Exam

CGRC

Certified in Governance, Risk and Compliance (CGRC)

Free demo	80 sample questions
Full exam	725 questions with answers and explanations
Contents	Questions with answers and explanations

Exam domains

Domain	Exam weight	Questions
D1 Security and Privacy Governance, Risk Management, and Compliance Program	16%	25
D2 Scope of the System	10%	11
D3 Selection and Approval of Framework, Security, and Privacy Controls	14%	10
D4 Implementation of Security and Privacy Controls	17%	4
D5 Assessment/Audit of Security and Privacy Controls	16%	13
D6 System Compliance	14%	6
D7 Compliance Maintenance	13%	11

This is a free demo from Dumpsgate: 80 of the exam's 725 questions. **Get the full CGRC exam** with every question, answer and explanation.

Question 1

Single choice · Domain: D1 Security and Privacy Governance, Risk Management, and Compliance Program › 1.1 - Demonstrate knowledge in security and privacy governance, risk management, and compliance program

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?

Response:

A. Risk avoidance
B. Mitigation-ready project management
C. Risk utility function
D. Risk-reward mentality

Answer: C. Risk utility function

Explanation

The project has high stakes for organizational profitability, and management wants to weigh the costs and benefits of risk events while avoiding them. A risk utility function represents a stakeholder's attitude toward risk; a low tolerance indicates a risk-averse attitude. Therefore, the term sought is "risk utility function."

✗ **A** Risk avoidance
Risk avoidance is a response strategy that seeks to eliminate a particular risk or its exposure. It does not name the measure or concept describing stakeholders' low tolerance for risk.

✗ **B** Mitigation-ready project management
This describes an approach focused on being prepared to reduce risks, not the term for stakeholder risk tolerance. The question asks what low tolerance is called, rather than how the project should manage each risk.

✓ **C** Risk utility function
A risk utility function expresses how a stakeholder values outcomes involving risk and reflects their willingness to accept risk. In this scenario, low stakeholder tolerance corresponds to a risk-averse attitude, making this the applicable term.

✗ **D** Risk-reward mentality
A risk-reward mentality concerns weighing potential gains against exposure to risk. It does not specifically describe the low level of stakeholder risk tolerance asked about here.

Free demo · full exam: 725 questions

Question 2

Single choice · Domain: D1 Security and Privacy Governance, Risk Management, and Compliance Program › 1.1 - Demonstrate knowledge in security and privacy governance, risk management, and compliance program

What tools is MOST appropriate to assess whether information security governance objectives are being met?

Response:

A. Balanced scorecard. A BSC is most effective for evaluating the degree to which information security objectives are being met.

B. Balanced scorecard. A BSC is most effective for disconnecting the degree to which information security objectives are being met.

C. Balanced scorecard. A BSC is most uneffective for evaluating the degree to which information security objectives are being met.

D. Balanced scorecard. A BSS is most uneffective for disconnecting the degree to which information security objectives are being met.

Answer: A. Balanced scorecard. A BSC is most effective for evaluating the degree to which information security objectives are being met.

Explanation

A balanced scorecard (BSC) is appropriate because it helps assess performance against defined objectives, including information security governance objectives. The question asks whether objectives are being met, so an evaluation tool is needed; option A correctly describes that use. The other options distort that purpose by saying the scorecard disconnects objectives or is ineffective.

✓ **A** Balanced scorecard. A BSC is most effective for evaluating the degree to which information security objectives are being met.
This directly addresses the question: a balanced scorecard can compare performance measures with the information security objectives and show the extent to which they are being achieved.

✗ **B** Balanced scorecard. A BSC is most effective for disconnecting the degree to which information security objectives are being met.
A governance assessment should evaluate progress toward objectives, not disconnect or separate that assessment from them. The phrase does not describe the purpose relevant to the question.

✗ **C** Balanced scorecard. A BSC is most uneffective for evaluating the degree to which information security objectives are being met.
This says the BSC is ineffective for the exact evaluation the question requires. Option A gives the suitable use of the tool instead.

✗ **D** Balanced scorecard. A BSS is most uneffective for disconnecting the degree to which information security objectives are being met.
This describes the tool as ineffective and says it disconnects the assessment from the objectives. Neither supports determining whether the information security governance objectives are being met.

Free demo · full exam: 725 questions

Question 3

Single choice · Domain: D1 Security and Privacy Governance, Risk Management, and Compliance Program › 1.2 - Demonstrate knowledge in security and privacy governance, risk management and compliance program processes

Managing information security risk from an organization-wide perspective has to do with the following processes except one. Choose the exception.

Response:

A. responding to rist
B. Framing risk
C. Assessing risk
D. Mitigating risk

Answer: D. Mitigating risk

Explanation

The question asks which choice is the exception among organization-wide information security risk processes. Framing, assessing, and responding to risk are recognized processes; mitigating risk is an action that may be used when responding to risk rather than a separate process in this list. Therefore, D is the exception.

✗ **A** Responding to risk
Responding to risk is one of the organization-wide risk management processes. It involves deciding how to address assessed risks, so it is not the exception.

✗ **B** Framing risk
Framing risk establishes the context and approach for managing risk across the organization. It is one of the processes named in the question's category.

✗ **C** Assessing risk
Assessing risk identifies and evaluates risks to inform decisions about how to address them. It is a risk management process, not the exception.

✓ **D** Mitigating risk
Mitigation is a way to address or reduce risk, typically considered as part of responding to risk. It is not listed here as a separate organization-wide process, so it is the exception.

Dumpsgate

Question 4

Single choice · Domain: D1 Security and Privacy Governance, Risk Management, and Compliance Program › 1.2 - Demonstrate knowledge in security and privacy governance, risk management and compliance program processes

What is NIST SP 800-37 R1?

Response:

A. Guide for Applying the Risk Management Framework to Federal Information Systems. A Security Life Cycle Approach

B. Guide for Applying the Risk Management Framework to Federal Information Systems. A unsecure Life Cycle Approach

C. Guide for Applying the Safe Management Framework to Federal Information Systems. A Security Life Cycle Approach

D. Guide for Applying the Risk Management Framework to Federal Information Systems. A Security Life Cycle Unapproachable.

Answer: A. Guide for Applying the Risk Management Framework to Federal Information Systems. A Security Life Cycle Approach

Explanation

NIST SP 800-37 Revision 1 is titled “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.” Option A gives this title accurately, including both the Risk Management Framework and the security life cycle wording. [1]

https://csrc.nist.gov/pubs/sp/800/37/r1/upd1/final

✓ **A** Guide for Applying the Risk Management Framework to Federal Information Systems. A Security Life Cycle Approach
This is the correct title of NIST SP 800-37 Revision 1. It correctly identifies the Risk Management Framework and describes the approach as a security life cycle approach. [1]

https://csrc.nist.gov/pubs/sp/800/37/r1/upd1/final

✗ **B** Guide for Applying the Risk Management Framework to Federal Information Systems. A unsecure Life Cycle Approach
The title specifies a “Security Life Cycle Approach,” not an “unsecure” life cycle approach. That changed wording makes this option inaccurate. [1]

https://csrc.nist.gov/pubs/sp/800/37/r1/upd1/final

✗ **C** Guide for Applying the Safe Management Framework to Federal Information Systems. A Security Life Cycle Approach
The title refers to the “Risk Management Framework,” not a “Safe Management Framework.” Although the rest resembles the title, this substitution makes the option incorrect. [1]

https://csrc.nist.gov/pubs/sp/800/37/r1/upd1/final

✗ **D** Guide for Applying the Risk Management Framework to Federal Information Systems. A Security Life Cycle Unapproachable.
The title ends with “A Security Life Cycle Approach,” not “A Security Life Cycle Unapproachable.” The altered final phrase does not match the publication title. [1]

https://csrc.nist.gov/pubs/sp/800/37/r1/upd1/final

Free demo · full exam: 725 questions

Question 5

Single choice · Domain: D1 Security and Privacy Governance, Risk Management, and Compliance Program › 1.2 - Demonstrate knowledge in security and privacy governance, risk management and compliance program processes

Which publication primarily targets activities in Tier 3 of Risk Management approach/pyramid?

Response:

A. NIST SP 800-37
B. NIST SP 800-38
C. NIST SP 800-53
D. NIST SP 800-53A

Answer: A. NIST SP 800-37

Explanation

NIST SP 800-37 is the publication associated with the Risk Management Framework (RMF), including the process for managing security and privacy risk at the system level, which corresponds to Tier 3 in the risk management approach. Therefore, it is the best match for activities primarily targeting that tier. [2][3]

https://csrc.nist.gov/pubs/sp/800/37/r2/final
https://csrc.nist.gov/files/pubs/sp/800/37/r1/final/docs/sp800-37-rev1-final.pdf

✓ **A** NIST SP 800-37
NIST SP 800-37 describes the Risk Management Framework and its application to information systems, aligning it with Tier 3 activities. It is therefore the correct publication for the tier identified in the question. [2][3]

https://csrc.nist.gov/pubs/sp/800/37/r2/final
https://csrc.nist.gov/files/pubs/sp/800/37/r1/final/docs/sp800-37-rev1-final.pdf

✗ **B** NIST SP 800-38
NIST SP 800-38 is a series focused on cryptographic standards and modes of operation, rather than the risk-management activities targeted at Tier 3. It does not match the question's focus on the risk management approach/pyramid.

✗ **C** NIST SP 800-53
NIST SP 800-53 provides security and privacy controls for information systems and organizations. While those controls are used within risk management, this option is not the publication identified as primarily targeting Tier 3 activities; that role is associated with SP 800-37. [6]

https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/downloads

✗ **D** NIST SP 800-53A
NIST SP 800-53A provides procedures for assessing security and privacy controls, rather than being the primary publication for Tier 3 risk-management activities. It supports control assessment within the broader RMF, but SP 800-37 is the relevant choice. [12]

https://csrc.nist.gov/news/2022/security-privacy-control-assessment-procedures

Question 6

Single choice · Domain: D1 Security and Privacy Governance, Risk Management, and Compliance Program › 1.1 - Demonstrate knowledge in security and privacy governance, risk management, and compliance program

What is BRM?

Response:

A. The Business Reference Model (BRM) provides an organized, hierarchical framework for describing the day-to-day business operations of the federal government. The BRM is the first layer of the Federal Enterprise Architecture (FEA) and provides a good viewpoint from which to analyze data, service components, and technology.

B. The Business Reference Model (BRM) provides an organized, hierarchical framework for describing the day-to-day business operations of the federal government. The BRM is the last layer of the Federal Enterprise Architecture (FEA) and provides a good viewpoint from which to analyze data, service components, and technology.

C. The Business Reference Model (BRM) provides an organized, hierarchical framework for describing the month to month business operations of the federal government. The BRM is the last layer of the Federal Enterprise Architecture (FEA) and provides a good viewpoint from which to analyze data, service components, and technology.

D. The Business Reference Model (BRM) provides an organized, hierarchical framework for describing the day-to-day business operations of the federal government. The BRM is the first layer of the Federal Enterprise Architecture (FEA) and provides a bad viewpoint from which to analyze data or service components or technology.

Answer: A. The Business Reference Model (BRM) provides an organized, hierarchical framework for describing the day-to-day business operations of the federal government. The BRM is the first layer of the Federal Enterprise Architecture (FEA) and provides a good viewpoint from which to analyze data, service components, and technology.

Explanation

A is correct because the BRM is described as a hierarchical framework for the federal government's day-to-day business operations. It is the first layer of the FEA and provides a viewpoint for analyzing data, service components, and technology.

✓ **A** The BRM describes the federal government's day-to-day business operations, is the first layer of the FEA, and provides a viewpoint for analyzing data, service components, and technology.
This matches the definition in the option: the BRM organizes federal business operations hierarchically and is identified as the first FEA layer. Its viewpoint supports analysis of data, service components, and technology.

✗ **B** The BRM describes the federal government's day-to-day business operations and is the last layer of the FEA.
The option correctly describes the day-to-day operations, but incorrectly calls the BRM the last layer of the FEA. The BRM is the first layer.

✗ **C** The BRM describes the federal government's month-to-month business operations and is the last layer of the FEA.
This changes day-to-day operations to month-to-month operations and incorrectly identifies the BRM as the last FEA layer. The correct description is day-to-day operations and the first layer.

✗ **D** The BRM describes the federal government's day-to-day business operations and is the first layer of the FEA, but provides a bad viewpoint for analysis.

Free demo · full exam: 725 questions

The option correctly identifies the operations and the BRM's position as the first FEA layer, but incorrectly says it provides a bad viewpoint. It provides a useful viewpoint for analyzing data, service components, and technology.

Question 7

Multiple choice · Domain: D1 Security and Privacy Governance, Risk Management, and Compliance Program › 1.3 - Understand regulatory and legal requirements

Which of the following acts promote a risk-based policy for cost effective security?

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

Response:

A. Clinger-Cohen Act
B. Lanham Act
C. Computer Misuse Act
D. Paperwork Reduction Act (PRA)

Answer

- A. **Clinger-Cohen Act**
- D. **Paperwork Reduction Act (PRA)**

Explanation

The Clinger-Cohen Act and the Paperwork Reduction Act support risk-based, cost-effective management of federal information resources and technology. The other choices address trademark protection or criminal computer misuse, rather than promoting this kind of policy.

✓ **A** Clinger-Cohen Act
The Act calls for federal agencies to manage information technology investments with attention to risk, performance, and cost-effectiveness. That aligns with promoting a risk-based policy for security.

✗ **B** Lanham Act
The Lanham Act primarily concerns trademarks and unfair competition. It does not promote a risk-based policy for cost-effective security.

✗ **C** Computer Misuse Act
The Computer Misuse Act establishes offenses involving unauthorized computer access and misuse. It is a criminal-law measure, not a policy framework for risk-based, cost-effective security.

✓ **D** Paperwork Reduction Act (PRA)
The PRA supports efficient management of federal information resources and reducing unnecessary information-collection burdens. Its emphasis on efficient, cost-conscious management makes it part of the risk-based policy approach described in the question.

Free demo · full exam: 725 questions

Question 8

Multiple choice · Domain: D1 Security and Privacy Governance, Risk Management, and Compliance Program › 1.1 - Demonstrate knowledge in security and privacy governance, risk management, and compliance program

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.

Response:

A. Systematic
B. Informative
C. Regulatory
D. Advisory

Answer

- B. **Informative**
- C. **Regulatory**
- D. **Advisory**

Explanation

The three recognized types of information security policies are regulatory, advisory, and informative. Regulatory policies are required to meet external rules, advisory policies state management's required or prohibited practices, and informative policies communicate information about security. "Systematic" is not one of these policy types.

✗ **A** Systematic
Systematic is not a recognized type in the standard classification of security policies. The types that fit the question are regulatory, advisory, and informative.

✓ **B** Informative
An informative policy communicates information about security, such as the organization's security goals or practices. It is one of the recognized policy types.

✓ **C** Regulatory
A regulatory policy addresses security requirements imposed by laws, regulations, or other external rules. It is one of the recognized policy types.

✓ **D** Advisory
An advisory policy tells employees what security practices are required or prohibited by the organization. It is one of the recognized policy types.

Free demo · full exam: 725 questions

Question 9

Single choice · Domain: D1 Security and Privacy Governance, Risk Management, and Compliance Program › 1.3 - Understand regulatory and legal requirements

Which law was superseded by FISMA?

The law required that systems processing federal data be authorized to process by a management official, and failure to do so will constitutes a violation of a federal directive.

