DUMPSBOSS.

Certified Authorization Professional

ISC2 CAP

Version Demo

Total Demo Questions: 39

Total Premium Questions: 399

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Information Security Risk Management Program	165
Topic 2, Scope of the Information System	19
Topic 3, Selection and Approval of Security and Privacy Controls	28
Topic 4, Implementation of Security and Privacy Controls	38
Topic 5, Assessment/Audit of Security and Privacy Controls	51
Topic 6, Authorization/Approval of Information System	30
Topic 7, Continuous Monitoring	16
Topic 8, Mix Questions	52
Total	399

QUESTION NO: 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. Registration

B. Document mission need

C. Negotiation

D. Initial Certification Analysis

ANSWER: A B C

Explanation:

DITSCAP's Definition Phase establishes the basis on which the system will be assessed and accredited. **Registration** initiates the C&A effort by identifying the system and bringing the responsible stakeholders into the process. This provides the administrative starting point for assigning C&A ownership and scoping the effort.

Document mission need captures the system's operational purpose, the mission it supports, and the consequences of inadequate security. That mission context is essential for determining the appropriate assurance expectations and for ensuring that security requirements are tied to operational risk rather than treated as a purely technical exercise.

Negotiation is also a Definition Phase activity because the principal C&A participants must reach agreement on the security approach, responsibilities, level of effort, and evidence needed for the accreditation decision. This agreement was historically captured through the System Security Authorization Agreement process. DITSCAP was later superseded in DoD practice by the Risk Management Framework, but its emphasis on early system characterization, stakeholder roles, risk-informed requirements, and documented authorization planning remains consistent with modern guidance. See NIST SP 800-37 Rev. 2 and DoD Instruction 8510.01.

QUESTION NO: 2 - (SIMULATION)

SIMULATION

Fill in the blank with an appropriate word.

_____ ensures that the information is not disclosed to unauthorized persons or processes.

ANSWER: See the explanation for the answer

Explanation:

Answer: Confidentiality

Confidentiality ensures that information is not disclosed to unauthorized persons, entities, or processes. It is one of the core objectives of the CIA triad: confidentiality, integrity, and availability.

QUESTION NO: 3

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. IATO

B. ATO

C. IATT

D. ATT

E. DATO

ANSWER: A B C E

Explanation:

In the legacy Department of Defense certification-and-accreditation terminology used by this question, the Designated Approving Authority makes the risk-based accreditation decision after considering the certification results and the IAM/CA's recommendation. An **ATO** authorizes the system to operate when the DAA accepts the residual risk. An **IATO** provides a time-limited authorization while specified deficiencies, controls, or documentation are completed. A **DATO** is the DAA's formal determination that the system is not authorized to operate because the residual risk is unacceptable. An **IATT** is a limited, interim authorization from the DAA that permits testing in an operational environment when such testing is needed before a full operational authorization can be decided.

These determinations reflect the DAA's accountability for accepting, deferring, or rejecting operational risk, rather than the IAM/CA's responsibility to perform or coordinate certification activities. The terminology is associated with the former DoD DIACAP process. Current DoD risk-management practice uses RMF and the term Authorizing Official, but understanding the historical DAA decision terms remains relevant for legacy CAP material. See DoD Instruction 8510.01 and NIST SP 800-37 Rev. 1.

QUESTION NO: 4

Beth is the project manager of the BFG Project for her company. In this project Beth has decided to create a contingency response based on the performance of the project schedule. If the project schedule variance is greater than $10,000 the contingency plan will be implemented. What is the formula for the schedule variance?

A. SV=EV-PV

B. SV=EV/AC

C. SV=PV-EV

D. SV=EV/PV

ANSWER: A

Explanation:

The correct formula is **SV = EV − PV**, where schedule variance (SV) is calculated by subtracting planned value (PV) from earned value (EV). This is the standard earned value management calculation used to express schedule performance in monetary units, such as dollars. Earned value represents the budgeted value of work actually completed by the reporting date, while planned value represents the budgeted value of work that was scheduled to be completed by that date. Comparing these values shows whether the project has accomplished more or less work than planned.

Because the contingency threshold in the question is stated as **$10,000**, a variance formula that produces a currency amount is required. The SV calculation does this directly. A positive schedule variance means the budgeted value of completed work exceeds the budgeted value of planned work, indicating favorable schedule performance; a negative result indicates that less work has been completed than was planned. This measure supports objective schedule-performance monitoring and can be used to trigger predefined contingency actions. See the Project Management Institute's overview of earned value management and the U.S. Department of Energy's Earned Value Management System guidance.

QUESTION NO: 5

You work as a project manager for BlueWell Inc. There has been a delay in your project work that is adversely affecting the project schedule. You decided, with your stakeholders' approval, to fast track the project work to get the project done faster. When you fast track the project which of the following are likely to increase?

A. Quality control concerns

B. Costs

C. Risks

D. Human resource needs

ANSWER: C

Explanation:

Risks is correct because fast tracking is a schedule-compression technique that shortens the project duration by performing activities or phases in parallel that were originally planned to occur in sequence. Starting successor work before all predecessor work and deliverables are fully complete introduces greater uncertainty into execution. For example, a downstream team may proceed using assumptions or preliminary outputs that later change, creating the possibility of rework, integration issues, defects, coordination problems, or unmet dependencies. These are project risks because they are uncertain events or conditions that could affect objectives such as scope, schedule, cost, and quality.

Fast tracking is therefore appropriate only when the project team and stakeholders understand and accept the added exposure, and when the team actively identifies, analyzes, assigns, monitors, and responds to the resulting risks. The project manager should document the schedule-compression decision, update the risk register, clarify handoffs and decision points, and closely manage changes as concurrent work proceeds. PMI describes fast tracking as performing activities or phases in parallel that would normally be done in sequence, and notes that this approach can increase risk and cause rework. See the PMI discussion of fast tracking and schedule compression and the PMBOK Guide resources.

QUESTION NO: 6

Determine the primary defense against a SQL injection vulnerability

A. Using a Web Application Firewall (WAF)

B. Prepared Statements with Parameterized Queries

C. Use of NoSQL Database

D. Blacklisting Single Quote Character (‘)

ANSWER: B

Explanation:

Prepared Statements with Parameterized Queries are the primary defense against SQL injection because they maintain a strict separation between the SQL command structure and untrusted input. The application first defines the intended query using parameter placeholders, then supplies user-provided values separately through the database driver or API. As a result, the database interprets those values solely as data, rather than as SQL syntax that can change the query’s logic or execute additional commands. This directly addresses the underlying condition that enables SQL injection: constructing dynamic SQL statements by concatenating untrusted input into executable query text.

