Exam

# CISM

## Certified Information Security Manager (CISM)

| | |
|---|---|
| **Free demo** | 80 sample questions |
| **Full exam** | 967 questions with answers and explanations |
| **Contents** | Questions with answers and explanations |
| **Generated** | 05 November 2026 |

### Exam domains

| Domain | Exam weight | Questions |
|---|---|---|
| D1 Information Security Governance | 17% | 15 |
| D2 Information Risk Management | 20% | 18 |
| D3 Information Security Program | 33% | 29 |
| D4 Incident Management | 30% | 18 |

This is a free demo from Dumpsgate: 80 of the exam's 967 questions. **Get the full CISM exam** with every question, answer and explanation.

## Question 1

Single choice · Domain: D1 Information Security Governance › Integrate information security governance into corporate governance.

The BEST way to integrate information security governance with corporate governance is to ensure:

**A.** the information security steering committee monitors compliance with security policies.
**B.** management teams embed information security into business processes.
**C.** awareness programs include industry best practice for information security governance.
**D.** the information security program is included in regular external audits.

**Answer:** B. management teams embed information security into business processes.

**Explanation**

Embedding information security into business processes makes security part of how the organization pursues and governs its business objectives, rather than a separate compliance or audit activity. This directly integrates information security governance with corporate governance. [7, 9]

https://www.isaca.org/resources/isaca-journal/issues/2019/volume-4/redefining-corporate-governance-for-better-cyberrisk-management
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/how-to-involve-senior-management-in-the-information-security-governance-process

✗ **A** The information security steering committee monitors compliance with security policies.
Monitoring policy compliance helps oversee the security program, but it does not by itself make security part of corporate decision-making and routine business processes. It is narrower than the integration the question asks for.

✓ **B** Management teams embed information security into business processes.
This links security decisions and practices to the processes through which the organization conducts and governs its business. It therefore integrates information security governance with corporate governance.

https://www.isaca.org/resources/isaca-journal/issues/2019/volume-4/redefining-corporate-governance-for-better-cyberrisk-management
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/how-to-involve-senior-management-in-the-information-security-governance-process

✗ **C** Awareness programs include industry best practice for information security governance.
Awareness programs can help employees understand security expectations, but including best practices in training does not ensure that security is integrated into corporate governance or business processes.

✗ **D** The information security program is included in regular external audits.
External audits can provide independent assurance about the security program, but they assess it rather than embed security in corporate governance and day-to-day business processes.


Free demo · full exam: 967 questions

## Question 2

Single choice · Domain: D1 Information Security Governance › Establish and/or maintain information security policies to guide the development of standards, procedures and guidelines in support of information security strategy.

Which of the following is the PRIMARY reason to involve stakeholders from various business units when developing an information security policy?

**A.** To reduce the overall cost of policy development
**B.** To share responsibility for addressing security breaches
**C.** To decrease the workload of the IT department
**D.** To gain acceptance of the policy across the organization

**Answer:** D. To gain acceptance of the policy across the organization

**Explanation**

Involving stakeholders from different business units helps ensure that the information security policy reflects how the organization works and that affected teams have a voice in its development. That participation makes the policy more likely to be understood, accepted, and followed across the organization. The primary goal is organizational acceptance, not cost reduction or shifting IT's workload.

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/how-to-involve-senior-management-in-the-information-security-governance-process
https://www.isaca.org/resources/isaca-journal/past-issues/2011/2011-planning-for-and-implementing-iso-27001
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/embedding-security-and-continuity-culture

✗ **A** To reduce the overall cost of policy development
Cross-unit participation may require additional coordination rather than reduce development costs. Cost savings are not the primary reason to involve stakeholders in creating a policy.

✗ **B** To share responsibility for addressing security breaches
Stakeholders may have responsibilities for following or implementing the policy, but involving them is not primarily about distributing responsibility for responding to breaches. The main benefit is gaining organizational support for the policy.

✗ **C** To decrease the workload of the IT department
Including business units does not primarily aim to shift or reduce IT's workload. It helps make the policy relevant and acceptable to the people and teams it affects.

✓ **D** To gain acceptance of the policy across the organization
Stakeholders can provide input on how the policy applies to their business units, which promotes understanding and buy-in. Organization-wide acceptance makes the policy more practical to implement and more likely to be followed.

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/how-to-involve-senior-management-in-the-information-security-governance-process
https://www.isaca.org/resources/isaca-journal/past-issues/2011/2011-planning-for-and-implementing-iso-27001
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/embedding-security-and-continuity-culture


Free demo · full exam: 967 questions

## Question 3

Single choice · Domain: D1 Information Security Governance › Identify internal and external influences to the organization (e.g., technology, business environment, risk tolerance, geographic location, legal and regulatory requirements) to ensure that these factors are addressed by the information security strategy.

An organization plans to implement a new e-commerce operation in a highly regulated market.

Which of the following is MOST important to consider when updating the risk management strategy?

**A.** Strategy of industry peers
**B.** Outsourcing needs
**C.** Business culture
**D.** Compliance requirements

**Answer:** D. Compliance requirements

**Explanation**

Because the e-commerce operation will enter a highly regulated market, the updated risk management strategy must account for the applicable compliance obligations. Those requirements can shape the risks the organization must assess and how it manages them. Industry practices, outsourcing, and business culture may also matter, but they are not as directly decisive in this scenario.

https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/the-optimal-risk-management-framework-identifying-the-requirements-and-selecting-the-framework

✗ **A** Strategy of industry peers
Peer strategies can offer useful context, but they do not establish which obligations apply to this organization in a highly regulated market. The risk strategy must be tailored to the organization's own compliance requirements.

✗ **B** Outsourcing needs
Outsourcing can introduce third-party risks and may need to be addressed if relevant to the planned operation. However, the scenario's defining requirement is operating in a highly regulated market, making compliance requirements the most important consideration.

✗ **C** Business culture
Business culture can influence how risk is understood and managed, but it does not replace identifying the market's applicable regulatory obligations. Those obligations are the most direct factor to incorporate when updating the strategy for this operation.

✓ **D** Compliance requirements
A highly regulated market imposes compliance obligations that the e-commerce operation must address. The updated risk management strategy should incorporate those requirements so relevant risks and controls are identified and managed.

https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/the-optimal-risk-management-framework-identifying-the-requirements-and-selecting-the-framework


Free demo · full exam: 967 questions

## Question 4

Single choice · Domain: D1 Information Security Governance › Identify internal and external influences to the organization (e.g., technology, business environment, risk tolerance, geographic location, legal and regulatory requirements) to ensure that these factors are addressed by the information security strategy.

A global organization is considering its geopolitical security risks. Which of the following is the information security manager's BEST approach?

**A.** Seek advice from environmental and physical security experts
**B.** Implement a third-party risk management framework
**C.** Implement controls that deny access from specific jurisdictions
**D.** Seek advice from enterprise risk and legal experts

**Answer:** D. Seek advice from enterprise risk and legal experts

**Explanation**

Geopolitical security risks can affect the organization across enterprise risk, regulatory, and legal dimensions, so the information security manager should consult enterprise risk and legal experts. This provides context for assessing the organization's exposure before selecting specific security measures. The other approaches focus on narrower risks or jump to controls before that broader assessment.

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2024/volume-15/five-key-considerations-for-defensible-and-reasonable-risk-and-security
https://www.isaca.org/resources/isaca-journal/issues/2022/volume-5/managing-cybersecurity-risk-as-enterprise-risk

✗ **A** Seek advice from environmental and physical security experts
Environmental and physical security experts may help assess related physical threats, but geopolitical risks can also have broad enterprise and legal implications. They are not the best primary advisers for evaluating that wider organizational risk.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-5/managing-cybersecurity-risk-as-enterprise-risk

✗ **B** Implement a third-party risk management framework
A third-party risk framework addresses risks arising from vendors and other external parties, which may be relevant but does not by itself assess the organization's broader geopolitical exposure. The manager should first seek enterprise risk and legal input.

https://www.isaca.org/resources/isaca-journal/issues/2024/volume-5/building-a-robust-third-party-risk-management-program-in-a-connected-ecosystem
https://www.isaca.org/resources/isaca-journal/issues/2022/volume-5/managing-cybersecurity-risk-as-enterprise-risk

✗ **C** Implement controls that deny access from specific jurisdictions
Blocking access by jurisdiction is a specific control, not a complete assessment of geopolitical security risk. Choosing such a measure without enterprise risk and legal advice could overlook broader impacts and relevant legal considerations.

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2024/volume-15/five-key-considerations-for-defensible-and-reasonable-risk-and-security
https://www.isaca.org/resources/isaca-journal/issues/2022/volume-5/managing-cybersecurity-risk-as-enterprise-risk

✓ **D** Seek advice from enterprise risk and legal experts
This brings in expertise suited to evaluating geopolitical issues in the context of the organization's overall risk and legal obligations. Their advice can inform a proportionate response before particular controls are selected.

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2024/volume-15/five-key-considerations-for-defensible-and-reasonable-risk-and-security
https://www.isaca.org/resources/isaca-journal/issues/2022/volume-5/managing-cybersecurity-risk-as-enterprise-risk


Free demo · full exam: 967 questions

## Question 5

Single choice · Domain: D1 Information Security Governance › Identify internal and external influences to the organization (e.g., technology, business environment, risk tolerance, geographic location, legal and regulatory requirements) to ensure that these factors are addressed by the information security strategy.

A new information security reporting requirement will soon become effective. Which of the following should be the information security manager's FIRST action?

**A.** Conduct a cost-benefit analysis related to noncompliance with the new requirement.
**B.** Perform a gap assessment against the new requirement.
**C.** Investigate to determine whether the new requirement applies to the business.
**D.** Inform senior management of the new requirement.

**Answer:** C. Investigate to determine whether the new requirement applies to the business.

**Explanation**

Before planning a response to a new reporting requirement, the information security manager should first determine whether it applies to the business. If it does not apply, a gap assessment, noncompliance cost analysis, or management notification about an obligation would be premature; if it does apply, those actions can follow as appropriate.

✗ **A** Conduct a cost-benefit analysis related to noncompliance with the new requirement.
This assumes the requirement applies and shifts attention to the consequences of noncompliance. First establish whether the business is in scope; only then would evaluating consequences be relevant.

✗ **B** Perform a gap assessment against the new requirement.
A gap assessment would compare current practices with an applicable obligation. The manager must first determine whether the requirement applies to the business, or the assessment could be unnecessary.

✓ **C** Investigate to determine whether the new requirement applies to the business.
Applicability is the threshold question: the requirement may depend on factors such as the business's activities or circumstances. Establishing that first determines whether further compliance work is needed.

✗ **D** Inform senior management of the new requirement.
Management should be informed when there is a meaningful obligation or exposure to report. First determine whether the requirement applies to the business so that any communication is accurate and relevant.

Dumpsgate

## Question 6

Single choice · Domain: D1 Information Security Governance › Establish and/or maintain information security policies to guide the development of standards, procedures and guidelines in support of information security strategy.

What is the PRIMARY reason to involve stakeholders from various business units when developing an information security policy?

**A.** To share responsibility for addressing security breaches
**B.** To gain acceptance of the policy across the organization
**C.** To decrease the workload of the IT department
**D.** To reduce the overall cost of policy development

**Answer:** B. To gain acceptance of the policy across the organization

**Explanation**

Involving stakeholders from multiple business units helps ensure the information security policy reflects organization-wide needs and that the people expected to follow it support it. Gaining broad acceptance is the primary reason: a policy is more likely to be adopted and followed when affected stakeholders have had a voice in developing it.

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/six-steps-to-a-mature-policy-management-program
https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/moving-toward-better-security-for-today-and-tomorrow-establishing-a-cybersecurity-culture

✗ **A** To share responsibility for addressing security breaches
Stakeholder involvement can clarify that security is a shared concern, but the main purpose of involving business units in policy development is not to distribute responsibility for responding to breaches. The question asks why they should be involved in developing the policy, and gaining organizational acceptance is the primary reason.

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/six-steps-to-a-mature-policy-management-program

✓ **B** To gain acceptance of the policy across the organization
Business-unit stakeholders can contribute their needs and perspectives, making the policy more relevant and increasing their willingness to support and follow it. Broad organizational acceptance is therefore the primary benefit of involving them in its development.

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/six-steps-to-a-mature-policy-management-program
https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/moving-toward-better-security-for-today-and-tomorrow-establishing-a-cybersecurity-culture

✗ **C** To decrease the workload of the IT department
Involving other business units does not primarily aim to reduce IT's workload. Their participation is intended to build a policy that the organization accepts and can apply, rather than shift IT tasks to other departments.

✗ **D** To reduce the overall cost of policy development
Cost reduction is not the primary reason to involve stakeholders from different business units. The key benefit is that their participation builds support for the policy across the organization.

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/six-steps-to-a-mature-policy-management-program


Free demo · full exam: 967 questions

## Question 7

Single choice · Domain: D1 Information Security Governance › Establish and/or maintain information security policies to guide the development of standards, procedures and guidelines in support of information security strategy.

Which of the following should have the MOST influence on the development of information security policies?

**A.** Business strategy
**B.** Past and current threats
**C.** IT security framework
**D.** Industry standards

**Answer:** A. Business strategy

**Explanation**

Business strategy should have the most influence because information security policies need to support the organization's objectives, operations, and risk tolerance. Threats, frameworks, and industry standards can inform policy content, but they are inputs rather than the primary driver of what the organization needs its policies to achieve.

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/differentiating-key-terms-in-the-information-security-hierarchy
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-2

✓ **A** Business strategy
Policies should enable the organization's business objectives while establishing appropriate security requirements. This makes business strategy the primary influence; controls and requirements should be tailored to the organization rather than adopted without regard to its goals.

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/differentiating-key-terms-in-the-information-security-hierarchy
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-2

✗ **B** Past and current threats
Threat information helps identify risks and shape security measures, but it does not determine the organization's overall objectives or priorities. Policies must address threats in a way that supports the business strategy.

https://www.isaca.org/resources/white-papers/2025/threat-modeling-revisited
https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2024/volume-15/five-key-considerations-for-defensible-and-reasonable-risk-and-security

✗ **C** IT security framework
A framework can provide structure and recommended practices for developing security policies. It is a guide, however, and should be selected or applied to fit the organization's strategy and needs.

https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/essential-functions-of-a-cybersecurity-program
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/differentiating-key-terms-in-the-information-security-hierarchy

✗ **D** Industry standards
Industry standards may provide useful requirements or benchmarks, including obligations the organization must meet. They do not replace the need to align policies with the organization's own business strategy.

https://www.isaca.org/resources/isaca-journal/issues/2024/volume-3/navigating-the-iso-iec-27001-2022-transition-a-90-day-challenge


Free demo · full exam: 967 questions

## Question 8

Single choice · Domain: D1 Information Security Governance › Obtain commitment from senior management and other stakeholders to support the successful implementation of the information security strategy.

An organization has identified a weakness in the ability of its employees to identify and report cybersecurity incidents. Although training materials have been provided, employees show a lack of interest. Which of the following is the information security manager's BEST course of action?

**A.** Block network access until security awareness training is complete.
**B.** Conduct an enterprise cybersecurity risk assessment.
**C.** Obtain key stakeholder and leadership support.
**D.** Send an email mandating training for the employees.

**Answer:** C. Obtain key stakeholder and leadership support.

**Explanation**

The organization has already identified the specific weakness: employees are not engaged with training intended to help them identify and report incidents. The best next step is to obtain support from key stakeholders and leadership so the awareness effort can be prioritized, reinforced, and made more effective—not merely distribute more material or issue a directive. This addresses the stated lack of interest while supporting a stronger security culture.

https://www.isaca.org/resources/isaca-journal/issues/2023/volume-2/considerations-for-developing-cybersecurity-awareness-training
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/embedding-security-and-continuity-culture

✗ **A** Block network access until security awareness training is complete.
Blocking access is a punitive operational measure and does not address why employees are uninterested or help build lasting incident-reporting behavior. It may disrupt work without creating genuine engagement with the awareness effort.

✗ **B** Conduct an enterprise cybersecurity risk assessment.
The question already identifies the relevant weakness in employees' ability to recognize and report incidents. A broad risk assessment may identify or prioritize risks, but it does not directly solve the stated lack of employee interest in the training.

https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/addressing-risk-using-the-new-enterprise-security-risk-management-cycle

✓ **C** Obtain key stakeholder and leadership support.
Leadership and stakeholder backing can give the awareness effort visibility, priority, and organizational reinforcement, helping address employees' lack of interest rather than relying only on provided materials. This is the best course of action for improving engagement and embedding security awareness into the organization.

https://www.isaca.org/resources/isaca-journal/issues/2023/volume-2/considerations-for-developing-cybersecurity-awareness-training
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/embedding-security-and-continuity-culture

✗ **D** Send an email mandating training for the employees.
A mandate may prompt attendance, but an email alone does not address why employees are disengaged or establish broader organizational support for effective awareness. Leadership and stakeholder support is a stronger first step for making the training meaningful and sustained.

https://www.isaca.org/resources/isaca-journal/issues/2023/volume-2/considerations-for-developing-cybersecurity-


Free demo · full exam: 967 questions

awareness-training
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/embedding-security-and-continuity-culture

## Question 9

Single choice · Domain: D1 Information Security Governance › Establish and/or maintain information security policies to guide the development of standards, procedures and guidelines in support of information security strategy.

Information security policies should PRIMARILY reflect alignment with:

**A.** an information security framework.
**B.** industry best practices.
**C.** data security standards.
**D.** senior management intent.

**Answer:** D. senior management intent.

**Explanation**

Information security policies should primarily express what senior management intends the organization to protect and how it will govern security. Frameworks, industry practices, and standards can guide policy design, but they are supporting inputs rather than the primary alignment target. Therefore, D is the best answer. [7]

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/differentiating-key-terms-in-the-information-security-hierarchy

✗ **A** an information security framework.
A framework can provide structure and guidance for developing policies, but it does not replace alignment with the organization's leadership intent. The policy should reflect the organization's chosen priorities and direction. [7]

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/differentiating-key-terms-in-the-information-security-hierarchy

✗ **B** industry best practices.
Best practices can inform policy choices, but following them is not the primary purpose of an organization's security policies. Policies must fit the organization's own objectives and management direction. [7]

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/differentiating-key-terms-in-the-information-security-hierarchy

✗ **C** data security standards.
Standards may establish relevant controls or compliance requirements, but they are narrower inputs to policy development. The policies should primarily align with senior management's intent. [7]

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/differentiating-key-terms-in-the-information-security-hierarchy

✓ **D** senior management intent.
Security policies establish the organization's authoritative direction and expectations for information security, so they should reflect the intent of senior management. Frameworks, practices, and standards can help implement that direction but do not supersede it. [7]

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/differentiating-key-terms-in-the-information-security-hierarchy


Free demo · full exam: 967 questions

## Question 10

Single choice · Domain: D1 Information Security Governance › Establish and/or maintain information security policies to guide the development of standards, procedures and guidelines in support of information security strategy.

An information security policy was amended recently to support an organization's new information security strategy. Which of the following should be the information security manager's NEXT step?

**A.** Evaluate the alignment with business strategy.
**B.** Review technical controls.
**C.** Update standards and procedures.
**D.** Refresh the security training program.

**Answer:** C. Update standards and procedures.

**Explanation**

Because the policy has already been amended to support the new information security strategy, the next step is to translate its requirements into aligned standards and procedures. Those provide the specific direction needed for implementation; reviewing technical controls and updating training can follow once the supporting requirements are defined.

✗ **A** Evaluate the alignment with business strategy.
The scenario says the policy was amended to support the organization's new information security strategy, so alignment with business strategy is not the next action after that amendment. The immediate follow-up is to make the policy actionable through supporting standards and procedures.

✗ **B** Review technical controls.
Technical controls are implementation measures, and reviewing them is premature before the updated policy has been translated into detailed standards and procedures. Defining those requirements first provides a basis for assessing whether controls are appropriate.

✓ **C** Update standards and procedures.
Standards and procedures operationalize the amended policy by specifying how its requirements are to be implemented. Updating them is therefore the next step after the policy has been changed to support the new strategy.