Response:

A. FIPS 102, 1983
B. Computer security Act of 1987
C. OMB Circular A-130
D. Clinger-Cohen Act of 1996

Answer: B. Computer security Act of 1987

Explanation

The correct answer is the Computer Security Act of 1987. It established federal computer-security requirements, including management authorization for systems processing sensitive federal information, and FISMA superseded it. This matches the question's description of a system needing approval from a management official before processing federal data.

https://csrc.nist.gov/Topics/Laws-and-Regulations/laws/FISMA
https://csrc.nist.gov/projects/risk-management/fisma-background

✗ **A** FIPS 102, 1983
FIPS 102 was a federal information processing standard, not the law identified as having been superseded by FISMA. The requirement described in the question corresponds to the Computer Security Act of 1987.

https://www.nist.gov/standardsgov/compliance-faqs-federal-information-processing-standards-fips
https://www.nist.gov/itl/fips-general-information

✓ **B** Computer security Act of 1987
The Computer Security Act of 1987 required security measures for federal computer systems, including management authorization for systems processing sensitive information. FISMA superseded this law.

https://csrc.nist.gov/Topics/Laws-and-Regulations/laws/FISMA
https://csrc.nist.gov/projects/risk-management/fisma-background

✗ **C** OMB Circular A-130
OMB Circular A-130 provides federal information-resource management policy and guidance; it is not the law that FISMA superseded in the scenario. The described management-authorization requirement points to the Computer Security Act of 1987.

https://csrc.nist.gov/Topics/Laws-and-Regulations/laws/FISMA
https://csrc.nist.gov/projects/risk-management/fisma-background

✗ **D** Clinger-Cohen Act of 1996
The Clinger-Cohen Act addresses federal information-technology management, but it is not the law identified as superseded by FISMA. The requirement described in the question is associated with the Computer Security Act of 1987.

https://csrc.nist.gov/Topics/Laws-and-Regulations/laws/FISMA
https://csrc.nist.gov/projects/risk-management/fisma-background

Free demo · full exam: 725 questions

Question 10

Multiple choice · Domain: D1 Security and Privacy Governance, Risk Management, and Compliance Program › 1.1 - Demonstrate knowledge in security and privacy governance, risk management, and compliance program

Which of the following approaches can be used to build a security program?

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

Response:

A. Bottom-Up Approach
B. Right-Up Approach
C. Top-Down Approach
D. Left-Up Approach

Answer

- A. **Bottom-Up Approach**
- C. **Top-Down Approach**

Explanation

A security program can be built using either a top-down or a bottom-up approach. Top-down starts with leadership setting direction and supporting the program, while bottom-up builds from security needs and activities at operational levels. “Right-Up” and “Left-Up” are not the recognized approaches listed here.

https://www.isc2.org/Insights/2024/04/The-Crucial-Role-of-Leadership-in-Information-Security?trk=article-ssr-frontend-pulse_little-text-block
https://www.isc2.org/Insights/2024/10/CybersecurityAwarenessMonth-Cyber-Leadership

✓ **A** Bottom-Up Approach
A bottom-up approach builds the security program from operational needs and security work at lower organizational levels. It is one of the two applicable approaches.

✗ **B** Right-Up Approach
“Right-Up” is not a recognized approach for building a security program in this question. The applicable approaches are bottom-up and top-down.

✓ **C** Top-Down Approach
A top-down approach starts with leadership establishing the security program’s direction and providing support. Leadership’s role in setting information-security priorities supports this approach.

https://www.isc2.org/Insights/2024/04/The-Crucial-Role-of-Leadership-in-Information-Security?trk=article-ssr-frontend-pulse_little-text-block
https://www.isc2.org/Insights/2024/10/CybersecurityAwarenessMonth-Cyber-Leadership

✗ **D** Left-Up Approach
“Left-Up” is not a recognized approach for building a security program in this question. It is not one of the two applicable approaches.

Free demo · full exam: 725 questions

Question 11

Single choice · Domain: D1 Security and Privacy Governance, Risk Management, and Compliance Program › 1.2 - Demonstrate knowledge in security and privacy governance, risk management and compliance program processes

Which of the following relations correctly describes residual risk?

Response:

A. Residual Risk = Threats x Vulnerability x Asset Gap x Control Gap
B. Residual Risk = Threats x Exploit x Asset Value x Control Gap
C. Residual Risk = Threats x Exploit x Asset Value x Control Gap
D. Residual Risk = Threats x Vulnerability x Asset Value x Control Gap

Answer: D. Residual Risk = Threats x Vulnerability x Asset Value x Control Gap

Explanation

Option D gives the stated residual-risk relationship: threats × vulnerability × asset value × control gap. It includes the asset's value and the remaining gap in controls, along with threats and vulnerability; the other choices substitute a different factor or omit asset value. The listed references do not clearly support this specific formula, so no reference is cited.

✗ **A** Residual Risk = Threats x Vulnerability x Asset Gap x Control Gap
This uses "Asset Gap" instead of asset value. That is not the relationship specified by the correct answer.

✗ **B** Residual Risk = Threats x Exploit x Asset Value x Control Gap
This substitutes exploit for vulnerability. The specified relationship uses vulnerability as a factor.

✗ **C** Residual Risk = Threats x Exploit x Asset Value x Control Gap
Like option B, this uses exploit rather than vulnerability. It therefore does not match the specified formula.

✓ **D** Residual Risk = Threats x Vulnerability x Asset Value x Control Gap
This matches the stated relationship, combining threats, vulnerability, asset value, and the control gap. It is the only option with all four specified factors.

Question 12

Single choice · Domain: D1 Security and Privacy Governance, Risk Management, and Compliance Program › 1.2 - Demonstrate knowledge in security and privacy governance, risk management and compliance program processes

What publication provides an approach for performing system-level risk assessments?

Response:

A. NIST SP 800-30
B. NIST SP 800-39
C. NIST SP 800-60
D. NIST SP 800-50

Answer: A. NIST SP 800-30

Explanation

NIST SP 800-30 provides guidance for conducting risk assessments, including assessments at the system level. It is therefore the publication that matches the question; the other options address broader risk management, security categorization, or security awareness and training.

https://csrc.nist.gov/pubs/sp/800/30/r1/final
https://csrc.nist.gov/pubs/sp/800/30/final

✓ **A** NIST SP 800-30
NIST SP 800-30 is the guide for conducting risk assessments, including system-level assessments. It directly matches the requested approach.

https://csrc.nist.gov/pubs/sp/800/30/r1/final
https://csrc.nist.gov/pubs/sp/800/30/final

✗ **B** NIST SP 800-39
NIST SP 800-39 addresses organization-wide information security risk management, rather than providing the risk-assessment guide requested here.

https://csrc.nist.gov/publications/sp800
https://csrc.nist.gov/Projects/Risk-Management/publications

✗ **C** NIST SP 800-60
NIST SP 800-60 concerns mapping information and information systems to security categories; it is not the publication that provides an approach for performing system-level risk assessments.

https://csrc.nist.gov/publications/sp800

✗ **D** NIST SP 800-50
NIST SP 800-50 concerns building and managing security awareness and training programs, not conducting system-level risk assessments.

https://csrc.nist.gov/publications/sp800

Question 13

Single choice · Domain: D1 Security and Privacy Governance, Risk Management, and Compliance Program › 1.1 - Demonstrate knowledge in security and privacy governance, risk management, and compliance program

What is the position Senior Information Security Officer, or Chief Information Security Officer, known as at the the agency level?

Response:

A. Chief Information Officer
B. Information System Security Officer
C. Senior Agency Information Security Officer
D. Senior Information System Security Officer

Answer: C. Senior Agency Information Security Officer

Dumpsgate

Question 14

Single choice · Domain: D1 Security and Privacy Governance, Risk Management, and Compliance Program › 1.2 - Demonstrate knowledge in security and privacy governance, risk management and compliance program processes

What are the nine steps of Risk Assessment Methodology?

Response:

A. 1 - System Characterization 2 - Threat identification 3 - Vulnerability Identification 4 - Control Analysis 5 - Likelihood Determination 6 - Impact Analysis 7 - Risk Determination 8 - Control Recommendation 9 - Results Documentation

B. 1 - Impact Analysis 2 - Risk Determination 3 - Control Recommendation 4 - Results Documentation 5. Threat identification 6. Control Analysis 7. Vulnerability Identification 8. System Characterization 9. Likelihood Determination

C. 1 - System Characterization 2 - Threat identification 3 - Vulnerability Identification 4 - Control Analysis 5. Likelihood Determination 6. Results Documentation 7. Impact Analysis 8. Risk Determination 9. Control Recommendation

D. 1 - Control Analysis 2 - Likelihood Determination 3 - Impact Analysis 4 - Risk Determination 5. Likelihood Determination 6. Results Documentation 7. Risk Determination 8. Control Recommendation 9. System Characterization

Answer: A. 1 - System Characterization 2 - Threat identification 3 - Vulnerability Identification 4 - Control Analysis 5 - Likelihood Determination 6 - Impact Analysis 7 - Risk Determination 8 - Control Recommendation 9 - Results Documentation

Explanation

Option A gives the nine Risk Assessment Methodology steps in their correct sequence, from defining the system through documenting the results. The sequence proceeds from identifying the system, threats, vulnerabilities, and controls to evaluating likelihood and impact, determining risk, recommending controls, and recording the outcome. The other options either reorder these stages or repeat and omit steps.

✓ **A** 1 - System Characterization 2 - Threat identification 3 - Vulnerability Identification 4 - Control Analysis 5 - Likelihood Determination 6 - Impact Analysis 7 - Risk Determination 8 - Control Recommendation 9 - Results Documentation
This is the correct sequence of the nine steps. It starts by characterizing the system and identifying threats, vulnerabilities, and controls, then evaluates likelihood and impact before determining risk, recommending controls, and documenting results.

✗ **B** 1 - Impact Analysis 2 - Risk Determination 3 - Control Recommendation 4 - Results Documentation 5. Threat identification 6. Control Analysis 7. Vulnerability Identification 8. System Characterization 9. Likelihood Determination
This option places impact analysis and risk determination before system characterization, threat identification, and vulnerability identification. Those foundational assessment steps must come earlier in the methodology, not after recommendations and documentation.

✗ **C** 1 - System Characterization 2 - Threat identification 3 - Vulnerability Identification 4 - Control Analysis 5. Likelihood Determination 6. Results Documentation 7. Impact Analysis 8. Risk Determination 9. Control Recommendation
Although its first five steps match the correct order, it documents results before completing impact analysis, risk determination, and control recommendation. Results documentation is the final step, not step 6.

Free demo · full exam: 725 questions

✗ **D** 1 - Control Analysis 2 - Likelihood Determination 3 - Impact Analysis 4 - Risk Determination 5. Likelihood Determination 6. Results Documentation 7. Risk Determination 8. Control Recommendation 9. System Characterization
This option omits threat identification and vulnerability identification, repeats likelihood determination and risk determination, and puts system characterization last. These errors prevent it from representing the nine distinct steps in the correct sequence.

Question 15

Multiple choice · Domain: D1 Security and Privacy Governance, Risk Management, and Compliance Program › 1.1 - Demonstrate knowledge in security and privacy governance, risk management, and compliance program

Which of the following concepts represent the three fundamental principles of information security?

Each correct answer represents a complete solution. Choose three.

Response:

A. Privacy
B. Integrity
C. Availability
D. Confidentiality

Dumpsgate

Answer

- B. **Integrity**
- C. **Availability**
- D. **Confidentiality**

Explanation

The three fundamental principles of information security are confidentiality, integrity, and availability (the CIA triad). Together, they address preventing unauthorized disclosure, preserving accuracy and completeness, and ensuring information and services are accessible when needed. Privacy is important but is not one of these three principles.

https://www.isc2.org/certifications/cc/cc-certification-exam-outline
https://www.isc2.org/certifications/cissp/cissp-certification-exam-outline
https://www.isc2.org/certifications/cissp/cissp-student-glossary

✗ **A** Privacy
Privacy concerns appropriate handling of personal information, but it is not one of the three fundamental information security principles. The requested principles are confidentiality, integrity, and availability.

✓ **B** Integrity
Integrity is a fundamental principle: it protects information from improper alteration or destruction and helps ensure it remains accurate and complete.

https://www.isc2.org/certifications/cc/cc-certification-exam-outline
https://www.isc2.org/certifications/cissp/cissp-certification-exam-outline
https://www.isc2.org/certifications/cissp/cissp-student-glossary

✓ **C** Availability
Availability is a fundamental principle: it ensures that information and systems can be accessed by authorized users when needed.

https://www.isc2.org/certifications/cc/cc-certification-exam-outline

Free demo · full exam: 725 questions

https://www.isc2.org/certifications/cissp/cissp-certification-exam-outline
https://www.isc2.org/certifications/cissp/cissp-student-glossary

✓ **D** Confidentiality
Confidentiality is a fundamental principle: it protects information from unauthorized access or disclosure.

https://www.isc2.org/certifications/cc/cc-certification-exam-outline
https://www.isc2.org/certifications/cissp/cissp-certification-exam-outline
https://www.isc2.org/certifications/cissp/cissp-student-glossary

Question 16

Single choice · Domain: D1 Security and Privacy Governance, Risk Management, and Compliance Program › 1.2 - Demonstrate knowledge in security and privacy governance, risk management and compliance program processes

A condition that exists within an organization, a mission/business process, enterprise architecture, or information system including its environment of operation, which contributes to (i.e., increases or decreases) the likelihood that one or more threat events, once initiated, will result in undesirable consequences or adverse impact to organizational operations and assets, individuals, other organizations, or the Nation.

Response:

A. Predisposing Condition
B. Unsusceptibility Condition
C. Abnormality Condition
D. Disposing Condition

Answer: A. Predisposing Condition

Explanation

The definition describes a predisposing condition: an existing condition in the organization, process, architecture, or system environment that changes the likelihood that a threat event will cause adverse consequences. Because the question explicitly describes that role, option A is correct. [1]

https://csrc.nist.gov/glossary/term/Predisposing_Condition

✓ **A** Predisposing Condition
This is the term for a condition that affects the likelihood or impact of a threat event, as described in the question. The definition specifically includes conditions within an organization, mission/business process, enterprise architecture, or information system and its operating environment. [1]

https://csrc.nist.gov/glossary/term/Predisposing_Condition

✗ **B** Unsusceptibility Condition
This is not the term defined in the question. The description concerns a condition that changes the likelihood of adverse consequences, not a named “unsusceptibility” condition. [1]

https://csrc.nist.gov/glossary/term/Predisposing_Condition

✗ **C** Abnormality Condition
This is not the NIST term matching the definition. The question describes an existing factor that can increase or decrease the likelihood of adverse impact, which is a predisposing condition. [1]

https://csrc.nist.gov/glossary/term/Predisposing_Condition

✗ **D** Disposing Condition

Free demo · full exam: 725 questions

This is not the term used for a condition that influences the likelihood of adverse consequences from a threat event. The matching term is “Predisposing Condition.” [1]

https://csrc.nist.gov/glossary/term/Predisposing_Condition

Question 17

Single choice · Domain: D1 Security and Privacy Governance, Risk Management, and Compliance Program › 1.2 - Demonstrate knowledge in security and privacy governance, risk management and compliance program processes

Which of the following statements is true about residual risks?

Response:

A. It is a weakness or lack of safeguard that can be exploited by a threat.
B. It can be considered as an indicator of threats coupled with vulnerability.
C. It is the probabilistic risk after implementing all security measures.
D. It is the probabilistic risk before implementing all security measures.

Answer: C. It is the probabilistic risk after implementing all security measures.

Explanation

Residual risk is the risk that remains after security measures or controls have been implemented. Therefore, option C correctly describes it as the probabilistic risk after implementing all security measures; risk before controls is not residual risk.

https://www.isc2.org/Insights/2021/09/Security-Does-Not-End-with-Implementing-Controls

✗ **A** It is a weakness or lack of safeguard that can be exploited by a threat.
This describes a vulnerability, not residual risk. Residual risk refers to risk remaining after controls are applied, rather than the weakness itself.

✗ **B** It can be considered as an indicator of threats coupled with vulnerability.
This is not the definition of residual risk. The option describes a relationship between threats and vulnerabilities, but does not specify the risk remaining after security measures are implemented.

✓ **C** It is the probabilistic risk after implementing all security measures.
Residual risk is the risk that remains after safeguards or controls have been implemented. Security measures can reduce risk, but they do not necessarily eliminate it.

https://www.isc2.org/Insights/2021/09/Security-Does-Not-End-with-Implementing-Controls

✗ **D** It is the probabilistic risk before implementing all security measures.
Risk before controls are implemented is generally described as inherent or initial risk. Residual risk is assessed after the security measures have been applied.

Free demo · full exam: 725 questions

Question 18

Single choice · Domain: D1 Security and Privacy Governance, Risk Management, and Compliance Program › 1.1 - Demonstrate knowledge in security and privacy governance, risk management, and compliance program

The Risk Management Framwork (RMF) provides an organized approach for organization-wide risk management. What are the tiers of the organization-wide perspective?