This control should be applied consistently wherever untrusted data is used in database operations, including search fields, identifiers where supported by an appropriate allow-listing design, form submissions, API parameters, and background-job inputs. Parameterization is a secure coding control rather than a compensating perimeter measure, making it the preferred foundational safeguard in an authorization-oriented risk assessment. OWASP identifies parameterized queries as its primary SQL-injection prevention technique, and the OWASP Application Security Verification Standard requires applications to use parameterized queries or other safe query interfaces for database access. See the OWASP SQL Injection Prevention Cheat Sheet and OWASP Application Security Verification Standard.

QUESTION NO: 7

Which of the following is used throughout the entire C&A process?

A. DAA

B. DITSCAP

C. SSAA

D. DIACAP

ANSWER: C

Explanation:

SSAA is correct because the System Security Authorization Agreement is the central, living agreement used across the legacy DoD Certification and Accreditation process. It records the system's security requirements, agreed protection level, planned safeguards, residual risks, roles, responsibilities, milestones, and the authorization decision context. As certification activities produce evidence and identify findings, the SSAA is maintained to reflect the current security posture and the commitments of the system owner, certifier, and approving authority. It therefore provides continuity from initial definition and negotiation of security requirements through assessment, risk acceptance, authorization, and subsequent management of the system's security posture.

This terminology comes from the legacy DITSCAP-era C&A model. Modern RMF practice has replaced the SSAA with a broader set of authorization-package artifacts and ongoing authorization activities, but CAP questions using traditional C&A vocabulary commonly test the SSAA's role as the agreement maintained throughout that process. NIST's glossary identifies the System Security Authorization Agreement as a defined security-authorization term; see the NIST CSRC SSAA glossary entry. For the modern risk-management context that succeeded traditional C&A, see NIST SP 800-37 Rev. 2.

QUESTION NO: 8

Which of the following NIST documents provides a guideline for identifying an information system as a National Security System?

A. NIST SP 800-53

B. NIST SP 800-59

C. NIST SP 800-53A

D. NIST SP 800-37

E. NIST SP 800-60

ANSWER: B

Explanation:

NIST SP 800-59 is correct because it is specifically titled *Guideline for Identifying an Information System as a National Security System*. It was issued to help federal agencies determine whether an information system meets the statutory definition of a national security system under the Federal Information Security Management Act framework. The publication addresses the required decision process and the criteria that distinguish systems used for intelligence activities, cryptologic activities, military command and control, weapons-system functions, or other activities that are critical to fulfilling military or intelligence missions. Correctly making this determination is important because national security systems have distinct oversight and security requirements from other federal information systems. The guidance also emphasizes that the designation must be based on the system's function and use, rather than simply on the organization operating it or the sensitivity of information in isolation. NIST's publication record identifies SP 800-59 as the authoritative guideline for this purpose, and its full text provides the definitions and identification methodology used in the determination. See the NIST SP 800-59 publication page and the full SP 800-59 document.

QUESTION NO: 9

Which HTTP header is used by the CORS (Cross-origin resource sharing) standard to control access to resources on a server?

A. Access-Control-Request-Method

B. Access-Control-Request-Headers

C. Access-Control-Allow-Headers

D. None of the above

E. Access-Control-Allow-Origin

ANSWER: E

Explanation:

Access-Control-Allow-Origin is the CORS response header that controls whether a browser may expose a server's resource to a requesting origin. The server includes it in its HTTP response and assigns either a specific allowed origin, such as `https://example.com`, or, where appropriate for public non-credentialed resources, the wildcard value `*`. The browser compares the requesting page's `Origin` with this response value when enforcing the same-origin policy. If the origin is permitted, the browser allows the calling script to read the cross-origin response; otherwise, it blocks that script-level access.

This header is therefore the central CORS mechanism for authorizing cross-origin access to a resource. CORS can also use additional response headers to authorize particular methods, request headers, credentials, or response headers, especially following a preflight request. Those controls supplement origin authorization rather than replacing it. In particular, resource access under CORS starts with the server declaring which origin is allowed through **Access-Control-Allow-Origin**. MDN's CORS guide describes this header as the response mechanism used to identify the origins permitted to access a resource, and the Fetch Standard defines its processing as part of the CORS protocol. See MDN: Access-Control-Allow-Origin and WHATWG Fetch Standard: CORS protocol.

QUESTION NO: 10

Which of the following tasks are identified by the Plan of Action and Milestones document? Each correct answer represents a complete solution. Choose all that apply.

A. The plans that need to be implemented

B. The resources needed to accomplish the elements of the plan

C. Any milestones that are needed in meeting the tasks

D. The tasks that are required to be accomplished

E. Scheduled completion dates for the milestones

ANSWER: B C D E

Explanation:

A Plan of Action and Milestones (POA&M) is the formal management document used to track and remediate identified security and privacy weaknesses. It turns remediation into an accountable, measurable effort by documenting the tasks that must be completed to address a weakness, the resources required to carry out those tasks, and the intermediate milestones used to measure progress. It also records scheduled completion dates for milestones, allowing authorizing officials and system owners to monitor whether corrective actions are progressing on time and to make risk-based decisions when schedules or resources change.

Accordingly, "The resources needed to accomplish the elements of the plan," "Any milestones that are needed in meeting the tasks," "The tasks that are required to be accomplished," and "Scheduled completion dates for the milestones" are all core POA&M content. NIST describes a POA&M as identifying the tasks, resources, milestones, and scheduled completion dates needed to correct weaknesses. This structured information supports ongoing remediation tracking within the system authorization and continuous monitoring process. See NIST's POA&M glossary definition and NIST SP 800-53A Rev. 5.

QUESTION NO: 11

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

B. Project risk management happens at every milestone.

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

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

ANSWER: A

Explanation:

At every status meeting the project team project risk management is an agenda item. Risk reassessment is not a one-time planning activity; it is a continuing project-management discipline. Discussing risk management during each status meeting gives the team a regular, practical control point to review whether previously identified risks have changed in probability, impact, urgency, or ownership. It also supports identifying newly emerging risks, retiring risks that are no longer relevant, checking the effectiveness of response actions, and escalating material changes to the appropriate stakeholders.