✗ **D** Refresh the security training program.
Training should communicate relevant security requirements, but the supporting standards and procedures should first be updated so the training reflects the policy's current implementation requirements. It is a subsequent step, not the immediate next one.


Free demo · full exam: 967 questions

## Question 11

Single choice · Domain: D1 Information Security Governance › Identify internal and external influences to the organization (e.g., technology, business environment, risk tolerance, geographic location, legal and regulatory requirements) to ensure that these factors are addressed by the information security strategy.

Which of the following should be an information security manager's PRIMARY concern when an organization is expanding business to a new country?

**A.** Compliance with local regulations
**B.** Changes in IT infrastructure
**C.** Cultural differences in the new country
**D.** Ability to gather customer data

**Answer:** A. Compliance with local regulations

**Explanation**

When entering a new country, the information security manager must ensure the organization understands and complies with that jurisdiction's laws and regulations. These may impose requirements on security controls, data handling, privacy, and reporting, and noncompliance can create legal and business risks. Infrastructure, culture, and customer-data capabilities matter, but they do not take priority over meeting applicable local requirements.

https://www.isaca.org/resources/isaca-journal/issues/2024/volume-2/building-compliance-resilience-amid-a-patchwork-of-data-protection-and-privacy-laws

✓ **A** Compliance with local regulations
The organization must identify and meet the new country's applicable legal and regulatory requirements, including rules that may affect privacy and data protection. These obligations can determine how information is collected, stored, transferred, and secured, making compliance the primary concern.

https://www.isaca.org/resources/isaca-journal/issues/2024/volume-2/building-compliance-resilience-amid-a-patchwork-of-data-protection-and-privacy-laws

✗ **B** Changes in IT infrastructure
Expansion may require infrastructure changes, but those are implementation considerations rather than the primary information security concern. Local legal requirements should first be understood because they may dictate what infrastructure or safeguards are necessary.

https://www.isaca.org/resources/isaca-journal/issues/2024/volume-2/building-compliance-resilience-amid-a-patchwork-of-data-protection-and-privacy-laws

✗ **C** Cultural differences in the new country
Cultural differences can affect security awareness and how policies are communicated or adopted. They are important to address, but they do not supersede the need to comply with the country's laws and regulations.

https://www.isaca.org/resources/isaca-journal/issues/2023/volume-5/raising-security-awareness-in-cross-cultural-work-and-collaboration

✗ **D** Ability to gather customer data
The organization's ability to gather customer data is not the primary security concern. Whether and how it may collect that data should be assessed in light of local privacy and data-protection requirements.

https://www.isaca.org/resources/isaca-journal/issues/2024/volume-2/building-compliance-resilience-amid-a-patchwork-of-data-protection-and-privacy-laws


Free demo · full exam: 967 questions

## Question 12

Single choice · Domain: D1 Information Security Governance › Establish and/or maintain an information security strategy aligned with organizational goals and objectives to guide the establishment and ongoing management of the information security program.

Which of the following should be the MOST important consideration when reviewing an information security strategy?

**A.** Recent security incidents
**B.** New business initiatives
**C.** Industry security standards
**D.** Internal audit findings

**Answer:** B. New business initiatives

**Explanation**

An information security strategy should enable and protect the organization's business objectives, so reviewing it against new business initiatives is most important. New initiatives can change business priorities, processes, and risk exposure, requiring security priorities and resources to remain aligned. Incidents, standards, and audit findings are useful inputs, but they do not replace alignment with the organization's direction.

https://www.isaca.org/resources/isaca-journal/issues/2015/volume-1/porters-elements-for-a-business-information-security-strategy
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/bridging-the-gap-between-security-and-the-business

✗ **A** Recent security incidents
Recent incidents can reveal weaknesses and should inform security improvements. However, a review should primarily ensure the strategy supports the organization's current and emerging business direction, rather than focus chiefly on past events.

https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/essential-functions-of-a-cybersecurity-program

✓ **B** New business initiatives
New initiatives may change business objectives, technology use, and risk exposure. The security strategy needs to align with and enable those initiatives, making them the most important consideration when reviewing it.

https://www.isaca.org/resources/isaca-journal/issues/2015/volume-1/porters-elements-for-a-business-information-security-strategy
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/bridging-the-gap-between-security-and-the-business

✗ **C** Industry security standards
Industry standards can provide useful requirements and benchmarks, but applying them alone may not ensure that the strategy addresses the organization's specific business priorities. Business alignment is the more important consideration in this review.

https://www.isaca.org/resources/isaca-journal/issues/2015/volume-1/porters-elements-for-a-business-information-security-strategy

✗ **D** Internal audit findings
Audit findings can identify control gaps and warrant corrective action. They are an important input, but the strategy review must also be oriented to the organization's changing business objectives, represented here by new initiatives.

https://www.isaca.org/resources/isaca-journal/past-issues/2010/developing-an-information-security-and-risk-management-strategy


Free demo · full exam: 967 questions

## Question 13

Single choice · Domain: D1 Information Security Governance › Establish and/or maintain an information security governance framework to guide activities that support the information security strategy.

Which of the following is MOST important when designing an information security governance framework?

**A.** Aligning with the information security strategy
**B.** Assessing the availability of information security resources
**C.** Aligning with industry best practice frameworks
**D.** Assessing the current state of information security

**Answer:** A. Aligning with the information security strategy

**Explanation**

The governance framework should be aligned with the information security strategy so that governance priorities, decision rights, and oversight support the organization's security objectives. This alignment is more fundamental than selecting an external framework, assessing resources, or documenting the current state, which can inform implementation but do not establish that it serves the strategy.

https://www.isaca.org/certifications/additional-resources/-/media/35de8580e8834504b9275eb57e1c48e8.ashx
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/how-to-construct-a-governance-system-from-the-board-level-to-the-code-level
https://www.isaca.org/resources/isaca-journal/issues/2019/volume-6/security-governance-or-an-elephant-fight

✓ **A** Aligning with the information security strategy
A governance framework needs to direct and oversee security in support of the organization's information security strategy. Alignment ensures governance choices advance the intended security objectives rather than operating as an isolated set of controls or processes.

https://www.isaca.org/certifications/additional-resources/-/media/35de8580e8834504b9275eb57e1c48e8.ashx
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/how-to-construct-a-governance-system-from-the-board-level-to-the-code-level
https://www.isaca.org/resources/isaca-journal/issues/2019/volume-6/security-governance-or-an-elephant-fight

✗ **B** Assessing the availability of information security resources
Resource availability matters when planning and implementing governance, but it does not determine the framework's governing purpose or priorities. Those should be aligned with the information security strategy.

✗ **C** Aligning with industry best practice frameworks
Industry frameworks can provide useful guidance, but adopting or aligning with them is secondary to ensuring the governance framework fits the organization's information security strategy. Best-practice alignment alone does not establish that fit.

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/finding-or-building-the-right-framework-for-your-organization

✗ **D** Assessing the current state of information security
A current-state assessment can identify gaps and help shape implementation, but it is a diagnostic input rather than the most important design principle. The framework must ultimately support the information security strategy.

https://www.isaca.org/certifications/additional-resources/-/media/35de8580e8834504b9275eb57e1c48e8.ashx


Free demo · full exam: 967 questions

## Question 14

Single choice · Domain: D1 Information Security Governance › Integrate information security governance into corporate governance.

Which of the following has the GREATEST impact on the effectiveness of an organization's security posture?

**A.** Incident metrics are frequently compared against industry benchmarks
**B.** New hires are mandated to attend security training
**C.** Security is embedded in organizational culture
**D.** Senior management has approved and endorsed security practices

**Answer:** C. Security is embedded in organizational culture

**Explanation**

Embedding security in organizational culture has the greatest impact because it makes secure behavior part of everyday decisions and practices across the organization, rather than a one-time activity or a leadership-only endorsement. This broad, sustained influence helps employees consistently follow security expectations and reinforces the organization's overall security posture.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/embedding-security-and-continuity-culture
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/building-a-culture-of-security
https://www.isaca.org/resources/isaca-journal/issues/2022/volume-6/optimum-security-cognizance-through-people-process-and-behavior-transformation

✗ **A** Incident metrics are frequently compared against industry benchmarks
Benchmarking can help an organization evaluate and improve incident-response performance, but it is a measurement and improvement activity. It does not itself ensure that secure behavior is consistently practiced throughout the organization.

✗ **B** New hires are mandated to attend security training
Training new hires builds awareness, but it is limited to onboarding and does not necessarily sustain secure behavior across all employees over time. A security culture influences routine actions more broadly.

https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/building-a-culture-of-security
https://www.isaca.org/resources/isaca-journal/issues/2022/volume-6/optimum-security-cognizance-through-people-process-and-behavior-transformation

✓ **C** Security is embedded in organizational culture
When security is embedded in organizational culture, employees treat security as part of their normal work and decisions. This organization-wide, continuing influence makes it more impactful than isolated training, benchmarking, or formal endorsement alone.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/embedding-security-and-continuity-culture
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/building-a-culture-of-security
https://www.isaca.org/resources/isaca-journal/issues/2022/volume-6/optimum-security-cognizance-through-people-process-and-behavior-transformation

✗ **D** Senior management has approved and endorsed security practices
Senior management support is important for establishing priorities and providing authority or resources. However, endorsement alone does not ensure that security practices are consistently adopted in everyday work; embedding security in the culture has broader influence.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/embedding-security-and-continuity-culture
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/building-a-culture-of-security

## Question 15

Single choice · Domain: D1 Information Security Governance › Establish and/or maintain an information security strategy aligned with organizational goals and objectives to guide the establishment and ongoing management of the information security program.

Of the following, who would provide the MOST relevant input when aligning the information security strategy with organizational goals?

**A.** Enterprise risk committee
**B.** Information security steering committee
**C.** Data privacy officer (DPO)
**D.** Chief information security officer (CISO)

**Answer:** B. Information security steering committee

**Explanation**

The information security steering committee is the most relevant source of input because it can bring together business and security stakeholders to guide security priorities in line with organizational goals. The CISO leads the security function, but the committee provides a governance forum for aligning its strategy with broader business needs. [5]

https://www.isaca.org/resources/isaca-journal/past-issues/2010/developing-an-information-security-and-risk-management-strategy

✗ **A** Enterprise risk committee
An enterprise risk committee can provide useful input on organizational risks, but its remit is broader than setting the direction of the information security strategy. The steering committee is the more direct forum for connecting security priorities with organizational goals.

✓ **B** Information security steering committee
This committee can bring relevant business and security stakeholders together to guide information security priorities and ensure they support organizational goals. That makes it the most relevant source of input for aligning the strategy. [5]

https://www.isaca.org/resources/isaca-journal/past-issues/2010/developing-an-information-security-and-risk-management-strategy

✗ **C** Data privacy officer (DPO)
A DPO's focus is data protection and privacy obligations, which are important but narrower than the organization-wide information security strategy. The steering committee is better placed to align security priorities across organizational functions. [7]

https://www.isaca.org/career-center/career-journey/privacy-compliance/data-protection-officer

✗ **D** Chief information security officer (CISO)
The CISO is responsible for leading and managing information security, so their input is important. However, the question asks who would provide the most relevant input for alignment with organizational goals; a steering committee offers a broader governance forum that can incorporate business perspectives. [6]

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/three-essentials-to-thrive-in-a-high-pressure-ciso-role


Free demo · full exam: 967 questions

## Question 16

Single choice · Domain: D2 Information Risk Management › Establish and/or maintain a process for information risk assessment and treatment to ensure that risk is managed to acceptable levels.

An organization has implemented controls to mitigate risks resulting from identified vulnerabilities in an application. Which of the following is the BEST way to verify all weaknesses have been addressed?

**A.** Conduct an internal audit.
**B.** Conduct penetration testing.
**C.** Perform a vulnerability assessment.
**D.** Prepare compensating controls.

**Answer:** C. Perform a vulnerability assessment.

**Explanation**

A vulnerability assessment is the best fit because it systematically identifies weaknesses in the application and can be repeated after controls are implemented to check whether those weaknesses remain. This directly verifies remediation across the identified vulnerabilities, whereas a penetration test attempts to exploit selected weaknesses and an audit reviews control processes rather than comprehensively checking the application for remaining vulnerabilities.

https://www.isaca.org/resources/white-papers/vulnerability-assessment
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/enterprise-vulnerability-management

✗ **A** Conduct an internal audit.
An internal audit can assess whether controls and procedures are properly designed or followed, but it is not the most direct way to check the application for remaining technical weaknesses. The organization needs a vulnerability-focused check after implementing its controls.

✗ **B** Conduct penetration testing.
Penetration testing attempts to exploit weaknesses to demonstrate their impact, often within a defined scope. It can provide valuable assurance, but a vulnerability assessment is more directly suited to systematically checking whether the identified weaknesses have been addressed.

https://www.isaca.org/resources/news-and-trends/industry-news/2022/taking-a-risk-based-approach-to-pen-testing

✓ **C** Perform a vulnerability assessment.
A vulnerability assessment systematically identifies weaknesses in the application and can be performed again after remediation to see whether they have been eliminated. That makes it the best choice for verifying that all identified weaknesses have been addressed.

https://www.isaca.org/resources/white-papers/vulnerability-assessment
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/enterprise-vulnerability-management

✗ **D** Prepare compensating controls.
Compensating controls may reduce risk when a weakness cannot be directly removed, but preparing them does not verify that all weaknesses have been addressed. Verification requires assessing the application after the controls are implemented.


Free demo · full exam: 967 questions

## Question 17

Single choice · Domain: D2 Information Risk Management › Establish and/or maintain a process for information risk assessment and treatment to ensure that risk is managed to acceptable levels.

The PRIMARY purpose for conducting cybersecurity risk assessments is to:

**A.** Assist in security reporting to senior management
**B.** Provide metrics to indicate cybersecurity program effectiveness
**C.** Verify compliance across multiple sectors
**D.** Understand the organization's current security posture

**Answer:** D. Understand the organization's current security posture

**Explanation**

The primary purpose of a cybersecurity risk assessment is to identify and understand the organization's risks and establish its current security posture. That understanding helps the organization decide what needs attention and how to prioritize risk treatment. Reporting, program metrics, and compliance checks may benefit from assessment results, but they are not the central purpose in this question.

https://www.isaca.org/resources/white-papers/conducting-an-it-security-risk-assessment
https://www.isaca.org/resources/isaca-journal/past-issues/2010/performing-a-security-risk-assessment
https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/building-a-strong-security-posture-begins-with-assessment

✗ **A** Assist in security reporting to senior management
Assessment results can inform reports to senior management, but reporting is a way to communicate findings rather than the primary reason to conduct the assessment. The assessment first establishes what risks and security conditions exist.

https://www.isaca.org/resources/white-papers/conducting-an-it-security-risk-assessment
https://www.isaca.org/resources/isaca-journal/past-issues/2010/performing-a-security-risk-assessment

✗ **B** Provide metrics to indicate cybersecurity program effectiveness
Metrics can help evaluate aspects of a cybersecurity program, but producing effectiveness metrics is not the primary purpose of a risk assessment. The assessment is primarily used to understand risks and the organization's security posture.

https://www.isaca.org/resources/white-papers/conducting-an-it-security-risk-assessment
https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/building-a-strong-security-posture-begins-with-assessment

✗ **C** Verify compliance across multiple sectors
A risk assessment may reveal compliance-related risks, but verifying compliance across sectors is a separate objective and is not the primary purpose described here. The broader purpose is to understand the organization's security posture and risks.

https://www.isaca.org/resources/white-papers/conducting-an-it-security-risk-assessment
https://www.isaca.org/resources/isaca-journal/past-issues/2010/performing-a-security-risk-assessment

✓ **D** Understand the organization's current security posture
A cybersecurity risk assessment identifies and evaluates the organization's risks, helping it understand its current security posture. This understanding provides a basis for deciding which risks require attention and prioritizing action.

https://www.isaca.org/resources/white-papers/conducting-an-it-security-risk-assessment
https://www.isaca.org/resources/isaca-journal/past-issues/2010/performing-a-security-risk-assessment
https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/building-a-strong-security-posture-begins-with-assessment


Free demo · full exam: 967 questions

## Question 18

Single choice · Domain: D2 Information Risk Management › Establish and/or maintain a process for information risk assessment and treatment to ensure that risk is managed to acceptable levels.

Which of the following is the BEST course of action after management has reviewed an identified risk and determines the risk is below the defined risk appetite?

**A.** Accept
**B.** Avoid
**C.** Transfer
**D.** Mitigate

**Answer:** A. Accept

**Explanation**

Because management determined the risk is below the organization's defined risk appetite, the risk can be accepted rather than treated with additional controls or avoided. Acceptance means acknowledging and retaining the risk, while continuing to manage it as appropriate. [1]

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-6/not-all-risk-treatment-options-are-the-same

✓ **A** Accept
Acceptance is appropriate because the assessed risk is below the defined risk appetite, so management can retain it without taking further treatment action. The decision should still be documented and monitored as needed. [1]

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-6/not-all-risk-treatment-options-are-the-same

✗ **B** Avoid
Avoidance would mean stopping or changing the activity that gives rise to the risk. The scenario does not indicate that a below-appetite risk warrants eliminating the activity.

✗ **C** Transfer
Transfer shifts some responsibility or financial impact of the risk to another party. Since management has determined the risk is below appetite, transferring it is not necessary based on the scenario.

✗ **D** Mitigate
Mitigation applies controls or other measures to reduce the risk. The risk is already below the defined appetite, so further reduction is not the best course of action described here.


Free demo · full exam: 967 questions

## Question 19

Single choice · Domain: D2 Information Risk Management › Monitor existing risk to ensure that changes are identified and managed appropriately.

An information security manager learns that an existing supplier plans to begin using its recently developed generative AI technology for the same scope of service. A risk assessment was performed on the supplier three months ago with no outstanding findings. Which of the following is the BEST course of action to address the associated risk?

**A.** Suspend the use of the supplier until a risk assessment of the AI technology has been performed
**B.** Report the change in risk to senior management
**C.** Review the results of the previous risk assessment
**D.** Add an indemnity clause in the contractual agreement at the renewal stage

**Answer:** A. Suspend the use of the supplier until a risk assessment of the AI technology has been performed

**Explanation**

The supplier's planned use of generative AI is a material change to its service and introduces risks that the assessment from three months ago may not have evaluated. The organization should suspend use of the supplier until the AI technology has been assessed, preventing exposure to unassessed risks while due diligence is completed. A clean prior assessment does not cover this new technology.

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2025/six-steps-for-third-party-ai-risk-management
https://www.isaca.org/resources/news-and-trends/industry-news/2025/vendor-risk-assessments-do-organizations-still-need-them

✓ **A** Suspend the use of the supplier until a risk assessment of the AI technology has been performed
The supplier is introducing generative AI into the same service scope, creating a new risk that was not covered by the earlier assessment. Suspending use until the AI-specific assessment is complete avoids continuing the service while this changed risk is unknown.

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2025/six-steps-for-third-party-ai-risk-management
https://www.isaca.org/resources/news-and-trends/industry-news/2025/vendor-risk-assessments-do-organizations-still-need-them

✗ **B** Report the change in risk to senior management
Escalation can inform oversight, but it does not assess the new AI risks or prevent exposure to them. The immediate priority is to pause use until the technology has been assessed.

✗ **C** Review the results of the previous risk assessment
The prior assessment found no outstanding issues, but it predates the supplier's planned use of generative AI. Reviewing it would not establish whether the new technology creates additional risks.

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2025/six-steps-for-third-party-ai-risk-management
https://www.isaca.org/resources/news-and-trends/industry-news/2025/vendor-risk-assessments-do-organizations-still-need-them

✗ **D** Add an indemnity clause in the contractual agreement at the renewal stage
An indemnity clause may address contractual allocation of liability, but it does not evaluate or mitigate the technology's risks before it is used. Waiting until renewal also fails to address the immediate change in the supplier's service.


Free demo · full exam: 967 questions

## Question 20

Single choice · Domain: D2 Information Risk Management › Establish and/or maintain a process for information risk assessment and treatment to ensure that risk is managed to acceptable levels.