Response:

A. The C-suit level, The Authorization level, and the system level
B. Organizational level, common control level, and system level
C. Level one, two, and three
D. Organization, mission/business process, and system

Answer: D. Organization, mission/business process, and system

Explanation

The RMF's organization-wide perspective is structured across three tiers: organization, mission/business process, and system. This progression connects enterprise-level risk decisions to the processes that carry out the mission and to the systems that support them, so option D is correct.

✗ **A** The C-suit level, The Authorization level, and the system level
This is not the RMF's named three-tier structure. It substitutes executive and authorization roles for the organization and mission/business-process tiers.

✗ **B** Organizational level, common control level, and system level
Common controls are relevant to RMF implementation, but "common control level" is not one of the three tiers in the organization-wide perspective. The middle tier is mission/business process.

✗ **C** Level one, two, and three
This gives generic numbered levels without identifying the RMF tiers. The question asks for the organization-wide perspective's specific categories.

✓ **D** Organization, mission/business process, and system
These are the three tiers of the RMF's organization-wide perspective. They span enterprise governance, mission and business processes, and the systems that support those processes.

Free demo · full exam: 725 questions

Question 19

Single choice · Domain: D1 Security and Privacy Governance, Risk Management, and Compliance Program › 1.2 - Demonstrate knowledge in security and privacy governance, risk management and compliance program processes

According to the PMBOK Guide's historical approach, where are an organization's predefined risk-rating rules generally maintained before being tailored for a specific project?

A. Risk probability and impact matrix
B. Organizational process assets
C. Enterprise environmental factors
D. Risk management plan

Answer: B. Organizational process assets

Explanation

The correct answer is B. In the PMBOK Guide's historical approach, an organization's established risk-rating rules are organizational process assets: reusable organizational methods, policies, and procedures available to projects. The project can tailor those predefined rules for its own risk management plan and context; the rules are not themselves the project-specific matrix or plan.

✗ **A** Risk probability and impact matrix
The matrix is a tool for rating and prioritizing risks, typically using probability and impact categories. It is not where the organization generally maintains its predefined rules before project tailoring.

✓ **B** Organizational process assets
Organizational process assets include the organization's established policies, procedures, and methods that can be reused by projects. Predefined risk-rating rules are maintained there before being tailored to a specific project.

✗ **C** Enterprise environmental factors
Enterprise environmental factors are conditions that influence a project, such as organizational culture or external regulations. They are not the general repository for predefined organizational risk-rating rules.

✗ **D** Risk management plan
The risk management plan describes how risk management will be carried out for the particular project, including project-tailored approaches. The question asks where the organization's predefined rules are maintained before that tailoring.

Free demo · full exam: 725 questions

Question 20

Single choice · Domain: D1 Security and Privacy Governance, Risk Management, and Compliance Program › 1.1 - Demonstrate knowledge in security and privacy governance, risk management, and compliance program

Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

Response:

A. Adequate Security
B. Security Category
C. Security Controls
D. Security Categorization

Answer: A. Adequate Security

Explanation

The statement defines adequate security: security measures must be sufficient in relation to the risk and the potential harm from information being lost, misused, accessed without authorization, or modified without authorization. Therefore, option A is correct. [1]

https://csrc.nist.gov/glossary/term/adequate_security

✓ **A** Adequate Security
This is the term for security commensurate with the risk and the magnitude of harm that could result from loss, misuse, unauthorized access, or modification of information. [1]

https://csrc.nist.gov/glossary/term/adequate_security

✗ **B** Security Category
A security category classifies information or a system according to impact levels; it is not the definition of security measures being proportionate to risk and potential harm.

✗ **C** Security Controls
Security controls are safeguards or countermeasures used to protect information and systems. The statement describes the required sufficiency of security, rather than the controls themselves.

✗ **D** Security Categorization
Security categorization is the process of determining an information type or system's security category. It does not mean providing security commensurate with risk and potential harm.

Free demo · full exam: 725 questions

Question 21

Multiple choice · Domain: D1 Security and Privacy Governance, Risk Management, and Compliance Program › 1.2 - Demonstrate knowledge in security and privacy governance, risk management and compliance program processes

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.

Response:

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. **Document and implement a mitigation plan.**
- C. **Agree on a strategy to mitigate risks.**
- D. **Evaluate mitigation progress and plan next assessment.**

Explanation

Phase 3 is mitigation planning, so it includes deciding how to address the identified risks, documenting and implementing that plan, and reviewing progress to determine when the next assessment is needed. Identifying the threats, vulnerabilities, and controls to evaluate is an earlier assessment activity, not mitigation planning.

✗ **A** Identify threats, vulnerabilities, and controls that will be evaluated.
This identifies what will be examined during risk assessment. It precedes the mitigation-planning activities in phase 3.

✓ **B** Document and implement a mitigation plan.
Documenting and putting the selected response into action are core parts of mitigation planning. This directly addresses how the risks will be treated.

✓ **C** Agree on a strategy to mitigate risks.
Choosing and agreeing on a risk-mitigation strategy is a key planning decision in phase 3. The strategy guides the mitigation plan.

✓ **D** Evaluate mitigation progress and plan next assessment.
Reviewing progress checks whether mitigation is advancing as intended and helps determine the next assessment. These activities support the mitigation-planning phase described in the question.

Free demo · full exam: 725 questions

Question 22

Single choice · Domain: D1 Security and Privacy Governance, Risk Management, and Compliance Program › 1.1 - Demonstrate knowledge in security and privacy governance, risk management, and compliance program

Which of the following C&A professionals plays the role of an advisor?

Response:

A. Information System Security Engineer (ISSE)
B. Chief Information Officer (CIO)
C. Authorizing Official
D. Information Owner

Answer: A. Information System Security Engineer (ISSE)

Explanation

The Information System Security Engineer (ISSE) serves in an advisory and engineering-support capacity in the certification and accreditation (C&A) process. The ISSE helps address security requirements and controls, while the Authorizing Official makes the authorization decision and the CIO and Information Owner have different organizational responsibilities.

✓ **A** Information System Security Engineer (ISSE)
The ISSE provides security engineering expertise and advises on how security requirements and controls are addressed for the system. That advisory role makes this the correct choice.

✗ **B** Chief Information Officer (CIO)
The CIO is a senior information-technology leader, not the C&A professional identified as the advisor in this question. The ISSE provides the relevant security-engineering advice.

✗ **C** Authorizing Official
The Authorizing Official is responsible for deciding whether to authorize the system to operate, rather than serving as its security-engineering advisor. That advisory function belongs to the ISSE.

✗ **D** Information Owner
The Information Owner is concerned with responsibility for the information and its protection requirements, not the C&A advisory role asked about here. The ISSE is the advisor among these choices.

Free demo · full exam: 725 questions

Question 23

Single choice · Domain: D1 Security and Privacy Governance, Risk Management, and Compliance Program › 1.1 - Demonstrate knowledge in security and privacy governance, risk management, and compliance program

Who initiates system authorization process and has the full responsibility over the life cycle of an information system?

Response:

A. Security Control Assessor (SCA) and Risk Executive
B. Information System Owner (ISO)
C. Authorizing Official (AO)
D. Information System Security Officer (ISSO)

Answer: B. Information System Owner (ISO)

Explanation

The Information System Owner (ISO) is responsible for the information system across its life cycle and initiates the system authorization process. The Authorizing Official makes the authorization decision, while the assessor and security officer perform supporting assessment and security duties; those roles do not hold the ISO's full life-cycle responsibility. [1][10]

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
https://csrc.nist.gov/glossary/term/information_system_owner

✗ **A** Security Control Assessor (SCA) and Risk Executive
The SCA assesses security controls, and the Risk Executive provides organization-level risk perspective. Neither role is the system owner responsible for its full life cycle and for initiating its authorization process.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
https://csrc.nist.gov/files/pubs/sp/800/37/r1/final/docs/sp800-37-rev1-final.pdf

✓ **B** Information System Owner (ISO)
The Information System Owner is responsible for the information system throughout its life cycle and initiates the system authorization process. This matches both responsibilities asked about in the question.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
https://csrc.nist.gov/glossary/term/information_system_owner

✗ **C** Authorizing Official (AO)
The AO reviews the authorization package and makes the risk-based authorization decision. That is distinct from owning the system throughout its life cycle and initiating its authorization process.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
https://csrc.nist.gov/files/pubs/sp/800/37/r1/final/docs/sp800-37-rev1-final.pdf

✗ **D** Information System Security Officer (ISSO)
The ISSO supports information-system security activities, but does not hold the system owner's full life-cycle responsibility or initiate the authorization process in that capacity.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
https://csrc.nist.gov/files/pubs/sp/800/37/r1/final/docs/sp800-37-rev1-final.pdf

Free demo · full exam: 725 questions

Question 24

Single choice · Domain: D1 Security and Privacy Governance, Risk Management, and Compliance Program › 1.2 - Demonstrate knowledge in security and privacy governance, risk management and compliance program processes

Which of the following RMF phases is known as risk analysis?

Response:

A. Phase 2
B. Phase 1
C. Phase 0
D. Phase 3

Answer: A. Phase 2

Explanation

Phase 2 is the phase identified as risk analysis, so option A answers the question. The other options name different phases and do not match the requested phase.

✓ **A** Phase 2
This is the phase identified as risk analysis in the question's RMF phase numbering.

✗ **B** Phase 1
Phase 1 is not the phase identified as risk analysis; the correct choice is Phase 2.

✗ **C** Phase 0
Phase 0 is not the phase identified as risk analysis; the correct choice is Phase 2.

✗ **D** Phase 3
Phase 3 is not the phase identified as risk analysis; the correct choice is Phase 2.

Question 25

Multiple choice · Domain: D1 Security and Privacy Governance, Risk Management, and Compliance Program › 1.1 - Demonstrate knowledge in security and privacy governance, risk management, and compliance program

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.

Response:

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

Free demo · full exam: 725 questions

Answer

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

Explanation

The CIO is the senior executive responsible for aligning the enterprise's technology with its goals and ensuring that plans can be carried out within budget. The role also includes organizational leadership and establishing an effective continuous monitoring program. Sharing security risk information specifically among authorizing officials is not the CIO responsibility described here.

✓ **A** Preserving high-level communications and working group relationships in an organization
This is an organizational leadership responsibility that supports coordination across the enterprise. A CIO can help maintain the high-level communication and working relationships needed to align IT activities with organizational needs.

✗ **B** Facilitating the sharing of security risk-related information among authorizing officials
This describes coordination of risk information among authorizing officials, rather than the CIO's broader executive responsibilities for enterprise IT. It is therefore not one of the correct choices in this question.

✓ **C** Establishing effective continuous monitoring program for the organization
Establishing an effective organization-wide continuous monitoring program is part of ensuring that IT and security activities are governed and monitored. This fits the CIO's senior responsibility for the enterprise's IT program.

✓ **D** Proposing the information technology needed by an enterprise to achieve its goals and then working within a budget to implement the plan
This directly describes strategic IT planning: identifying technology needed to meet enterprise goals and implementing the plan within budget. Those are central responsibilities of a CIO.

Question 26

Single choice · Domain: D2 Scope of the System › 2.1 - Describe the system

A complex system of systems composed of subsystems and services that are part of a continuously evolving, complex community of people, devices, information and services interconnected by a network that enhances information sharing and collaboration. Subsystems and services may or may not be developed or owned by the same entity, and, in general, will not be continually present during the full lifecycle of the system of systems.

Response:

A. Net-Centric Architecture
B. Federal Enterprise Architecture
C. Event-Driven Architecture
D. Industry Standard Architecture

Free demo · full exam: 725 questions

Answer: A. Net-Centric Architecture

Explanation

Net-Centric Architecture is the best match because the description centers on a network-connected community that enables information sharing and collaboration. It also describes a system of systems whose subsystems and services may have different owners and may not remain present throughout the overall system's lifecycle. Those characteristics distinguish it from the specific enterprise, event-driven, and hardware-bus architectures in the other options.

✓ **A** Net-Centric Architecture
This architecture fits the described system of systems: independently developed or owned subsystems and services are interconnected through a network. The network supports information sharing and collaboration among a changing community of people, devices, information, and services.

✗ **B** Federal Enterprise Architecture
Federal Enterprise Architecture is a framework for organizing and describing government agency business, data, applications, and technology. The question instead defines a networked, evolving community of potentially independent systems and services.

✗ **C** Event-Driven Architecture
Event-Driven Architecture organizes software interactions around the production, detection, and response to events. The description focuses on network-based interconnection and collaboration across a system of systems, not event-triggered communication.

✗ **D** Industry Standard Architecture
Industry Standard Architecture refers to a computer expansion-bus standard, not an architecture for an evolving networked system of systems. It does not account for the described community of people, devices, information, and independently owned services.

Question 27

Single choice · Domain: D2 Scope of the System › 2.2 - Determine security compliance required

The potential impact is high if-The loss of confidentiality, integrity, or availability could be expected to have a.....

Response:

A. severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

B. limited adverse effect on organizational operations, organizational assets, or individuals.

C. no adverse effect on organizational operations, organizational assets, or individuals.

D. serious adverse effect on organizational operations, organizational assets, or individuals

Answer: A. severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Explanation

NIST defines a high potential impact as one in which loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. Therefore, option A completes the statement correctly.

https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf
https://csrc.nist.gov/glossary/term/potential_impact

✓ **A** severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
This is the NIST definition of a high potential impact: the loss could cause severe or catastrophic harm to operations, assets, or individuals.

https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf
https://csrc.nist.gov/glossary/term/potential_impact

✗ **B** limited adverse effect on organizational operations, organizational assets, or individuals.
A limited adverse effect describes a low potential impact, not a high one. The question asks for the impact level associated with severe consequences.

https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf

✗ **C** no adverse effect on organizational operations, organizational assets, or individuals.
No adverse effect does not meet the definition of high potential impact. High impact requires the possibility of severe or catastrophic harm.

https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf

✗ **D** serious adverse effect on organizational operations, organizational assets, or individuals
Although serious harm sounds substantial, it is not the wording of the high-impact category in the NIST definition. The specified level is severe or catastrophic adverse effect.

https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf

Question 28

Single choice · Domain: D2 Scope of the System › 2.2 - Determine security compliance required required

The Security Category that primarily deals with ensuring timely and reliable access to information.

Response:

A. Availability
B. Authenticity
C. Confidentiality
D. Integrity

Answer: A. Availability

Explanation

Availability is the security category concerned with ensuring information and systems can be accessed reliably and when needed. The question specifically describes timely and reliable access, so Availability is the correct choice.

https://www.isc2.org/certifications/cissp/cissp-student-glossary
https://www.isc2.org/certifications/cc/cc-certification-exam-outline

✓ **A** Availability
Availability means information and systems are accessible to authorized users when needed. That directly

Free demo · full exam: 725 questions

matches the requirement for timely and reliable access.

https://www.isc2.org/certifications/cissp/cissp-student-glossary
https://www.isc2.org/certifications/cc/cc-certification-exam-outline

✗ **B** Authenticity
Authenticity concerns verifying that an identity, source, or information is genuine. It does not primarily address whether information is available reliably and on time.

https://www.isc2.org/certifications/cissp/cissp-student-glossary

✗ **C** Confidentiality
Confidentiality protects information from unauthorized disclosure. The question asks about access being timely and reliable, not restricting who can see the information.

https://www.isc2.org/certifications/cissp/cissp-student-glossary
https://www.isc2.org/certifications/cc/cc-certification-exam-outline

✗ **D** Integrity
Integrity concerns protecting information from improper alteration or destruction and preserving its accuracy. It does not primarily ensure timely, reliable access.

https://www.isc2.org/certifications/cissp/cissp-student-glossary
https://www.isc2.org/certifications/cc/cc-certification-exam-outline

Question 29

Single choice · Domain: D2 Scope of the System › 2.1 - Describe the system

The term relates to the system as a whole where as Sensitivity relates to the data that the system processes.

Response:

A. Criticality
B. Sensitivity
C. Availability

Answer: A. Criticality

Explanation

Criticality describes the importance or business impact of a system as a whole, while sensitivity describes how important or protected the data processed by that system is. The question contrasts the system-level concept with the data-level concept, so Criticality is the correct choice.

https://www.isc2.org/certifications/cissp/cissp-student-glossary

✓ **A** Criticality
Criticality concerns the significance of the system itself, such as the impact if the system is unavailable or compromised. That matches the system-level concept contrasted with data Sensitivity in the question.

https://www.isc2.org/certifications/cissp/cissp-student-glossary

✗ **B** Sensitivity
Sensitivity describes the data and the level of protection it requires, not the importance of the system as a whole. The question already assigns Sensitivity to the data.

https://www.isc2.org/certifications/cissp/cissp-student-glossary

✗ **C** Availability

Free demo · full exam: 725 questions

Availability is the property of being accessible and usable when needed. It does not name the system-level importance that is contrasted with data Sensitivity here.