For an 18-month project, conditions such as scope decisions, schedule performance, resource availability, technical results, supplier performance, and organizational priorities can change frequently. Making risk management a standing status-meeting agenda item ensures that those changes are considered promptly and that the risk register and response actions remain current throughout project execution. This approach reflects the principle that risk management is integrated into normal project monitoring and decision-making, rather than performed only at isolated points in the lifecycle. PMI describes risk management as a structured, ongoing process across project work; see PMI's Standard for Risk Management in Portfolios, Programs, and Projects and its project risk management guidance.

QUESTION NO: 12

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

A. Certification and Accreditation (C&A)

B. Information Assurance (IA)

C. Five Pillars model

D. Classic information security model

ANSWER: A

Explanation:

Certification and Accreditation (C&A) is the correct answer because it is a structured, risk-based process historically used to implement, assess, authorize, and maintain information security for information systems. Under C&A, a system's security controls are documented and evaluated to determine whether they are implemented correctly, operating as intended, and sufficient for the system's risk environment. The resulting assessment supports an authorizing official's decision to accept the residual risk and authorize the system to operate, or to require additional remediation.

In current U.S. federal guidance, this lifecycle has been incorporated and modernized within the Risk Management Framework (RMF). RMF retains the essential concepts of security control implementation, security-control assessment, risk determination, authorization, and continuous monitoring. Thus, C&A directly describes a process used to put information-security requirements and controls into operation and obtain formal management authorization based on assessed risk. NIST describes the RMF authorization lifecycle in NIST Special Publication 800-37 Rev. 2, while the control-assessment activities that support certification are detailed in NIST Special Publication 800-53A Rev. 5.

QUESTION NO: 13

You are preparing to start the qualitative risk analysis process for your project. You will be relying on some organizational process assets to influence the process. Which one of the following is NOT a probable reason for relying on organizational process assets as an input for qualitative risk analysis?

A. Information on prior, similar projects

B. Review of vendor contracts to examine risks in past projects

C. Risk databases that may be available from industry sources

D. Studies of similar projects by risk specialists

ANSWER: B

Explanation:

Review of vendor contracts to examine risks in past projects is correct because vendor contracts are generally project procurement documents or contractual records, rather than a standard organizational process asset used as an input to qualitative risk analysis. Qualitative risk analysis uses established organizational knowledge to assess each identified risk's probability and impact and to prioritize risks for further action. Organizational process assets support that work when they provide reusable historical knowledge, such as prior-project risk information, lessons learned, risk-category structures, and organizational risk databases. A contract may contain terms that create or allocate risks for the current procurement, and it may be reviewed during procurement or contract-risk activities. However, merely reviewing vendor contracts from past projects is not the expected organizational process asset input identified for the qualitative risk analysis process. The distinction is important: the process draws on institutional risk knowledge that can improve consistency in probability and impact assessments, rather than treating individual historical contracts as a defined source of risk-analysis methodology or risk data. PMI describes project risk management as including the processes for conducting risk management planning, identification, analysis, response planning, response implementation, and monitoring; see PMI's risk management practice standard overview and the PMBOK Guide and standards resources.

QUESTION NO: 14

The Software Configuration Management (SCM) process 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. What are the procedures that must be defined for each software project to ensure that a sound SCM process is implemented?

Each correct answer represents a complete solution. Choose all that apply.

A. Configuration status accounting

B. Configuration change control

C. Configuration deployment

D. Configuration audits

E. Configuration identification

F. Configuration implementation

ANSWER: A B D E

Explanation:

A sound Software Configuration Management process defines the core control activities needed to establish trusted software baselines, evaluate and authorize changes, retain an accurate record of configuration information, and independently verify the released product. **Configuration identification** establishes the configuration items, naming conventions, versioning approach, and baselines that must be controlled. This creates the defined reference point from which changes can be traced.

Configuration change control provides the documented process for submitting, evaluating, approving, implementing, and tracking proposed changes to controlled items. It ensures that planned enhancements are incorporated deliberately and under authorization. **Configuration status accounting** records and reports the current and historical state of configuration items, change requests, versions, and baselines, providing the evidence needed to determine what is included in a release.

Configuration audits verify that the delivered software and its associated records conform to approved requirements, change authorizations, and the stated baseline. Together, these procedures support traceability and release verification. NIST describes configuration management as a process for establishing and maintaining the integrity of systems through control of configuration items and changes; see the NIST Configuration Management glossary entry and NIST SP 800-128.

QUESTION NO: 15

In which of the following DIACAP phases is residual risk analyzed?

A. Phase 2

B. Phase 4

C. Phase 5

D. Phase 3

E. Phase 1

ANSWER: B

Explanation:

Phase 4 is correct because this is the DIACAP accreditation-decision stage, where the Designated Approving Authority considers the certification evidence, the system's security posture, any unresolved weaknesses, and the resulting residual risk. Residual risk is the risk remaining after the prescribed information-assurance controls have been implemented and assessed. The decision authority uses that analysis to determine whether the risk is acceptable for the system's mission and whether to grant an authorization, grant an authorization with conditions, or deny authorization. This makes residual-risk analysis central to the accreditation decision rather than merely a technical control-validation activity.

DIACAP was the Department of Defense authorization framework preceding the broader transition to the Risk Management Framework. Its accreditation decision reflected the accountable senior official's explicit acceptance, rejection, or conditional acceptance of the remaining risk to DoD operations, assets, and information. The same risk-based authorization principle is retained in current RMF guidance: an authorizing official makes a risk-based decision based on the security assessment results and plan of action and milestones. See DoDI 8510.01, Risk Management Framework for DoD Systems and NIST SP 800-37 Rev. 2.

QUESTION NO: 16

Which of the following activities are performed by a Security Control Assessor during an RMF assessment?

Each correct answer represents a complete solution. Choose all that apply.

A. Examine control documentation and implementation evidence

B. Interview personnel responsible for control implementation

C. Test controls using approved assessment procedures

D. Accept residual risk for system operation

E. Document assessment results in an assessment report

ANSWER: A B C E

Explanation:

A Security Control Assessor determines the extent to which security and privacy controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security and privacy requirements. The assessor develops or applies assessment procedures, examines evidence, interviews personnel, and tests implemented controls. These activities provide the factual basis for determining control effectiveness.