Which of the following is the MOST important consideration when defining control objectives?

**A.** Senior management support
**B.** Risk appetite
**C.** Threat environment
**D.** Budget allocation

**Answer:** B. Risk appetite

**Explanation**

Risk appetite is the most important consideration because control objectives should reflect the level of risk the organization is willing to accept. That alignment helps ensure controls address risks that matter to organizational objectives without requiring controls beyond the organization's tolerance.

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-6/tips-for-effective-control-design
https://www.isaca.org/resources/isaca-journal/issues/2019/volume-3/a-model-and-best-practices-for-risk-transformation

✗ **A** Senior management support
Senior management support helps establish and implement controls, but it does not determine the level of risk the organization is prepared to accept. Control objectives should first align with that risk appetite.

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-6/tips-for-effective-control-design

✓ **B** Risk appetite
Risk appetite defines the amount and type of risk the organization is willing to accept. Control objectives should be set in line with it so controls focus on keeping risk within acceptable limits.

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-6/tips-for-effective-control-design
https://www.isaca.org/resources/isaca-journal/issues/2019/volume-3/a-model-and-best-practices-for-risk-transformation

✗ **C** Threat environment
The threat environment informs risk assessment and can affect which controls are appropriate. However, it does not by itself establish the organization's tolerance for risk, which is the key consideration when defining control objectives.

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-6/tips-for-effective-control-design
https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/is-audit-basics-auditing-isit-risk-management-part-2

✗ **D** Budget allocation
Budget affects which controls can be implemented and maintained, but it is a resource constraint rather than the basis for setting control objectives. Objectives should be driven by the organization's risk appetite, then resourced appropriately.

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-6/tips-for-effective-control-design


Free demo · full exam: 967 questions

## Question 21

Single choice · Domain: D2 Information Risk Management › Establish and/or maintain a process for information risk assessment and treatment to ensure that risk is managed to acceptable levels.

An information security team has started work to mitigate findings from a recent penetration test. Which of the following presents the GREATEST risk to the organization?

**A.** Some findings were reclassified to low risk after evaluation
**B.** Not all findings from the penetration test report were fixed
**C.** The penetration testing report did not contain any high-risk findings
**D.** Risk classification of penetration test findings was not performed

**Answer:** D. Risk classification of penetration test findings was not performed

**Explanation**

The greatest risk is failing to classify the penetration-test findings by risk. Without that assessment, the team cannot reliably prioritize remediation or determine which unresolved findings could pose the greatest threat to the organization. Reclassification after evaluation and leaving some findings unfixed can be reasonable when decisions are risk-based; a report with no high-risk findings does not by itself indicate a process failure.

https://www.isaca.org/resources/news-and-trends/industry-news/2022/taking-a-risk-based-approach-to-pen-testing
https://www.isaca.org/resources/isaca-journal/issues/2023/volume-1/mitigating-technical-vulnerabilities-with-risk-assessment

✗ **A** Some findings were reclassified to low risk after evaluation
Reclassification after evaluation indicates that the findings were assessed rather than automatically treated as high priority. A justified lower-risk rating can guide the team to allocate remediation effort to more significant issues.

https://www.isaca.org/resources/news-and-trends/industry-news/2022/taking-a-risk-based-approach-to-pen-testing

✗ **B** Not all findings from the penetration test report were fixed
Leaving some findings unresolved can create exposure, but the team may reasonably prioritize remediation according to assessed risk and the organization's ability to address the findings. The scenario does not say that the remaining findings were high risk or ignored without assessment.

https://www.isaca.org/resources/news-and-trends/industry-news/2022/taking-a-risk-based-approach-to-pen-testing
https://www.isaca.org/resources/isaca-journal/issues/2023/volume-1/mitigating-technical-vulnerabilities-with-risk-assessment

✗ **C** The penetration testing report did not contain any high-risk findings
A report with no high-risk findings is not, by itself, evidence of a serious security-management failure; the findings may have been assessed as lower risk. The more concerning issue is the absence of risk classification, which prevents informed prioritization.

https://www.isaca.org/resources/news-and-trends/industry-news/2022/taking-a-risk-based-approach-to-pen-testing

✓ **D** Risk classification of penetration test findings was not performed
Without risk classification, the team lacks a sound basis for deciding which findings require urgent remediation and which can be addressed later or accepted. This undermines risk-based prioritization and can leave the organization unaware of its most consequential exposures.

https://www.isaca.org/resources/news-and-trends/industry-news/2022/taking-a-risk-based-approach-to-pen-testing
https://www.isaca.org/resources/isaca-journal/issues/2023/volume-1/mitigating-technical-vulnerabilities-with-risk-assessment

## Question 22

Single choice · Domain: D2 Information Risk Management › Establish and/or maintain a process for information risk assessment and treatment to ensure that risk is managed to acceptable levels.

An information security manager is assessing security risk associated with a cloud service provider.

Which of the following is the MOST appropriate reference to consult when performing this assessment?

**A.** Previous provider service level agreements (SLAs)
**B.** Security control frameworks
**C.** Threat intelligence reports
**D.** Penetration test results from the provider

**Answer:** B. Security control frameworks

**Explanation**

A security control framework is the most appropriate starting point because it provides structured, broadly applicable criteria for assessing a provider's security controls and identifying gaps. This directly supports an assessment of security risk, rather than focusing on the terms of a past contract or on particular evidence sources that may cover only part of the risk picture. Frameworks can also help organize assessment of third-party and cloud risks. [1][9]

https://www.isaca.org/resources/isaca-journal/issues/2020/volume-1/the-nist-cybersecurity-framework-third-parties-need-not-comply
https://www.isaca.org/resources/isaca-journal/past-issues/2012/cloud-risk-10-principles-and-a-framework-for-assessment

✗ **A** Previous provider service level agreements (SLAs)
Past SLAs may help establish what service commitments a provider has made, but they are contractual documents and may not comprehensively describe the provider's security controls or risks. They are therefore less suitable than a security control framework as the primary reference for this assessment.

✓ **B** Security control frameworks
A security control framework provides organized criteria for assessing security practices, controls, and gaps. That makes it the most appropriate reference for systematically evaluating the security risk associated with a cloud service provider. [1][9]

https://www.isaca.org/resources/isaca-journal/issues/2020/volume-1/the-nist-cybersecurity-framework-third-parties-need-not-comply
https://www.isaca.org/resources/isaca-journal/past-issues/2012/cloud-risk-10-principles-and-a-framework-for-assessment

✗ **C** Threat intelligence reports
Threat intelligence can inform an assessment about current threats and threat actors, but it does not by itself provide a structured basis for evaluating the provider's security controls. It is a useful input, not the best overall reference for this assessment.

✗ **D** Penetration test results from the provider
Penetration test results can reveal certain technical vulnerabilities, but they represent a limited point-in-time view and may not cover the provider's full security program or the customer's relevant risks. A security control framework is a more comprehensive reference for structuring the assessment.


Free demo · full exam: 967 questions

## Question 23

Single choice · Domain: D2 Information Risk Management › Determine and/or maintain a risk treatment plan to ensure that risk is managed to an acceptable level.

Which of the following is the BEST strategy when determining an organization's approach to risk treatment?

**A.** Advancing the maturity of existing controls based on risk tolerance
**B.** Prioritizing controls that directly mitigate the organization's most critical risks
**C.** Implementing risk mitigation controls that are considered quick wins
**D.** Implementing a one-size-fits-all set of controls across all organizational units

**Answer:** B. Prioritizing controls that directly mitigate the organization's most critical risks

**Explanation**

The best strategy is to prioritize controls that directly address the organization's most critical risks. Risk treatment should be guided by assessed risk and its significance, so resources focus first on exposures that matter most rather than on convenience or a uniform control set. This approach aligns control decisions with organizational priorities.

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2019/volume-15/tips-for-prioritizing-risk-in-your-risk-register
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/risk-assessment-and-analysis-methods

✗ **A** Advancing the maturity of existing controls based on risk tolerance
Risk tolerance can inform risk-treatment decisions, and improving control maturity may be useful. However, this option does not directly ensure that controls are prioritized according to the organization's most critical risks, which is the key consideration in choosing an approach.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/risk-assessment-and-analysis-methods
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/a-kind-of-quantitative-approach-to-organizational-risk-tolerance

✓ **B** Prioritizing controls that directly mitigate the organization's most critical risks
This directs effort toward controls that address the organization's highest-priority exposures. Prioritizing risks and matching treatment to their significance helps ensure that control resources are focused where they can reduce the most important risks.

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2019/volume-15/tips-for-prioritizing-risk-in-your-risk-register
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/risk-assessment-and-analysis-methods

✗ **C** Implementing risk mitigation controls that are considered quick wins
Quick wins may be efficient, but ease or speed of implementation alone does not establish that a control addresses a critical risk. Choosing them ahead of controls for the most significant risks could leave major exposures insufficiently treated.

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2019/volume-15/tips-for-prioritizing-risk-in-your-risk-register
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/risk-assessment-and-analysis-methods

✗ **D** Implementing a one-size-fits-all set of controls across all organizational units
A uniform control set can overlook differences in risks, activities, and priorities among organizational units. Risk treatment should be informed by the risks being addressed rather than applying the same controls everywhere regardless of context.


Free demo · full exam: 967 questions

https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/addressing-risk-using-the-new-enterprise-security-risk-management-cycle
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/risk-assessment-and-analysis-methods

## Question 24

Single choice · Domain: D2 Information Risk Management › Report significant changes in information risk to appropriate management to assist in the management of risk.

The department head of application development has decided to accept the risks identified in a recent assessment. No recommendations will be implemented, even though the recommendations are required by regulatory oversight. What should the information security manager do NEXT?

**A.** Review the risk monitoring plan.
**B.** Formally document the decision.
**C.** Review the regulations.
**D.** Advise the risk management team.

**Answer:** D. Advise the risk management team.

**Explanation**

The department head is accepting a risk while refusing recommendations that are required by regulatory oversight, so the decision creates a compliance concern that should be raised with the risk management team. The information security manager should advise that team next so the issue can be addressed through the organization's risk governance and escalation process. Merely documenting the decision or monitoring the risk would not resolve the conflict with the regulatory requirement.

✗ **A** Review the risk monitoring plan.
Monitoring can track changes in risk, but it does not address the department head's refusal to implement recommendations required by regulatory oversight. The immediate need is to bring the noncompliant decision to the risk management team.

✗ **B** Formally document the decision.
Documentation is important, but recording an acceptance does not make it appropriate to disregard a regulatory requirement. The issue should first be brought to the risk management team for governance and escalation.

✗ **C** Review the regulations.
The scenario already establishes that regulatory oversight requires the recommendations. Reviewing the regulations is therefore not the next action; the manager should advise the risk management team about the decision that conflicts with that requirement.

✓ **D** Advise the risk management team.
The proposed risk acceptance conflicts with recommendations required by regulatory oversight. Advising the risk management team raises the issue to the appropriate governance body so it can be addressed rather than treated as an ordinary risk acceptance.


Free demo · full exam: 967 questions

## Question 25

Single choice · Domain: D2 Information Risk Management › Establish and/or maintain a process for information asset classification and ownership to ensure that measures taken to protect assets are appropriate.

Which of the following business units should own the data that populates an identity management system?

**A.** Human resources (HR)
**B.** Legal
**C.** Information technology
**D.** Information security

**Answer:** A. Human resources (HR)

**Explanation**

Human resources should own the employee data that populates an identity management system because HR is the business unit responsible for authoritative personnel records, such as employment status and job details. IT may operate the system and information security may define controls, but neither should be the business owner of those underlying personnel records.

https://www.isaca.org/resources/isaca-journal/issues/2020/volume-2/data-ownership

✓ **A** Human resources (HR)
HR maintains authoritative employee records and is therefore the appropriate owner of the personnel data used to create and update identities. This helps identity records reflect changes such as hires, role changes, and departures.

https://www.isaca.org/resources/isaca-journal/issues/2020/volume-2/data-ownership

✗ **B** Legal
Legal may advise on privacy, regulatory, and employment-law requirements, but it is not ordinarily responsible for maintaining the organization's authoritative employee records. Those records are the source data for employee identities.

✗ **C** Information technology
IT may administer the identity management system and its integrations, but operating the system does not make IT the business owner of the employee data it contains. The data should be owned by the function that maintains the authoritative personnel records.

https://www.isaca.org/resources/isaca-journal/issues/2020/volume-2/data-ownership

✗ **D** Information security
Information security may establish access-control and identity-management requirements, but its role is to protect and govern access to data rather than own the underlying employee records. HR is the appropriate owner of those records.


Free demo · full exam: 967 questions

## Question 26

Single choice · Domain: D2 Information Risk Management › Establish and/or maintain a process for information risk assessment and treatment to ensure that risk is managed to acceptable levels.

Which of the following tasks would provide a newly appointed information security manager with the BEST view of the organization's existing security posture?

**A.** Reviewing policies and procedures
**B.** Performing a risk assessment
**C.** Interviewing business managers and employees
**D.** Performing a business impact analysis (BIA)

**Answer:** B. Performing a risk assessment

**Explanation**

A risk assessment gives the new information security manager the broadest evidence-based view of the organization's existing security posture by examining risks to its information and systems. It can identify relevant threats and vulnerabilities and assess how well existing safeguards address them, rather than relying only on documented intentions or stakeholder impressions. This makes it a stronger overall starting point than reviewing policies, conducting interviews, or performing a BIA.

https://www.isaca.org/resources/white-papers/conducting-an-it-security-risk-assessment
https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/building-a-strong-security-posture-begins-with-assessment
https://www.isaca.org/resources/isaca-journal/past-issues/2010/performing-a-security-risk-assessment
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/it-risk-assessments-a-process-your-cio-or-ciso-will-thank-you-for

✗ **A** Reviewing policies and procedures
Policies and procedures show what the organization expects people and processes to do, but they do not by themselves establish whether those controls are implemented effectively or address the organization's actual risks. Reviewing them can inform an assessment, but it gives a narrower view of security posture than performing a risk assessment.

https://www.isaca.org/resources/white-papers/conducting-an-it-security-risk-assessment
https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/building-a-strong-security-posture-begins-with-assessment

✓ **B** Performing a risk assessment
A risk assessment evaluates risks to the organization's information and systems, helping identify relevant threats and vulnerabilities and consider the effectiveness of existing safeguards. That gives the newly appointed manager the most comprehensive view of the current security posture among these choices.

https://www.isaca.org/resources/white-papers/conducting-an-it-security-risk-assessment
https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/building-a-strong-security-posture-begins-with-assessment
https://www.isaca.org/resources/isaca-journal/past-issues/2010/performing-a-security-risk-assessment
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/it-risk-assessments-a-process-your-cio-or-ciso-will-thank-you-for

✗ **C** Interviewing business managers and employees
Interviews can reveal how people understand and experience security practices, but their findings are based on individual perspectives and may not cover the organization's full set of risks or controls. They may contribute useful information to a risk assessment, but are not the best standalone task for an overall view.

https://www.isaca.org/resources/white-papers/conducting-an-it-security-risk-assessment
https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/building-a-strong-security-posture-begins-with-


Free demo · full exam: 967 questions

assessment

✗ **D** Performing a business impact analysis (BIA)
A BIA focuses on the consequences of disruption to business activities and helps determine their importance and recovery needs. Although that information is valuable for continuity planning, it does not provide as broad an assessment of threats, vulnerabilities, and safeguards as a security risk assessment.

https://www.isaca.org/resources/glossary
https://www.isaca.org/certifications/additional-resources/-/media/35de8580e8834504b9275eb57e1c48e8.ashx

## Question 27

Single choice · Domain: D2 Information Risk Management › Report significant changes in information risk to appropriate management to assist in the management of risk.

Which of the following is MOST relevant for an information security manager to communicate to the board of directors?

**A.** The level of inherent risk
**B.** Vulnerability assessments
**C.** The level of exposure
**D.** Threat assessments

**Answer:** C. The level of exposure

**Explanation**

The board needs information that helps it understand the organization's business risk and make informed decisions. The level of exposure communicates how significantly the organization is affected by information security risk, making it more useful to directors than technical assessment activities or threat details. This aligns with guidance to report cybersecurity risk to the board in decision-relevant terms. [1] [2]

https://www.isaca.org/resources/white-papers/reporting-cybersecurity-risk-to-the-board-of-directors
https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2024/volume-23/five-key-considerations-for-crafting-board-presentations-on-information-risk-and-security

✗ **A** The level of inherent risk
Inherent risk can help describe risk before controls are considered, but it does not by itself convey the organization's resulting exposure or business impact. For board communication, the focus should be on what risk means for the organization and its decisions.

https://www.isaca.org/resources/white-papers/reporting-cybersecurity-risk-to-the-board-of-directors
https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2024/volume-23/five-key-considerations-for-crafting-board-presentations-on-information-risk-and-security

✗ **B** Vulnerability assessments
Vulnerability assessments are technical activities used to identify weaknesses; reporting the assessment itself is less useful to directors than explaining the resulting organizational risk. The board needs a decision-relevant view rather than operational detail.

https://www.isaca.org/resources/white-papers/reporting-cybersecurity-risk-to-the-board-of-directors
https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2024/volume-23/five-key-considerations-for-crafting-board-presentations-on-information-risk-and-security

✓ **C** The level of exposure
The level of exposure conveys how much the organization is at risk, which is directly relevant to board


Free demo · full exam: 967 questions

oversight and decisions about priorities and resources. It translates security concerns into the organization-level risk the board needs to understand.

https://www.isaca.org/resources/white-papers/reporting-cybersecurity-risk-to-the-board-of-directors
https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2024/volume-23/five-key-considerations-for-crafting-board-presentations-on-information-risk-and-security

✗ **D** Threat assessments
Threat assessments provide information about potential adversaries and threats, but that information alone does not show the board the organization's actual level of exposure. Directors need the business relevance and consequences of those threats, not just the assessment detail.

https://www.isaca.org/resources/white-papers/reporting-cybersecurity-risk-to-the-board-of-directors
https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2024/volume-23/five-key-considerations-for-crafting-board-presentations-on-information-risk-and-security

## Question 28

Single choice · Domain: D2 Information Risk Management › Establish and/or maintain a process for information risk assessment and treatment to ensure that risk is managed to acceptable levels.

An organization would like to invest in a new emerging technology. Which of the following is MOST important for the information security manager to consider when evaluating its impact?

**A.** Secure configuration
**B.** Vulnerabilities in the technology
**C.** Systems compatibility
**D.** Industry peer reviews of the technology

**Answer:** B. Vulnerabilities in the technology

**Explanation**

When evaluating an emerging technology, the information security manager should first identify vulnerabilities that could expose the organization to security risk. Secure configuration can reduce some risks, but it does not eliminate weaknesses inherent in the technology. Compatibility and peer reviews may inform adoption decisions, but they are less directly important to assessing the technology's security impact.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-6/performing-risk-assessments-of-emerging-technologies

✗ **A** Secure configuration
Secure configuration is an important safeguard once the technology is deployed, but it does not reveal or address all vulnerabilities inherent in a new technology. The manager should first understand those weaknesses to assess the potential security impact.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-6/performing-risk-assessments-of-emerging-technologies

✓ **B** Vulnerabilities in the technology
Identifying vulnerabilities is central to assessing how an emerging technology could create security exposure for the organization. This helps the manager evaluate risk before adoption and determine what mitigations may be needed.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-6/performing-risk-assessments-of-emerging-technologies


Free demo · full exam: 967 questions

✗ **C** Systems compatibility
Compatibility matters for integration and operation, but it does not by itself establish the technology's information security impact. Security weaknesses can remain even when the technology works well with existing systems.

✗ **D** Industry peer reviews of the technology
Peer reviews may provide useful context about others' experiences, but they are indirect evidence and may not identify vulnerabilities relevant to this organization's use. The manager should evaluate the technology's security weaknesses directly.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-6/performing-risk-assessments-of-emerging-technologies

## Question 29

Single choice · Domain: D2 Information Risk Management › Establish and/or maintain a process for information risk assessment and treatment to ensure that risk is managed to acceptable levels.

