awareness training.

E. It operates the selected controls.

Suggested Answer: *A, B*
The 'Do' cycle component performs the following activities: It operates the selected controls. It detects and responds to incidents properly. It performs component of PDCA.

Community vote distribution
AE (100%)

74gjd_37 Most Recent 1 year, 10 months ago
The correct options are: A. It detects and responds to incidents properly. E. It operates the selected controls. The 'Do' cycle component of PDCA involves performing the identified activities or implementing the chosen solutions. This includes operating the selected controls and detecting/responding to incidents that take place when those controls are in operation. Managing resources, determining control objectives, and performing security awareness training belong to other components in the PDCA cycle (Planning, Checking, and Acting).
upvoted 1 times

Question #31 *Topic 2*

Numerous information security standards promote good security practices and define frameworks or systems to structure the analysis and design for managing information security controls. Which of the following are the international information security standards? Each correct answer represents a complete solution.
Choose all that apply.

A. AU audit and accountability

B. Human resources security

C. Organization of information security

D. Risk assessment and treatment

Suggested Answer: *A*
Following are the various international information security standards: Risk assessment and treatment: Analysis of the organization's information security risks Security policy: Management direction Organization of information security: Governance of information security Asset management: Inventory and classification of information assets Human resources security: Security aspects for employees joining, moving, and leaving an organization Physical and environmental security: Protection of the computer facilities Communications and operations management: Management of technical security controls in systems and networks Access control: Restriction of access rights to networks, systems, applications, functions, and data Information systems acquisition, development and maintenance: Building security into applications Information security incident management: Anticipating and responding appropriately to information security breaches Business continuity management: Protecting, maintaining, and recovering business- audit and accountability is a U.S. Federal Government information security standard.

Community vote distribution

BCD (100%)

74gjd_37 Most Recent 1 year, 10 months ago

B. Human resources security C. Organization of information security D. Risk assessment and treatment

upvoted 1 times

Question #32 *Topic 2*

The Data and Analysis Center for Software (DACS) specifies three general principles for software assurance which work as a framework in order to categorize various secure design principles. Which of the following principles and practices does the General Principle 1 include? Each correct answer represents a complete solution. Choose two.

A. Principle of separation of privileges, duties, and roles

B. Assume environment data is not trustworthy

C. Simplify the design

D. Principle of least privilege

Suggested Answer: *B*

General Principle 1- Minimize the number of high-consequence targets includes the following principles and practices:

Community vote distribution

AD (100%)

74gjd_37 Most Recent 1 year, 10 months ago

Selected Answer: AD

The General Principle 1 includes the following principles and practices:

A. Principle of separation of privileges, duties, and roles

D. Principle of least privilege

So the correct answer is A and D.

upvoted 1 times

74gjd_37 1 year, 10 months ago

The General Principle 1 includes the following principles and practices: A. Principle of separation of privileges, duties, and roles D. Principle of least privilege So the correct answer is A and D.General Principle 1 of DACS emphasizes on ensuring the correct execution of software functions without being affected by security vulnerabilities. This principle generally includes three practices: The Principle of Least Privilege: A process or system should be given only the minimum access rights and permissions necessary to complete its designated task. Separation of Duties, Privileges, and Roles: A single user should not have authorization for all aspects of a system; rather different users with different roles and responsibilities must work together collaboratively in order to achieve the intended outcome. Assume Environment Data is Potentially Hostile: One cannot assume that input data from external sources will always be clean and accurate; hence all inputs must be validated before processing them in order to avoid potential threats coming from malicious attacks or errors, committed either intentionally by human beings or accidentally due to hardware issues etc.