The assessor documents the results of those activities in a security and privacy assessment report, including findings, weaknesses, and recommendations where applicable. The assessor does not accept system risk or approve operation; those are Authorizing Official responsibilities. Likewise, remediation planning is normally coordinated by the system owner and other responsible officials. See NIST SP 800-53A Rev. 5 and NIST SP 800-37 Rev. 2.

QUESTION NO: 17

Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in. What are the different categories of penetration testing?

Each correct answer represents a complete solution. Choose all that apply.

A. Full-box

B. Zero-knowledge test

C. Full-knowledge test

D. Open-box

E. Partial-knowledge test

F. Closed-box

ANSWER: B C D E F

Explanation:

Penetration-test categories commonly describe the amount of prior knowledge, access, and documentation provided to the testers. A **Zero-knowledge test** begins with no meaningful internal information about the target and models an external attacker's perspective. This approach is also commonly called a **Closed-box** test: the testers must perform reconnaissance and discovery before attempting exploitation. At the other end, a **Full-knowledge test** provides extensive information, such as architecture details, credentials, source material, or network diagrams. This is also known as an **Open-box** test, because the assessment team is given substantial visibility into the environment. A **Partial-knowledge test** supplies limited information or access, simulating an attacker or insider who has obtained some initial knowledge but not complete visibility. It is often described as a gray-box assessment. These terms identify valid test categories or established synonymous labels based on tester knowledge, and organizations select among them according to the threat scenario, assessment objectives, time available, and authorized scope. OWASP describes black-box, gray-box, and white-box testing perspectives in its Web Security Testing Guide. NIST also provides guidance for planning and conducting authorized technical assessments in SP 800-115, Technical Guide to Information Security Testing and Assessment.

QUESTION NO: 18

Salt is a cryptographically secure random string that is added to a password before it is hashed. In this context, what is the primary objective of salting?

A. To defend against dictionary attacks or attacks against hashed passwords using a rainbow table.

B. To slow down the hash calculation process.

C. To generate a long password hash that is difficult to crack.

D. To add a secret message to the password hash.

ANSWER: A

Explanation:

To defend against dictionary attacks or attacks against hashed passwords using a rainbow table is correct because a unique, cryptographically random salt changes the hash input for every password record. Consequently, two accounts using the same password will have different stored hash values. An attacker therefore cannot efficiently use one precomputed collection of password hashes, such as a rainbow table, against all users or reuse cracking work across identically hashed passwords. Instead, the attacker must incorporate the specific salt associated with each stored credential and perform guesses separately for that record. This makes large-scale offline password-hash attacks substantially less efficient and prevents direct comparison of a candidate password's unsalted hash with the database value. Salts must be unique per password and may be stored alongside the resulting password hash; their protection comes from uniqueness and unpredictability rather than secrecy. Effective password storage also combines salting with a deliberately slow, memory-hard password-hashing function, but the salt's primary function is defeating precomputation and reducing reusable dictionary-guessing work. See NIST SP 800-63B and the OWASP Password Storage Cheat Sheet.

QUESTION NO: 19

Which is the most effective way of input validation to prevent Cross-Site Scripting attacks?

A. Blacklisting HTML and other harmful characters

B. Whitelisting and allowing only trusted input

C. Using a Web Application Firewall (WAF)

D. Marking Cookie as HttpOnly

ANSWER: B

Explanation:

Whitelisting and allowing only trusted input is the most effective input-validation approach because it defines the narrow set of characters, formats, lengths, and values that an application legitimately expects, then rejects anything outside that specification. For example, a field intended to contain an account number can be limited to a defined length and numeric characters, while an enumerated field can accept only values from a fixed list. This positive, allow-list model is more dependable for handling untrusted input because it validates against the application's actual business requirements rather than attempting to anticipate every potentially malicious payload or encoding variation.

For XSS defense, validation should occur as close as possible to the point where data enters the application and should be implemented server-side. The validation rule must be appropriate to the field's intended purpose; free-form text may require more flexible validation than identifiers or numeric fields. Input validation is an important layer of defense, and it should be paired with context-aware output encoding when data is rendered in HTML, attributes, JavaScript, URLs, or CSS. OWASP identifies allow-list validation as the preferred validation strategy and describes output encoding as a primary XSS control: OWASP Input Validation Cheat Sheet and OWASP Cross Site Scripting Prevention Cheat Sheet.

QUESTION NO: 20

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 provides advice on the impacts of system changes.

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

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

D. An ISSO takes part in the development activities that are required to implement system changes.

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

ANSWER: A C E

Explanation:

The correct statements align with the distinct operational and engineering responsibilities assigned to the Information System Security Officer and Information System Security Engineer in the NIST RMF role definitions. “An ISSO manages the security of the information system that is slated for Certification & Accreditation (C&A).” is correct because the ISSO supports the authorizing official and system owner by managing day-to-day system security responsibilities, including maintaining the security posture and supporting authorization activities. Although current NIST publications use the term authorization rather than C&A, the underlying responsibility remains applicable.

“An ISSE provides advice on the impacts of system changes.” is correct because the ISSE supplies system-security engineering expertise throughout the system life cycle. This includes advising stakeholders about how proposed changes affect security requirements, architecture, controls, and risk.

“An ISSE provides advice on the continuous monitoring of the information system.” is also correct. Continuous monitoring depends on technically informed decisions about control assessment, configuration changes, vulnerabilities, and risk posture; the ISSE is an appropriate advisor for those engineering aspects. NIST describes these role responsibilities in its RMF guidance and explains how ongoing monitoring supports maintaining authorization decisions. See NIST SP 800-37 Rev. 1 and NIST SP 800-37 Rev. 2.

QUESTION NO: 21

You are the project manager of the NKJ Project for your company. The project's success or failure will have a significant impact on your organization's profitability for the coming year. Management has asked you to identify the risk events and communicate the event's probability and impact as early as possible in the project. Management wants to avoid risk events and needs to analyze the cost-benefits of each risk event in this project. What term is assigned to the low-level of stakeholder tolerance in this project?