The PRIMARY purpose of vulnerability identification is to:

**A.** Remediate vulnerabilities before they are exploited
**B.** Discover control deficiencies
**C.** Provide vulnerability identifiers for risk reporting
**D.** Prioritize vulnerability remediation

**Answer:** B. Discover control deficiencies

**Explanation**

Vulnerability identification is primarily about finding weaknesses in systems or deficiencies in the controls intended to protect them. In this question, discovering control deficiencies is the identification outcome; remediation and prioritization happen after identified issues are assessed. [1][4]

https://www.isaca.org/career-center/career-journey/vulnerability-discovery-and-assessment
https://www.isaca.org/resources/white-papers/vulnerability-assessment

✗ **A** Remediate vulnerabilities before they are exploited
Remediation is a response to vulnerabilities that have already been identified, not the primary purpose of the identification activity itself. Identification helps reveal what needs attention; it does not itself fix the weaknesses.

https://www.isaca.org/career-center/career-journey/vulnerability-discovery-and-assessment
https://www.isaca.org/resources/white-papers/vulnerability-assessment

✓ **B** Discover control deficiencies
Identifying vulnerabilities reveals weaknesses, including deficiencies in security controls. That discovery is the primary purpose asked for here; remediation or further risk-based decisions can follow.

https://www.isaca.org/career-center/career-journey/vulnerability-discovery-and-assessment
https://www.isaca.org/resources/white-papers/vulnerability-assessment

✗ **C** Provide vulnerability identifiers for risk reporting
Identifiers may help document or communicate vulnerabilities, but producing identifiers is not the primary objective of finding them. The central objective is to discover weaknesses or control deficiencies.

✗ **D** Prioritize vulnerability remediation
Prioritization determines which identified vulnerabilities should be addressed first, typically using risk


Free demo · full exam: 967 questions

considerations. It is a later decision, distinct from the initial identification of control deficiencies.

https://www.isaca.org/resources/news-and-trends/industry-news/2023/using-a-risk-based-approach-to-prioritize-vulnerability-remediation
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/risk-assessment-for-technical-vulnerabilities

## Question 30

Single choice · Domain: D2 Information Risk Management › Monitor existing risk to ensure that changes are identified and managed appropriately.

An information security manager has been notified that two senior executives have the ability to elevate their own privileges in the corporate accounting system, in violation of policy. What is the FIRST step to address this issue?

**A.** Immediately suspend the executives' access privileges.
**B.** Notify the CISO of the security policy violation.
**C.** Perform a full review of all system transactions over the past 90 days.
**D.** Perform a system access review.

**Answer:** D. Perform a system access review.

**Explanation**

A system access review is the first step because it establishes which privileges the executives have and whether those privileges violate policy. This assessment helps determine the scope and appropriate remediation before access is changed or transaction history is investigated. The review should focus on the accounting system and the reported ability to elevate privileges.

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/user-access-review-verification-a-step-by-step-guide
https://www.isaca.org/resources/isaca-journal/issues/2019/volume-4/effective-user-access-reviews

✗ **A** Immediately suspend the executives' access privileges.
Suspending access before reviewing it may disrupt legitimate work and does not first establish the exact access or policy violation. The access review provides the information needed to decide what privileges should be removed or restricted.

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/user-access-review-verification-a-step-by-step-guide
https://www.isaca.org/resources/isaca-journal/issues/2019/volume-4/effective-user-access-reviews

✗ **B** Notify the CISO of the security policy violation.
Escalation may be appropriate, but the first step is to review the system access and verify the nature and scope of the reported privilege issue. That assessment gives decision-makers concrete information for follow-up.

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/user-access-review-verification-a-step-by-step-guide
https://www.isaca.org/resources/isaca-journal/issues/2019/volume-4/effective-user-access-reviews

✗ **C** Perform a full review of all system transactions over the past 90 days.
A 90-day transaction review is a broad investigative action and does not first establish what access the executives have or whether they used elevated privileges. An access review can clarify the exposure and inform whether transaction analysis is needed.

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/user-access-review-verification-a-step-by-


Free demo · full exam: 967 questions

step-guide
https://www.isaca.org/resources/isaca-journal/issues/2019/volume-4/effective-user-access-reviews

✓ **D** Perform a system access review.
The access review directly checks the executives' permissions and ability to elevate privileges against policy. It provides the necessary basis for deciding on targeted remediation and any further investigation.

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/user-access-review-verification-a-step-by-step-guide
https://www.isaca.org/resources/isaca-journal/issues/2019/volume-4/effective-user-access-reviews

## Question 31

Single choice · Domain: D2 Information Risk Management › Monitor existing risk to ensure that changes are identified and managed appropriately.

Which of the following is an information security manager's MOST important course of action after receiving information about a new cybersecurity threat?

**A.** Assess the impact of the new threat on the organization in the event of materialization.
**B.** Update correlation rules for log monitoring to detect the possible emerging threat.
**C.** Report the threat to senior management immediately to enable an informed decision.
**D.** Review the enterprise architecture (EA) for vulnerabilities exploited by the threat.

**Answer:** A. Assess the impact of the new threat on the organization in the event of materialization.

**Explanation**

The manager's first priority is to determine how the threat could affect this organization if it materializes. That impact assessment establishes the threat's relevance and potential risk, which can then guide whether to adjust monitoring, review architecture, or escalate the issue to senior management. References on evidence-based threat prioritization and risk assessment support evaluating organizational impact before choosing a response.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/evidence-based-prioritization-of-cybersecurity-threats
https://www.isaca.org/resources/isaca-journal/issues/2023/volume-1/mitigating-technical-vulnerabilities-with-risk-assessment

✓ **A** Assess the impact of the new threat on the organization in the event of materialization.
This establishes the threat's potential consequences for this specific organization and supports prioritizing an appropriate response. The manager needs this assessment before deciding whether technical changes or immediate escalation are warranted.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/evidence-based-prioritization-of-cybersecurity-threats
https://www.isaca.org/resources/isaca-journal/issues/2023/volume-1/mitigating-technical-vulnerabilities-with-risk-assessment

✗ **B** Update correlation rules for log monitoring to detect the possible emerging threat.
Changing monitoring rules is a possible operational response, but it is premature before determining whether the threat is relevant to the organization and what its potential impact is. The assessment should inform whether this action is needed.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/evidence-based-prioritization-of-cybersecurity-

threats
https://www.isaca.org/resources/isaca-journal/issues/2023/volume-3/a-framework-for-siem-implementation

✗ **C** Report the threat to senior management immediately to enable an informed decision.
Escalation may be appropriate, but an informed management decision requires understanding the threat's potential impact on the organization. Assess that impact first, then communicate the threat with its organizational risk and context.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/evidence-based-prioritization-of-cybersecurity-threats

✗ **D** Review the enterprise architecture (EA) for vulnerabilities exploited by the threat.
An architecture review may be useful if the threat exploits weaknesses present in the organization's environment. The manager should first assess the threat's potential organizational impact to determine whether this review is relevant and how urgently it is needed.

https://www.isaca.org/resources/isaca-journal/issues/2023/volume-1/mitigating-technical-vulnerabilities-with-risk-assessment

## Question 32

Single choice · Domain: D2 Information Risk Management › Establish and/or maintain a process for information risk assessment and treatment to ensure that risk is managed to acceptable levels.

What should be an information security manager's FIRST course of action upon learning a business unit is bypassing an existing control in order to increase operational efficiency?

**A.** Report the noncompliance to senior management.
**B.** Assess the risk of noncompliance.
**C.** Activate the incident response plan.
**D.** Evaluate possible compensating controls.

**Answer:** B. Assess the risk of noncompliance.

**Explanation**

The manager's first step should be to assess the risk created by bypassing the control. That assessment establishes the potential impact and likelihood of the noncompliance and helps determine an appropriate response. Reporting the issue or considering compensating controls may follow, informed by the assessment; an incident response plan is not automatically warranted just because a control is being bypassed.

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2019/volume-14/five-key-considerations-when-developing-information-security-risk-treatment-plans
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/a-holistic-approach-to-controls-risk-and-maturity

✗ **A** Report the noncompliance to senior management.
Escalation may be appropriate after the situation and its risk are understood, but it is not the best first course of action here. Assessing the risk provides a basis for deciding the urgency and appropriate level of escalation.

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2019/volume-14/five-key-considerations-when-developing-information-security-risk-treatment-plans

✓ **B** Assess the risk of noncompliance.
The manager should first determine the consequences and degree of risk created by bypassing the control. That understanding informs whether to escalate, require corrective action, or consider a


Free demo · full exam: 967 questions

compensating control.

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2019/volume-14/five-key-considerations-when-developing-information-security-risk-treatment-plans
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/a-holistic-approach-to-controls-risk-and-maturity

✗ **C** Activate the incident response plan.
The scenario describes deliberate control bypass for operational efficiency, but does not indicate that a security incident has occurred or that incident-response criteria have been met. Activating that plan is therefore premature before assessing the risk and circumstances.

https://www.isaca.org/resources/isaca-journal/past-issues/2011/jonline-an-introduction-to-information-security-incident-management-based-on-iso-iec-tr-18044-2004
https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance

✗ **D** Evaluate possible compensating controls.
A compensating control could be considered as a way to address the risk, but selecting or evaluating treatments should be informed by an assessment of the risk first. The manager needs to understand what risk the bypass creates before deciding what alternative control may be suitable.

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2019/volume-14/five-key-considerations-when-developing-information-security-risk-treatment-plans
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/a-holistic-approach-to-controls-risk-and-maturity

## Question 33

Single choice · Domain: D2 Information Risk Management › Establish and/or maintain a process for information risk assessment and treatment to ensure that risk is managed to acceptable levels.

During the due diligence phase of an acquisition, the MOST important course of action for an information security manager is to:

**A.** Perform a risk assessment
**B.** Perform a gap analysis
**C.** Review information security policies
**D.** Review the state of security awareness

**Answer:** A. Perform a risk assessment

**Explanation**

During acquisition due diligence, the information security manager needs to identify and evaluate the target organization's security risks so decision-makers can understand potential exposure before the transaction proceeds. A risk assessment provides that broad view and can inform later actions such as remediation planning or integration. Reviewing policies, awareness, or gaps may be useful inputs, but each is narrower than assessing overall risk. [5]

https://www.isaca.org/resources/isaca-journal/issues/2025/volume-3/mergers-and-acquisitions

✓ **A** Perform a risk assessment
A risk assessment evaluates the security risks associated with the acquisition target, giving decision-makers a basis for understanding potential exposure during due diligence. Its scope is broader than examining one specific control area and can guide subsequent remediation and integration priorities. [5]

https://www.isaca.org/resources/isaca-journal/issues/2025/volume-3/mergers-and-acquisitions

✗ **B** Perform a gap analysis

A gap analysis can identify differences between the target's current practices and a desired framework or standard. By itself, it does not provide the broad evaluation of risks and their potential impact that is most important during acquisition due diligence.

✗ **C** Review information security policies
Policy review can reveal governance requirements and possible deficiencies, but it examines only documented rules and direction. It does not establish the target's overall security risk exposure.

✗ **D** Review the state of security awareness
Assessing security awareness may uncover human-factor weaknesses, but it addresses only one part of the security posture. Due diligence calls first for a broader assessment of the target's risks.

## Question 34

Single choice · Domain: D3 Information Security Program › Integrate information security requirements into organizational processes (e.g., change management, mergers and acquisitions, development, business continuity, disaster recovery) to maintain the organization's security strategy.

Which of the following would be the BEST way to reduce the risk of disruption resulting from an emergency system change?

**A.** Confirm the change implementation is scheduled.
**B.** Verify the change request has been approved.
**C.** Confirm rollback plans are in place.
**D.** Notify users affected by the change.

**Answer:** C. Confirm rollback plans are in place.

**Explanation**

An emergency system change may need to be implemented quickly, but it can still cause outages or other unintended effects. Confirming that a rollback plan is ready provides a way to restore the prior state if the change causes disruption, directly reducing the risk named in the question. Scheduling, approval, and notifying affected users support change coordination but do not by themselves provide a recovery path.

https://www.isaca.org/resources/isaca-journal/past-issues/2011/auditing-it-risk-associated-with-change-management-and-application-development
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/information-system-contingency-planning-guidance

✗ **A** Confirm the change implementation is scheduled.
Scheduling helps coordinate when the change occurs, but it does not reduce the impact if the emergency change fails or disrupts the system. A rollback plan provides a direct means to recover from that outcome.

https://www.isaca.org/resources/isaca-journal/past-issues/2011/auditing-it-risk-associated-with-change-management-and-application-development

✗ **B** Verify the change request has been approved.
Approval is an important control over whether a change is authorized, but it does not ensure the system can be restored if the implementation causes disruption. The question asks for the best way to reduce that operational risk.

https://www.isaca.org/resources/isaca-journal/past-issues/2011/auditing-it-risk-associated-with-change-management-and-application-development


Free demo · full exam: 967 questions

✓ **C** Confirm rollback plans are in place.
A rollback plan makes it possible to return the system to its prior state if the emergency change causes problems. That recovery capability directly limits the duration and consequences of disruption.

https://www.isaca.org/resources/isaca-journal/past-issues/2011/auditing-it-risk-associated-with-change-management-and-application-development
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/information-system-contingency-planning-guidance

✗ **D** Notify users affected by the change.
Notifying users can help them prepare for an outage or change in service, but it does not prevent or reverse a disruption. A rollback plan better addresses the risk that the emergency change itself adversely affects the system.

https://www.isaca.org/resources/isaca-journal/past-issues/2011/auditing-it-risk-associated-with-change-management-and-application-development

## Question 35

Single choice · Domain: D3 Information Security Program › Establish and/or maintain a security awareness and training program.

An organization has an ongoing security awareness training program. Employee participation has been decreasing over the year, while the number of malware and phishing incidents from email has been increasing. What is the information security manager's BEST course of action?

**A.** Report the findings to senior management with recommendations.
**B.** Implement a phishing reporting tool in the email system.
**C.** Include regular phishing campaigns after each training session.
**D.** Make the training program mandatory for all employees.

**Answer:** D. Make the training program mandatory for all employees.

**Explanation**

Because participation is declining while email-related malware and phishing incidents are increasing, the immediate priority is to ensure employees receive the awareness training. Making the program mandatory directly addresses the participation gap and establishes consistent coverage across the workforce. Reporting, a reporting tool, or phishing campaigns may help, but none by itself ensures that employees take the existing training.

✗ **A** Report the findings to senior management with recommendations.
Escalating the trend may gain management attention, but it does not directly resolve declining employee participation. The manager should take the direct step of requiring training so employees receive the awareness intervention.

✗ **B** Implement a phishing reporting tool in the email system.
A reporting tool can help employees report suspicious messages, but it does not ensure they participate in the awareness program. It addresses one response capability rather than the stated participation problem.

✗ **C** Include regular phishing campaigns after each training session.
Phishing campaigns can reinforce training and measure employee responses, but they do not ensure that employees attend or complete training. With participation declining, making the training mandatory is the more direct action.


Free demo · full exam: 967 questions

✓ **D** Make the training program mandatory for all employees.
Mandatory training directly addresses the falling participation and ensures employees receive consistent security awareness instruction. This is especially pertinent given the concurrent increase in email-based malware and phishing incidents.

## Question 36

Single choice · Domain: D3 Information Security Program › Integrate information security requirements into organizational processes (e.g., change management, mergers and acquisitions, development, business continuity, disaster recovery) to maintain the organization's security strategy.

Which of the following should an information security manager do FIRST when developing an organization's disaster recovery plan (DRP)?

**A.** Conduct a risk assessment.
**B.** Document disaster recovery procedures.
**C.** Identify business requirements.
**D.** Perform a business impact analysis (BIA).

**Answer:** D. Perform a business impact analysis (BIA).

**Explanation**

A business impact analysis (BIA) should be performed first because it identifies the impact of disruptions on business functions and establishes recovery priorities and requirements. Those findings give the DRP a business-focused foundation before specific procedures are documented. Risk assessment and identifying requirements are important activities, but the keyed first step is the BIA.

✗ **A** Conduct a risk assessment.
A risk assessment identifies threats and vulnerabilities, but it does not by itself establish which business functions are most critical or their recovery priorities. The BIA is the first step specified for grounding this DRP in business impacts.

✗ **B** Document disaster recovery procedures.
Procedures should be documented only after the organization understands the impacts of disruption and its recovery priorities. Starting with procedures would risk creating plans that do not address the most important business needs.

✗ **C** Identify business requirements.
Business requirements are important to DR planning, but the BIA first analyzes the consequences of disruption and helps establish recovery priorities. This makes the BIA the best first action among the choices.

✓ **D** Perform a business impact analysis (BIA).
The BIA determines how disruptions affect business functions and helps prioritize what must be recovered and how quickly. These findings provide the foundation for developing the DRP and its procedures.


Free demo · full exam: 967 questions

## Question 37

Single choice · Domain: D3 Information Security Program › Establish, monitor and report program management and operational metrics to evaluate the effectiveness and efficiency of the information security program.

A department has reported that a security control is no longer effective. Which of the following is the information security manager's BEST course of action?

**A.** Assess the control state.
**B.** Replace the control.
**C.** Report the failure to management.
**D.** Check for defense in depth.

**Answer:** A. Assess the control state.

**Explanation**

The department's report is an indication that the control may not be working as intended, but the manager should first assess its current state and verify the problem. That assessment provides a basis for deciding whether the control needs repair, replacement, or another response. Replacing it or escalating the failure before assessing it would skip this important first step.

✓ **A** Assess the control state.
This is the best first action because it verifies the control's actual condition and effectiveness rather than relying only on the department's report. The results can then guide an appropriate response, such as remediation or replacement.

✗ **B** Replace the control.
Replacement is premature before determining whether the control has actually failed and what caused the reported issue. Assessing its state first helps establish whether replacement is necessary or whether another corrective action would address the problem.

✗ **C** Report the failure to management.
The report is not yet a confirmed failure; the manager should first assess the control's state. Once the issue and its significance are established, management can be informed as appropriate.

✗ **D** Check for defense in depth.
Defense in depth may help determine whether other safeguards reduce risk, but it does not establish whether this particular control is ineffective. The immediate best action is to assess the reported control itself.


Free demo · full exam: 967 questions

## Question 38

Single choice · Domain: D3 Information Security Program › Establish, communicate and maintain organizational information security standards, procedures and other documentation.

When defining a security baseline, it is MOST important that the baseline:

**A.** can vary depending on the security classification of systems.
**B.** is uniform for all assets of the same type.
**C.** is developed based on stakeholder consensus.
**D.** aligns to key risk indicators (KRIs).

**Answer:** B. is uniform for all assets of the same type.

**Explanation**

A security baseline establishes a consistent minimum set of security requirements for assets of the same type. Applying it uniformly makes expected controls clear and repeatable; different asset types may require different baselines, but assets within the same type should follow the same baseline. [1]

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/differentiating-key-terms-in-the-information-security-hierarchy

✗ **A** can vary depending on the security classification of systems.
Classification can inform which baseline applies, and differently classified systems may need different baselines. However, the key requirement is consistency among assets of the same type, rather than allowing a baseline to vary without regard to asset type.

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/differentiating-key-terms-in-the-information-security-hierarchy

✓ **B** is uniform for all assets of the same type.
A baseline provides a consistent set of security requirements for assets that share a type. Uniform application makes the expected protections repeatable and provides a common standard for assessing those assets.

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/differentiating-key-terms-in-the-information-security-hierarchy

✗ **C** is developed based on stakeholder consensus.
Stakeholder input can help shape security requirements, but consensus is not the defining property of a baseline. The baseline must provide consistent requirements for assets of the same type.

✗ **D** aligns to key risk indicators (KRIs).
KRIs are indicators used to monitor or communicate risk; alignment to them is not what makes a security baseline effective. A baseline's central purpose is to specify consistent security requirements for comparable assets.


Free demo · full exam: 967 questions

## Question 39

Single choice · Domain: D3 Information Security Program › Integrate information security requirements into organizational processes (e.g., change management, mergers and acquisitions, development, business continuity, disaster recovery) to maintain the organization's security strategy.