Question 30

Single choice · Domain: D2 Scope of the System › 2.1 - Describe the system

When attempting to categorize a system, which two RMF starting point inputs should be accounted for?

Response:

A. Federal laws and organizational policies
B. Federal laws and OMB policies
C. Architecture descriptions and organizational inputs
D. FISMA and the Privacy Act

Answer: C. Architecture descriptions and organizational inputs

Explanation

The RMF system-categorization starting point uses architecture descriptions together with organizational inputs. These provide context about the system and the organization needed to determine its security categorization, so option C is correct.

✗ **A** Federal laws and organizational policies
Federal laws and organizational policies can impose requirements, but they are not the two starting-point inputs identified for categorizing a system in this question. The stated inputs are architecture descriptions and organizational inputs.

✗ **B** Federal laws and OMB policies
These are sources of legal or policy requirements, not the paired RMF starting-point inputs for system categorization. This option does not include either of the expected input categories as a pair.

✓ **C** Architecture descriptions and organizational inputs
These are the two inputs to account for when beginning RMF system categorization. Architecture descriptions provide information about the system, while organizational inputs supply relevant context from the organization.

✗ **D** FISMA and the Privacy Act
FISMA and the Privacy Act are laws, not the two RMF starting-point inputs requested. They may shape compliance obligations, but they do not form the architecture-and-organization input pair.

Free demo · full exam: 725 questions

Question 31

Single choice · Domain: D2 Scope of the System › 2.2 - Determine security compliance required

According to NIST SP 800-60v2r1, intellectual property protection information type may be categorized as low but trade secrets are categorized as:

Response:

A. Moderate for confidentiality
B. High for confidentiality
C. Moderate for integrity
D. Moderate for availability

Answer: B. High for confidentiality

Explanation

NIST SP 800-60 Vol. 2 Rev. 1 distinguishes general intellectual property protection information, which may be categorized as low, from trade secrets. Trade secrets require high confidentiality because unauthorized disclosure could cause serious harm, so option B is correct.

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-60v2r1.pdf

✗ **A** Moderate for confidentiality
This does not match the categorization for trade secrets in NIST SP 800-60 Vol. 2 Rev. 1. The specified confidentiality impact level is high, not moderate.

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-60v2r1.pdf

✓ **B** High for confidentiality
NIST categorizes trade secrets as high for confidentiality. Disclosure of trade secrets can seriously harm the organization, distinguishing them from intellectual property protection information that may be categorized as low.

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-60v2r1.pdf

✗ **C** Moderate for integrity
The question asks for the trade-secret categorization, which is a high confidentiality impact. Moderate integrity is not the categorization identified for trade secrets here.

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-60v2r1.pdf

✗ **D** Moderate for availability
This describes an availability impact level, not the relevant confidentiality categorization. NIST identifies trade secrets as high for confidentiality.

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-60v2r1.pdf

Free demo · full exam: 725 questions

Question 32

Single choice · Domain: D2 Scope of the System › 2.1 - Describe the system

What are the three primary considerations for defining system boundaries?

Response:

A. 1. Normally be under the same direct management control. 2. Usually support the same mission/ business objectives or functions and have the same basic operating characteristics and information security requirements. 3. Reside in the same general operating environment or in various locations with like operating environments in the case of a distributed information system.

B. 1. Abnormally be under the same direct management control. 2. Usually support the same mission/business objectives or functions and have the same basic operating characteristics and information security requirements. 3. Reside in the same general operating environment or in various locations with like operating environments in the case of a distributed information system.

C. 1. Normally be under the same indirect management control. 2. Usually support the same mission/business objectives or functions and have the same basic operating characteristics and information security requirements. 3. Reside in the same general operating environment or in various locations with like operating environments in the case of a distributed information system.

D. 1. Normally be under the same direct management control. 2. Unusually support the same mission/business objectives or functions and have the same basic operating characteristics and information security requirements. 3. Reside in the same general operating environment or in same locations with like operating environments in the case of a distributed information system.

Answer: A. 1. Normally be under the same direct management control. 2. Usually support the same mission/business objectives or functions and have the same basic operating characteristics and information security requirements. 3. Reside in the same general operating environment or in various locations with like operating environments in the case of a distributed information system.

Explanation

A is correct because system boundaries are defined using three considerations: systems normally share direct management control, support the same mission or business functions with similar operating and security characteristics, and operate in the same or like environments. The other options change one or more of these requirements, such as substituting indirect control or unusual support, or altering the location criterion. [1]

https://csrc.nist.gov/csrc/media/projects/risk-management/documents/categorize/faq-categorize-step1.pdf

✓ **A** 1. Normally be under the same direct management control. 2. Usually support the same mission/ business objectives or functions and have the same basic operating characteristics and information security requirements. 3. Reside in the same general operating environment or in various locations with like operating environments in the case of a distributed information system.
This correctly states all three considerations: normally the same direct management control, usually shared mission or functions and similar operating and security characteristics, and the same or like operating environments. These considerations allow a distributed system to span locations when its environments are alike. [1]

https://csrc.nist.gov/csrc/media/projects/risk-management/documents/categorize/faq-categorize-step1.pdf

✗ **B** 1. Abnormally be under the same direct management control. 2. Usually support the same mission/ business objectives or functions and have the same basic operating characteristics and information security requirements. 3. Reside in the same general operating environment or in various locations with

Free demo · full exam: 725 questions

like operating environments in the case of a distributed information system.
The management-control consideration is misstated: the systems should normally, not abnormally, be under the same direct management control. The other two considerations match the required wording, but that change makes the option incorrect. [1]

https://csrc.nist.gov/csrc/media/projects/risk-management/documents/categorize/faq-categorize-step1.pdf

✗ **C** 1. Normally be under the same indirect management control. 2. Usually support the same mission/ business objectives or functions and have the same basic operating characteristics and information security requirements. 3. Reside in the same general operating environment or in various locations with like operating environments in the case of a distributed information system.
The first consideration specifies the same direct management control, not indirect management control. The mission, operating-characteristics, security, and environment considerations are otherwise stated correctly. [1]

https://csrc.nist.gov/csrc/media/projects/risk-management/documents/categorize/faq-categorize-step1.pdf

✗ **D** 1. Normally be under the same direct management control. 2. Unusually support the same mission/ business objectives or functions and have the same basic operating characteristics and information security requirements. 3. Reside in the same general operating environment or in same locations with like operating environments in the case of a distributed information system.
The second consideration says systems usually support the same mission or functions, not unusually. The third also changes the allowance for distributed systems: they may be in various locations with like operating environments, rather than being limited to the same locations. [1]

https://csrc.nist.gov/csrc/media/projects/risk-management/documents/categorize/faq-categorize-step1.pdf

Dumpsgate

Question 33

Single choice · Domain: D2 Scope of the System › 2.1 - Describe the system

Organization official that's responsible for procurement, development, integration, modification, operation, maintenance, and disposal of an Information System.

Response:

A. Information System Owner
B. Authorizing Official
C. Information Security Architect
D. Chief Information Officer

Answer: A. Information System Owner

Explanation

The Information System Owner is the organization official responsible for the system across its lifecycle, including procurement, development, integration, modification, operation, maintenance, and disposal. That matches the full set of responsibilities in the question. The other roles focus on authorization decisions, security architecture, or organization-wide information technology leadership rather than ownership of this system's lifecycle.

✓ **A** Information System Owner
This is the official responsible for the information system throughout its lifecycle. The listed duties—from procurement and development through operation, maintenance, and disposal—match the role described in the question.

Free demo · full exam: 725 questions

✗ **B** Authorizing Official
An Authorizing Official makes the decision to authorize a system to operate, typically based on its security risk. That authorization responsibility does not make the official responsible for carrying out the system's full lifecycle activities listed here.

✗ **C** Information Security Architect
An Information Security Architect designs or advises on security architecture. That role does not encompass organizational responsibility for procuring, operating, maintaining, and disposing of the entire information system.

✗ **D** Chief Information Officer
A Chief Information Officer provides leadership for an organization's information technology function. The question asks for the official accountable for the lifecycle of a particular information system, which is the Information System Owner.

Question 34

Single choice · Domain: D2 Scope of the System › 2.1 - Describe the system

What are the three tools necessary for managing the inventory program?

Response:

A. 1. Inventory form. 2. Inventory change form. 3. Organization inventory summary.
B. 1. Inventory change form. 2. Organization inventory summary. 3. Inventory form.
C. 1. Acquisition/Development 2. Inventory change form. 3. Organization inventory summary.
D. 1. Acquisition/Development 2. Organization inventory summary. 3. Inventory change form.

Answer: A. 1. Inventory form. 2. Inventory change form. 3. Organization inventory summary.

Explanation

The inventory program is managed using the inventory form, the inventory change form, and the organization inventory summary. Option A gives these three tools in the specified sequence; the other choices either change that sequence or substitute Acquisition/Development for one of the tools. [1]

https://community.isc2.org/ijoyk78323/attachments/ijoyk78323/industry-news/6754/1/cfdir-quantum-readiness-best-practices-v03.pdf?inline=true

✓ **A** 1. Inventory form. 2. Inventory change form. 3. Organization inventory summary.
This lists the three tools used to manage the inventory program in the specified order: the inventory form, the form for recording changes, and the organization-level summary. [1]

https://community.isc2.org/ijoyk78323/attachments/ijoyk78323/industry-news/6754/1/cfdir-quantum-readiness-best-practices-v03.pdf?inline=true

✗ **B** 1. Inventory change form. 2. Organization inventory summary. 3. Inventory form.
It names the same three tools, but does not give them in the specified sequence. The inventory form is listed first, followed by the inventory change form and then the organization inventory summary. [1]

https://community.isc2.org/ijoyk78323/attachments/ijoyk78323/industry-news/6754/1/cfdir-quantum-readiness-best-practices-v03.pdf?inline=true

✗ **C** 1. Acquisition/Development 2. Inventory change form. 3. Organization inventory summary.
Acquisition/Development is not the inventory form, one of the three tools in the required set. This option therefore omits the inventory form. [1]

https://community.isc2.org/ijoyk78323/attachments/ijoyk78323/industry-news/6754/1/cfdir-quantum-readiness-best-

practices-v03.pdf?inline=true

✗ **D** 1. Acquisition/Development 2. Organization inventory summary. 3. Inventory change form.
This substitutes Acquisition/Development for the inventory form and also reverses the order of the last two tools. It does not match the specified set and sequence. [1]

https://community.isc2.org/ijoyk78323/attachments/ijoyk78323/industry-news/6754/1/cfdir-quantum-readiness-best-practices-v03.pdf?inline=true

Question 35

Single choice · Domain: D2 Scope of the System › 2.1 - Describe the system

An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency, or, as appropriate, any of its operational elements).

Response:

A. Organization
B. Information
C. Implementation
D. Operation

Answer: A. Organization

Explanation

The description defines an organization: an entity that can be of any size or complexity and can occupy any position in an organizational structure. A federal agency and its operational elements are examples of entities covered by that definition, so option A is correct. [3]

https://csrc.nist.gov/glossary/term/organization

✓ **A** Organization
This matches the definition in the question: an entity of any size, complexity, or position within an organizational structure. The federal-agency example also fits this meaning. [3]

https://csrc.nist.gov/glossary/term/organization

✗ **B** Information
The description is about an entity or structural unit, not information such as data or knowledge. Information is not the term that identifies a federal agency or one of its operational elements.

✗ **C** Implementation
Implementation refers to carrying out or putting something into effect; it does not name an entity within an organizational structure. The question asks for the kind of entity described, not an activity.

✗ **D** Operation
An operation is an activity or process, rather than the entity conducting it. The described federal agency or operational element is an organization.

Free demo · full exam: 725 questions

Question 36

Single choice · Domain: D2 Scope of the System › 2.1 - Describe the system

Who has the authority to divide a complex system in order to establish realistic security authorization boundaries?

Response:

A. Authorizing Official (AO) and Senior Information Security Officer (SISO)
B. Authorizing Official (AO) and Information System Security Officer (ISSO)
C. Security Control Assessor (SCA) and Risk Executive
D. Security Control Assessor (SCA) and Information System Security Officer (ISSO)

Answer: B. Authorizing Official (AO) and Information System Security Officer (ISSO)

Explanation

The Authorizing Official (AO) and Information System Security Officer (ISSO) are the correct pair for dividing a complex system to establish realistic security authorization boundaries. The AO is responsible for the authorization decision, while the ISSO supports the system's security and authorization activities; a Security Control Assessor evaluates controls rather than defining the boundary. [1][3]

https://www.isc2.org/Insights/2021/11/decisions-and-the-role-of-authorization
https://www.isc2.org/certifications/cgrc/cgrc-certification-exam-outline

✗ **A** Authorizing Official (AO) and Senior Information Security Officer (SISO)
The AO has an authorization role, but the SISO is not the system-level partner identified for establishing these boundaries. The ISSO works with the AO on the information system's security authorization activities.

https://www.isc2.org/Insights/2021/11/decisions-and-the-role-of-authorization
https://www.isc2.org/certifications/cgrc/cgrc-certification-exam-outline

✓ **B** Authorizing Official (AO) and Information System Security Officer (ISSO)
The AO and ISSO are the appropriate pair to divide a complex system into realistic security authorization boundaries. Their roles connect the authorization decision with the system-specific security work needed to define those boundaries.

https://www.isc2.org/Insights/2021/11/decisions-and-the-role-of-authorization
https://www.isc2.org/certifications/cgrc/cgrc-certification-exam-outline

✗ **C** Security Control Assessor (SCA) and Risk Executive
An SCA assesses security controls, and the Risk Executive provides organization-level risk perspective; neither is the designated system-level authorization partner for this task. The AO and ISSO are the relevant roles for establishing the system's authorization boundaries.

https://www.isc2.org/certifications/cgrc/cgrc-certification-exam-outline

✗ **D** Security Control Assessor (SCA) and Information System Security Officer (ISSO)
Although the ISSO has a system-specific security role, the SCA's function is to independently assess controls rather than to make the authorization-boundary decision with the ISSO. The AO, not the SCA, is the appropriate partner for this task.

https://www.isc2.org/Insights/2021/11/decisions-and-the-role-of-authorization
https://www.isc2.org/certifications/cgrc/cgrc-certification-exam-outline

Free demo · full exam: 725 questions

Question 37

Single choice · Domain: D3 Selection and Approval of Framework, Security, and Privacy Controls › 3.1 - Identify and document baseline and inherited controls

An organizational official responsible for the development, implementation, assessment, and monitoring of security controls inherited by information systems is called... Response:

A. Information System Security Engineer (ISSE)
B. Information System Owner (ISO)
C. Common Control Provider (CCP)
D. Chief Information Officer (CIO)

Answer: C. Common Control Provider (CCP)

Explanation

The role described is the Common Control Provider (CCP): it is responsible for developing, implementing, assessing, and monitoring security controls that information systems inherit. That responsibility distinguishes the CCP from roles focused on an individual system, engineering, or organizational IT leadership.

https://xmc-prod-vercel.isc2.org/certifications/cgrc/cgrc-certification-exam-outline
https://www.isc2.org/certifications/cgrc/cgrc-certification-exam-outline
https://xmc-qa-vercel.isc2.org/certifications/cgrc/cgrc-certification-exam-outline

✗ **A** Information System Security Engineer (ISSE)
An ISSE applies security engineering expertise to information systems and their security requirements. The question instead asks for the organizational official responsible for controls inherited by systems, which is the Common Control Provider.

https://www.isc2.org/certifications/issep/issep-certification-exam-outline
https://xmc-qa-vercel.isc2.org/certifications/issep/issep-certification-exam-outline
https://www.isc2.org/certifications/issep

✗ **B** Information System Owner (ISO)
An Information System Owner is associated with responsibility for a particular information system. The scenario describes responsibility for shared controls that other systems inherit, not ownership of an individual system.

https://xmc-prod-vercel.isc2.org/certifications/cgrc/cgrc-certification-exam-outline
https://www.isc2.org/certifications/cgrc/cgrc-certification-exam-outline
https://xmc-qa-vercel.isc2.org/certifications/cgrc/cgrc-certification-exam-outline

✓ **C** Common Control Provider (CCP)
A Common Control Provider is responsible for developing, implementing, assessing, and monitoring common security controls that information systems may inherit. Those duties match the description in the question.

https://xmc-prod-vercel.isc2.org/certifications/cgrc/cgrc-certification-exam-outline
https://www.isc2.org/certifications/cgrc/cgrc-certification-exam-outline
https://xmc-qa-vercel.isc2.org/certifications/cgrc/cgrc-certification-exam-outline

✗ **D** Chief Information Officer (CIO)
A CIO provides organizational leadership for information technology and related strategy. The specific responsibility for the lifecycle of controls inherited by information systems is assigned to the Common Control Provider, not the CIO.