A. Risk avoidance

B. Mitigation-ready project management

C. Risk utility function

D. Risk-reward mentality

ANSWER: C

Explanation:

Risk utility function is correct because it is the decision-analysis concept used to express how a stakeholder values potential outcomes when uncertainty is present. It translates the stakeholder’s risk attitude and tolerance into a relationship between a possible gain or loss and the utility, or perceived value, assigned to that outcome. Where management has a low tolerance for uncertainty and adverse outcomes could materially affect organizational profitability, the utility function reflects a risk-averse preference: avoiding a loss or reducing exposure has comparatively high value, even when doing so requires spending resources on controls or response actions.

Using a risk utility function supports the requested cost-benefit analysis by making stakeholder preferences explicit rather than relying solely on probability and impact scores. The project manager can use this information to prioritize risk responses and present decisions in terms that align with management’s tolerance for uncertainty. PMI recognizes risk appetite and risk tolerance as inputs that shape risk-management decisions; utility theory provides a structured means of representing those preferences in uncertain choices. See PMI’s Project Management Lexicon and the Standard for Risk Management in Portfolios, Programs, and Projects.

QUESTION NO: 22

The Chief Information Officer (CIO), or Information Technology (IT) director, is a job title commonly given to the most senior executive in an enterprise. What are the responsibilities of a Chief Information Officer?

Each correct answer represents a complete solution. Choose all that apply.

A. Preserving high-level communications and working group relationships in an organization

B. Facilitating the sharing of security risk-related information among authorizing officials

C. Establishing effective continuous monitoring program for the organization

D. Proposing the information technology needed by an enterprise to achieve its goals and then working within a budget to implement the plan

ANSWER: A C D

Explanation:

A CIO provides enterprise-level leadership for the planning, acquisition, operation, and governance of information technology. “Proposing the information technology needed by an enterprise to achieve its goals and then working within a budget to implement the plan” reflects the CIO’s core strategic and capital-planning role: aligning technology capabilities and investments with mission and business objectives. The CIO also needs to preserve high-level communications and working group relationships in an organization, because effective IT governance requires sustained coordination among executive leadership, business stakeholders, security leaders, and operational teams.

“Establishing effective continuous monitoring program for the organization” is also a CIO responsibility in the federal risk-management context. An organization-wide continuous-monitoring program supplies leadership with current information about security-control effectiveness, vulnerabilities, threats, and risk, supporting timely risk-based decisions and authorization activities. NIST describes continuous monitoring as a program-level capability that should be established and maintained across the organization, rather than as an isolated technical activity. These responsibilities collectively support accountable, mission-aligned IT management and informed organizational risk decisions. See NIST SP 800-37 Rev. 2 and NIST SP 800-137.

QUESTION NO: 23

Sam is the project manager of a construction project in south Florida. This area of the United

States is prone to hurricanes during certain parts of the year. As part of the project plan Sam and the project team acknowledge the possibility of hurricanes and the damage the hurricane could have on the project's deliverables, the schedule of the project, and the overall cost of the project. Once Sam and the project stakeholders acknowledge the risk of the hurricane they go on planning the project as if the risk is not likely to happen. What type of risk response is Sam using?

A. Mitigation

B. Avoidance

C. Passive acceptance

D. Active acceptance

ANSWER: C

Explanation:

Passive acceptance is correct because Sam and the stakeholders have identified and acknowledged that hurricanes are a credible threat to project deliverables, schedule, and cost, but they take no planned action to alter the likelihood or impact of that threat. They continue planning without defining a contingency response, setting aside reserves, relocating work, changing the schedule, or otherwise preparing specifically for a hurricane event. This reflects acceptance of the residual exposure with no proactive management activity beyond recognizing that the risk exists.

In risk management, acceptance is an appropriate response when a risk is consciously tolerated rather than eliminated or reduced. Passive acceptance is distinguished by the absence of a documented contingency plan or other advance action; the project team will address the consequences only if the event occurs. Risk-response decisions should be based on risk context, organizational risk tolerance, and the practical feasibility of treatment measures. This treatment-oriented approach is consistent with NIST’s guidance that organizations select and implement responses for identified risks as part of an ongoing risk-management process. See NIST SP 800-37 Rev. 2 and the ISC2 CAP Exam Outline.

QUESTION NO: 24

The phase 3 of the Risk Management Framework (RMF) process is known as mitigation planning.

Which of the following processes take place in phase 3?

Each correct answer represents a complete solution. Choose all that apply.

A. Identify threats, vulnerabilities, and controls that will be evaluated.

B. Document and implement a mitigation plan.

C. Agree on a strategy to mitigate risks.

D. Evaluate mitigation progress and plan next assessment.

ANSWER: B C D

Explanation:

Mitigation planning translates assessed risk into accountable, actionable risk-response work. “Agree on a strategy to mitigate risks” is correct because the organization must decide how each risk will be handled, such as by implementing controls, accepting the risk within approved tolerance, avoiding the activity, or transferring elements of the risk. The selected approach establishes priorities, ownership, resources, and expected outcomes.

“Document and implement a mitigation plan” is also correct because risk treatment must be recorded in a plan that identifies the actions, responsible parties, milestones, required resources, and control or remediation activities. Implementation turns the agreed strategy into operational change and provides evidence for authorization and governance decisions.

“Evaluate mitigation progress and plan next assessment” is correct because mitigation is not a one-time event. Risk owners and system stakeholders need to track whether planned actions are completed, determine whether residual risk is acceptable, and schedule reassessment when conditions, threats, vulnerabilities, or system changes warrant it. This feedback loop supports continuous risk management and maintains visibility into the effectiveness of risk responses. NIST describes risk response and ongoing monitoring as essential components of organization-wide risk management in NIST SP 800-39; continuous monitoring concepts are further addressed in NIST SP 800-137.

QUESTION NO: 25

Which of the following actions support the Monitor step of the RMF?

Each correct answer represents a complete solution. Choose all that apply.

A. Monitoring the effectiveness of implemented controls

B. Assessing the security impact of system and environmental changes

C. Updating authorization information to reflect significant findings and changes

D. Reporting risk status to appropriate organizational officials

E. Eliminating assessment activities after initial authorization

ANSWER: A B C D

Explanation:

The Monitor step maintains ongoing awareness of the security and privacy posture of an information system and its operating environment. Organizations monitor control effectiveness, assess the impact of system and environmental changes, conduct ongoing risk assessments, and report relevant risk information to appropriate officials. These activities provide current evidence for maintaining an authorization decision.