Which of the following has the GREATEST impact on the ability to successfully execute a disaster recovery plan (DRP)?

**A.** Conducting tabletop exercises of the plan
**B.** Updating the plan periodically
**C.** Communicating the plan to all stakeholders
**D.** Reviewing escalation procedures

**Answer:** A. Conducting tabletop exercises of the plan

**Explanation**

Conducting tabletop exercises has the greatest impact because it lets stakeholders rehearse the DRP, test whether roles and actions work as intended, and identify gaps before a real disruption. This directly builds the organization's ability to execute the plan, rather than only keeping the document current or familiarizing people with it. A

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-48/five-key-considerations-for-developing-crisis-management-and-incident-response-tabletop-exercises
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/using-tabletops-and-simulations-to-build-better-incident-responders
https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance

✓ **A** Conducting tabletop exercises of the plan
Tabletop exercises walk participants through disaster scenarios and let them practice decisions, responsibilities, and coordination using the DRP. That rehearsal can expose practical gaps and improve readiness to execute the plan under pressure.

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-48/five-key-considerations-for-developing-crisis-management-and-incident-response-tabletop-exercises
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/using-tabletops-and-simulations-to-build-better-incident-responders
https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance

✗ **B** Updating the plan periodically
Periodic updates help keep the DRP accurate as systems, personnel, and business requirements change. However, updates alone do not demonstrate that people can carry out the procedures successfully; exercises provide that practical test.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/reduced-appetite-how-covid-19-will-impact-future-business-continuity-planning
https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/is-audit-basics-backup-and-recovery

✗ **C** Communicating the plan to all stakeholders
Stakeholders need to know the plan and their responsibilities, but distributing or communicating it does not ensure they can coordinate and act effectively during a disaster. Tabletop exercises actively rehearse those actions and reveal execution problems.

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-48/five-key-considerations-for-developing-crisis-management-and-incident-response-tabletop-exercises
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/using-tabletops-and-simulations-to-build-better-incident-responders

✗ **D** Reviewing escalation procedures
Reviewing escalation procedures can clarify when and how an incident is raised to the appropriate decision-makers. It is narrower than exercising the DRP as a whole and does not provide the same opportunity to rehearse and validate execution across roles.

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-48/five-key-considerations-for-developing-crisis-management-and-incident-response-tabletop-exercises
https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance

## Question 40

Single choice · Domain: D3 Information Security Program › Establish and maintain information security architectures (people, process, technology) to execute the information security program.

Which of the following is the BEST way to evaluate the effectiveness of physical and environmental security controls implemented for fire-related disasters?

**A.** Conduct evacuation exercises
**B.** Review the disaster recovery plan (DRP)
**C.** Conduct awareness sessions
**D.** Review emergency management team procedures

**Answer:** A. Conduct evacuation exercises

**Explanation**

Evacuation exercises directly test how well fire-related physical and environmental safeguards work in practice, including whether alarms, egress routes, and evacuation arrangements support a safe and timely response. They provide observable evidence of control effectiveness, whereas reviewing plans or holding awareness sessions does not test the controls under simulated conditions.

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/ensuring-you-have-the-right-governance-in-place-for-physical-and-environmental-controls
https://www.isaca.org/about-us/newsroom/press-releases/2022/isaca-introduces-new-audit-program-for-physical-and-environmental-security

✓ **A** Conduct evacuation exercises
An evacuation exercise puts fire-response arrangements into practice and can reveal whether alarms, exits, and evacuation procedures work effectively. This is the most direct way among the choices to evaluate the controls in operation.

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/ensuring-you-have-the-right-governance-in-place-for-physical-and-environmental-controls
https://www.isaca.org/about-us/newsroom/press-releases/2022/isaca-introduces-new-audit-program-for-physical-and-environmental-security

✗ **B** Review the disaster recovery plan (DRP)
A DRP review checks the written recovery approach, but does not demonstrate that physical safeguards or evacuation arrangements function effectively during a fire-related event. An exercise provides more direct evidence of operational effectiveness.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/information-system-contingency-planning-guidance

✗ **C** Conduct awareness sessions

Awareness sessions can inform personnel about fire risks and required actions, but they do not test whether physical and environmental controls work or whether occupants can evacuate successfully. They are a preparedness measure rather than the best effectiveness evaluation.

✗ **D** Review emergency management team procedures
Reviewing procedures can identify gaps in documentation, but it does not show whether the controls and response arrangements work in practice. An evacuation exercise tests these arrangements more directly.

https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/ensuring-you-have-the-right-governance-in-place-for-physical-and-environmental-controls

## Question 41

Single choice · Domain: D3 Information Security Program › Integrate information security requirements into contracts and activities of third parties (e.g., joint ventures, outsourced providers, business partners, customers) to maintain the organization's security strategy.

Which of the following should be of GREATEST concern to an information security manager when evaluating a cloud service provider?

**A.** Data retention policies are not documented
**B.** There is no right to audit the security of the provider
**C.** The provider is new to the market and lacks references
**D.** Security controls offered by the provider are inadequate

**Answer:** D. Security controls offered by the provider are inadequate

**Explanation**

Inadequate security controls are the greatest concern because they mean the provider may not be able to protect the organization’s data and systems to the required level. Documentation, audit rights, and provider experience can help assess or oversee risk, but they do not substitute for controls that actually reduce security risk.

✗ **A** Data retention policies are not documented
This creates uncertainty about how long the provider keeps data and how it is disposed of, so it is a meaningful governance concern. However, it is less fundamental than inadequate security controls, which directly leave data and systems insufficiently protected.

✗ **B** There is no right to audit the security of the provider
The lack of audit rights can limit the organization’s ability to verify the provider’s security practices. It is a serious oversight limitation, but it does not itself establish that the provider’s security controls are inadequate; the controls’ actual adequacy is the greater concern.

✗ **C** The provider is new to the market and lacks references
Limited operating history and references make it harder to assess the provider’s reliability and experience. This is a warning sign, but it is less directly consequential than security controls that are known to be inadequate.

✓ **D** Security controls offered by the provider are inadequate
A cloud provider’s controls need to protect the organization’s information and services against relevant threats. If those controls are inadequate, the organization faces direct exposure that documentation, audit access, or the provider’s market history cannot make acceptable.


Free demo · full exam: 967 questions

## Question 42

Single choice · Domain: D3 Information Security Program › Integrate information security requirements into organizational processes (e.g., change management, mergers and acquisitions, development, business continuity, disaster recovery) to maintain the organization's security strategy.

Which of the following should an information security manager do FIRST when developing an organization's disaster recovery plan (DRP)?

**A.** Identify business requirements
**B.** Document disaster recovery procedures
**C.** Conduct a risk assessment
**D.** Perform a business impact analysis (BIA)

**Answer:** D. Perform a business impact analysis (BIA)

**Explanation**

A business impact analysis (BIA) should come first because it identifies the business processes and systems that matter most, the consequences of disruption, and the recovery priorities the DRP must address. Those findings give the organization a basis for shaping recovery requirements and procedures. Risk assessment is useful, but it does not replace the BIA's role in establishing business impact and recovery priorities.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/information-system-contingency-planning-guidance
https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-30/understanding-the-information-system-contingency-plan

✗ **A** Identify business requirements
Business requirements for recovery should be informed by the BIA, which establishes the business impact of disruption and the priorities for restoring operations. Identifying requirements before that analysis risks setting recovery goals without understanding which activities are most critical.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/information-system-contingency-planning-guidance
https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-30/understanding-the-information-system-contingency-plan

✗ **B** Document disaster recovery procedures
Procedures are developed after the organization has determined what must be recovered and in what order. Documenting them first could produce steps that do not reflect business priorities or required recovery objectives.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/information-system-contingency-planning-guidance
https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-30/understanding-the-information-system-contingency-plan

✗ **C** Conduct a risk assessment
A risk assessment helps identify and evaluate threats, but the question asks for the first step in developing the DRP. The BIA first establishes the consequences of disruption and recovery priorities that the plan needs to address.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/information-system-contingency-planning-guidance
https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-30/understanding-the-


Free demo · full exam: 967 questions

information-system-contingency-plan

✓ **D** Perform a business impact analysis (BIA)
The BIA identifies critical business functions, assesses the effects of their disruption, and establishes recovery priorities. This provides the foundation for determining recovery requirements and developing appropriate DRP procedures.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/information-system-contingency-planning-guidance
https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-30/understanding-the-information-system-contingency-plan

## Question 43

Single choice · Domain: D3 Information Security Program › Establish, monitor and report program management and operational metrics to evaluate the effectiveness and efficiency of the information security program.

An organization has implemented controls to mitigate risks resulting from identified vulnerabilities in an application. Which of the following is the BEST way to verify all weaknesses have been addressed?

**A.** Perform a vulnerability assessment
**B.** Conduct an internal audit
**C.** Conduct penetration testing
**D.** Prepare compensating controls

**Answer:** C. Conduct penetration testing

**Explanation**

Penetration testing is the best way to verify whether the controls implemented to address the application's identified vulnerabilities actually work. By attempting to exploit weaknesses under authorized conditions, testing can reveal remaining exploitable gaps that a vulnerability assessment or control review might not demonstrate. [1]

https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/planning-for-information-security-testinga-practical-approach

✗ **A** Perform a vulnerability assessment
A vulnerability assessment can identify and rank known weaknesses, but it does not necessarily demonstrate whether an attacker can exploit them or whether the implemented controls effectively prevent exploitation. The question asks to verify that the weaknesses have been addressed, making penetration testing more suitable.

https://www.isaca.org/resources/white-papers/vulnerability-assessment

✗ **B** Conduct an internal audit
An internal audit can assess whether processes and controls are designed or operating as required, but it is not the strongest way to test whether application weaknesses remain exploitable. The scenario calls for practical validation of the application's technical defenses.

✓ **C** Conduct penetration testing
Penetration testing attempts to exploit weaknesses in a controlled, authorized manner, helping determine whether vulnerabilities remain exploitable after controls were implemented. That makes it the best choice for validating the effectiveness of the controls against the identified application risks.

https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/planning-for-information-security-testinga-practical-approach


Free demo · full exam: 967 questions

https://www.isaca.org/career-center/career-journey/vulnerability-discovery-and-assessment/penetration-tester

✗ **D** Prepare compensating controls
Compensating controls are alternative safeguards used when a preferred control cannot be implemented or is insufficient; preparing them does not verify that existing controls addressed the application's weaknesses. The scenario asks for testing, not another risk-treatment measure.

## Question 44

Single choice · Domain: D3 Information Security Program › Integrate information security requirements into contracts and activities of third parties (e.g., joint ventures, outsourced providers, business partners, customers) to maintain the organization's security strategy.

A global organization has outsourced security processes to a service provider by means of a global agreement. What is the MOST efficient approach to meet country-specific regulatory requirements?

**A.** Include binding corporate rules into the global agreement
**B.** Set up a governance organization for each country
**C.** Review the agreement for each country separately
**D.** Set up companion agreements for each country

**Answer:** D. Set up companion agreements for each country

**Explanation**

Companion agreements let the organization retain one global agreement while adding terms needed to address each country's regulatory requirements. This is more efficient than creating separate governance organizations or repeatedly reviewing the global agreement without adding country-specific contractual provisions. Binding corporate rules address a narrower set of data-protection needs, not all country-specific security requirements.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/the-impact-of-schrems-ii-on-the-modern-multinational-information-security-practice-part-1
https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/technology-and-regulatory-compliance-in-global-organizations-stuck-between-a-rock-and-a-hard-place

✗ **A** Include binding corporate rules into the global agreement
Binding corporate rules can support certain cross-border personal-data transfers, but they do not necessarily address the full range of country-specific security and regulatory requirements in this scenario. They are therefore less suitable than country-specific companion agreements.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/the-impact-of-schrems-ii-on-the-modern-multinational-information-security-practice-part-1

✗ **B** Set up a governance organization for each country
Separate governance organizations would add substantial administrative overhead across countries. The question asks for the most efficient approach, and country-specific contractual terms can address local requirements without duplicating governance structures.

https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/technology-and-regulatory-compliance-in-global-organizations-stuck-between-a-rock-and-a-hard-place

✗ **C** Review the agreement for each country separately
Reviewing the global agreement can identify local requirements, but review alone does not provide country-specific contractual terms to meet them. It also repeats effort for each country rather than using a targeted contractual supplement.


Free demo · full exam: 967 questions

https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/technology-and-regulatory-compliance-in-global-organizations-stuck-between-a-rock-and-a-hard-place

✓ **D** Set up companion agreements for each country
Companion agreements allow country-specific regulatory terms to supplement the existing global agreement. This preserves the efficiency of a common global framework while addressing local requirements where they apply.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/the-impact-of-schrems-ii-on-the-modern-multinational-information-security-practice-part-1
https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/technology-and-regulatory-compliance-in-global-organizations-stuck-between-a-rock-and-a-hard-place

## Question 45

Single choice · Domain: D3 Information Security Program › Establish and maintain information security architectures (people, process, technology) to execute the information security program.

For an e-business that requires high availability, which of the following design principles is BEST?

**A.** Manual failover to the website of another e-business that meets the user's needs
**B.** A single point of entry allowing transactions to be received and processed quickly
**C.** Intelligent middleware to direct transactions from a downed system to an alternative
**D.** Availability of an adjacent cold site and a standby server with mirrored copies of critical data

**Answer:** C. Intelligent middleware to direct transactions from a downed system to an alternative

**Explanation**

Intelligent middleware can detect when a system is unavailable and route transactions to an alternative system, helping the e-business continue operating with minimal interruption. This supports high availability more directly than manual recovery or a cold-site arrangement, which may involve delays before service resumes.

✗ **A** Manual failover to the website of another e-business that meets the user's needs
This depends on people recognizing the outage and manually directing users elsewhere, so it does not provide seamless or rapid continuity. It also shifts transactions away from the e-business's own service.

✗ **B** A single point of entry allowing transactions to be received and processed quickly
A single entry point can itself become a single point of failure. Processing transactions quickly when the system is operating does not ensure that service remains available during a failure.

✓ **C** Intelligent middleware to direct transactions from a downed system to an alternative
Middleware can redirect transactions automatically or intelligently when a system goes down, allowing an alternative system to continue serving users. That failover capability directly supports the high-availability requirement.

✗ **D** Availability of an adjacent cold site and a standby server with mirrored copies of critical data
A cold site generally requires setup and recovery work before it can take over, so it may not restore service quickly. A standby server and mirrored data can help recovery, but this option is less effective for maintaining continuous availability than routing traffic to an available alternative.


Free demo · full exam: 967 questions

## Question 46

Single choice · Domain: D3 Information Security Program › Integrate information security requirements into contracts and activities of third parties (e.g., joint ventures, outsourced providers, business partners, customers) to maintain the organization's security strategy.

Which of the following BEST helps to ensure a third-party backup site continues to meet the organization’s information security standards?

**A.** Service level agreement (SLA)
**B.** Memorandum of understanding (MoU)
**C.** Business continuity plan (BCP)
**D.** Disaster recovery plan (DRP)

**Answer:** A. Service level agreement (SLA)

**Explanation**

A service level agreement (SLA) can specify the security requirements, service expectations, and monitoring or reporting obligations the third-party backup site must meet. This makes it the best choice for helping ensure the provider continues to align with the organization’s information security standards. A BCP or DRP guides continuity or recovery activities, while an MoU generally documents an understanding rather than defining enforceable service requirements.

https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/ensuring-vendor-compliance-and-thirdparty-risk-mitigation

✓ **A** Service level agreement (SLA)
An SLA can set out the provider’s required security controls and service commitments, along with measures for checking performance. Those contractual requirements help the organization ensure the third-party backup site continues to meet its standards.

https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/ensuring-vendor-compliance-and-thirdparty-risk-mitigation

✗ **B** Memorandum of understanding (MoU)
An MoU generally records the parties’ understanding or intentions, but is less suited than an SLA to establishing specific, measurable ongoing security and service requirements for the backup provider.

✗ **C** Business continuity plan (BCP)
A BCP describes how the organization maintains or restores business operations during disruption. It does not, by itself, set or enforce the third-party site’s ongoing information security obligations.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/information-system-contingency-planning-guidance

✗ **D** Disaster recovery plan (DRP)
A DRP focuses on restoring systems and data after a disaster. It may address use of a backup site, but it does not establish the provider’s continuing security commitments as directly as an SLA does.

https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/information-security-matters-do-you-need-a-disaster-recovery-plan


Free demo · full exam: 967 questions

## Question 47

Single choice · Domain: D3 Information Security Program › Establish, monitor and report program management and operational metrics to evaluate the effectiveness and efficiency of the information security program.

Which of the following provides the MOST comprehensive understanding of an organization's information security posture?

**A.** Security maturity assessment results
**B.** Threat analysis of the organization's environment
**C.** Results of vulnerability assessments
**D.** External penetration test findings

**Answer:** A. Security maturity assessment results

**Explanation**

A security maturity assessment gives the broadest view because it evaluates how systematically the organization manages security, rather than examining only a particular threat set or testing for specific weaknesses. This makes it the best fit for understanding the organization's overall information security posture. [12]

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/a-holistic-approach-to-controls-risk-and-maturity

✓ **A** Security maturity assessment results
A maturity assessment provides an organization-level view of security practices and capabilities, making it more comprehensive than findings from an individual technical assessment. The cited discussion addresses a holistic approach to controls, risk, and maturity. [12]

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/a-holistic-approach-to-controls-risk-and-maturity

✗ **B** Threat analysis of the organization's environment
Threat analysis helps characterize threats relevant to the organization, but it does not by itself assess the maturity or effectiveness of the organization's security practices. It therefore provides a narrower view of posture than a maturity assessment.

✗ **C** Results of vulnerability assessments
Vulnerability assessments identify weaknesses in systems or environments, but those findings alone do not describe the organization's broader security processes and capabilities. They are one input to understanding posture, not the most comprehensive assessment. [10]

https://www.isaca.org/resources/white-papers/vulnerability-assessment

✗ **D** External penetration test findings
An external penetration test examines how an outside attacker might exploit selected exposed systems or weaknesses. Its findings are useful but limited to the scope of that test, so they do not provide as broad an organizational view as a maturity assessment. [11]

https://www.isaca.org/resources/white-papers/2023/physical-penetration-testing?Appeal=pr&cid=pr_3000061


Free demo · full exam: 967 questions

## Question 48

Single choice · Domain: D3 Information Security Program › Integrate information security requirements into organizational processes (e.g., change management, mergers and acquisitions, development, business continuity, disaster recovery) to maintain the organization's security strategy.

Which of the following is the MOST important consideration during the design phase of a business impact analysis (BIA)?

**A.** Selecting quality metrics to monitor business performance
**B.** Estimating the likelihood that end-to-end processes will be disrupted
**C.** Obtaining reserve funding to prepare for possible business failures
**D.** Identifying critical functions for business operations

**Answer:** D. Identifying critical functions for business operations

**Explanation**

The design phase of a BIA should establish which business functions are critical so their continuity and recovery needs can be assessed and prioritized. Identifying these functions is therefore the most important consideration among the choices. Estimating disruption likelihood is primarily a risk-assessment concern, while performance metrics and reserve funding do not define the BIA's core purpose.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/information-system-contingency-planning-guidance
https://www.isaca.org/resources/isaca-journal/past-issues/2012/key-issues-challenges-and-resolutions-in-implementing-business-continuity-projects

✗ **A** Selecting quality metrics to monitor business performance
Quality metrics monitor how well the business performs, but they do not identify which functions must be prioritized in a BIA. They are not the central design consideration for analyzing business impact and continuity needs.