upvoted 1 times

74gjd_37 1 year, 10 months ago

General Principle 1 of DACS emphasizes on ensuring the correct execution of software functions without being affected by security vulnerabilities. This principle generally includes three practices: The Principle of Least Privilege: A process or system should be given only the minimum access rights and permissions necessary to complete its designated task. Separation of Duties, Privileges, and Roles: A single user should not have authorization for all aspects of a system; rather different users with different roles and responsibilities must work together collaboratively in order to achieve the intended outcome. Assume Environment Data is Potentially Hostile: One cannot assume that input data from external sources will always be clean and accurate; hence all inputs must be validated before processing them in order to avoid potential threats coming from malicious attacks or errors, committed either intentionally by human beings or accidentally due to hardware issues etc.

upvoted 1 times

Question #33 *Topic 2*

SIMULATION -

Fill in the blank with the appropriate security mechanism. is a computer hardware mechanism or programming language construct which handles the occurrence of exceptional events.

Suggested Answer:

Exception handling is a computer hardware mechanism or programming language construct that handles the occurrence of events. These events occur during the software execution process and interrupt the instruction flow. Exception handling performs the specific activities for managing the exceptional events.

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

Question #34 *Topic 2*

In which of the following phases of the DITSCAP process does Security Test and Evaluation (ST&E) occur?

A. Phase 2

B. Phase 4

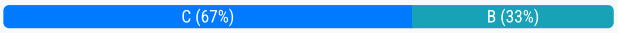
C. Phase 3

D. Phase 1

Suggested Answer: *C, A, D*

known as Definition Phase. The goal of this phase is to define the C&A level of effort, identify the main C&A roles and responsibilities, and create an agreement on the method for implementing the security requirements. The Phase 1 starts with the input of the mission need. This phase comprises three process activities: obtain a fully integrated system for certification testing and accreditation. This phase takes place between the signing of the initial version of the SSAA and the formal accreditation of the system. This phase verifies security requirements during system development. The process activities of this phase are as follows: DITSCAP C&A is known as Post Accreditation. This phase starts after the system has been accredited in the Phase 3. The goal of this phase is to continue to operate and manage the system and to ensure that it will maintain an acceptable level of residual risk. The process activities of this phase are as follows: System operations Security operations Maintenance of the SSAA Change management Compliance validation

Community vote distribution



DiPalma184 Most Recent 1 year, 11 months ago

In the DITSCAP (DoD Information Technology Security Certification and Accreditation Process), Phase 3 is known as the Validation Phase, where Security Test and Evaluation (ST&E) occurs. This phase involves verifying that the security controls are implemented correctly and operate as intended, and that they meet the security requirements. ST&E is a crucial activity to assess the effectiveness of the security controls in protecting the information system.

upvoted 2 times

74gjd_37 2 years, 10 months ago

Security Test and Evaluation (ST&E) occurs in Phase 4 of the DITSCAP process. So, the answer is B. DITSCAP stands for "DoD Information Technology Security Certification and Accreditation Process". It is a formal process used by the United States Department of Defense (DoD) to certify and accredit information systems before they are put into operation. The DITSCAP process provides a standard methodology for evaluating the security posture of DoD information systems, ensuring that appropriate security controls are implemented, tested, and validated before an authorization to operate (ATO) is granted.

upvoted 1 times

Question #35 *Topic 2*

Which of the following access control models uses a predefined set of access privileges for an object of a system?

A. Role-Based Access Control

B. Discretionary Access Control

C. Policy Access Control

D. Mandatory Access Control

Suggested Answer: *B, D, A, C*

Mandatory Access Control (MAC) is a model that uses a predefined set of access privileges for an object of the system. Access to an object is restricted on the basis of the sensitivity of the object and granted through authorization. Sensitivity of an object is defined by the label assigned to it. For example, if a user receives a copy of an object that is marked as "secret", he cannot grant permission to other users to see this object unless they have the appropriate incorrect. Role-based access control (RBAC) is an access control model. In this model, a user can access resources according to his role in the organization. For example, a backup administrator is responsible for taking backups of important data. Therefore, he is only authorized to access this data for backing it up. incorrect. There is no such access control model as Policy Access Control.