Monitoring also includes updating authorization-related documentation when changes, assessment results, vulnerabilities, or remediation activities affect the system’s risk posture. The objective is not to repeat the full initial authorization process on a

fixed schedule regardless of circumstances; instead, the organization uses ongoing information to determine when additional assessment or reauthorization is necessary. See NIST SP 800-37 Rev. 2 and NIST SP 800-137.

QUESTION NO: 26

What NIACAP certification levels are recommended by the certifier?

Each correct answer represents a complete solution. Choose all that apply.

A. Minimum Analysis

B. Basic System Review

C. Detailed Analysis

D. Maximum Analysis

E. Comprehensive Analysis

F. Basic Security Review

ANSWER: A C E F

Explanation:

The NIACAP certification levels recommended by the certifier are *Basic Security Review*, *Minimum Analysis*, *Detailed Analysis*, and *Comprehensive Analysis*. NIACAP—the National Information Assurance Certification and Accreditation Process—used these levels to tailor the depth and rigor of certification activity to the system's security needs, mission importance, operational environment, and assessed risk. A Basic Security Review provides the least intensive certification approach, while Minimum Analysis and Detailed Analysis apply progressively greater examination of security controls, documentation, vulnerabilities, and residual risk. Comprehensive Analysis is the most extensive level, appropriate when the system or its information requires the greatest confidence in the adequacy of implemented safeguards. The certifier recommends the appropriate level after considering the evidence needed to support an informed accreditation decision; the accreditation authority then uses the certification results as part of the authorization decision. NIACAP is a legacy process, but its risk-based tailoring principle remains consistent with modern authorization practice described by NIST. See NIST's NIACAP glossary entry and NIST SP 800-37 Rev. 1 for authorization-process context.

QUESTION NO: 27

Which of the following statements about Discretionary Access Control List (DACL) is true?

A. It is a rule list containing access control entries.

B. It specifies whether an audit activity should be performed when an object attempts to access a resource.

C. It is a unique number that identifies a user, group, and computer account.

D. It is a list containing user accounts, groups, and computers that are allowed (or denied) access to the object.

ANSWER: A

Explanation:

"It is a rule list containing access control entries." is correct because a discretionary access control list is the portion of a Windows security descriptor that contains access control entries (ACEs). Each ACE is a rule that identifies a security principal, typically through its security identifier (SID), and states the access rights that are allowed or denied for that principal. When a subject requests access to a securable object, Windows evaluates the ACEs in the object's DACL to determine whether the requested access can be granted. The owner of an object generally has discretion to modify its DACL, subject to applicable permissions and privileges; this discretionary management is the source of the term "discretionary" access control. DACLs therefore provide the authorization rules used to enforce object-level permissions, such as reading, writing, modifying, or deleting a file, registry key, service, or other securable resource. Microsoft's security

descriptor documentation defines a DACL as a list of ACEs governing access to the object, and its access-control model explains how those ACEs are evaluated during access checks. See Microsoft: DACLs and ACEs and Microsoft: Access Control Model.

QUESTION NO: 28

The phase 0 of Risk Management Framework (RMF) is known as strategic risk assessment planning. Which of the following processes take place in phase 0?

Each correct answer represents a complete solution. Choose all that apply.

A. Review documentation and technical data.

B. Apply classification criteria to rank data assets and related IT resources.

C. Establish criteria that will be used to classify and rank data assets.

D. Identify threats, vulnerabilities, and controls that will be evaluated.

E. Establish criteria that will be used to evaluate threats, vulnerabilities, and controls.

ANSWER: A C E

Explanation:

Strategic risk assessment planning is the preparatory activity that establishes a consistent basis for later risk-assessment work. “Review documentation and technical data” is appropriate at this stage because organizational policies, system information, architectural material, inventories, and available technical evidence provide the context needed to define a useful assessment approach. “Establish criteria that will be used to classify and rank data assets” is also a planning activity: the organization must define impact, value, criticality, and sensitivity criteria before those criteria can be consistently used throughout the assessment. Likewise, “Establish criteria that will be used to evaluate threats, vulnerabilities, and controls” belongs in strategic planning because the organization needs agreed evaluation factors, scales, and decision thresholds before conducting detailed analysis. These activities support an organization-wide, repeatable risk-management process by setting the assessment scope, inputs, and evaluation standards in advance. NIST describes risk management as an organization-wide process that relies on defined strategy, context, and risk-assessment activities; see NIST SP 800-39. The RMF also emphasizes preparing the organization and system environment before risk-management activities are executed; see NIST SP 800-37 Rev. 2.

QUESTION NO: 29

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. Custodian

B. User

C. Security auditor

D. Editor

E. Owner

ANSWER: A B E

Explanation:

An effective information-classification program assigns accountability and handling responsibilities throughout the data lifecycle. **Owner** is a core role because the owner is accountable for determining the information’s business value, classification, required protection, and authorized uses. This accountability ensures that classification decisions reflect organizational mission, legal, privacy, and operational needs.

Custodian is also a common role. Custodians implement and operate the safeguards specified for the information, such as storage, backup, access-control administration, retention support, and secure disposal procedures. They protect information in accordance with the owner's requirements rather than independently establishing the classification.

User is a recognized data role because authorized users must access, handle, share, and protect information according to its assigned classification and applicable handling procedures. Classification is only effective when users understand and follow the rules associated with the data they use.

These roles establish clear governance: ownership defines protection requirements, custody operationalizes them, and authorized use applies them in day-to-day activities. This division aligns with NIST guidance on assigning security and privacy responsibilities and protecting information based on impact and organizational requirements. See NIST SP 800-60 Volume I and NIST SP 800-53 Rev. 5.

QUESTION NO: 30

An organization is preparing an authorization package for a major application. Which of the following are core components of an authorization package?

Each correct answer represents a complete solution. Choose all that apply.

A. System security plan

B. Security and privacy assessment report

C. Plan of action and milestones

D. Contingency plan

ANSWER: A B C

Explanation:

The **system security plan**, **security and privacy assessment report**, and **plan of action and milestones** are core components of an authorization package. The system security plan describes the system, its environment of operation, implemented controls, planned controls, and responsibilities. It gives the authorizing official the context needed to understand how the system is protected.