✗ **B** Estimating the likelihood that end-to-end processes will be disrupted
Estimating the likelihood of disruption is a risk-assessment activity. A BIA focuses on the consequences of disruption to business functions rather than primarily predicting how likely disruption is.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/information-system-contingency-planning-guidance

✗ **C** Obtaining reserve funding to prepare for possible business failures
Securing reserve funding may be part of broader preparedness or response planning, but it is not the BIA design phase's most important consideration. The BIA first needs to identify what business functions are critical and assess the impact of their disruption.

https://www.isaca.org/resources/isaca-journal/past-issues/2012/key-issues-challenges-and-resolutions-in-implementing-business-continuity-projects

✓ **D** Identifying critical functions for business operations
A BIA determines which business functions are critical and assesses the effects of their interruption. Identifying those functions provides the basis for prioritizing continuity and recovery planning.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/information-system-contingency-planning-guidance
https://www.isaca.org/resources/isaca-journal/past-issues/2012/key-issues-challenges-and-resolutions-in-implementing-business-continuity-projects


Free demo · full exam: 967 questions

## Question 49

Single choice · Domain: D3 Information Security Program › Establish, monitor and report program management and operational metrics to evaluate the effectiveness and efficiency of the information security program.

Which of the following should be of GREATEST concern regarding an organization's security controls?

**A.** Some controls are performing outside of an acceptable range.
**B.** No key control indicators (KCIs) have been implemented.
**C.** Control ownership has not been updated.
**D.** Control gap analysis is outdated.

**Answer:** A. Some controls are performing outside of an acceptable range.

**Explanation**

Controls that are performing outside an acceptable range may not be achieving their intended risk-reduction objectives, creating an immediate indication that security exposure is not being adequately managed. This is more urgent than missing monitoring indicators, stale ownership information, or an outdated gap analysis, which are governance or assessment weaknesses but do not by themselves show that controls are currently underperforming.

https://www.isaca.org/en/credentialing/-/media/fa494652c5f149289af38cef18328650.ashx
https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-6/tips-for-effective-control-design

✓ **A** Some controls are performing outside of an acceptable range.
This is the greatest concern because it is direct evidence that existing controls are not operating at the expected level. The organization should investigate and address the resulting risk exposure promptly.

https://www.isaca.org/en/credentialing/-/media/fa494652c5f149289af38cef18328650.ashx
https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-6/tips-for-effective-control-design

✗ **B** No key control indicators (KCIs) have been implemented.
Without KCIs, the organization has less visibility into control performance, which is a significant monitoring weakness. However, it does not establish that controls are currently performing poorly, unlike option A.

https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-2
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-1

✗ **C** Control ownership has not been updated.
Outdated ownership can make accountability and follow-up less effective. It is a governance concern, but it does not directly demonstrate that a control is failing or outside its acceptable performance range.

✗ **D** Control gap analysis is outdated.
An outdated gap analysis can leave the organization with an incomplete or stale view of control deficiencies. Still, it is an assessment-process weakness rather than direct evidence of current control performance problems.

https://www.isaca.org/en/credentialing/-/media/fa494652c5f149289af38cef18328650.ashx
https://www.isaca.org/credentialing/crisc/crisc-exam-content-outline


Free demo · full exam: 967 questions

## Question 50

Single choice · Domain: D3 Information Security Program › Establish and/or maintain a security awareness and training program.

Which type of policy BEST helps to ensure that all employees, contractors, and third-party users receive formal communication regarding an organization's security program?

**A.** Management review policy
**B.** Business continuity management policy
**C.** Information security training policy
**D.** Security incident management policy

**Answer:** C. Information security training policy

**Explanation**

An information security training policy is the best fit because the requirement is to formally communicate the organization's security program to employees, contractors, and third-party users. Training and awareness policies establish how security information is communicated to the people who need to understand and follow it.

https://www.isaca.org/resources/isaca-journal/issues/2018/volume-6/a-heightened-sense-of-awareness-what-the-internal-auditor-should-know-about-information-security-awa
https://www.isaca.org/resources/isaca-journal/issues/2023/volume-2/considerations-for-developing-cybersecurity-awareness-training
https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/the-benefits-of-information-security-and-privacy-awareness-training-programs

✗ **A** Management review policy
A management review policy concerns oversight and evaluation of the security program by management. It does not primarily define how the program is formally communicated to all employees, contractors, and third-party users.

✗ **B** Business continuity management policy
A business continuity management policy addresses maintaining or restoring operations during disruptions. That is different from communicating the organization's security program to all user groups.

✓ **C** Information security training policy
An information security training policy establishes how personnel receive security education and awareness. It best supports formal communication of the security program to employees, contractors, and third-party users.

https://www.isaca.org/resources/isaca-journal/issues/2018/volume-6/a-heightened-sense-of-awareness-what-the-internal-auditor-should-know-about-information-security-awa
https://www.isaca.org/resources/isaca-journal/issues/2023/volume-2/considerations-for-developing-cybersecurity-awareness-training
https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/the-benefits-of-information-security-and-privacy-awareness-training-programs

✗ **D** Security incident management policy
A security incident management policy guides the reporting, assessment, and response to security incidents. Its focus is incident handling, not broad communication of the security program to all users.

https://www.isaca.org/resources/isaca-journal/past-issues/2011/jonline-an-introduction-to-information-security-incident-management-based-on-iso-iec-tr-18044-2004


Free demo · full exam: 967 questions

## Question 51

Single choice · Domain: D3 Information Security Program › Establish, monitor and report program management and operational metrics to evaluate the effectiveness and efficiency of the information security program.

Which of the following BEST enables an information security manager to demonstrate the effectiveness of the information security and risk program to senior management?

**A.** Updated risk assessments
**B.** Counts of information security incidents
**C.** Audit reports
**D.** Monthly metrics

**Answer:** D. Monthly metrics

**Explanation**

Monthly metrics give senior management a recurring, measurable view of whether the information security and risk program is meeting its objectives and how performance changes over time. This makes them more useful for demonstrating program effectiveness than isolated assessments, incident counts, or audit reports. [3][11]

https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-1
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-2

✗ **A** Updated risk assessments
Updated risk assessments help identify and evaluate risks, but they are not by themselves a recurring measure of how effectively the overall program is performing. They provide a point-in-time view rather than the ongoing evidence senior management needs.

✗ **B** Counts of information security incidents
Incident counts show one aspect of security activity, but they do not establish overall program effectiveness on their own. Counts also lack context about severity, trends, risk reduction, and performance against program objectives.

✗ **C** Audit reports
Audit reports can identify control weaknesses and provide assurance, but they are typically periodic and focused on audit scope. They do not provide the regular, broad performance tracking that monthly metrics offer.

✓ **D** Monthly metrics
Monthly metrics provide recurring measures that can show trends and whether security and risk activities are achieving their objectives. This gives senior management a practical basis for assessing program effectiveness over time.

https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-1
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-2
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/standardized-scoring-for-security-and-risk-metrics


Free demo · full exam: 967 questions

## Question 52

Single choice · Domain: D3 Information Security Program › Integrate information security requirements into organizational processes (e.g., change management, mergers and acquisitions, development, business continuity, disaster recovery) to maintain the organization's security strategy.

A business continuity plan (BCP) should contain:

**A.** information about eradication activities.
**B.** hardware and software inventories.
**C.** data restoration procedures.
**D.** criteria for activation.

**Answer:** D. criteria for activation.

**Explanation**

A business continuity plan (BCP) needs to specify when it should be activated so personnel can respond consistently when a disruption threatens business operations. Therefore, criteria for activation are the best choice. Eradication activities and data restoration procedures are more closely associated with incident response and disaster recovery, while hardware and software inventories are supporting asset information rather than the key BCP requirement asked here.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/information-system-contingency-planning-guidance
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/working-toward-a-managed-mature-business-continuity-plan

✗ **A** information about eradication activities.
Eradication describes removing a threat or its effects during incident response. It is not the defining BCP content being asked for; a BCP focuses on maintaining or resuming business operations during disruption.

✗ **B** hardware and software inventories.
Inventories may support planning by documenting technology assets, but they do not establish when the continuity plan should be invoked. The best answer is the plan's activation criteria.

✗ **C** data restoration procedures.
Procedures for restoring data are typically part of disaster recovery planning. They may support continuity, but they are not the best answer to what a BCP should contain in this question.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/information-system-contingency-planning-guidance

✓ **D** criteria for activation.
Activation criteria define the conditions under which the organization should put its BCP into effect. This gives decision-makers a clear trigger for initiating continuity measures when disruption occurs.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/information-system-contingency-planning-guidance
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/working-toward-a-managed-mature-business-continuity-plan


Free demo · full exam: 967 questions

## Question 53

Single choice · Domain: D3 Information Security Program › Establish and/or maintain a security awareness and training program.

Which of the following is the BEST way to improve an organization's ability to detect and respond to incidents?

**A.** Conduct a business impact analysis (BIA).
**B.** Conduct periodic awareness training.
**C.** Perform a security gap analysis.
**D.** Perform network penetration testing.

**Answer:** B. Conduct periodic awareness training.

**Explanation**

Periodic awareness training helps employees recognize potential security incidents and report them promptly, improving the organization's ability to detect and respond. The other choices primarily support business continuity planning or identify security weaknesses rather than preparing people to recognize and report incidents.

https://www.isaca.org/resources/isaca-journal/issues/2023/volume-2/considerations-for-developing-cybersecurity-awareness-training

✗ **A** Conduct a business impact analysis (BIA).
A BIA identifies the effects of disruptions on business operations and helps prioritize recovery needs. It does not directly prepare employees to detect or report security incidents.

✓ **B** Conduct periodic awareness training.
Awareness training can help employees recognize suspicious activity and understand how to report it, supporting earlier detection and a coordinated response. Periodic training reinforces that knowledge over time.

https://www.isaca.org/resources/isaca-journal/issues/2023/volume-2/considerations-for-developing-cybersecurity-awareness-training

✗ **C** Perform a security gap analysis.
A gap analysis identifies differences between current security practices and desired requirements. It can guide improvements, but does not by itself equip employees to recognize and report incidents.

✗ **D** Perform network penetration testing.
Penetration testing can reveal exploitable weaknesses in network defenses. It does not directly improve the organization's ongoing ability to notice incidents or ensure that staff know how to respond.

Dumpsgate

## Question 54

Single choice · Domain: D3 Information Security Program › Integrate information security requirements into organizational processes (e.g., change management, mergers and acquisitions, development, business continuity, disaster recovery) to maintain the organization's security strategy.

A startup company deployed several new applications with vulnerabilities into production because security reviews were not conducted. What will BEST help to ensure effective application risk management going forward?

**A.** Conduct automated scans on applications before deployment.
**B.** Supplement existing development teams with security engineers.
**C.** Integrate information security into existing change management.
**D.** Create a new governance council for application security.

**Answer:** C. Integrate information security into existing change management.

**Explanation**

The company's failure was that security reviews were not part of the process for moving applications into production. Integrating information security into existing change management makes security review a routine part of evaluating and approving changes, helping identify and address application risk before deployment. This embeds the control in an established workflow rather than relying only on extra tools or staff. [2][10]

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-47/five-key-components-of-an-application-security-program
https://www.isaca.org/resources/isaca-journal/issues/2018/volume-5/speeding-up-software-delivery-with-effective-change-management

✗ **A** Conduct automated scans on applications before deployment.
Automated scans can help detect vulnerabilities, but they are only one control and do not by themselves ensure that security risks are reviewed and managed as part of the production deployment process. Integrating security into change management addresses the underlying process gap.

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-47/five-key-components-of-an-application-security-program

✗ **B** Supplement existing development teams with security engineers.
Security engineers could provide valuable expertise, but adding staff alone does not ensure that security reviews occur for each production change. The more direct remedy is to make security review part of the existing change-management workflow.

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-47/five-key-components-of-an-application-security-program

✓ **C** Integrate information security into existing change management.
This directly addresses the failure described: applications reached production without security reviews. Making information security part of change management establishes a repeatable point for assessing application risk before changes are approved and deployed.

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-47/five-key-components-of-an-application-security-program
https://www.isaca.org/resources/isaca-journal/issues/2018/volume-5/speeding-up-software-delivery-with-effective-change-management

✗ **D** Create a new governance council for application security.
A council could provide oversight, but creating one does not necessarily ensure that application changes receive security reviews before deployment. Integrating security into the existing change process is a more direct way to make those reviews routine.


Free demo · full exam: 967 questions

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-47/five-key-components-of-an-application-security-program
https://www.isaca.org/resources/isaca-journal/issues/2018/volume-5/speeding-up-software-delivery-with-effective-change-management

## Question 55

Single choice · Domain: D3 Information Security Program › Establish and maintain information security architectures (people, process, technology) to execute the information security program.

Which of the following is the BEST course of action when using a web application that has known vulnerabilities?

**A.** Monitor application level logs.
**B.** Deploy host-based intrusion detection.
**C.** Deploy an application firewall.
**D.** Install anti-spyware software.

**Answer:** C. Deploy an application firewall.

**Explanation**

Because the web application has known vulnerabilities, an application firewall is the best listed control for inspecting web traffic and blocking malicious requests that target those weaknesses. It can provide a protective layer while the vulnerabilities remain, whereas the other choices primarily detect activity or address different threats rather than directly filtering attacks against the application.

✗ **A** Monitor application level logs.
Application logs can help identify suspicious activity or support investigation, but monitoring does not itself block requests that exploit the known vulnerabilities. It is less protective than deploying an application firewall in this scenario.

✗ **B** Deploy host-based intrusion detection.
Host-based intrusion detection can alert on suspicious activity on the server, but it is primarily a detection measure and does not directly filter web requests targeting application vulnerabilities. An application firewall is the better immediate defensive layer among these options.

✓ **C** Deploy an application firewall.
An application firewall can inspect and filter application-layer traffic, blocking requests that match attacks against the known vulnerabilities. This provides a direct protective measure for the exposed web application while the underlying issues remain.

✗ **D** Install anti-spyware software.
Anti-spyware software addresses spyware and related endpoint threats, not attacks exploiting vulnerabilities in a web application. It would not provide the targeted traffic filtering needed here.


Free demo · full exam: 967 questions

## Question 56

Single choice · Domain: D3 Information Security Program › Integrate information security requirements into organizational processes (e.g., change management, mergers and acquisitions, development, business continuity, disaster recovery) to maintain the organization's security strategy.

Which of the following is the FIRST step in developing a business continuity plan (BCP)?

**A.** Determine the business recovery strategy
**B.** Determine available resources.
**C.** Identify the applications with the shortest recovery time objectives (RTOs).
**D.** Identify critical business processes.

**Answer:** D. Identify critical business processes.

**Explanation**

The first step is to identify the critical business processes that must continue or be restored after a disruption. This establishes what the continuity plan needs to protect and provides the basis for assessing impacts and recovery priorities. Recovery strategies and resource decisions come later, after those business needs are understood.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/working-toward-a-managed-mature-business-continuity-plan
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/information-system-contingency-planning-guidance

✗ **A** Determine the business recovery strategy
A recovery strategy is selected after the organization understands which business processes are critical and what their recovery needs are. Choosing a strategy before identifying those needs risks planning for the wrong priorities.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/working-toward-a-managed-mature-business-continuity-plan
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/information-system-contingency-planning-guidance

✗ **B** Determine available resources.
Available resources affect which recovery approaches are feasible, but they do not establish what the business must prioritize. The plan first needs to identify critical processes, then assess the resources needed to support their recovery.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/working-toward-a-managed-mature-business-continuity-plan
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/information-system-contingency-planning-guidance

✗ **C** Identify the applications with the shortest recovery time objectives (RTOs).
Application RTOs are relevant to prioritizing technology recovery, but they are not the first step in developing the overall BCP. The organization must first identify the critical business processes that drive those application recovery requirements.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/information-system-contingency-planning-guidance

✓ **D** Identify critical business processes.
The BCP must begin by establishing which business processes are critical to the organization. Those processes provide the basis for analyzing impacts, setting recovery priorities, and selecting suitable strategies and resources.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/working-toward-a-managed-mature-business-


Free demo · full exam: 967 questions

continuity-plan
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/information-system-contingency-planning-guidance

## Question 57

Single choice · Domain: D3 Information Security Program › Establish and/or maintain a security awareness and training program.

Which of the following is the PRIMARY impact of organizational culture on the effectiveness of an information security program?

**A.** The culture shapes behaviors toward information security.
**B.** The culture defines responsibilities necessary for program implementation.
**C.** The culture helps determine budget for information security controls.
**D.** The culture has minimal impact as long as information security controls are adhered to.

**Answer:** A. The culture shapes behaviors toward information security.

**Explanation**

Organizational culture primarily affects how people think and behave toward information security, including whether they follow secure practices and take responsibility for protecting information. Even well-designed controls may be less effective if the culture does not support secure behavior, so A best describes culture's impact on program effectiveness.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/organizational-culture-for-information-security
https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/the-human-factor-in-information-security
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/embedding-security-and-continuity-culture

✓ **A** The culture shapes behaviors toward information security.
Culture influences employees' attitudes and everyday actions, including whether they take security practices seriously and follow them. Those behaviors directly affect how effectively an information security program works.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/organizational-culture-for-information-security
https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/the-human-factor-in-information-security
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/embedding-security-and-continuity-culture

✗ **B** The culture defines responsibilities necessary for program implementation.
Culture can influence how people respond to their responsibilities, but it does not primarily define the roles and accountability needed to implement a program. Those are generally established through governance, policies, and organizational structures.

https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/essential-functions-of-a-cybersecurity-program
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/organizational-culture-for-information-security

✗ **C** The culture helps determine budget for information security controls.
Culture may affect how leaders perceive and prioritize security, but determining a control budget is not its primary impact on program effectiveness. The more direct effect is on people's security-related behaviors.

https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/essential-functions-of-a-cybersecurity-program
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/organizational-culture-for-information-security

✗ **D** The culture has minimal impact as long as information security controls are adhered to.
Culture has a meaningful impact because it helps shape whether people adhere to controls and how they

act when security situations arise. Having controls in place does not make supportive security behaviors or organizational culture unimportant.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/organizational-culture-for-information-security
https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/the-human-factor-in-information-security
https://www.isaca.org/resources/isaca-journal/issues/2021/volume-3/embedding-security-and-continuity-culture

## Question 58

Single choice · Domain: D3 Information Security Program › Establish, monitor and report program management and operational metrics to evaluate the effectiveness and efficiency of the information security program.

When is the BEST time to verify that a production system's security mechanisms meet control objectives?

**A.** During quality and acceptance checks
**B.** On a continuous basis through monitoring activities and automated tooling
**C.** After remediations recommended by penetration tests have been completed
**D.** During annual internal and compliance audits

**Answer:** B. On a continuous basis through monitoring activities and automated tooling

**Explanation**

The question asks when to verify that a production system's security mechanisms continue to meet control objectives. Continuous monitoring, supported by automated tooling, provides ongoing evidence about control effectiveness and can identify changes or failures promptly. Quality checks, penetration-test follow-up, and annual audits are periodic activities and do not provide the same ongoing assurance.

https://www.isaca.org/resources/isaca-journal/issues/2015/volume-2/a-practical-approach-to-continuous-control-monitoring

✗ **A** During quality and acceptance checks
Quality and acceptance checks can verify security requirements before or as a system is put into service. They do not provide ongoing assurance that controls in a production system continue to meet their objectives.

✓ **B** On a continuous basis through monitoring activities and automated tooling
Continuous monitoring and automation can repeatedly assess security controls in the production environment and surface deviations as they occur. This is the best fit for verifying ongoing control effectiveness rather than relying on occasional reviews.

https://www.isaca.org/resources/isaca-journal/issues/2015/volume-2/a-practical-approach-to-continuous-control-monitoring

✗ **C** After remediations recommended by penetration tests have been completed
Checking remediation after a penetration test can confirm that particular findings were addressed, but it is a point-in-time activity. It does not establish that all security mechanisms continue to meet control objectives over time.

https://www.isaca.org/resources/news-and-trends/industry-news/2022/taking-a-risk-based-approach-to-pen-testing
https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/planning-for-information-security-testinga-practical-approach

✗ **D** During annual internal and compliance audits
Annual audits can provide valuable periodic assurance, but they leave long intervals in which a control failure or configuration change may go undetected. Continuous monitoring is better suited to verifying


Free demo · full exam: 967 questions

controls in a production system on an ongoing basis.
https://www.isaca.org/resources/isaca-journal/issues/2015/volume-2/a-practical-approach-to-continuous-control-monitoring

## Question 59

Single choice · Domain: D3 Information Security Program › Establish, monitor and report program management and operational metrics to evaluate the effectiveness and efficiency of the information security program.