Free demo · full exam: 725 questions

Question 38

Single choice · Domain: D3 Selection and Approval of Framework, Security, and Privacy Controls › 3.2 - Select and tailor controls

The RMF Step and task where the System Security Plan is initially approved by the AO or AODR.

Response:

A. RMF Step 2, Task 4
B. RMF Step 2, Task 2
C. RMF Step 2, Task 3
D. RMF Step 2, Task 1

Answer: A. RMF Step 2, Task 4

Explanation

The correct choice is RMF Step 2, Task 4. This task covers developing and documenting the System Security Plan and obtaining its initial approval from the Authorizing Official (AO) or AO Designated Representative (AODR), as stated in the question.

https://csrc.nist.gov/pubs/sp/800/37/r2/final

✓ **A** RMF Step 2, Task 4
This is the task identified for initial AO or AODR approval of the System Security Plan. It therefore matches the specific approval action asked about.

https://csrc.nist.gov/pubs/sp/800/37/r2/final

✗ **B** RMF Step 2, Task 2
Task 2 is not the task for obtaining initial approval of the System Security Plan by the AO or AODR. The question describes the approval action assigned to Task 4.

https://csrc.nist.gov/pubs/sp/800/37/r2/final

✗ **C** RMF Step 2, Task 3
Task 3 is not the task that specifies initial AO or AODR approval of the System Security Plan. Task 4 is the matching task.

https://csrc.nist.gov/pubs/sp/800/37/r2/final

✗ **D** RMF Step 2, Task 1
Task 1 is not the task for initial approval of the System Security Plan by the AO or AODR. The approval requirement in the question corresponds to Task 4.

https://csrc.nist.gov/pubs/sp/800/37/r2/final

Dumpsgate

Question 39

Single choice · Domain: D3 Selection and Approval of Framework, Security, and Privacy Controls › 3.2 - Select and tailor controls

Which of the following statements about role-based access control (RBAC) model is true?

Response:

A. In this model, the permissions are uniquely assigned to each user account.
B. In this model, a user can access resources according to his role in the organization.
C. In this model, the same permission is assigned to each user account.
D. In this model, the users canaccess resources according to their seniority.

Answer: B. In this model, a user can access resources according to his role in the organization.

Explanation

RBAC grants access through roles: permissions are associated with roles, and users receive access based on the role or roles assigned to them. Therefore, option B describes the model. RBAC does not inherently assign unique permissions to every user, give every user identical permissions, or determine access by seniority.

https://csrc.nist.gov/glossary/term/role_based_access_control
https://csrc.nist.gov/Projects/role-based-access-control/faqs

✗ **A** In this model, the permissions are uniquely assigned to each user account.
This describes assigning permissions directly to individual user accounts, rather than granting them through roles. In RBAC, permissions are associated with roles and users obtain them through their role assignments.

https://csrc.nist.gov/glossary/term/role_based_access_control
https://csrc.nist.gov/Projects/role-based-access-control/faqs

✓ **B** In this model, a user can access resources according to his role in the organization.
RBAC grants users access according to the roles assigned to them, with permissions associated with those roles. This is the defining idea of role-based access control.

https://csrc.nist.gov/glossary/term/role_based_access_control
https://csrc.nist.gov/Projects/role-based-access-control/faqs

✗ **C** In this model, the same permission is assigned to each user account.
RBAC does not require all users to have the same permissions. Users assigned different roles can receive different sets of permissions.

https://csrc.nist.gov/glossary/term/role_based_access_control
https://csrc.nist.gov/Projects/role-based-access-control/faqs

✗ **D** In this model, the users canaccess resources according to their seniority.
Seniority is not the basis of access in RBAC. Access is determined by the roles assigned to users and the permissions associated with those roles.

https://csrc.nist.gov/glossary/term/role_based_access_control
https://csrc.nist.gov/Projects/role-based-access-control/faqs

Free demo · full exam: 725 questions

Question 40

Single choice · Domain: D3 Selection and Approval of Framework, Security, and Privacy Controls › 3.2 - Select and tailor controls

Which of the following specifies security requirements for federal information and information systems in 17 security-related areas that represent a broad-based, balanced information security program?

Response:

A. Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems

B. FIPS 200, Minimum Security Requirements for Federal Information and Information Systems

C. Committee on National Security Systems (CNSS) Instruction No. 1253, Security Categorization and Control Selection for National Security Systems

D. Section 3541 Title 44 U.S.C. Federal Information Security Management Act of 2002

Answer: B. FIPS 200, Minimum Security Requirements for Federal Information and Information Systems

Explanation

FIPS 200 is the correct choice because it establishes minimum security requirements for federal information and information systems across 17 security-related areas. Those areas support a broad-based, balanced information security program, matching the question's description. [1][2]

https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf
https://csrc.nist.gov/pubs/fips/200/final

✗ **A** Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems
FIPS 199 establishes standards for categorizing federal information and information systems according to their security impact. It addresses categorization, not the minimum security requirements across 17 security-related areas described in the question. [3]

https://csrc.nist.gov/pubs/fips/199/final?trk=article-ssr-frontend-pulse_little-text-block

✓ **B** FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
FIPS 200 specifies minimum security requirements for federal information and information systems. It organizes those requirements across 17 security-related areas to provide a broad-based, balanced information security program. [1][2]

https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf
https://csrc.nist.gov/pubs/fips/200/final

✗ **C** Committee on National Security Systems (CNSS) Instruction No. 1253, Security Categorization and Control Selection for National Security Systems
CNSS Instruction No. 1253 concerns security categorization and control selection for national security systems. The question asks for the standard that specifies minimum security requirements across 17 areas for federal information and systems, which is FIPS 200.

✗ **D** Section 3541 Title 44 U.S.C. Federal Information Security Management Act of 2002
The Federal Information Security Management Act of 2002 established statutory responsibilities for federal information security, rather than specifying the particular 17-area set of minimum security requirements asked about here. FIPS 200 provides those requirements. [7][8]

https://csrc.nist.gov/nist-cyber-history/risk-management/chapter
https://csrc.nist.gov/Projects/risk-management/fisma-background

Free demo · full exam: 725 questions

Question 41

Single choice · Domain: D3 Selection and Approval of Framework, Security, and Privacy Controls › 3.1 - Identify and document baseline and inherited controls

Security controls that can support multiple information systems efficiently and effectively as a common capability.

Their implementation results in a security capability that is inheritable by multiple information systems; such as Network boundary defense, management constraints, personnel security, security of physical structures, etc..

Response:

A. Common Controls
B. Common Controls Provider
C. Inherited Control
D. Security Controls

Answer: A. Common Controls

Explanation

The description matches common controls: controls implemented once as a shared capability that supports multiple information systems and can be inherited by them. Network boundary defense, personnel security, and physical security are examples of capabilities that can be provided commonly. Therefore, option A is correct.

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf?4d18fa22_page=3&b542f830_page=5&bc45c90c_page=2
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

✓ **A** Common Controls
Common controls are security controls that support multiple information systems and are provided as a shared capability. The examples in the question, such as network boundary defense and personnel security, fit this definition.

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf?4d18fa22_page=3&b542f830_page=5&bc45c90c_page=2
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

✗ **B** Common Controls Provider
A common controls provider is the organization or entity responsible for implementing, assessing, and maintaining common controls. The question asks for the controls themselves, not the party that provides them.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
https://csrc.nist.gov/glossary/term/common_control_provider

✗ **C** Inherited Control
An inherited control is a control an information system receives from a common control provider rather than implementing itself. The question describes the shared controls that can be inherited, not the system's act of inheriting them.

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

✗ **D** Security Controls
Security controls is a broad category that includes controls designed for individual systems as well as

Free demo · full exam: 725 questions

controls shared across multiple systems. The question specifically describes the shared, inheritable subset: common controls.

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf?4d18fa22_page=3&b542f830_page=5&bc45c90c_page=2

Question 42

Single choice · Domain: D3 Selection and Approval of Framework, Security, and Privacy Controls › 3.2 - Select and tailor controls

A specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines.

The specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems.

Response:

A. Overlay
B. Safeguards
C. Baseline
D. Feature

Dumpsgate

Answer: A. Overlay

Explanation

The description matches an overlay: a specification of controls and related guidance used in tailoring to complement and further refine a security control baseline. An overlay may set requirements more or less stringent than the baseline and can apply to multiple information systems. Therefore, option A is correct. [1]

https://csrc.nist.gov/glossary/term/overlay

✓ **A** Overlay
An overlay is a tailored specification of security controls and related information that supplements or refines a baseline. It can be more or less stringent than the baseline and can apply to multiple systems, matching the description. [1]

https://csrc.nist.gov/glossary/term/overlay

✗ **B** Safeguards
Safeguards are protective measures, not the name for a specification used to complement and refine a security control baseline. The description specifically defines an overlay. [1]

https://csrc.nist.gov/glossary/term/overlay

✗ **C** Baseline
A baseline is the starting set of security controls, whereas the described specification is applied during tailoring to complement and further refine that baseline. [1]

https://csrc.nist.gov/glossary/term/overlay

✗ **D** Feature
“Feature” does not describe the defined specification of controls and supporting information used to

Free demo · full exam: 725 questions

tailor a baseline. The term that fits this description is overlay. [1]
https://csrc.nist.gov/glossary/term/overlay

Question 43

Single choice · Domain: D3 Selection and Approval of Framework, Security, and Privacy Controls › 3.1 - Identify and document baseline and inherited controls

The National Institutes of Standards and Technology (NIST) guidance classifies security controls as?

Response:

A. System-specific, Common and Hybrid
B. Production, development, and test.
C. People, process, and technology.
D. Technical, administrative, and program.

Answer: A. System-specific, Common and Hybrid

Explanation

NIST guidance classifies security controls by how they are implemented: as common controls, system-specific controls, or hybrid controls that combine both approaches. Therefore, option A is correct; the other choices describe different ways of grouping environments or security concepts, not this NIST classification.

✓ **A** System-specific, Common and Hybrid
These are the three implementation-based categories in the NIST control classification described by the question. Common controls are shared, system-specific controls apply to an individual system, and hybrid controls combine aspects of both.

✗ **B** Production, development, and test.
These are common environment or lifecycle labels, not NIST's categories for classifying security controls by implementation. The question asks about control classification, not system environments.

✗ **C** People, process, and technology.
This is a broad way to describe security considerations or resources, not the NIST implementation categories for security controls. It does not identify common, system-specific, and hybrid controls.

✗ **D** Technical, administrative, and program.
These terms refer to other possible groupings of controls or security activities, but they are not the NIST categories asked for here. NIST's relevant categories are common, system-specific, and hybrid.

Free demo · full exam: 725 questions

Question 44

Single choice · Domain: D3 Selection and Approval of Framework, Security, and Privacy Controls › 3.2 - Select and tailor controls

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

Response:

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

Explanation

A DACL controls access to an object by listing the users, groups, or computers whose access is allowed or denied. Therefore, option D best describes the DACL in this question.

✗ **A** It is a rule list containing access control entries.
This is too general to distinguish a DACL from other access-control lists. A DACL's entries specify which principals are allowed or denied access to the object, as described more specifically in option D.

✗ **B** It specifies whether an audit activity should be performed when an object attempts to access a resource.
This describes the purpose of a System Access Control List (SACL), which is used for auditing access attempts, not a DACL's access permissions.

✗ **C** It is a unique number that identifies a user, group,and computer account.
This describes a security identifier (SID), not a DACL. A DACL is a list of access-control entries governing access to an object.

✓ **D** It is a list containing user accounts, groups, and computers that are allowed (or denied) access to the object.
A DACL contains entries that grant or deny access to an object for users, groups, or other security principals. This directly matches the question's description of a DACL.

Free demo · full exam: 725 questions

Question 45

Single choice · Domain: D3 Selection and Approval of Framework, Security, and Privacy Controls › 3.2 - Select and tailor controls

NIST guidance classifies security controls as Response:

A. Production, development, and test.
B. Technical, Operational, Management.
C. System specific, common, and hybrid.
D. People, process, and technology

Answer: B. Technical, Operational, Management.

Explanation

The correct answer is B: NIST classifies security controls as technical, operational, and management controls. These categories describe the general nature of the controls; the other options use different ways of organizing environments, control implementation, or security concepts. [1]

https://csrc.nist.gov/glossary/term/security_controls

✗ **A** Production, development, and test.
These are types of system environments, not NIST's categories for security controls. They do not identify whether a control is technical, operational, or management-oriented.

✓ **B** Technical, Operational, Management.
This is the NIST classification of security controls by type. It distinguishes controls implemented through technology, operational procedures, and management practices.

https://csrc.nist.gov/glossary/term/security_controls

✗ **C** System specific, common, and hybrid.
These describe how controls are allocated or shared among systems and organizations, rather than the control-type classification asked for. The relevant types are technical, operational, and management.

✗ **D** People, process, and technology
People, process, and technology is a broad security framing, not the NIST control classification requested here. NIST's categories in this question are technical, operational, and management.

Question 46

Single choice · Domain: D3 Selection and Approval of Framework, Security, and Privacy Controls › 3.2 - Select and tailor controls

During which Risk Management Framework (RMF) step is the system security plan initially approved?

Response:

A. RMF Step 1 Categorize Information System
B. RMF Step 2 Select Security Controls
C. RMF Step 3 Implement Security Controls
D. RMF Step 5 Authorize Information System

Answer: B. RMF Step 2 Select Security Controls

Explanation

The system security plan is initially approved during RMF Step 2, Select Security Controls. That step establishes the controls and documents them in the plan before they are implemented. Step 5 is the later authorization decision, not the plan's initial approval.

✗ **A** RMF Step 1 Categorize Information System
Step 1 categorizes the system and its information according to impact. It does not initially approve the system security plan.

✓ **B** RMF Step 2 Select Security Controls
Step 2 selects the security controls and documents them in the system security plan, which is initially approved at this stage. Implementation and authorization occur in later steps.

✗ **C** RMF Step 3 Implement Security Controls
Step 3 puts the selected controls into operation and documents how they were implemented. The plan is initially approved in Step 2, before implementation.

✗ **D** RMF Step 5 Authorize Information System
Step 5 is where the authorizing official makes the authorization decision based on the system's security information. That is distinct from the plan's initial approval in Step 2.

Question 47

Single choice · Domain: D4 Implementation of Security and Privacy Controls › 4.2 - Implement selected controls

What is RMF Step 3?

Response:

A. Implement Controls
B. Select Controls
C. Assess Controls
D. Monitor

Free demo · full exam: 725 questions

Answer: A. Implement Controls

Explanation

In the six-step RMF sequence used by this question, Step 3 is Implement Controls: the organization puts the selected security controls into operation. Selecting controls comes before implementation, while assessing and monitoring them occur later.

https://www.isc2.org/Insights/2021/07/implementing-controls-assessment

✓ **A** Implement Controls
This is the answer identified by the question. In the six-step sequence, implementation follows control selection and precedes assessment, so Step 3 is Implement Controls.

https://www.isc2.org/Insights/2021/07/implementing-controls-assessment

✗ **B** Select Controls
Control selection is the step before implementation in the sequence, not Step 3 in the six-step ordering used here.

✗ **C** Assess Controls
Assessment occurs after the controls have been implemented, so it is a later RMF step.

https://www.isc2.org/Insights/2021/07/implementing-controls-assessment

✗ **D** Monitor
Monitoring is a later, ongoing RMF activity that follows implementation, assessment, and authorization; it is not Step 3.

https://www.isc2.org/Insights/2021/09/Security-Does-Not-End-with-Implementing-Controls

Question 48

Single choice · Domain: D4 Implementation of Security and Privacy Controls › 4.3 - Document control implementation

Which of the following is used to indicate that the software has met a defined quality level and is ready for mass distribution either by electronic means or by physical media?