The assessment report documents the results of assessing implemented controls, including deficiencies and findings. The plan of action and milestones identifies how weaknesses will be remediated, including responsible parties, resources, and scheduled completion dates. Together, these documents provide the evidence necessary for an informed risk-based authorization decision.

A contingency plan is an important system security document, but it is not one of the primary authorization-package components identified by the RMF. See NIST SP 800-37 Rev. 2 and NIST SP 800-53A Rev. 5.

QUESTION NO: 31

Which of the following requires all general support systems and major applications to be fully certified and accredited before these systems and applications are put into production?

Each correct answer represents a part of the solution. Choose all that apply.

A. NIST

B. FIPS

C. FISMA

D. Office of Management and Budget (OMB)

ANSWER: C D

Explanation:

FISMA and the Office of Management and Budget (OMB) are correct because they establish the federal policy basis for requiring security authorization before a federal information system is placed into operation. FISMA requires agencies to implement an agency-wide information security program and to ensure that security controls for information systems are assessed and authorized as part of managing organizational risk. In the terminology used when this question was written, the authorization decision was called accreditation, and it was supported by certification activities. Modern federal guidance instead uses the terms *security control assessment* and *authorization*, but the governance objective is the same: a senior official accepts the system's security risk before operation.

OMB implements and operationalizes these statutory responsibilities for executive-branch agencies through federal information policy. OMB Circular A-130 directs agencies to authorize information systems and maintain authorization information as part of their security and privacy programs. Thus, FISMA supplies the legal requirement for an agency information-security program, while OMB policy directs agencies' implementation and oversight of the authorization process for general support systems and major applications before production use. See the FISMA requirements in 44 U.S.C. § 3554 and OMB Circular A-130.

QUESTION NO: 32

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

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

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

D. An ISSO takes part in the development activities that are required to implement system ch anges.

E. An ISSE provides advice on the impacts of system changes.

ANSWER: A C E

Explanation:

An ISSO manages the security of the information system that is slated for Certification & Accreditation (C&A). The ISSO is the operational security representative for the system, supporting the system owner by managing day-to-day security activities, coordinating security-control implementation, maintaining security documentation, and helping ensure that the system is prepared for the authorization process. Although current federal guidance generally uses the term authorization rather than C&A, the underlying ISSO responsibility remains management of the system's security posture.

An ISSE provides advice on the continuous monitoring of the information system. The ISSE brings security engineering expertise to the system life cycle and advises stakeholders on how security controls, architecture, and technical solutions can be monitored and sustained as the environment changes. This advisory role helps ensure that monitoring is technically meaningful and aligned with risk-management needs.

An ISSE provides advice on the impacts of system changes. Security engineering review is essential when changes affect architecture, interfaces, configurations, or controls. The ISSE helps identify security implications and ensures that security requirements remain integrated into the changed system. These responsibilities are consistent with the role descriptions in NIST SP 800-37 Rev. 1 and the system-security-engineering approach described in NIST SP 800-160 Vol. 1.

QUESTION NO: 33

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

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

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

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

ANSWER: A D

Explanation:

In the traditional Certification and Accreditation terminology used in earlier U.S. federal information-security guidance, accreditation is the formal, explicit management authorization for an information system to operate. This decision is made by a senior official with responsibility and accountability for accepting the system's residual risk. Therefore, "Accreditation is the official management decision given by a senior agency official to authorize operation of an information system." correctly describes the authorization and risk-acceptance function.

Certification is the detailed security evaluation that supports that management decision. It assesses the effectiveness of implemented management, operational, and technical controls and documents the system's security posture, including evidence needed for the authorizing official to make an informed risk-based decision. Thus, "Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system." correctly captures the assessment function. Modern NIST guidance has replaced the C&A terminology with assessment and authorization under the Risk Management Framework, but the underlying distinction remains: controls are assessed and the system is then authorized by the responsible official. See NIST SP 800-37 Rev. 1 and FIPS 200.

QUESTION NO: 34

Tracy is the project manager of the NLT Project for her company. The NLT Project is scheduled to last 14 months and has a budget at completion of $4,555,000. Tracy's organization will receive a bonus of $80,000 per day that the project is completed early up to $800,000. Tracy realizes that there are several opportunities within the project to save on time by crashing the project work. Crashing the project is what type of risk response?

A. Mitigation

B. Exploit

C. Enhance

D. Transference

ANSWER: C

Explanation:

Enhance is correct because the early-completion bonus is a positive risk, or opportunity, and crashing is a deliberate action intended to increase the likelihood and potential value of that opportunity. In project schedule management, crashing means applying additional resources, typically at added cost, to activities on the critical path so that the overall project duration can be reduced. By selectively crashing eligible work, Tracy increases the chance that the project finishes ahead of its planned completion date. Each additional day saved also increases the financial benefit available to the organization, subject to the stated maximum bonus. This is therefore an opportunity response that improves the probability of realizing an early finish and can increase the opportunity's positive impact. The project's budget at completion provides a basis for evaluating whether the incremental cost of crashing is justified by the available bonus, but it does not change the response classification. PMI identifies enhancing as an opportunity-response strategy used when a team wants to raise the probability or impact of a beneficial uncertain event. See PMI's Project Management Lexicon and its overview of positive risk management.

QUESTION NO: 35

Observe the HTTP request below and identify the vulnerability attempted.

GET /help.php?file=../../../etc/passwd HTTP/1.1

Host: example.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/107.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: en-GB,en;q=0.5

Accept-Encoding: gzip, deflate

Upgrade-Insecure-Requests: 1

Sec-Fetch-Dest: document

Sec-Fetch-Mode: navigate

Sec-Fetch-Site: none

Sec-Fetch-User: ?1

Cookie: JSESSIONID=38RB5ECV10785B53AF29816E92E2E50

Te: trailers

Connection: keep-alive

A. Cross-Site Request Forgery Vulnerability

B. Path Traversal Vulnerability

C. Code Injection Vulnerability

D. All of the above

ANSWER: B

Explanation:

Path Traversal Vulnerability is the correct answer. The `file` parameter contains `../../../etc/passwd`, where each `../` sequence requests navigation to a parent directory. This is a common path-traversal payload intended to escape the application's expected file directory and reach a sensitive operating-system file. On Unix-like systems, `/etc/passwd` traditionally stores account-related information, so its disclosure can provide useful reconnaissance data to an attacker.