Which of the following is MOST important for an organization to have in place to determine the effectiveness of information security governance?

**A.** Program metrics
**B.** Key risk indicators (KRIs)
**C.** Risk register
**D.** Security strategy

**Answer:** A. Program metrics

**Explanation**

Program metrics are the most important choice because they provide measurable evidence of whether the information security program—and its governance objectives—are achieving the intended results. KRIs and a risk register help monitor and document risk, while a security strategy sets direction; none directly determines effectiveness as well as metrics designed to evaluate performance.
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-2
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-1
https://www.isaca.org/resources/isaca-journal/past-issues/2013/how-to-measure-security-from-a-governance-perspective

✓ **A** Program metrics
Program metrics give the organization measurable indicators for assessing security performance and progress against governance objectives. They therefore directly support determining whether information security governance is effective.
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-2
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-1
https://www.isaca.org/resources/isaca-journal/past-issues/2013/how-to-measure-security-from-a-governance-perspective

✗ **B** Key risk indicators (KRIs)
KRIs signal changes in risk exposure and help identify when risk may exceed acceptable levels. They are useful for risk monitoring, but do not by themselves provide the broader performance measures needed to determine governance effectiveness.
https://www.isaca.org/resources/glossary
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/standardized-scoring-for-security-and-risk-metrics

✗ **C** Risk register
A risk register records identified risks and related information, supporting risk assessment and

management. It is not a set of performance measures for evaluating how effectively security governance is operating.

https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/security-adjustments-to-strengthen-the-bond-between-risk-registers-and-information

✗ **D** Security strategy
A security strategy establishes direction and priorities for information security. It can define what the organization intends to accomplish, but metrics are needed to measure whether governance is achieving those aims.

https://www.isaca.org/resources/isaca-journal/past-issues/2010/developing-an-information-security-and-risk-management-strategy

## Question 60

Single choice · Domain: D3 Information Security Program › Integrate information security requirements into contracts and activities of third parties (e.g., joint ventures, outsourced providers, business partners, customers) to maintain the organization's security strategy.

Which of the following provides the MOST assurance that a third-party hosting provider will be able to meet availability requirements?

**A.** Right-to-audit clause
**B.** The third party's incident response plan
**C.** Service level agreement (SLA)
**D.** The third party's business continuity plan (BCP)

**Answer:** C. Service level agreement (SLA)

**Explanation**

A service level agreement (SLA) is the clearest contractual basis for assessing whether a hosting provider will meet specified availability requirements. It can define measurable availability targets and the provider's obligations if those targets are missed. The other choices may help evaluate or improve resilience, but do not provide the same direct commitment to required availability.

✗ **A** Right-to-audit clause
A right-to-audit clause allows the customer to examine or obtain assurance about the provider's controls. It does not itself set a required availability level or commit the provider to meet one.

✗ **B** The third party's incident response plan
An incident response plan describes how the provider handles incidents. It may support recovery, but does not establish a measurable availability commitment for the hosting service.

✓ **C** Service level agreement (SLA)
An SLA can specify availability targets, how availability is measured, and the provider's responsibilities when targets are not met. Those explicit commitments provide the most direct assurance against the stated availability requirements.

✗ **D** The third party's business continuity plan (BCP)
A BCP describes how the provider intends to continue or restore operations during a disruption. Reviewing it can provide information about resilience, but it does not by itself guarantee or contractually define that the service will meet a particular availability target.


Free demo · full exam: 967 questions

## Question 61

Single choice · Domain: D3 Information Security Program › Integrate information security requirements into organizational processes (e.g., change management, mergers and acquisitions, development, business continuity, disaster recovery) to maintain the organization's security strategy.

Which of the following is the MOST important reason for an information security manager to archive and retain the organization's electronic communication and email data?

**A.** To track personal use of electronic communication by users
**B.** To provide as evidence in legal proceedings when required
**C.** To meet the requirements of global security standards
**D.** To identify and scan attachments for malware

**Answer:** B. To provide as evidence in legal proceedings when required

**Explanation**

The primary reason to archive and retain organizational email and electronic communications is to preserve records that may be needed as evidence in legal proceedings. Proper retention makes relevant communications available when required, whereas monitoring personal use, satisfying a particular security standard, or scanning attachments are different objectives. [1][10]

https://www.isaca.org/resources/isaca-journal/past-issues/2010/an-introduction-to-digital-records-management
https://www.isaca.org/resources/isaca-journal/past-issues/2014/importance-of-forensic-readiness

✗ **A** To track personal use of electronic communication by users
Tracking personal use is a monitoring or acceptable-use enforcement objective, not the principal reason to retain communications. Retention may incidentally preserve information relevant to such reviews, but that does not make it the most important purpose here.

✓ **B** To provide as evidence in legal proceedings when required
Archived communications can preserve records that the organization may need to produce or rely on in legal proceedings. Retention therefore supports legal and evidentiary needs, which is the strongest reason among the choices. [1][10]

https://www.isaca.org/resources/isaca-journal/past-issues/2010/an-introduction-to-digital-records-management
https://www.isaca.org/resources/isaca-journal/past-issues/2014/importance-of-forensic-readiness

✗ **C** To meet the requirements of global security standards
Some standards may require controls for records or information, but this choice is too broad to be the most important general reason for retaining email. The specific and central purpose in this question is preserving communications that may be required as legal evidence.

✗ **D** To identify and scan attachments for malware
Scanning attachments for malware is a preventive security function performed by email security or endpoint controls. It does not require archiving and retaining communications, and it does not address the evidentiary purpose of retention.


Free demo · full exam: 967 questions

## Question 62

Single choice · Domain: D3 Information Security Program › Establish, monitor and report program management and operational metrics to evaluate the effectiveness and efficiency of the information security program.

When selecting metrics to monitor the effectiveness of an information security program, it is MOST important for an information security manager to:

**A.** consider the organizations business strategy.
**B.** consider the strategic objectives of the program.
**C.** leverage industry benchmarks.
**D.** identify the program's risk and compensating controls.

**Answer:** B. consider the strategic objectives of the program.

**Explanation**

Metrics should be selected to show whether the information security program is achieving its intended outcomes. The program's strategic objectives provide the direct basis for choosing relevant measures and evaluating effectiveness. Business strategy, benchmarks, and risk controls may inform the selection, but they do not replace alignment with the program's objectives.

https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-1
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-2

✗ **A** consider the organizations business strategy.
Business strategy provides important context for the security program, but it is not the most direct basis for measuring the program's effectiveness. Metrics should specifically track whether the program is meeting its strategic objectives.

https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-1
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-2

✓ **B** consider the strategic objectives of the program.
Program metrics should measure progress toward the outcomes the program is intended to achieve. Aligning metrics with the program's strategic objectives makes them relevant for assessing its effectiveness.

https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-1
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-2

✗ **C** leverage industry benchmarks.
Benchmarks can help compare performance with peers, but they do not establish whether the organization's own program is achieving its objectives. They are supplementary to selecting measures aligned with those objectives.

https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-1
https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/standardized-scoring-for-security-and-risk-metrics

✗ **D** identify the program's risk and compensating controls.
Understanding risks and controls can inform what the security program addresses, but identifying them alone does not determine the most appropriate effectiveness metrics. Measures should be chosen to


Free demo · full exam: 967 questions

evaluate progress against the program's strategic objectives.

https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-1
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-2

## Question 63

Single choice · Domain: D4 Incident Management › Develop and maintain processes to ensure the timely identification of information security incidents.

Which type of system is MOST effective for prioritizing cyber incidents based on impact and tracking them until they are closed?

**A.** Security information and event management (SIEM)
**B.** Extended detection and response (XDR)
**C.** Endpoint detection and response (EDR)
**D.** Network intrusion detection system (NIDS)

**Answer:** A. Security information and event management (SIEM)

**Explanation**

A SIEM is the best fit because it centralizes and correlates security events to help teams identify and prioritize incidents according to their significance. It also supports incident workflows and tracking through investigation and closure, matching both requirements in the question. The other choices are primarily focused on detecting or responding to threats within particular data sources or environments rather than providing this broader prioritization and tracking role.

https://www.isaca.org/resources/isaca-journal/issues/2023/volume-3/a-framework-for-siem-implementation
https://www.isaca.org/resources/white-papers/security-information-and-event-management

✓ **A** Security information and event management (SIEM)
A SIEM collects and correlates security events across sources, helping analysts assess incident significance and prioritize response. Its centralized monitoring and incident-management capabilities make it the best choice for tracking incidents through to closure.

https://www.isaca.org/resources/isaca-journal/issues/2023/volume-3/a-framework-for-siem-implementation
https://www.isaca.org/resources/white-papers/security-information-and-event-management

✗ **B** Extended detection and response (XDR)
XDR correlates detection and response signals across multiple security layers, but the question specifically asks for a system to prioritize incidents by impact and track them until closure. SIEM is the more direct fit for centralized event analysis and incident tracking.

https://www.isaca.org/resources/isaca-journal/issues/2023/volume-3/a-framework-for-siem-implementation
https://www.isaca.org/resources/white-papers/security-information-and-event-management

✗ **C** Endpoint detection and response (EDR)
EDR focuses on detecting and responding to threats on endpoints. That narrower scope does not make it the best system for prioritizing cyber incidents across the organization and tracking them through closure.

https://www.isaca.org/resources/white-papers/security-information-and-event-management

✗ **D** Network intrusion detection system (NIDS)


Free demo · full exam: 967 questions

A NIDS monitors network traffic for suspicious activity or known attack patterns. It can provide alerts, but it is not the best option for broad incident-impact prioritization and end-to-end incident tracking.

https://www.isaca.org/resources/isaca-journal/issues/2015/volume-5/cybersecurity-detective-controlsmonitoring-to-identify-and-respond-to-threats
https://www.isaca.org/resources/white-papers/security-information-and-event-management

## Question 64

Single choice · Domain: D4 Incident Management › Develop and maintain processes to ensure the timely identification of information security incidents.

Which of the following should be an information security manager's FIRST course of action when a potential business breach is discovered in a critical business system?

**A.** Implement mitigating actions immediately.
**B.** Invoke the incident response plan.
**C.** Inform senior management of the breach.
**D.** Validate the breach.

**Answer:** D. Validate the breach.

**Explanation**

The first step is to validate that the reported event is actually a breach. This avoids triggering response actions or escalating an unconfirmed report as a confirmed incident; once validated, the manager can follow the incident response process and notify the appropriate stakeholders.

✗ **A** Implement mitigating actions immediately.
Mitigation should follow confirmation and assessment of the event. Acting immediately on an unverified report could disrupt a critical business system unnecessarily or address the wrong issue.

✗ **B** Invoke the incident response plan.
The incident response plan is appropriate once the potential breach has been validated as an incident. The question asks for the first course of action after a potential breach is discovered, so validation comes first.

✗ **C** Inform senior management of the breach.
Escalation may be required after the event is confirmed and its significance is understood. Reporting an unvalidated suspicion as a breach risks conveying inaccurate information.

✓ **D** Validate the breach.
Validation establishes whether the indication represents a genuine breach rather than a false alarm or misinterpretation. That confirmation provides a sound basis for response actions and escalation.


Free demo · full exam: 967 questions

## Question 65

Single choice · Domain: D4 Incident Management › Test and review the incident response plan periodically to ensure effectiveness and make improvements as needed.

An information security manager is updating the organization's incident response plan. Which of the following is the BEST way to validate that the process and procedures provided by IT and business units are complete, accurate, and known by all responsible teams?

**A.** Review the test objectives with stakeholders.
**B.** Conduct a data breach incident tabletop exercise.
**C.** Conduct an incident response plan survey.
**D.** Review data breach incident triage steps.

**Answer:** B. Conduct a data breach incident tabletop exercise.

**Explanation**

A data breach tabletop exercise brings the responsible IT and business teams together to work through a realistic incident using the documented processes and procedures. Their participation can reveal whether procedures are complete and accurate, whether responsibilities are understood, and where the plan needs improvement. Reviewing objectives, surveying teams, or examining only triage steps does not validate the broader response process in the same way.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/using-tabletops-and-simulations-to-build-better-incident-responders
https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-48/five-key-considerations-for-developing-crisis-management-and-incident-response-tabletop-exercises

✗ **A** Review the test objectives with stakeholders.
Reviewing objectives can confirm that stakeholders agree on what a test should cover, but it does not demonstrate that the documented procedures are complete or accurate. Nor does it verify that all responsible teams know how to carry them out.

✓ **B** Conduct a data breach incident tabletop exercise.
A tabletop exercise has responsible teams work through a data breach scenario using the incident response plan. This lets the organization assess whether procedures are workable and understood, and identify gaps or inaccuracies that need correction.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/using-tabletops-and-simulations-to-build-better-incident-responders
https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-48/five-key-considerations-for-developing-crisis-management-and-incident-response-tabletop-exercises

✗ **C** Conduct an incident response plan survey.
A survey may collect feedback about whether teams believe they know the plan, but it does not test their understanding or ability to follow procedures in a coordinated incident. It is therefore a weaker way to validate completeness and accuracy.

✗ **D** Review data breach incident triage steps.
Reviewing triage steps examines only one part of the incident response process. It does not validate the broader procedures provided by IT and business units or establish that all responsible teams know their roles.


Free demo · full exam: 967 questions

## Question 66

Single choice · Domain: D4 Incident Management › Develop and maintain processes to ensure the timely identification of information security incidents.

Which of the following is MOST likely to reduce the effectiveness of a SIEM system?

**A.** Complex user interface
**B.** Misconfiguration of alert thresholds
**C.** Weakly encrypted log files
**D.** Lack of multi-factor authentication (MFA) for system access

**Answer:** B. Misconfiguration of alert thresholds

**Explanation**

Misconfigured alert thresholds can directly undermine SIEM detection: thresholds that are too high may miss meaningful events, while thresholds that are too low can generate excessive false alerts and overwhelm analysts. Either outcome makes it harder for the SIEM team to identify and respond to real threats, so this is the most likely option to reduce effectiveness. [1][10]

https://www.isaca.org/resources/isaca-journal/issues/2023/volume-3/a-framework-for-siem-implementation
https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/going-beyond-the-technical-in-siem

✗ **A** Complex user interface
A difficult interface may slow analysts or make the system less convenient to use, but it does not necessarily impair the SIEM's ability to collect, correlate, and alert on security events. Incorrect alert thresholds more directly affect threat detection and analyst workload.

https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/going-beyond-the-technical-in-siem

✓ **B** Misconfiguration of alert thresholds
Thresholds determine which events generate alerts and how many alerts analysts must handle. If they are set incorrectly, the SIEM can miss important activity or produce so many false positives that genuine threats are obscured, directly reducing its effectiveness.

https://www.isaca.org/resources/isaca-journal/issues/2023/volume-3/a-framework-for-siem-implementation
https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/going-beyond-the-technical-in-siem

✗ **C** Weakly encrypted log files
Weak encryption can put log confidentiality at risk, but it does not by itself prevent the SIEM from analyzing those logs or producing useful alerts. The question asks what is most likely to reduce the SIEM's effectiveness, and incorrect alert thresholds have a more direct effect on detection.

✗ **D** Lack of multi-factor authentication (MFA) for system access
Without MFA, unauthorized access to the SIEM may be easier, creating a serious access-control risk. However, this does not inherently make its monitoring and alerting less effective in the way that misconfigured thresholds can.


Free demo · full exam: 967 questions

## Question 67

Single choice · Domain: D4 Incident Management › Develop and maintain processes to ensure the timely identification of information security incidents.

Which type of system is MOST effective for monitoring cyber incidents based on impact and tracking them until they are closed?

**A.** Endpoint detection and response (EDR)
**B.** Network intrusion detection system (NIDS)
**C.** Extended detection and response (XDR)
**D.** Security information and event management (SIEM)

**Answer:** D. Security information and event management (SIEM)

**Explanation**

A SIEM aggregates and analyzes security events from across an environment, helping teams identify and prioritize incidents by their potential impact. It also supports tracking incidents through investigation and response until they are closed, which matches both requirements in the question. EDR and NIDS focus on particular sources of detection, while XDR emphasizes cross-domain detection and response rather than being the best fit for this incident-tracking need.

https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/security-monitoring-as-part-of-the-infosec-playbook
https://www.isaca.org/resources/isaca-journal/past-issues/2011/jonline-an-introduction-to-information-security-incident-management-based-on-iec-tr-18044-2004

✗ **A** Endpoint detection and response (EDR)
EDR monitors and responds to threats on endpoint devices. Its endpoint-focused scope makes it less suitable than a SIEM for monitoring incidents across the environment and tracking them through closure.

https://www.isaca.org/resources/isaca-journal/issues/2025/volume-3/detecting-and-mitigating-apts-in-endpoints

✗ **B** Network intrusion detection system (NIDS)
A NIDS detects suspicious activity on network traffic, but it is not primarily an incident-management system. It does not best meet the requirement to assess incidents by impact and follow them through to closure.

https://www.isaca.org/resources/isaca-journal/issues/2015/volume-5/cybersecurity-detective-controlsmonitoring-to-identify-and-respond-to-threats

✗ **C** Extended detection and response (XDR)
XDR correlates threat signals across multiple security domains and supports detection and response. The question specifically emphasizes prioritizing incidents by impact and tracking them until closure, which is a stronger fit for SIEM-supported monitoring and incident management.

https://www.isaca.org/resources/isaca-journal/issues/2023/volume-5/how-to-elevate-the-soc-to-the-next-level
https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/security-monitoring-as-part-of-the-infosec-playbook

✓ **D** Security information and event management (SIEM)
A SIEM collects and analyzes security events from multiple sources, supporting centralized monitoring and incident prioritization. That makes it the best choice for assessing impact and tracking incidents through investigation until they are closed.

https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/security-monitoring-as-part-of-the-infosec-playbook
https://www.isaca.org/resources/isaca-journal/past-issues/2011/jonline-an-introduction-to-information-security-incident-management-based-on-iec-tr-18044-2004


Free demo · full exam: 967 questions

## Question 68

Single choice · Domain: D4 Incident Management › Conduct post-incident reviews to determine the root cause of information security incidents and identify opportunities for improvement.

The PRIMARY goal when conducting post-incident reviews is to identify:

**A.** Additional cybersecurity budget needs
**B.** Weaknesses in incident response plans
**C.** Information to be shared with senior management
**D.** Individuals that need additional training

**Answer:** B. Weaknesses in incident response plans

**Explanation**

The primary purpose of a post-incident review is to learn from how the incident was handled and identify deficiencies that can be corrected. Finding weaknesses in the incident response plan helps improve future response effectiveness; budget requests, management communications, and staff training may follow from the review but are not its primary goal.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/cybersecurity-incident-response

✗ **A** Additional cybersecurity budget needs
A review may reveal resource gaps that could support a budget request, but determining funding needs is a possible outcome rather than the primary purpose of reviewing the incident.

✓ **B** Weaknesses in incident response plans
Post-incident reviews assess what worked and what did not during the response, so weaknesses in the plans and procedures can be identified and addressed. This learning improves preparedness and future incident handling.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/cybersecurity-incident-response

✗ **C** Information to be shared with senior management
Senior management may receive a summary of the incident and review findings, but producing management communications is not the review's central objective. The main focus is identifying lessons and improvements, including weaknesses in response plans.

✗ **D** Individuals that need additional training
The review might uncover training needs, but focusing on particular individuals is narrower than its primary purpose. The review should identify response-process and plan improvements rather than primarily assign training to people.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/cybersecurity-incident-response


Free demo · full exam: 967 questions

## Question 69

Single choice · Domain: D4 Incident Management › Establish and maintain an organizational incident response plan to ensure an effective response to information security incidents.

Which of the following is the GREATEST benefit of classifying information security incidents?