Response:

A. RTM
B. CRO
C. DAA
D. ATM

Answer: A. RTM

Explanation

RTM means “Release to Manufacturing.” It indicates that the software has met its defined quality requirements and is approved for mass distribution, whether electronically or on physical media.

✓ **A** RTM
RTM stands for “Release to Manufacturing.” It is the status used when software has met its quality

Free demo · full exam: 725 questions

requirements and is ready for mass distribution.

✗ **B** CRO
CRO is not the release status described in the question. The required term is RTM, which indicates software is ready for mass distribution.

✗ **C** DAA
DAA does not indicate that software has passed its quality threshold and is ready for mass distribution. RTM is the term for that status.

✗ **D** ATM
ATM is not the designation for software approved for mass distribution after meeting its defined quality level. That designation is RTM.

Question 49

Single choice · Domain: D4 Implementation of Security and Privacy Controls › 4.3 - Document control implementation

Who is responsible for securing an information system, managing all security aspects of the system, and assembling the security accreditation package while serving as the point of contact for the security control assessor?

Response:

A. Information System Owner
B. Information System Security Officer (ISSO)
C. Common Control Provider (CCP)
D. Information System Security Engineer

Answer: B. Information System Security Officer (ISSO)

Explanation

The Information System Security Officer (ISSO) is responsible for the system's security activities, coordinating its security controls, assembling the security accreditation package, and acting as the contact for the security control assessor. These responsibilities match the role described in the question.

✗ **A** Information System Owner
The Information System Owner is accountable for the system and its overall risk and authorization decisions, but the duties in the question—managing security details, preparing the accreditation package, and coordinating with the assessor—identify the ISSO.

✓ **B** Information System Security Officer (ISSO)
The ISSO coordinates and manages the system's security activities and helps ensure security controls are addressed. The ISSO also assembles the security accreditation package and serves as the point of contact for the security control assessor, matching all the stated responsibilities.

✗ **C** Common Control Provider (CCP)
A Common Control Provider is responsible for implementing and documenting controls that can be inherited by multiple systems. That role does not match the system-specific security management and assessor-liaison responsibilities described here.

✗ **D** Information System Security Engineer
A security engineer focuses on engineering and integrating security requirements into the system. The question instead describes the ISSO's broader coordination, accreditation-package, and assessor-contact

Free demo · full exam: 725 questions

duties.

Question 50

Single choice · Domain: D4 Implementation of Security and Privacy Controls › 4.3 - Document control implementation

Functional description of security control implementation must include which of the following, primarily as related to technical controls employed in the system?

Response:

A. Planned inputs, expected behavior, and expected outputs.
B. Implementation statement and remediation plan.
C. Remediation plan and expected outputs
D. Planned inputs implementation statement and expected behavior

Answer: A. Planned inputs, expected behavior, and expected outputs.

Explanation

A functional description of a security control explains how it operates by identifying its planned inputs, the behavior expected when it processes them, and the outputs it should produce. Option A includes all three elements, which makes it the best fit for describing technical control implementation; remediation plans and implementation statements do not substitute for this operational description.

✓ **A** Planned inputs, expected behavior, and expected outputs.
These elements describe the control's functional operation: what it receives, how it is expected to act, and what it should produce. That directly addresses the requested functional description of technical controls.

✗ **B** Implementation statement and remediation plan.
An implementation statement and remediation plan may document status or corrective action, but they do not describe the control's planned inputs, behavior, and outputs. They therefore do not provide the functional description requested.

✗ **C** Remediation plan and expected outputs
Expected outputs are one part of a functional description, but a remediation plan concerns fixing deficiencies rather than explaining normal control operation. This choice also omits planned inputs and expected behavior.

✗ **D** Planned inputs implementation statement and expected behavior
This choice includes planned inputs and expected behavior, but it omits expected outputs, which are part of the functional description. An implementation statement does not make up for that missing element.

Free demo · full exam: 725 questions

Question 51

Single choice · Domain: D5 Assessment/Audit of Security and Privacy Controls › 5.2 - Conduct assessment/audit

When SCA conducted assessments are conducted in parallel with system development/acquisition & implementation; it "does not" permit early identification of weaknesses & cost-effective corrective action; True or False?

Response:

A. True
B. False

Answer: B. False

Explanation

The statement is false. Conducting security control assessments alongside system development, acquisition, and implementation can help identify weaknesses earlier and enable corrective action before they become more costly to address, so the claim that it does not permit this is incorrect.

https://csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-discussion-draft.pdf

✗ **A** True
This would affirm the claim that parallel SCA activities do not support early identification and cost-effective correction. That claim is incorrect: conducting assessments alongside development and implementation can reveal weaknesses early enough to address them more effectively.

https://csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-discussion-draft.pdf

✓ **B** False
This correctly rejects the claim. When SCA activities occur in parallel with system development, acquisition, and implementation, they can identify weaknesses early and support corrective action while changes are less costly.

https://csrc.nist.gov/CSRC/media/Publications/sp/800-37/rev-2/draft/documents/sp800-37r2-discussion-draft.pdf

Question 52

Single choice · Domain: D5 Assessment/Audit of Security and Privacy Controls › 5.1 - Prepare for assessment/audit

A planning estimate for the amount of days that it takes to assess a Moderate system is - days.

Response:

A. 3-5
B. 5-7
C. 3-6
D. 4-7

Answer: A. 3-5

Free demo · full exam: 725 questions

Question 53

Single choice · Domain: D5 Assessment/Audit of Security and Privacy Controls › 5.2 - Conduct assessment/audit

What type of testing is the Evaluation thru operation, movement, or adjustment under specific conditions to determine control success?

Response:

A. Demonstration
B. Inspection
C. Examination
D. Organization

Answer: A. Demonstration

Explanation

Demonstration is the correct choice because the question describes evaluating a control by operating, moving, or adjusting it under specified conditions to see whether it succeeds. That is a hands-on showing of the control in action, rather than a review of evidence or an unrelated organizational activity.

✓ **A** Demonstration
A demonstration evaluates a control by having it operated, moved, or adjusted under specific conditions. This directly matches the described way of determining whether the control works.

✗ **B** Inspection
Inspection generally involves looking at or reviewing an item or evidence. The question specifically describes operating or adjusting the control, which makes demonstration the better match.

✗ **C** Examination
Examination refers to reviewing or scrutinizing something, rather than evaluating it through operation or

Free demo · full exam: 725 questions

adjustment under specified conditions. The hands-on activity described points to demonstration.

✗ **D** Organization
Organization is not the testing approach described in the question. It does not refer to evaluating a control by operating, moving, or adjusting it.

Question 54

Multiple choice · Domain: D5 Assessment/Audit of Security and Privacy Controls › 5.3 - Prepare the initial assessment/ audit report

Which of the following are the objectives of the security certification documentation task?

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

Response:

A. To prepare the Plan of Action and Milestones (POAM) based on the security assessment
B. To provide the certification findings and recommendations to the information system owner
C. To assemble the final security accreditation package and then submit it to the authorizing o fficial
D. To update the system security plan based on the results of the security assessment

Answer

- A. **To prepare the Plan of Action and Milestones (POAM) based on the security assessment**
- B. **To provide the certification findings and recommendations to the information system owner**
- C. **To assemble the final security accreditation package and then submit it to the authorizing o fficial**
- D. **To update the system security plan based on the results of the security assessment**

Explanation

All four choices describe activities in the security certification documentation task: documenting assessment findings and recommendations, preparing the POA&M, updating the system security plan, and assembling and submitting the accreditation package. Together, these activities record the assessment results and provide the documentation the authorizing official needs for an accreditation decision.

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-37.pdf

✓ **A** To prepare the Plan of Action and Milestones (POAM) based on the security assessment
The POA&M records the security weaknesses identified during assessment and the planned actions for addressing them. Preparing it from the assessment results is part of documenting the certification findings.

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-37.pdf

✓ **B** To provide the certification findings and recommendations to the information system owner
The assessment findings and recommendations must be documented and communicated to the information system owner. This gives the owner a basis for addressing identified weaknesses and considering the certification results.

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-37.pdf

✓ **C** To assemble the final security accreditation package and then submit it to the authorizing o fficial

The certification documentation is assembled into the security accreditation package for the authorizing official. Submitting that package provides the documentation needed for the accreditation decision.

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-37.pdf

✓ **D** To update the system security plan based on the results of the security assessment
The system security plan is updated to reflect the assessment results, including any changes needed to accurately describe the system's security controls. This update is one of the documentation activities associated with certification.

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-37.pdf

Question 55

Single choice · Domain: D5 Assessment/Audit of Security and Privacy Controls › 5.2 - Conduct assessment/audit

There are different types of control assessments depending on the assessment objectives. Which of the following is not a type of control assessments?

Response:

A. Developmental testing and evaluation
B. Risk assessment
C. Indipendent verification and validation
D. Audits

Answer: B. Risk assessment

Explanation

Risk assessment is not a type of control assessment: it identifies and evaluates risks, rather than assessing how a control is designed or performs. Developmental testing and evaluation, independent verification and validation, and audits are control-assessment approaches, so B is the option that does not fit.

https://www.isc2.org/Insights/2021/07/implementing-controls-assessment

✗ **A** Developmental testing and evaluation
This is a control-assessment approach used to evaluate controls as they are developed or implemented. It is therefore one of the assessment types, not the answer to which choice is not a type.

https://www.isc2.org/Insights/2021/07/implementing-controls-assessment

✓ **B** Risk assessment
A risk assessment identifies and analyzes risks; it is not itself an assessment of a control. It is the choice that does not belong with the control-assessment types listed.

https://www.isc2.org/Insights/2021/07/implementing-controls-assessment

✗ **C** Indipendent verification and validation
Independent verification and validation assess whether controls or system components meet specified requirements and operate as intended. Despite the misspelling in the option, this is a control-assessment type.

https://www.isc2.org/Insights/2021/07/implementing-controls-assessment

✗ **D** Audits
Audits provide an assessment of controls, including whether they are appropriately implemented and operating. Therefore, audits are a type of control assessment.

Free demo · full exam: 725 questions

https://www.isc2.org/Insights/2021/07/implementing-controls-assessment

Question 56

Single choice · Domain: D5 Assessment/Audit of Security and Privacy Controls › 5.4 - Review initial assessment/audit report and plan risk response actions

An updated risk assessment in response to the security control assessment along with inputs from the risk executive helps to determine and prioritize... Response:

A. Plan of action and milestones
B. Initial remediation actions
C. Failed controls
D. Control reassessments

Answer: B. Initial remediation actions

Explanation

The updated risk assessment incorporates findings from the security control assessment and the risk executive's input to identify and prioritize what should be addressed first. These are initial remediation actions, so option B is correct.

✗ **A** Plan of action and milestones
A plan of action and milestones documents planned corrective work, but the question asks what the updated risk assessment and risk executive input help determine and prioritize. That is the initial remediation actions, which can then inform the plan.

✓ **B** Initial remediation actions
The assessment findings and risk executive's input help establish which remediation steps should be taken first. This directly matches the question's focus on determining and prioritizing initial actions.

✗ **C** Failed controls
A security control assessment identifies controls that fail to meet requirements; the updated risk assessment uses such findings along with risk executive input. The requested outcome is the prioritized response to those findings, not the identification of failed controls.

✗ **D** Control reassessments
Control reassessments evaluate controls again after changes or remediation. They are not the initial actions prioritized based on the updated risk assessment and risk executive input.

Question 57

Single choice · Domain: D5 Assessment/Audit of Security and Privacy Controls › 5.2 - Conduct assessment/audit

Prior to completion of the security assessment report (SAR), what type of analysis is performed when agile, iterative development is used?

Response:

A. Regression analysis
B. Interim assessment
C. Incremental assessment
D. Executive assessment

Answer: C. Incremental assessment

Explanation

With agile, iterative development, security assessment is performed incrementally as the system is developed, rather than waiting until the entire effort is complete. Those incremental assessment results are available before completion of the final security assessment report (SAR).

✗ **A** Regression analysis
Regression analysis checks whether changes have caused previously working functionality or controls to fail. It is not the type of security assessment performed across development increments before the SAR is complete.

✗ **B** Interim assessment
An interim assessment is a broad description of an assessment conducted before a final one, but the question specifically ties the analysis to agile, iterative development. The assessment is performed incrementally as development progresses.

✓ **C** Incremental assessment
Agile, iterative development delivers the system in increments, allowing security assessment to be conducted alongside those increments. This provides assessment results before the final SAR is completed.

✗ **D** Executive assessment
An executive assessment suggests a high-level review for leadership, not security assessment carried out alongside iterative development. It does not describe the method asked about in this scenario.

Free demo · full exam: 725 questions

Question 58

Single choice · Domain: D5 Assessment/Audit of Security and Privacy Controls › 5.6 - Develop risk response plan

What should the system owner use to prioritize mitigation actions when developing the plan of action and milestones (POA&M)?

Response:

A. Budget constraints
B. Risk assessment results
C. Continuous monitoring strategy
D. Recommendations of the information owners

Answer: B. Risk assessment results

Explanation

The system owner should use risk assessment results to prioritize POA&M mitigation actions. These results identify and characterize risks, helping the owner address the most significant risks first rather than prioritizing based on budget, monitoring plans, or stakeholder recommendations alone. [2][8]

https://csrc.nist.gov/csrc/media/projects/risk-management/documents/05-assess%20step/nist%20rmf%20assess%20step-faqs.pdf
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf

✗ **A** Budget constraints
Budget constraints may affect which mitigation actions can be funded or when they can be completed, but they do not indicate which risks should be treated as the highest priority. Prioritization should be grounded in the risk assessment results. [8]

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf

✓ **B** Risk assessment results
Risk assessment results characterize risks and provide the basis for deciding which mitigation actions should be prioritized in the POA&M. This aligns remediation planning with the assessed significance of the risks. [2][8]

https://csrc.nist.gov/csrc/media/projects/risk-management/documents/05-assess%20step/nist%20rmf%20assess%20step-faqs.pdf
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf

✗ **C** Continuous monitoring strategy
A continuous monitoring strategy guides ongoing observation and assessment of security controls and risks; it is not the primary basis for ranking mitigation actions in the POA&M. The risk assessment results provide that prioritization basis. [1][2]

https://csrc.nist.gov/CSRC/media/Projects/Risk-Management/documents/monitor/faq_monitor-step6.pdf
https://csrc.nist.gov/csrc/media/projects/risk-management/documents/05-assess%20step/nist%20rmf%20assess%20step-faqs.pdf

✗ **D** Recommendations of the information owners
Information owners may provide useful input, but their recommendations alone do not establish the relative severity of risks requiring mitigation. The system owner should prioritize actions using the risk assessment results. [2][8]

https://csrc.nist.gov/csrc/media/projects/risk-management/documents/05-assess%20step/nist%20rmf%20assess%20step-faqs.pdf
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf

Free demo · full exam: 725 questions

Question 59

Single choice · Domain: D5 Assessment/Audit of Security and Privacy Controls › 5.2 - Conduct assessment/audit

Which if the following is an example of the test assessment method?

Response:

A. Reading vulnerability scan policies and procedures
B. Asking administrators about the scanning process
C. Conducting a vulnerability scan on web applications
D. Reviewing the most recent scan reports

Answer: C. Conducting a vulnerability scan on web applications

Explanation

Conducting a vulnerability scan on web applications is a test assessment method because it directly exercises the systems being assessed to observe how they respond and identify vulnerabilities. The other options use interviews or review existing documentation and reports rather than testing the applications themselves.

✗ **A** Reading vulnerability scan policies and procedures
This is a review of written documentation, not a test of the web applications. It can show what the scanning process is supposed to be, but it does not directly assess system behavior.

✗ **B** Asking administrators about the scanning process
This is an interview or inquiry method. It gathers administrators' descriptions of the process rather than actively testing the applications.

✓ **C** Conducting a vulnerability scan on web applications
A vulnerability scan actively probes the web applications to test for security weaknesses. Directly exercising the target systems makes this the test assessment method.

✗ **D** Reviewing the most recent scan reports
This examines records of prior assessment results, rather than conducting a test. It is a review of existing evidence, not a direct test of the applications.