Community vote distribution

D (100%)

74gjd_37 1 year, 10 months ago

The answer is D. Mandatory Access Control uses a predefined set of access privileges for an object of a system, based on the security clearance level and need-to-know principle.The need-to-know principle is a security concept that states that a user should only have access to the information or resources they need to do their job, and not be given access to any additional resources or information beyond what is required for them to perform their duties. This helps limit the potential damage caused by unauthorized disclosure of sensitive information by controlling who has access to it. The principle applies in both physical and digital security contexts, and is often used in conjunction with other access control models such as mandatory or discretionary access control.The term "need-to-know" has been used in various contexts and organizations over the years, but its origins can be traced back to military and intelligence agencies. In these settings, access to sensitive information is restricted based on a person's security clearance level (which relates to their level of authorization) as well as their demonstrated need-to-know that information for their job duties. So the idea behind it comes from a historical context related to national security where only individuals with specialized knowledge, experience or authority were given access to certain types of classified information. The use of the term "need-to-know" likely arose naturally out of this principle-based practice -- a person should only have access when necessary in order for them carry out specific tasks successfully without endangering national interests. Today, the concept has become more widely applied in various industries beyond just government agencies and defense entities.The terms "need to know" and the principle of the "least privilege" the are related and often discussed together in access control discussions, but they have distinct origins and applications. The principle of least privilege inv

upvoted 1 times

74gjd_37 1 year, 10 months ago

Selected Answer: D

The answer is D. Mandatory Access Control uses a predefined set of access privileges for an object of a system, based on the security clearance level and need-to-know principle.

upvoted 1 times

74gjd_37 1 year, 10 months ago

The need-to-know principle is a security concept that states that a user should only have access to the information or resources they need to do their job, and not be given access to any additional resources or information beyond what is required for them to perform their duties. This helps limit the potential damage caused by unauthorized disclosure of sensitive information by controlling who has access to it. The principle applies in both physical and digital security contexts, and is often used in conjunction with other access control models such as mandatory or discretionary access control.

upvoted 1 times

74gjd_37 1 year, 10 months ago

The need-to-know principle is a security concept that states that a user should only have access to the information or resources they need to do their job, and not be given access to any additional resources or information beyond what is required for them to perform their duties. This helps limit the potential damage caused by unauthorized disclosure of sensitive information by controlling who has access to it. The principle applies in both

physical and digital security contexts, and is often used in conjunction with other access control models such as mandatory or discretionary access control.The term "need-to-know" has been used in various contexts and organizations over the years, but its origins can be traced back to military and intelligence agencies. In these settings, access to sensitive information is restricted based on a person's security clearance level (which relates to their level of authorization) as well as their demonstrated need-to-know that information for their job duties. So the idea behind it comes from a historical context related to national security where only individuals with specialized knowledge, experience or authority were given access to certain types of classified information. The use of the term "need-to-know" likely arose naturally out of this principle-based practice -- a person should only have access when necessary in order for them carry out specific tasks successfully without endangering national interests. Today, the concept has become more widely applied in various industries beyond just government agencies and defense entities.The terms "need to know" and the principle of the "least privilege" the are related and often discussed together in access control discussions, but they have distinct origins and applications. The principle of least privilege involves granting a user or process only those permissions necessary to perform its intended function, while minimizing additional privileges or access beyond what is required. Con

upvoted 1 times

74gjd_37 1 year, 10 months ago

The term "need-to-know" has been used in various contexts and organizations over the years, but its origins can be traced back to military and intelligence agencies. In these settings, access to sensitive information is restricted based on a person's security clearance level (which relates to their level of authorization) as well as their demonstrated need-to-know that information for their job duties. So the idea behind it comes from a historical context related to national security where only individuals with specialized knowledge, experience or authority were given access to certain types of classified information. The use of the term "need-to-know" likely arose naturally out of this principle-based practice -- a person should only have access when necessary in order for them carry out specific tasks successfully without endangering national interests. Today, the concept has become more widely applied in various industries beyond just government agencies and defense entities.The terms "need to know" and the principle of the "least privilege" the are related and often discussed together in access control discussions, but they have distinct origins and applications. The principle of least privilege involves granting a user or process only those permissions necessary to perform its intended function, while minimizing additional privileges or access beyond what is required. Conversely, the need-to-know principle refers to controlling who has access to confidential information based on their role and necessity for it in order to protect sensitive data from unauthorized disclosure. Both principles aim at reducing risk exposure by limiting unnecessary permissions/accesses within a specific system (such as an operating system) or with respect to information between multiple parties respectively. While they share some similarities in practice, their application has developed independently over time indicating a clear distinction between them when discussing cybersecurity