**A.** Reporting capabilities
**B.** Improved chain of custody
**C.** Comprehensive documentation
**D.** Prioritized recovery

**Answer:** D. Prioritized recovery

**Explanation**

Classifying security incidents groups them by factors such as severity and impact, helping an organization decide which incidents require attention first. The greatest benefit among these choices is therefore prioritized recovery: response and recovery resources can be directed to the most critical incidents before less urgent ones. Reporting, documentation, and chain-of-custody practices may also matter during incident handling, but they are not the primary benefit of classification in this question.

✗ **A** Reporting capabilities
Classification can make incident trends easier to report, but reporting is a secondary use of the resulting categories. It does not provide the most direct benefit compared with using severity or impact to decide which incident to recover from first.

✗ **B** Improved chain of custody
Chain of custody concerns documenting and preserving evidence so it can be reliably handled and examined. Classifying incidents does not itself ensure that evidence is collected or maintained properly, so this is not the greatest benefit.

✗ **C** Comprehensive documentation
Incident classifications can support consistent records, but documentation is a separate incident-management activity. The more important benefit of classification is enabling decisions about response urgency and recovery priorities.

✓ **D** Prioritized recovery
Classifying incidents helps distinguish those with greater severity or business impact from less urgent events. That distinction lets responders prioritize recovery efforts and allocate limited resources to the incidents that matter most.


Free demo · full exam: 967 questions

## Question 70

Single choice · Domain: D4 Incident Management › Conduct post-incident reviews to determine the root cause of information security incidents and identify opportunities for improvement.

Which of the following is the MOST important objective of post-incident review activities?

**A.** Evidence collection
**B.** Continuous improvement
**C.** Incident triage
**D.** Incident documentation

**Answer:** B. Continuous improvement

**Explanation**

The primary purpose of a post-incident review is to learn from the incident and improve processes, controls, and response capabilities so similar incidents can be handled better or prevented in the future. Evidence collection, triage, and documentation support incident handling, but they are not the central objective of the review itself.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance

✗ **A** Evidence collection
Evidence collection is important during incident response to investigate what happened and preserve relevant material. It is not the main objective of the post-incident review, which is to use the findings to improve future response and resilience.

✓ **B** Continuous improvement
A post-incident review examines the response and outcomes to identify lessons, gaps, and changes that can improve future incident handling. This makes continuous improvement the most important objective.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance

✗ **C** Incident triage
Triage is used to assess and prioritize an incident while it is being handled. Post-incident review occurs after the response and focuses on learning and improvement rather than initial prioritization.

✗ **D** Incident documentation
Documentation records the incident and the actions taken, and it can provide input to a review. However, recording events is a supporting activity; the review's main objective is to turn those records and lessons into improvements.


Free demo · full exam: 967 questions

## Question 71

Single choice · Domain: D4 Incident Management › Establish and maintain an organizational incident response plan to ensure an effective response to information security incidents.

As part of incident response activities, the BEST time to begin the recovery process is after:

**A.** The eradication phase has been completed
**B.** The incident response team has been established
**C.** The root cause has been determined
**D.** The incident manager has declared the incident

**Answer:** A. The eradication phase has been completed

**Explanation**

The recovery process should begin only after eradication is complete. Eradication removes the threat or its cause; beginning recovery before that could restore systems while they remain compromised. Establishing the team, declaring an incident, or identifying the root cause alone does not show that the threat has been removed.

https://www.isaca.org/credentialing/-/media/fa494652c5f149289af38cef18328650.ashx
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/incident-response-models

✓ **A** The eradication phase has been completed
Eradication addresses and removes the incident's cause or threat. Recovery should follow so affected systems can be restored without reintroducing the unresolved compromise.

https://www.isaca.org/credentialing/-/media/fa494652c5f149289af38cef18328650.ashx
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/incident-response-models

✗ **B** The incident response team has been established
Establishing the team supports the response, but it does not mean the incident has been contained or eradicated. Starting recovery at this point could restore systems before they are safe.

https://www.isaca.org/credentialing/-/media/fa494652c5f149289af38cef18328650.ashx
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/incident-response-models

✗ **C** The root cause has been determined
Determining the root cause informs remediation, but understanding the cause does not itself remove the threat. Recovery should wait until eradication is complete.

https://www.isaca.org/credentialing/-/media/fa494652c5f149289af38cef18328650.ashx
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/incident-response-models

✗ **D** The incident manager has declared the incident
Declaring an incident initiates or formalizes response activity; it does not indicate that the threat has been removed. Recovery is premature until eradication is complete.

https://www.isaca.org/credentialing/-/media/fa494652c5f149289af38cef18328650.ashx
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/incident-response-models


Free demo · full exam: 967 questions

## Question 72

Single choice · Domain: D4 Incident Management › Test and review the incident response plan periodically to ensure effectiveness and make improvements as needed.

Which of the following is MOST important to ensure incident management readiness?

**A.** The plan is compliant with industry standards.
**B.** The plan is regularly tested.
**C.** The plan is updated annually.
**D.** The plan is concise and includes a checklist.

**Answer:** B. The plan is regularly tested.

**Explanation**

Regularly testing an incident management plan is the strongest way to verify that people can use it, roles and communications work, and response procedures are practical before a real incident occurs. Compliance, scheduled updates, and concise checklists can all help, but they do not demonstrate readiness on their own. ISACA materials on incident-response exercises and simulations support the importance of testing and practicing response plans.

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-48/five-key-considerations-for-developing-crisis-management-and-incident-response-tabletop-exercises
https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/using-tabletops-and-simulations-to-build-better-incident-responders

✗ **A** The plan is compliant with industry standards.
Alignment with standards can make a plan well-structured, but it does not show that the organization can carry it out effectively. Testing is needed to validate that responders can follow the plan in practice.

✓ **B** The plan is regularly tested.
Regular testing exercises the plan and reveals whether response steps, roles, and coordination work as intended. This provides direct evidence of readiness and helps identify weaknesses before an actual incident.

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-48/five-key-considerations-for-developing-crisis-management-and-incident-response-tabletop-exercises
https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/using-tabletops-and-simulations-to-build-better-incident-responders

✗ **C** The plan is updated annually.
A yearly update schedule may not keep the plan aligned with changes that occur between reviews, and updating alone does not establish that the plan works. Regular testing provides practical evidence of readiness.

✗ **D** The plan is concise and includes a checklist.
A concise plan and checklist can make procedures easier to use, but they do not confirm that responders understand their roles or can execute those procedures. Testing is what checks operational readiness.


Free demo · full exam: 967 questions

## Question 73

Single choice · Domain: D4 Incident Management › Develop and maintain processes to ensure the timely identification of information security incidents.

Which of the following is the PRIMARY benefit of training service desk staff to recognize incidents?

**A.** Incident response plan can be activated in a timely manner.
**B.** Incident metrics can be communicated.
**C.** Risk response options can be identified quickly.
**D.** Incident classification times can be improved.

**Answer:** A. Incident response plan can be activated in a timely manner.

**Explanation**

Training service desk staff to recognize incidents helps ensure a potential incident is identified and escalated promptly. The primary benefit is that the incident response plan can then be activated without avoidable delay. Faster metrics communication, risk-option identification, and classification may be useful, but they are not the main outcome asked for here.

✓ **A** Incident response plan can be activated in a timely manner.
Recognizing an incident promptly allows staff to escalate it so the appropriate response process can begin. Timely activation is the primary benefit because it enables the organization to respond to the incident sooner.

✗ **B** Incident metrics can be communicated.
Communicating metrics may help with reporting and monitoring, but it does not directly describe the primary operational benefit of training staff to recognize incidents. The priority is to trigger a timely response.

✗ **C** Risk response options can be identified quickly.
Identifying risk response options is part of deciding how to address a risk, rather than the immediate purpose of incident recognition training. Recognition supports escalation and response-plan activation first.

✗ **D** Incident classification times can be improved.
Training may help staff classify incidents more quickly, but improved classification time is a narrower process benefit. The more important result is that recognizing an incident enables the response plan to be activated promptly.


Free demo · full exam: 967 questions

## Question 74

Single choice · Domain: D4 Incident Management › Establish and maintain an organizational incident response plan to ensure an effective response to information security incidents.

Which of the following is the MOST appropriate action during the containment phase of a cyber incident response?

**A.** Determine the final root cause of the incident.
**B.** Remove all instances of the incident from the network.
**C.** Mitigate exploited vulnerabilities to prevent future incidents.
**D.** Isolate affected systems to prevent the spread of damage.

**Answer:** D. Isolate affected systems to prevent the spread of damage.

**Explanation**

During containment, responders take immediate steps to limit an incident's impact and prevent it from spreading. Isolating affected systems directly serves that purpose, while root-cause analysis, complete removal, and longer-term vulnerability mitigation belong to later response or remediation work. [1][7]

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/incident-response-models

✗ **A** Determine the final root cause of the incident.
Root-cause analysis helps explain how the incident occurred, but it is not the most immediate containment action. Delaying isolation to establish the final cause could allow the incident to spread further.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/incident-response-models

✗ **B** Remove all instances of the incident from the network.
Removing malicious artifacts or fully eradicating the incident is an eradication activity, which follows containment. The immediate priority is to limit spread while preserving the ability to investigate and respond.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/incident-response-models

✗ **C** Mitigate exploited vulnerabilities to prevent future incidents.
Addressing exploited vulnerabilities reduces the chance of recurrence, but it is primarily a remediation or recovery measure. Containment first focuses on limiting the current incident's impact and spread.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/incident-response-models

✓ **D** Isolate affected systems to prevent the spread of damage.
Isolating affected systems limits an attacker's ability to move through the network and prevents additional systems from being impacted. This directly meets the goal of the containment phase: controlling the incident's scope and damage.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/incident-response-models


Free demo · full exam: 967 questions

## Question 75

Single choice · Domain: D4 Incident Management › Establish and maintain an organizational incident response plan to ensure an effective response to information security incidents.

An information security manager is alerted to multiple security incidents across different business units, with unauthorized access to sensitive data and potential data exfiltration from critical systems.

Which of the following is the BEST course of action to appropriately classify and prioritize these incidents?

**A.** Assemble the incident response team to evaluate the incidents
**B.** Initiate the crisis communication plan to notify stakeholders of the incidents
**C.** Engage external incident response consultants to conduct an independent investigation
**D.** Prioritize the incidents based on data classification standards

**Answer:** D. Prioritize the incidents based on data classification standards

**Explanation**

The incidents involve unauthorized access to sensitive data and possible exfiltration from critical systems, so their priority should reflect the sensitivity and business impact of the affected information. Data classification standards provide a consistent basis for assessing that significance across business units. Therefore, prioritizing the incidents based on those standards is the best choice; team evaluation and communications may follow as part of response, but do not themselves classify and prioritize the incidents.

✗ **A** Assemble the incident response team to evaluate the incidents
The response team can investigate and coordinate the incidents, but assembling it is not itself a consistent classification and prioritization method. The scenario specifically calls for determining priority across incidents, which should be grounded in the sensitivity of the affected data.

✗ **B** Initiate the crisis communication plan to notify stakeholders of the incidents
Stakeholder communication may be necessary once the incidents and their impact are understood. It does not establish which incidents should receive priority, and initiating it first may be premature without that assessment.

✗ **C** Engage external incident response consultants to conduct an independent investigation
External consultants may be useful if specialized expertise or independent investigation is needed, but that is not the immediate classification and prioritization step asked for. The organization can prioritize incidents using its data classification standards without first engaging outside investigators.

✓ **D** Prioritize the incidents based on data classification standards
Data classification indicates the sensitivity and importance of the information affected, which helps determine the relative urgency and impact of incidents. Applying the standards across these incidents gives the manager a consistent basis for prioritizing potential exfiltration from critical systems.


Free demo · full exam: 967 questions

## Question 76

Single choice · Domain: D4 Incident Management › Establish and maintain incident escalation and notification processes.

Which of the following is MOST important when responding to a major security incident?

**A.** Contacting forensic investigators
**B.** Following the escalation process
**C.** Notifying law enforcement
**D.** Identifying the indicators of compromise

**Answer:** B. Following the escalation process

**Explanation**

Following the escalation process is most important because it ensures a major security incident is reported to the appropriate people and handled through the organization's established response structure. This provides coordinated decision-making and helps ensure that actions such as investigation, containment, and external notification occur in the proper order. The other actions may be important, but they do not replace escalation.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance
https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2020/volume-24/five-key-considerations-for-developing-a-cybersecurity-emergency-action-plan
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/incident-response-models

✗ **A** Contacting forensic investigators
Forensic investigators may be needed to determine what happened and preserve evidence, but contacting them is a specific response action rather than the primary requirement for initiating a coordinated response. Escalation helps ensure the right resources are engaged at the appropriate time.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/incident-response-models

✓ **B** Following the escalation process
A major incident requires prompt, coordinated handling, and the escalation process routes it to the designated decision-makers and responders. Following that process also helps ensure subsequent actions are authorized and coordinated.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance
https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2020/volume-24/five-key-considerations-for-developing-a-cybersecurity-emergency-action-plan
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/incident-response-models

✗ **C** Notifying law enforcement
Law enforcement may need to be notified in some incidents, depending on the circumstances and organizational requirements. It is not the most important first consideration in every major incident; escalation ensures the appropriate internal decision-makers can determine whether and when to notify them.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance
https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2020/volume-24/five-key-considerations-for-developing-a-cybersecurity-emergency-action-plan

✗ **D** Identifying the indicators of compromise


Free demo · full exam: 967 questions

Identifying indicators of compromise supports detection and investigation, but it is only one technical task within incident response. For a major incident, the established escalation process is needed to coordinate the response and bring in appropriate expertise.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/incident-response-models

## Question 77

Single choice · Domain: D4 Incident Management › Establish and maintain an organizational incident response plan to ensure an effective response to information security incidents.

An information security manager has confirmed the organization's cloud provider has unintentionally published some of the organization's business dat a. Which of the following should be done NEXT?

**A.** Identify users associated with the exposed data.
**B.** Initiate the organization's data loss prevention (DLP) processes.
**C.** Review the cloud provider's service level agreement (SLA).
**D.** Invoke the incident response plan.

**Answer:** D. Invoke the incident response plan.

**Explanation**

The provider’s unintended publication confirms a security incident involving the organization’s business data. The next step is to invoke the incident response plan so the organization can coordinate containment, investigation, communications, and recovery under its established procedures. Identifying affected users and reviewing DLP processes or the SLA can follow as part of the response.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance

✗ **A** Identify users associated with the exposed data.
Determining which users are affected is useful during the incident investigation, but the organization should first activate its incident response process. That process helps coordinate the investigation and other response activities.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance

✗ **B** Initiate the organization's data loss prevention (DLP) processes.
DLP measures may help prevent or detect further data exposure, but they are not a substitute for activating the incident response plan after a confirmed disclosure. The plan provides the coordinated framework for handling the incident.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance
https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/data-loss-preventionnext-steps

✗ **C** Review the cloud provider's service level agreement (SLA).
The SLA may be relevant to responsibilities or remedies involving the provider, but reviewing it does not address the immediate need to manage a confirmed security incident. The incident response plan should be invoked first.

✓ **D** Invoke the incident response plan.


Free demo · full exam: 967 questions

The provider has confirmed an unintended publication of the organization's business data, so this is a security incident requiring a coordinated response. Invoking the plan establishes the appropriate process for managing immediate actions and subsequent investigation.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance

## Question 78

Single choice · Domain: D4 Incident Management › Establish and maintain processes to investigate and document information security incidents to determine appropriate response and root cause.

An incident handler is preparing a forensic image of a hard drive. Which of the following MUST be done to provide evidence that the image is an exact copy of the original?

**A.** Perform a manual verification of file counts.
**B.** Encrypt and back up the hard drive before copying.
**C.** Use the same hardware for the image as the original.
**D.** Perform digital hashing of the original and the image.

**Answer:** D. Perform digital hashing of the original and the image.

**Explanation**

To provide evidence that the forensic image is an exact copy, compare cryptographic hashes computed from the original drive and the image. Matching hashes show that their contents are identical for practical forensic verification. File counts do not establish that every bit matches, and using the same hardware or backing up the drive is not the required verification.

https://www.isaca.org/resources/white-papers/overview-of-digital-forensics

✗ **A** Perform a manual verification of file counts.
Matching file counts does not prove that the files' contents or other data on the drive are identical. A hash comparison provides a stronger integrity check of the original and image.

https://www.isaca.org/resources/white-papers/overview-of-digital-forensics

✗ **B** Encrypt and back up the hard drive before copying.
Encryption and backup are not evidence that the forensic image exactly matches the original. They do not verify the image's integrity against the source.

✗ **C** Use the same hardware for the image as the original.
The image does not need to be created using the same hardware as the original drive. Hardware similarity does not demonstrate that the copied data is identical.

✓ **D** Perform digital hashing of the original and the image.
Hashing both the original and the image allows their resulting hash values to be compared. Matching hashes provide evidence that the image is an exact copy of the original data.

https://www.isaca.org/resources/white-papers/overview-of-digital-forensics



Free demo · full exam: 967 questions

## Question 79

Single choice · Domain: D4 Incident Management › Organize, train and equip incident response teams to respond to information security incidents in an effective and timely manner.

A global organization is developing an incident response team. The organization wants to keep headquarters informed of all incidents and wants to be able to present a unified response to widely dispersed events. Which of the following BEST supports these objectives?

**A.** Virtual incident response team
**B.** Distributed incident response team
**C.** Outsourced incident response team
**D.** Centralized incident response team

**Answer:** D. Centralized incident response team

**Explanation**

A centralized incident response team provides headquarters with a single point of coordination and oversight, helping ensure incidents are reported consistently. Its centralized command structure also supports a unified response when events occur across widely dispersed locations.

✗ **A** Virtual incident response team
A virtual team works across locations using remote collaboration, but that does not by itself ensure headquarters is informed of all incidents or provide centralized command for a unified response. The scenario emphasizes coordination and oversight from headquarters.

✗ **B** Distributed incident response team
A distributed team places response capability across different locations, which can help with local events. However, dispersed teams do not inherently give headquarters a single point of oversight or ensure a unified response across locations.

✗ **C** Outsourced incident response team
An outsourced team provides response services through an external provider, but outsourcing does not specifically meet the requirements for headquarters visibility and a unified organizational response. Centralized coordination is the key need described.

✓ **D** Centralized incident response team
A centralized team gives headquarters a common point for incident reporting, coordination, and oversight. This structure supports consistent decisions and a unified response to events occurring across widely dispersed locations.


Free demo · full exam: 967 questions

## Question 80

Single choice · Domain: D4 Incident Management › Establish and maintain an organizational incident response plan to ensure an effective response to information security incidents.

Which of the following is the MOST appropriate action during the containment phase of a cyber incident response?

**A.** Isolate affected systems to prevent the spread of damage
**B.** Determine the final root cause of the incident
**C.** Mitigate exploited vulnerabilities to prevent future incidents
**D.** Remove all instances of the incident from the network

**Answer:** A. Isolate affected systems to prevent the spread of damage

**Explanation**

During containment, the immediate priority is to limit the incident's impact and stop it from spreading. Isolating affected systems does this while response teams continue investigation and recovery. Determining root cause, mitigating vulnerabilities, and removing the incident are addressed in later response activities.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/incident-response-models

✓ **A** Isolate affected systems to prevent the spread of damage
Isolation limits an incident's ability to spread to other systems and helps contain its impact. It is an immediate containment action, rather than a step that depends on completing the investigation or eradication first.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/incident-response-models

✗ **B** Determine the final root cause of the incident
Root-cause analysis is part of investigating and understanding the incident, not the immediate goal of containment. Waiting to determine the final cause before limiting spread could allow further damage.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/incident-response-models

✗ **C** Mitigate exploited vulnerabilities to prevent future incidents
Mitigating vulnerabilities is primarily a remediation or improvement activity intended to prevent recurrence. Containment focuses first on limiting the current incident's spread and impact.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/incident-response-models

✗ **D** Remove all instances of the incident from the network
Removing incident artifacts is eradication, which follows containment. Attempting removal before the incident is contained can leave active threats able to spread or interfere with response actions.

https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance
https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/incident-response-models


Free demo · full exam: 967 questions