Question 60

Single choice · Domain: D5 Assessment/Audit of Security and Privacy Controls › 5.1 - Prepare for assessment/audit

The scope of certification normally addresses all NIST SP control families with the purpose of uncovering design, implementation, and operational flows in those controls.

Response:

A. NIST SP 800-53
B. NIST SP 800-37
C. NIST SP 800-53A
D. NIST SP 800-39

Answer: C. NIST SP 800-53A

Explanation

NIST SP 800-53A is the assessment guide for evaluating security and privacy controls from SP 800-53. Its assessment procedures help determine whether controls are designed, implemented, and operating as intended across the control families, matching the question's focus on examining those control flows. Therefore, option C is correct.

https://csrc.nist.gov/pubs/sp/800/53/a/final
https://csrc.nist.gov/glossary/term/assessment

✗ **A** NIST SP 800-53
SP 800-53 provides the catalog of security and privacy controls, rather than the assessment procedures used to examine their design, implementation, and operation. The question describes the assessment focus associated with SP 800-53A.

https://csrc.nist.gov/projects/risk-management/sp800-53-controls

✗ **B** NIST SP 800-37
SP 800-37 describes the Risk Management Framework and its processes for managing security and privacy risk. It is not the publication that supplies procedures for assessing individual controls across the families.

✓ **C** NIST SP 800-53A
SP 800-53A provides assessment procedures for determining whether controls are implemented correctly, operating as intended, and producing the desired outcome. That directly matches the question's focus on uncovering control design, implementation, and operational flows.

https://csrc.nist.gov/pubs/sp/800/53/a/final
https://csrc.nist.gov/glossary/term/assessment

✗ **D** NIST SP 800-39
SP 800-39 addresses organization-wide information security risk management. The question instead asks about assessing controls across NIST SP control families, which is the role of SP 800-53A.

Free demo · full exam: 725 questions

Question 61

Single choice · Domain: D5 Assessment/Audit of Security and Privacy Controls › 5.1 - Prepare for assessment/audit

Which of the following in an assessment plan protects the security control assessment team from liability should the security control assessment result in unforeseen damage?

Response:

A. Non-invasive testing
B. Manual testing
C. Vulnerability scans
D. Rules of engagement

Answer: D. Rules of engagement

Explanation

Rules of engagement define the authorized scope, conditions, and boundaries for security control assessment activities. By documenting permissions and responsibilities—including how potential damage is handled—they help protect the assessment team from liability if unforeseen damage occurs.

✗ **A** Non-invasive testing
Non-invasive testing is intended to reduce the chance of disruption or damage, but it does not establish the authorization and liability terms that protect the assessment team if unforeseen damage nevertheless occurs.

✗ **B** Manual testing
Manual testing describes how assessment activities are performed; it does not by itself document authorization, responsibilities, or liability protections for unexpected damage.

✗ **C** Vulnerability scans
Vulnerability scans are a type of assessment activity and can still have unintended effects. They do not replace documented rules that authorize the work and establish the engagement terms.

✓ **D** Rules of engagement
Rules of engagement document the authorized scope and conditions for the assessment, including responsibilities and expectations if an activity causes unexpected damage. This makes them the relevant protection against liability in the scenario.

Free demo · full exam: 725 questions

Question 62

Multiple choice · Domain: D5 Assessment/Audit of Security and Privacy Controls › 5.2 - Conduct assessment/audit

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. What are the process activities of this phase? Each correct answer represents a complete solution.

Choose all that apply.

Response:

A. Configuring refinement of the SSAA
B. Assessment of the Analysis Results
C. System development
D. Certification analysis
E. Registration

Answer

- A. **Configuring refinement of the SSAA**
- B. **Assessment of the Analysis Results**
- C. **System development**
- D. **Certification analysis**

Explanation

Phase 2, Verification, advances the system toward an integrated state that can undergo certification testing and accreditation. Its activities include refining the SSAA, developing the system, performing certification analysis, and assessing the analysis results. Registration is a Phase 1 activity, not a Phase 2 activity.

✓ **A** Configuring refinement of the SSAA
Refining the SSAA is part of Verification, where system security requirements and the certification approach are developed further to guide the system toward testing.

✓ **B** Assessment of the Analysis Results
Assessing analysis results is one of the Verification activities and helps determine whether the system is progressing toward the required certification and accreditation objectives.

✓ **C** System development
System development occurs during Verification as the system is built and integrated in preparation for certification testing.

✓ **D** Certification analysis
Certification analysis is conducted during Verification to examine the system and its security posture in preparation for certification testing.

✗ **E** Registration
Registration is associated with Phase 1, Definition, rather than Phase 2, Verification. It is not one of the process activities asked for here.

Free demo · full exam: 725 questions

Question 63

Single choice · Domain: D5 Assessment/Audit of Security and Privacy Controls › 5.4 - Review initial assessment/audit report and plan risk response actions

Neil works as a project manager for SoftTech Inc. He is working with Tom, the COO of his company, on several risks within the project. Tom understands that through qualitative analysis Neil has identified many risks in the project.

Tom's concern, however, is that the priority list of these risk events are sorted in "high- risk," "moderate-risk," and "low-risk" as conditions apply within the project.

Tom wants to know that is there any other objective on which Neil can make the priority list for project risks. What will be Neil's reply to Tom?

Response:

A. Risk may be listed by the responses in the near-term
B. Risks may be listed by categories
C. Risks may be listed by the additional analysis and response
D. Risks may be listed by priority separately for schedule, cost, and performance

Answer: D. Risks may be listed by priority separately for schedule, cost, and performance

Explanation

Qualitative risk analysis can produce a prioritized list using probability and impact, including high-, moderate-, and low-risk rankings. Another way to present priorities is to rank risks separately by their potential effects on schedule, cost, and performance. This directly addresses Tom's request for an additional objective basis for the list.

✗ **A** Risk may be listed by the responses in the near-term
This describes organizing risks around near-term responses, not prioritizing them by a distinct impact objective. It does not provide the schedule, cost, and performance breakdown Tom is asking about.

✗ **B** Risks may be listed by categories
Categorizing risks groups them by source or type, but does not itself rank their priority against project objectives. The question asks for another basis for prioritizing the list.

✗ **C** Risks may be listed by the additional analysis and response
Additional analysis and response are activities for further evaluating or addressing risks, rather than an objective for sorting their priority. This does not specify the schedule, cost, and performance dimensions.

✓ **D** Risks may be listed by priority separately for schedule, cost, and performance
This provides an additional way to prioritize risks by showing which ones most affect each key project objective. It complements the high-, moderate-, and low-risk ranking Neil has already developed through qualitative analysis.

Question 64

Single choice · Domain: D6 System Compliance › 6.2 - Determine system risk posture

An official authorization decision that allows for a single authorization package to be developed for an archetype (i.e., common) version of a system. This best defines which of the follwing authorizations?

Response:

A. Authorization to test
B. Type authorization
C. Facility authorization
D. Traditional authorization

Answer: B. Type authorization

Explanation

Type authorization is the official authorization decision for an archetype, or common, version of a system. It allows one authorization package to be developed for that common version, matching the scenario's description.

✗ **A** Authorization to test
This is not the authorization described: the question specifies an authorization decision for a common archetype version that permits a single authorization package. That definition corresponds to type authorization.

✓ **B** Type authorization
Type authorization applies to an archetype, or common, version of a system and allows a single authorization package to be developed for it. This directly matches the definition in the question.

✗ **C** Facility authorization
The question is about authorizing a common version of a system, not authorization associated with a facility. It therefore does not fit the stated definition.

✗ **D** Traditional authorization
The scenario specifically describes one authorization package for an archetype version of a system. That is type authorization, not traditional authorization.

Dumpsgate

Free demo · full exam: 725 questions

Question 65

Single choice · Domain: D6 System Compliance › 6.2 - Determine system risk posture

Authorization to process should occur during what phase of the SDLC?

Response:

A. Implementation phase
B. Risk Determination
C. Threat Identification
D. Vulnerability Identification

Answer: A. Implementation phase

Explanation

Authorization to process is the formal decision to allow a system to operate after it has been implemented and assessed. Therefore, among the listed choices, the Implementation phase is the appropriate phase; Risk Determination, Threat Identification, and Vulnerability Identification are assessment activities rather than the phase identified for authorization.

https://www.isc2.org/Insights/2021/11/decisions-and-the-role-of-authorization
https://www.isc2.org/Insights/2021/07/implementing-controls-assessment

✓ **A** Implementation phase
Authorization to process is the approval to operate a system, which is considered after the system and its controls have been implemented and assessed. This makes the Implementation phase the best choice among the options.

https://www.isc2.org/Insights/2021/11/decisions-and-the-role-of-authorization
https://www.isc2.org/Insights/2021/07/implementing-controls-assessment

✗ **B** Risk Determination
Risk determination evaluates the level of risk; it is not the SDLC phase in which authorization to process occurs. The authorization decision follows the relevant implementation and assessment work.

https://www.isc2.org/Insights/2021/11/decisions-and-the-role-of-authorization

✗ **C** Threat Identification
Threat identification is part of analyzing potential security risks, not the phase for granting authorization to process. It informs risk decisions but does not itself authorize system operation.

✗ **D** Vulnerability Identification
Vulnerability identification finds weaknesses that may affect the system's risk. It is an assessment activity, not the SDLC phase in which authorization to process is granted.

Free demo · full exam: 725 questions

Question 66

Single choice · Domain: D6 System Compliance › 6.2 - Determine system risk posture

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

Response:

A. Chief Risk Officer
B. Data owner
C. Designated Approving Authority
D. Chief Information Officer

Answer: C. Designated Approving Authority

Explanation

The Designated Approving Authority (DAA) is also known as the accreditor. The DAA is the official who grants authorization for a system to operate, so option C is the role asked for.

✗ **A** Chief Risk Officer
A Chief Risk Officer oversees organizational risk management, but this role is not the accreditor identified in the question.

✗ **B** Data owner
A data owner is responsible for the organization's data, but is not the role also known as the accreditor.

✓ **C** Designated Approving Authority
The Designated Approving Authority is also known as the accreditor. This authority makes the authorization decision for a system to operate.

✗ **D** Chief Information Officer
A Chief Information Officer leads an organization's information technology function, but is not the role referred to as the accreditor here.

Question 67

Single choice · Domain: D6 System Compliance › 6.2 - Determine system risk posture

According to NIST SP 800-37 Rev 2 appendix F, there are several types of authorizations including all of the following, except one.

Response:

A. Initial authorization
B. Ongoing authorization
C. reauthorization
D. Authorization decision

Answer: D. Authorization decision

Free demo · full exam: 725 questions

Question 68

Single choice · Domain: D6 System Compliance › 6.2 - Determine system risk posture

The authorization decision may carry restrictions on system operation and caveats that must be followed to maintain the authorization, and other information as determined by the organization including:

Response:

A. Terms and conditions for the authorization
B. Events that may trigger a review of the authorization decision
C. The impact level supported by common controls
D. all of the above

Answer: D. all of the above

Explanation

The authorization decision can include both the terms and conditions the system must meet to retain authorization and events that may prompt the organization to review that decision. It may also include other organization-determined information, such as the impact level supported by common controls. Therefore, all three listed items apply.

https://csrc.nist.gov/CSRC/media/Projects/risk-management/documents/06-Authorize%20Step/NIST%20RMF%20Authorize%20Step-FAQs.pdf
https://csrc.nist.gov/files/pubs/sp/800/37/r2/ipd/docs/sp800-37r2-draft-ipd-with-line-nums.pdf

✓ **A** Terms and conditions for the authorization
Authorization terms and conditions specify restrictions or caveats that must be followed to maintain the authorization. This directly matches the question's description of restrictions on system operation.

https://csrc.nist.gov/CSRC/media/Projects/risk-management/documents/06-Authorize%20Step/NIST%20RMF%20Authorize%20Step-FAQs.pdf
https://csrc.nist.gov/files/pubs/sp/800/37/r2/ipd/docs/sp800-37r2-draft-ipd-with-line-nums.pdf

✓ **B** Events that may trigger a review of the authorization decision
The organization may identify events that could lead it to reconsider the authorization decision. Such review triggers are compatible with the question's inclusion of additional information determined by the organization.

https://csrc.nist.gov/CSRC/media/Projects/risk-management/documents/06-Authorize%20Step/NIST%20RMF%20Authorize%20Step-FAQs.pdf
https://csrc.nist.gov/files/pubs/sp/800/37/r2/ipd/docs/sp800-37r2-draft-ipd-with-line-nums.pdf

✓ **C** The impact level supported by common controls
The question includes the impact level supported by common controls among the additional information that may be specified by the organization. It is therefore part of the set of applicable items, even though it is not itself a restriction or caveat.

https://csrc.nist.gov/CSRC/media/Projects/risk-management/documents/06-Authorize%20Step/NIST%20RMF%20Authorize%20Step-FAQs.pdf
https://csrc.nist.gov/files/pubs/sp/800/37/r2/ipd/docs/sp800-37r2-draft-ipd-with-line-nums.pdf

✓ **D** all of the above
Each of A, B, and C is included in the authorization decision information described by the question. Thus, the inclusive choice is correct.

https://csrc.nist.gov/CSRC/media/Projects/risk-management/documents/06-Authorize%20Step/

Free demo · full exam: 725 questions

NIST%20RMF%20Authorize%20Step-FAQs.pdf
https://csrc.nist.gov/files/pubs/sp/800/37/r2/ipd/docs/sp800-37r2-draft-ipd-with-line-nums.pdf

Question 69

Single choice · Domain: D6 System Compliance › 6.2 - Determine system risk posture

What is the 3rd SDLC phase; which maps to RMF step 5 (Authorize)?

Response:

A. Implementation
B. Operation
C. Recommendation
D. Disposition

Answer: A. Implementation

Explanation

Implementation is the third SDLC phase in the sequence assumed by the question, and it is the phase identified as corresponding to RMF step 5, Authorize. Therefore, option A satisfies both parts of the question.

✓ **A** Implementation
Implementation is the third SDLC phase in the sequence referenced by the question. It is also the phase the question maps to RMF step 5, Authorize.

✗ **B** Operation
Operation follows implementation in the SDLC sequence. It is not the third phase asked for here.

✗ **C** Recommendation
Recommendation is not the name of the third SDLC phase in the sequence referenced by the question. It therefore does not match the requested phase.

✗ **D** Disposition
Disposition is associated with the end of a system's lifecycle, not its third SDLC phase. It does not match the phase corresponding to RMF step 5 in this question.

Free demo · full exam: 725 questions

Question 70

Single choice · Domain: D7 Compliance Maintenance › 7.2 - Perform ongoing compliance activities based on requirements

What is not a responsibility of the Risk Executive (Function) in an organization's ISCM?

Response:

A. Participate in the configuration management process
B. Review status reports from the ISCM process as input to information security risk posture and risk tolerance
C. Oversee the organization's ISCM program
D. Provide input to mission/business process and information tier entities on ISCM strategy

Answer: A. Participate in the configuration management process

Explanation

The Risk Executive (Function) helps guide the organization's ISCM strategy and use of monitoring information to understand risk. Reviewing ISCM status reports and providing strategy input are part of that role, as is overseeing the ISCM program. Participating in the configuration management process is not listed as a Risk Executive (Function) responsibility, so A is the correct answer. [1]

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

✓ **A** Participate in the configuration management process
This is not a responsibility assigned to the Risk Executive (Function) in the ISCM role descriptions. The function provides risk oversight and strategy input; participating in configuration management is a separate operational activity. [1]

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

✗ **B** Review status reports from the ISCM process as input to information security risk posture and risk tolerance
Reviewing ISCM status reports to inform the organization's understanding of its information security risk posture and risk tolerance is part of the Risk Executive (Function)'s role. Therefore, this is a responsibility, not the answer to what is not a responsibility. [1]

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

✗ **C** Oversee the organization's ISCM program
Providing oversight of the organization's ISCM program is consistent with the Risk Executive (Function)'s risk-oversight role. This makes the option a responsibility rather than the exception. [1]

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

✗ **D** Provide input to mission/business process and information tier entities on ISCM strategy
The Risk Executive (Function) provides input on ISCM strategy to organizational entities, including mission/business and information-related entities. This is a strategy-guidance responsibility, so it is not the correct answer. [1]

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

Free demo · full exam: 725 questions

Question 71

Single choice · Domain: D7 Compliance Maintenance › 7.1 - Perform system change management

Which of the following individuals is responsible for configuration management and control task?