The attempted attack depends on how `help.php` handles the supplied filename. If the application concatenates untrusted input into a filesystem path without canonicalizing it, enforcing an allowlist, and verifying that the resolved path remains within an approved base directory, the request could access files outside the intended location. This weakness is also commonly called directory traversal. Secure implementations avoid accepting arbitrary paths, map user selections to predefined server-side resources, and validate the canonical resolved path before opening a file.

OWASP describes path traversal as the manipulation of file-path inputs to access unauthorized files and recommends allowlisting and safe path validation techniques. See the OWASP Path Traversal guidance and the OWASP File Upload Cheat Sheet for related file-handling security practices.

QUESTION NO: 36

Which of the following are the tasks performed by the owner in the information classification schemes? Each correct answer represents a part of the solution. Choose three.

A. To make original determination to decide what level of classification the information requires, which is based on the business requirements for the safety of the data.

B. To perform data restoration from the backups whenever required.

C. To review the classification assignments from time to time and make alterations as the business requirements alter.

D. To delegate the responsibility of the data safeguard duties to the custodian.

ANSWER: A C D

Explanation:

Information ownership assigns accountability for information to the business role with the authority to determine its value, sensitivity, and required protection. “To make original determination to decide what level of classification the information requires, which is based on the business requirements for the safety of the data.” is therefore an owner responsibility: classification must reflect the potential business impact of unauthorized disclosure, alteration, or loss of availability. Owners also retain accountability after the initial decision, so “To review the classification assignments from time to time and make alterations as the business requirements alter.” is appropriate. Information, systems, legal obligations, and business impact can change, requiring a re-evaluation of classification and handling requirements.

“To delegate the responsibility of the data safeguard duties to the custodian.” is also consistent with the owner–custodian model. The owner establishes the classification and protection expectations, while a custodian is entrusted with implementing and operating the safeguards necessary to preserve the information in accordance with those requirements. Delegation of operational safeguarding does not remove the owner’s ultimate accountability for appropriate classification and protection. NIST describes categorization as a process based on impact and organizational risk considerations in FIPS 199; NIST’s security-control guidance further supports assigning and implementing controls consistent with defined protection needs in SP 800-53 Rev. 5.

QUESTION NO: 37

Henry is the project manager of the QBG Project for his company. This project has a budget of $4,576,900 and is expected to last 18 months to complete. The CIO, a stakeholder in the project, has introduced a scope change request for additional deliverables as part of the project work. What component of the change control system would review the proposed changes' impact on the features and functions of the project's product?

A. Cost change control system

B. Scope change control system

C. Integrated change control

D. Configuration management system

ANSWER: D

Explanation:

The **Configuration management system** is correct because it provides the structured approach for identifying product characteristics, recording their approved configuration, and evaluating proposed changes to those characteristics. Additional deliverables can alter the project product’s specified features and functions. Before implementation, the change must therefore be assessed against the approved product configuration to determine its technical and functional impact, including what configuration items, specifications, baselines, documentation, testing, and acceptance criteria may need revision.

Within project change control, configuration management supplies the product-focused controls that ensure the delivered result continues to match approved requirements and that changes are traceable throughout their life cycle. It supports identifying the affected configuration items, documenting the requested revision, reviewing impacts, obtaining the required approval, and maintaining an accurate record of the resulting product configuration. This is especially important where a stakeholder-requested scope addition changes what the finished product must do, rather than merely changing administrative project information. PMI describes configuration management as an important part of controlling changes to project deliverables and product-related baselines. See PMI’s overview of configuration management for project success and NIST’s guidance on security-focused configuration management.

QUESTION NO: 38

A security policy is an overall general statement produced by senior management that dictates what role security plays within the organization. What are the different types of policies?

Each correct answer represents a complete solution. Choose all that apply.

A. Systematic

B. Informative

C. Regulatory

D. Advisory

ANSWER: B C D

Explanation:

Informative, Regulatory, and Advisory are recognized policy types because they distinguish the source and degree of authority behind organizational security requirements. Regulatory policies implement obligations imposed by external authorities, such as legislation, regulations, contractual commitments, or requirements of a governing body. Their purpose is to ensure the organization establishes and maintains controls necessary to meet mandatory compliance obligations.

Advisory policies express management's expected practices and direction for personnel and organizational units. They provide an authoritative internal basis for consistent security behavior, risk treatment, and accountability, even where a requirement does not originate directly from a law or regulator. Informative policies provide explanatory material, context, and useful guidance that helps personnel understand security objectives and apply related requirements appropriately. Together, these types let an organization communicate mandatory external duties, internal management expectations, and supporting security knowledge in a structured way.

This policy approach supports the governance emphasis in NIST guidance: senior leadership establishes policy and assigns responsibilities so that security requirements can be implemented and managed throughout the organization. See NIST SP 800-12 Rev. 1, Introduction to Information Security and the NIST Cybersecurity Framework.

QUESTION NO: 39

You are the program manager for your project. You are working with the project managers regarding the procurement processes for their projects. You have ruled out one particular contract type because it is considered too risky for the program. Which one of the following contract types is usually considered to be the most dangerous for the buyer?

A. Cost plus incentive fee

B. Time and materials

C. Cost plus percentage of costs

D. Fixed fee

ANSWER: C

Explanation:

Cost plus percentage of costs is the contract type usually considered most dangerous for the buyer because the contractor's payment increases directly as allowable costs increase. The contractor receives reimbursement of incurred costs plus a fee calculated as a percentage of those costs. Consequently, higher spending produces a higher fee, creating an inherent misalignment between the buyer's objective of controlling total cost and the seller's financial incentive. This structure gives the buyer substantial exposure to cost growth and demands unusually rigorous cost monitoring, authorization, auditability, and scope control.

In U.S. federal contracting, this risk is significant enough that cost-plus-a-percentage-of-cost arrangements are expressly prohibited. The Federal Acquisition Regulation states that such contracts "shall not be used," reflecting the principle that a

contractor should not profit merely because the cost of performance rises. See FAR 16.102, Policies. Sound acquisition practice instead seeks contract structures that align compensation with defined performance, cost-control, or outcome objectives while maintaining appropriate oversight. The buyer's risk in this arrangement is therefore not merely uncertainty in final cost; it is the contract's built-in incentive for costs to increase.