upvoted 1 times

74gjd_37 1 year, 10 months ago

The term "need-to-know" has been used in various contexts and organizations over the years, but its origins can be traced back to military and intelligence agencies. In these settings, access to sensitive information is restricted based on a person's security clearance level (which relates to their level of authorization) as well as their demonstrated need-to-know that information for their job duties.

So the idea behind it comes from a historical context related to national security where only individuals with specialized knowledge, experience or authority were given access to certain types of classified information. The use of the term "need-to-know" likely arose naturally out of this principle-based practice -- a person should only have access when necessary in order for them carry out specific tasks successfully without endangering national interests. Today, the concept has become more widely applied in various industries beyond just government agencies and defense entities.

upvoted 1 times

74gjd_37 Most Recent 1 year, 10 months ago

The terms "need to know" and the principle of the "least privilege" the are related and often discussed together in access control discussions, but they have distinct origins and applications. The principle of least privilege involves granting a user or process only those permissions necessary to perform its intended function, while minimizing additional privileges or access beyond what is required. Conversely, the need-to-know principle refers to controlling who has access to confidential information based on their role and necessity for it in order to protect sensitive data from unauthorized disclosure. Both principles aim at reducing risk exposure by limiting unnecessary permissions/accesses within a specific system (such as an operating system) or with respect to information between multiple parties respectively. While they share some similarities in practice, their application has developed independently over time indicating a clear distinction between them when discussing cybersecurity best practices and techniques aimed at enhancing confidentiality/privacy/security.

upvoted 1 times

Question #36 *Topic 2*

Martha works as a Project Leader for BlueWell Inc. She and her team have developed accounting software. The software was performing well. Recently, the software has been modified. The users of this software are now complaining about the software not working properly. Which of the following actions will she take to test the software?

A. Perform integration testing

B. Perform regression testing

C. Perform unit testing

D. Perform acceptance testing

Suggested Answer: *D*

Regression testing can be performed any time when a program needs to be modified either to add a feature or to fix an error. It is a process of repeating Unit testing and Integration testing whenever existing tests need to be performed again along with the new tests. Regression testing is performed to its implementation into the production environment. It is done either by a client or an application specialist to ensure that the software meets the requirement for more units are combined into a component. During integration testing, a developer combines two units that have already been tested into a component, and tests the interface between the two units. Although integration testing can be performed in various ways, the following three approaches are generally used: The top- application is tested separately. During unit testing, a developer takes the smallest unit of an application, isolates it from the rest of the application code, and tests it to determine whether it works as expected. Unit testing is performed before integrating these independent units into modules. The most common approach to unit testing requires drivers and stubs to be written. Drivers and stubs are programs. A driver simulates a calling unit, and a stub simulates a called unit.

Community vote distribution

B (100%)

74gjd_37 Most Recent 1 year, 10 months ago

B. Regression testing Regression testing is the process of retesting modified software to ensure that any previously working functionality has not been impacted by the changes made. This would allow her to identify and fix any issues associated with the recent modifications to the software. Additionally, performing integration testing and unit testing could also be helpful in identifying potential issues within specific components or interactions between different parts of the system. Finally, acceptance testing can validate whether or not the product meets user needs as opposed to strictly verifying code quality which would be covered under regressions, units or integrations tests.

upvoted 1 times

Question #37 *Topic 2*

Which of the following sections come under the ISO/IEC 27002 standard?