Response:

A. Authorizing official
B. Information system owner
C. Chief information officer
D. Common control provider

Answer: B. Information system owner

Explanation

The information system owner is responsible for the system's configuration management and control. The other roles have different primary duties: authorization decisions, organization-wide IT leadership, or providing common controls.

✗ **A** Authorizing official
The authorizing official makes the risk-based decision to authorize the information system to operate. That approval role is distinct from managing the system's configuration and control tasks.

✓ **B** Information system owner
The information system owner is accountable for the system and its lifecycle, including its configuration management and control. This makes the owner the best match for the responsibility asked about.

✗ **C** Chief information officer
The chief information officer provides leadership for the organization's information technology program. The question asks about configuration management and control for an information system, a responsibility assigned to its owner.

✗ **D** Common control provider
A common control provider is responsible for controls that can be used by multiple systems. That role does not make the provider responsible for configuration management and control of the individual system in this question.

Dumpsgate

Question 72

Single choice · Domain: D7 Compliance Maintenance › 7.2 - Perform ongoing compliance activities based on requirements

In accordance with the organizational continuous monitoring strategy, the results of monitoring activities are documented and reported to:

Response:

A. Authorizing Official Designated Representative and Assessor
B. System Owner and System Administrator
C. Authorizing Official and other Organizational officials
D. System Owner and Common Control Provider

Answer: C. Authorizing Official and other Organizational officials

Explanation

The question asks who should receive documented and reported monitoring results under the organizational continuous monitoring strategy. The correct recipients are the Authorizing Official and other organizational officials, who need the information to oversee risk and make organization-level decisions. The other choices name narrower operational or assessment roles rather than the specified organizational decision-makers.

https://csrc.nist.gov/CSRC/media/Projects/risk-management/documents/07-Monitor%20Step/NIST%20RMF%20Monitor%20Step-FAQs.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

✗ **A** Authorizing Official Designated Representative and Assessor
This option substitutes a designated representative and assessor for the broader set of recipients in the question. Monitoring results must be reported to the Authorizing Official and other organizational officials, not limited to these roles.

https://csrc.nist.gov/CSRC/media/Projects/risk-management/documents/07-Monitor%20Step/NIST%20RMF%20Monitor%20Step-FAQs.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

✗ **B** System Owner and System Administrator
The system owner and administrator may use monitoring information for system-level operations, but they are not the recipients specified here. The question asks for reporting under the organizational continuous monitoring strategy, which includes the Authorizing Official and other organizational officials.

https://csrc.nist.gov/CSRC/media/Projects/risk-management/documents/07-Monitor%20Step/NIST%20RMF%20Monitor%20Step-FAQs.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

✓ **C** Authorizing Official and other Organizational officials
This matches the intended organizational reporting audience for documented monitoring results. These officials need the information to support oversight and risk-informed decisions across the organization.

https://csrc.nist.gov/CSRC/media/Projects/risk-management/documents/07-Monitor%20Step/NIST%20RMF%20Monitor%20Step-FAQs.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

✗ **D** System Owner and Common Control Provider
These are relevant system and control-management roles, but this choice does not include the Authorizing Official or the broader organizational officials. It therefore does not match the stated reporting audience.

https://csrc.nist.gov/CSRC/media/Projects/risk-management/documents/07-Monitor%20Step/

Free demo · full exam: 725 questions

NIST%20RMF%20Monitor%20Step-FAQs.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf

Question 73

Single choice · Domain: D7 Compliance Maintenance › 7.2 - Perform ongoing compliance activities based on requirements

The Security Content Automation Protocol (SCAP) is a method for which of the following?

Response:

A. Using specific standards to enable automated policy compliance evaluation
B. Automating the documentation of security controls
C. Facilitating interconnected systems to communicate regarding security control effectiveness
D. Automating the review of the security plan (SP)

Answer: A. Using specific standards to enable automated policy compliance evaluation

Explanation

SCAP uses defined, standardized formats and specifications to make security configuration and compliance checks automatable. Therefore, using specific standards to enable automated policy compliance evaluation is the best description; SCAP is not primarily a tool for documenting controls, connecting systems to discuss effectiveness, or reviewing a security plan. [1][2]

https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf

✓ **A** Using specific standards to enable automated policy compliance evaluation
SCAP specifies standardized ways to express and exchange security-related information, which supports automated evaluation of systems against policy or configuration requirements. This matches the purpose described in the question. [1][2]

https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf

✗ **B** Automating the documentation of security controls
SCAP can represent security-related data, but its central purpose is to support standardized, automated security assessment and compliance checking. Automating the documentation of controls does not capture that purpose.

https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf

✗ **C** Facilitating interconnected systems to communicate regarding security control effectiveness
SCAP standardizes security content and assessment-related information; it is not a general mechanism for interconnected systems to communicate about control effectiveness. The option describes a broader communication function than SCAP provides.

https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf

✗ **D** Automating the review of the security plan (SP)
SCAP supports automated evaluation of technical security information against defined requirements, rather than automating review of a security plan as a document. This is narrower and different from the compliance-evaluation purpose in option A.

https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf

Question 74

Single choice · Domain: D7 Compliance Maintenance › 7.2 - Perform ongoing compliance activities based on requirements

Based on the results of the continuous monitoring process, all excluding one of the following key documents are updated.

Response:

A. Plan of action and milestones
B. Continuous monitoring strategy
C. Security and privacy assessment results
D. Security plan

Answer: B. Continuous monitoring strategy

Explanation

The exception is the continuous monitoring strategy. It sets the approach and cadence for monitoring, rather than serving as a key document routinely revised as an output of monitoring results; findings instead inform the assessment results, plan of action and milestones, and security plan.

✗ **A** Plan of action and milestones
Monitoring can identify weaknesses or unmet requirements that need remediation. Those findings can be recorded in the plan of action and milestones, so it is one of the documents that may be updated based on monitoring results.

✓ **B** Continuous monitoring strategy
The strategy describes how continuous monitoring will be conducted, including its approach and cadence. It is not ordinarily updated as a direct result of each monitoring cycle's findings, making it the exception in this question.

✗ **C** Security and privacy assessment results
Continuous monitoring produces evidence about the system's security and privacy posture. New evidence and findings can therefore update the assessment results.

✗ **D** Security plan
Monitoring may reveal changes to the system or its controls that need to be reflected in the security plan. Thus, the plan can be updated based on monitoring results.

Question 75

Single choice · Domain: D7 Compliance Maintenance › 7.2 - Perform ongoing compliance activities based on requirements

Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.

Response:

A. Contingency Plan
B. Operations Plan
C. Disaster Recovery Plan
D. Incident Response Plan

Answer: A. Contingency Plan

Explanation

A contingency plan is the broad set of policies and procedures intended to maintain or restore business operations during emergencies, system failures, or disasters. The definition specifically includes continuing computer operations at an alternate location, which makes A the best match.

https://www.isc2.org/certifications/cissp/cissp-student-glossary

✓ **A** Contingency Plan
This matches the broad definition: procedures to maintain or restore business operations, potentially at an alternate location, when emergencies, failures, or disasters occur. The question's wording describes contingency planning rather than only one recovery activity.

https://www.isc2.org/certifications/cissp/cissp-student-glossary

✗ **B** Operations Plan
An operations plan generally describes how routine operations are carried out. It does not, by itself, denote the emergency measures for maintaining or restoring operations described here.

✗ **C** Disaster Recovery Plan
A disaster recovery plan focuses on recovering systems and infrastructure after a disruption. The question uses broader language covering policies and procedures to maintain or restore business operations, including at an alternate location.

https://www.isc2.org/certifications/cissp/cissp-student-glossary

✗ **D** Incident Response Plan
An incident response plan guides the handling of a security incident, such as detecting, containing, and addressing it. The scenario instead describes continuity and restoration of business operations across emergencies, failures, or disasters.

Question 76

Single choice · Domain: D7 Compliance Maintenance › 7.2 - Perform ongoing compliance activities based on requirements

The mitigation of violations of security policies and recommended practices.

Response:

A. Incident Handling
B. Episode Handling
C. Appointment Handling
D. Appendage Handling

Answer: A. Incident Handling

Explanation

Incident handling is the process for addressing and mitigating security incidents, including violations of security policies and recommended practices. That makes it the best fit for the response described in the question. The other choices are not the relevant security-management term.

https://www.isc2.org/professional-development/courses/incident-mgmt-prep-and-response

✓ **A** Incident Handling
Incident handling addresses security incidents and supports mitigating violations of security policies and recommended practices. It directly matches the requested response.

https://www.isc2.org/professional-development/courses/incident-mgmt-prep-and-response

✗ **B** Episode Handling
“Episode handling” is not the standard security-response term for mitigating policy violations. The matching term is incident handling.

✗ **C** Appointment Handling
Appointment handling concerns scheduling or appointments, not responding to security-policy violations. It does not meet the requirement described.

✗ **D** Appendage Handling
Appendage handling is not a recognized security response for mitigating policy violations. Incident handling is the relevant choice.

Free demo · full exam: 725 questions

Question 77

Single choice · Domain: D7 Compliance Maintenance › 7.2 - Perform ongoing compliance activities based on requirements

What is the system development life cycle phase for step six of the RMF for an existing system?

Response:

A. Development and Acquisition
B. Implementation/Assessment
C. Maintenance
D. Operations/Maintenance

Answer: D. Operations/Maintenance

Explanation

For an existing system, RMF step six is Monitor: controls and the system's security posture are monitored after authorization as the system continues to operate. That ongoing activity aligns with the Operations/Maintenance phase of the system development life cycle, so D is correct.

✗ **A** Development and Acquisition
This phase concerns developing or acquiring a system, not the ongoing monitoring of an existing system after authorization. RMF step six is associated with the system's operational life.

✗ **B** Implementation/Assessment
Implementation and assessment are associated with putting security controls in place and evaluating them, which occur earlier in the RMF process. Step six focuses on monitoring the system and its controls over time.

✗ **C** Maintenance
Maintenance is related to keeping a system functional, but this answer omits the operations portion of the SDLC phase named for an existing system. The intended phase is Operations/Maintenance.

✓ **D** Operations/Maintenance
RMF step six is Monitor, which applies after authorization while an existing system is operating. Ongoing monitoring and maintenance therefore map to the Operations/Maintenance SDLC phase.

Free demo · full exam: 725 questions

Question 78

Single choice · Domain: D7 Compliance Maintenance › 7.2 - Perform ongoing compliance activities based on requirements

An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

Response:

A. Business Impact Analysis (BIA)
B. Business Continuity Plan (BCP)
C. Business Recovery/Disruption Plan (BRP)
D. Disaster Recovery Plan (DRP)

Answer: A. Business Impact Analysis (BIA)

Explanation

A Business Impact Analysis (BIA) examines an information system's requirements, functions, and dependencies to determine the impact of disruption and establish contingency priorities. That matches the question's focus on characterizing system contingency requirements and priorities after a significant disruption. A BCP and DRP are plans for responding and recovering, rather than the analysis described here.

https://www.isc2.org/certifications/cissp/cissp-student-glossary

✓ **A** Business Impact Analysis (BIA)
A BIA analyzes system functions, requirements, and interdependencies to assess disruption impacts and set recovery or contingency priorities. This is exactly the analysis described in the question.

https://www.isc2.org/certifications/cissp/cissp-student-glossary

✗ **B** Business Continuity Plan (BCP)
A BCP documents how an organization will continue critical operations during and after a disruption. It is a response plan, not the analysis used to characterize requirements and priorities.

✗ **C** Business Recovery/Disruption Plan (BRP)
A recovery or disruption plan describes actions for responding to or recovering from a disruption. The question asks for the analysis that identifies contingency needs and priorities, which is the BIA.

✗ **D** Disaster Recovery Plan (DRP)
A DRP outlines how to restore systems and technology after a disaster. It uses recovery requirements and priorities rather than being the analysis that establishes them.

Free demo · full exam: 725 questions

Question 79

Single choice · Domain: D7 Compliance Maintenance › 7.1 - Perform system change management

After a monthly change control board meeting at which the team determined the security impact of proposed changes to an application, what would be the team's next action?

Response:

A. Prepare the plan of action and milestones based on the findings and recommendations of the security assessment report excluding any remediation actions taken.

B. Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment.

C. Update the security plan, security assessment report, and plan of action and milestones based on the results of the change control board's security impact analysis.

D. Assess a selected subset of the security controls employed within and inherited by the application in accordance with the organization-defined monitoring strategy.

Answer: C. Update the security plan, security assessment report, and plan of action and milestones based on the results of the change control board's security impact analysis.

Explanation

After the change control board determines the security impact of proposed application changes, the team should update the relevant security documentation to reflect that analysis. This includes the security plan, security assessment report, and plan of action and milestones, as stated in option C. The other choices describe separate assessment or reporting activities rather than the documentation update called for by the change-impact results.

https://csrc.nist.gov/files/pubs/sp/800/37/r1/final/docs/sp800-37-rev1-final.pdf
https://csrc.nist.gov/pubs/sp/800/37/r2/final

✗ **A** Prepare the plan of action and milestones based on the findings and recommendations of the security assessment report excluding any remediation actions taken.
This focuses narrowly on preparing the POA&M from an assessment report and says to exclude remediation actions. The scenario asks for the action following the board's security impact analysis, which calls for updating the security plan, assessment report, and POA&M based on that analysis.

https://csrc.nist.gov/files/pubs/sp/800/37/r1/final/docs/sp800-37-rev1-final.pdf
https://csrc.nist.gov/pubs/sp/800/37/r2/final

✗ **B** Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment.
Preparing a security assessment report documents the results of a security control assessment, not the next action after the change control board has analyzed the security impact of proposed changes. The relevant follow-up is to update the existing security documentation based on the impact analysis.

https://csrc.nist.gov/files/pubs/sp/800/37/r1/final/docs/sp800-37-rev1-final.pdf
https://csrc.nist.gov/pubs/sp/800/37/r2/final

✓ **C** Update the security plan, security assessment report, and plan of action and milestones based on the results of the change control board's security impact analysis.
The board has already determined the security impact of the proposed changes, so the next action is to reflect those results in the application's security documentation. Updating all three documents ensures the security plan, assessment report, and POA&M account for the impact analysis.

https://csrc.nist.gov/files/pubs/sp/800/37/r1/final/docs/sp800-37-rev1-final.pdf
https://csrc.nist.gov/pubs/sp/800/37/r2/final

✗ **D** Assess a selected subset of the security controls employed within and inherited by the application in

Free demo · full exam: 725 questions

accordance with the organization-defined monitoring strategy.
Assessing a selected subset of controls is a security-control monitoring activity. The scenario is specifically about the action after a change control board completes its security impact analysis, for which the next step is to update the relevant security documentation.

https://csrc.nist.gov/files/pubs/sp/800/37/r1/final/docs/sp800-37-rev1-final.pdf
https://csrc.nist.gov/pubs/sp/800/37/r2/final

Question 80

Single choice · Domain: D7 Compliance Maintenance › 7.2 - Perform ongoing compliance activities based on requirements

Which of the following statements is true about the continuous monitoring process?

Response:

A. It takes place in the middle of system security accreditation.
B. It takes place before and after system security accreditation.
C. It takes place before the initial system security accreditation.
D. It takes place after the initial system security accreditation.

Answer: D. It takes place after the initial system security accreditation.

Explanation

Continuous monitoring is performed after the system receives its initial security accreditation. It continues through the system's operational life to track security controls and changes, rather than occurring as a step before or during the initial accreditation.

✗ **A** It takes place in the middle of system security accreditation.
Continuous monitoring is not a middle stage of the initial accreditation process. It is carried out after the initial accreditation has been granted.

✗ **B** It takes place before and after system security accreditation.
This incorrectly places continuous monitoring on both sides of accreditation. The statement being tested concerns monitoring after the initial accreditation, not before it.

✗ **C** It takes place before the initial system security accreditation.
Monitoring before initial accreditation may be part of preparation or assessment, but continuous monitoring as described here follows the initial accreditation.

✓ **D** It takes place after the initial system security accreditation.
This correctly places continuous monitoring after the system's initial security accreditation. It provides ongoing oversight after that initial decision.

Free demo · full exam: 725 questions