A. Security policy

B. Asset management

C. Financial assessment

D. Risk assessment

Suggested Answer: *C*

ISO/IEC 27002 is an information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC) as ISO/IEC 17799:2005. This standard contains the following twelve main sections: 1.Risk assessment: It refers to assessment of risk. 2.Security policy: It deals with the security management. 3.Organization of information security: It deals with governance of information security. 4.Asset management: It refers to inventory and classification of information assets. 5.Human resources security: It deals with security aspects for employees joining, moving and leaving an organization. 6.Physical and environmental security: It is related to protection of the computer facilities. 7.Communications and operations management: It is the management of technical security controls in systems and networks. 8.Access control: It deals with the restriction of access rights to networks, systems, applications, functions and data. 9.Information systems acquisition, development and maintenance: It refers to build security into applications. 10.Information security incident management: It refers to anticipate and respond appropriately to information security breaches. 11.Business continuity management: It deals with protecting, maintaining and recovering business-critical processes and systems. assessment does not come under the ISO/IEC 27002 standard.

Community vote distribution

ABD (100%)

74gjd_37 1 year, 10 months ago

The sections that come under the ISO/IEC 27002 standard ("Information security, cybersecurity and privacy protection. Information security controls") are: A. Security policy B. Asset management D. Risk assessment Financial assessment is not specifically addressed in ISO/IEC 27002, although it may be indirectly covered in certain controls related to budgeting and cost analysis for implementing security measures.ISO/IEC 27002 is a code of practice for information security management. It provides guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The standard covers various aspects of information security including the establishment of policies and procedures to protect organizational assets such as intellectual property, financial information,, employee data, customer data etc., managing access control systems, providing staff training programs on cyber-security awareness topics like phishing scams or malware attacks , carrying out regular risk assessments to identify potential risks associated with technological infrastructure and processes in place followed by taking corrective measures .Implementing ISO/IEC 27002 can help organizations safeguard their sensitive information from unauthorized alterations or disclosure thereby protecting their reputation and enhancing their competitive advantage. Additionally adhering to this standard may also aid legal compliance with regulations that mandate specific safeguards around handling customer data confidentiality e.g GDPR (General Data Protection Regulation) applicable within European Union countries dictates strict controls over collection processing storing transfer and destruction of personal identifiable Information(PII).

upvoted 1 times

74gjd_37 1 year, 10 months ago

Selected Answer: ABD

The sections that come under the ISO/IEC 27002 standard ("Information security, cybersecurity and privacy protection. Information security controls") are:

A. Security policy B. Asset management D. Risk assessment

Financial assessment is not specifically addressed in ISO/IEC 27002, although it may be indirectly covered in certain controls related to budgeting and cost analysis for implementing security measures.

upvoted 1 times

74gjd_37 Most Recent 1 year, 10 months ago

ISO/IEC 27002 is a code of practice for information security management. It provides guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The standard covers various aspects of information security

including the establishment of policies and procedures to protect organizational assets such as intellectual property, financial information,, employee data, customer data etc., managing access control systems, providing staff training programs on cyber-security awareness topics like phishing scams or malware attacks , carrying out regular risk assessments to identify potential risks associated with technological infrastructure and processes in place followed by taking corrective measures .Implementing ISO/IEC 27002 can help organizations safeguard their sensitive information from unauthorized alterations or disclosure thereby protecting their reputation and enhancing their competitive advantage. Additionally adhering to this standard may also aid legal compliance with regulations that mandate specific safeguards around handling customer data confidentiality e.g GDPR (General Data Protection Regulation) applicable within European Union countries dictates strict controls over collection processing storing transfer and destruction of personal identifiable Information(PII).

upvoted 1 times

74gjd_37 1 year, 10 months ago

ISO/IEC 27002 is a code of practice for information security management. It provides guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The standard covers various aspects of information security including the establishment of policies and procedures to protect organizational assets such as intellectual property, financial information,, employee data, customer data etc., managing access control systems, providing staff training programs on cyber-security awareness topics like phishing scams or malware attacks , carrying out regular risk assessments to identify potential risks associated with technological infrastructure and processes in place followed by taking corrective measures .

upvoted 1 times

74gjd_37 1 year, 10 months ago

Implementing ISO/IEC 27002 can help organizations safeguard their sensitive information from unauthorized alterations or disclosure thereby protecting their reputation and enhancing their competitive advantage. Additionally adhering to this standard may also aid legal compliance with regulations that mandate specific safeguards around handling customer data confidentiality e.g GDPR (General Data Protection Regulation) applicable within European Union countries dictates strict controls over collection processing storing transfer and destruction of personal identifiable Information(PII).

upvoted 1 times

Question #38 *Topic 2*

Which of the following statements about the authentication concept of information security management is true?

A. It establishes the users' identity and ensures that the users are who they say they are.

B. It ensures the reliable and timely access to resources.

C. It determines the actions and behaviors of a single individual within a system, and identifies that particular individual.

D. It ensures that modifications are not made to data by unauthorized personnel or processes.

Suggested Answer: *B*
individual within a system, and identifies that particular individual.

Community vote distribution
A (100%)

74gjd_37 Most Recent 1 year, 10 months ago

The correct answer is A. It establishes the users' identity and ensures that the users are who they say they are. Authentication, in the context of information security management, verifies a user's identity before granting access to resources or systems. This verification process helps ensure that only authorized individuals have access to sensitive information and systems. In contrast: Option B refers to availability Option C refers to accountability/auditability Option D refers to integrity

upvoted 1 times

Question #39 *Topic 2*

Billy is the project manager of the HAR Project and is in month six of the project. The project is scheduled to last for 18 months. Management asks Billy how often the project team is participating in risk reassessment in this project. What should Billy tell management if he's following the best practices for risk management?

A. Project risk management happens at every milestone.

B. Project risk management has been concluded with the project planning.

C. Project risk management is scheduled for every month in the 18-month project.

D. At every status meeting the project team project risk management is an agenda item.

Suggested Answer: *A*

Official Answer: Risk management is an ongoing project activity. It should be an agenda item at every project status meeting. Answer: A is incorrect. Milestones are good times to

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

Option D, "At every status meeting, the project team risk management is an agenda item," would be the most appropriate answer if Billy is following best practices for risk management. Regular and frequent reassessment of risks is indeed critical to identifying new or changing risks as soon as possible, which allows teams to mitigate those risks effectively before they become major issues that threaten to derail a project. Therefore, discussing risks at each status meeting ensures that all potential challenges are identified and addressed promptly throughout the entirety of the 18-month HAR Project.

upvoted 1 times

Question #40 *Topic 2*

You work as a security manager for BlueWell Inc. You are going through the NIST SP 800-37 C&A methodology, which is based on four well defined phases. In which of the following phases of NIST SP 800-37 C&A methodology does the security categorization occur?

A. Security Accreditation

B. Security Certification

C. Continuous Monitoring

D. Initiation

Suggested Answer: *D*

The various phases of NIST SP 800-37 C&A are as follows: Phase 1: Initiation- This phase includes preparation, notification and resource identification. It performs the security plan analysis, update, and acceptance. Phase 2: Security Certification- The Security certification phase evaluates the controls and documentation. Phase 3: Security Accreditation- The security accreditation phase examines the residual risk for acceptability, and prepares the final security accreditation package. Phase 4: Continuous Monitoring-This phase monitors the configuration management and control, ongoing security control verification, and status reporting and documentation.

Community vote distribution



74gjd_37 Most Recent 1 year, 10 months ago

The answer is D. Initiation. The security categorization occurs in the initiation phase of NIST SP 800-37 C&A methodology. During this phase, an organization identifies its information system and assigns each system a security category based on the potential impact resulting from the loss of confidentiality, integrity, or availability of information processed, stored, or transmitted by that system.

upvoted 1 times