DUMPSBOSS.

Certified Information Security Manager

Isaca CISM

Version Demo

Total Demo Questions: 20

Total Premium Questions: 1864

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

Which of the following is the MOST effective approach to communicate general information security responsibilities across an organization?

A. Require staff to sign confidentiality agreements.

B. Develop a RACI matrix for the organization.

C. Specify information security responsibilities in job descriptions.

D. Provide regular security awareness training.

ANSWER: C

Explanation:

The most effective way to communicate general security responsibilities across the whole organization is to bake them into job descriptions. When responsibilities are written into each role, people know what's expected of them from day one, and managers can reinforce it during onboarding, performance reviews, and day-to-day supervision. It also makes accountability clearer because the responsibility is tied directly to the position, not just a one-time message.

Confidentiality agreements (A) are mostly about legal obligations and protecting information, but they don't explain the practical "what do I do?" responsibilities for security. A RACI matrix (B) is useful for specific processes and projects, but it's often too detailed and not something most employees will ever read. Security awareness training (D) is important, but it's more about education and reminders; it works best after the organization has already clearly defined who is responsible for what.

References: https://www.nist.gov/privacy-framework/nist-privacy-framework-and-cybersecurity-framework-resources (see the emphasis on roles and responsibilities) and https://www.iso.org/standard/27001 (ISO/IEC 27001 highlights assigning and communicating information security roles and responsibilities).

QUESTION NO: 2

Which of the following sites would be MOST appropriate in the case of a very short recovery time objective (RTO)?

A. Warm

B. Redundant

C. Shared

D. Mobile

E. Hot

ANSWER: E

Explanation:

If the business needs a very short RTO, you want a recovery site that's already up and running (or can be brought online almost immediately) with systems and data ready to go. That's why a **hot site** is usually the best fit for a "very short RTO" requirement.

A **warm site** can still take hours or even days to fully restore because it often has some infrastructure in place but may not have current data or fully configured systems. Options like **shared** or **mobile** sites can add extra delay due to logistics and availability. "**Redundant**" isn't really a standard recovery-site type on its own; it's more of a design approach (like active-active or active-passive) and doesn't clearly answer the "which site" question.

Reference: https://www.techtarget.com/searchdisasterrecovery/answer/What-is-the-difference-between-a-hot-site-and-a-cold-site-for-disaster-recovery and https://en.wikipedia.org/wiki/Hot_site

QUESTION NO: 3

Security audit reviews should PRIMARILY:

A. ensure that controls operate as required.

B. ensure that controls are cost-effective.

C. focus on preventive controls.

D. ensure controls are technologically current.

ANSWER: A

Explanation:

The main job of a security audit or review is to give management confidence that the security controls in place are actually working the way they're supposed to. In other words, the audit is there to check whether controls are designed properly and operating effectively—not just whether they exist on paper.

Cost, modern technology choices, and whether controls are preventive are all useful things to look at, but they're secondary. An audit shouldn't zoom in only on preventive controls, because detective and corrective controls matter too (for example, logging/monitoring and incident response). What matters most is whether the overall control set is operating as required to manage risk to an acceptable level.

References: https://www.isaca.org/resources/cobit and https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

QUESTION NO: 4

Which of the following would BEST protect an organization's confidential data stored on a laptop computer from unauthorized access?

A. Strong authentication by password

B. Encrypted hard drives

C. Multifactor authentication procedures

D. Network-based data backup

ANSWER: B

Explanation:

The best protection for confidential data on a laptop is full-disk (or strong drive) encryption. If the laptop is lost or stolen, encryption keeps the data unreadable without the decryption key, even if someone removes the drive and connects it to another computer. That's the key difference: it protects the data "at rest," not just access to the running device.

A strong password or even multifactor authentication helps when the attacker is trying to log in normally, but it doesn't necessarily stop an offline attack where the hard drive is taken out and examined separately. In that situation, encryption is what actually blocks access to the files.

Network-based backups are useful for recovery and availability, but they don't stop someone from reading what's already on the stolen laptop. For more on why encryption is the go-to control for lost devices, see https://csrc.nist.gov/publications/detail/sp/800-111/final and a practical overview at https://support.apple.com/guide/mac-help/protect-your-mac-information-with-encryption-mh40593/mac

QUESTION NO: 5

Which of the following needs to be established between an IT service provider and its clients to the BEST enable adequate continuity of service in preparation for an outage?

A. Data retention policies

B. Server maintenance plans

C. Recovery time objectives

D. Reciprocal site agreement

ANSWER: C

Explanation:

The key thing an IT service provider and its clients need to agree on ahead of time is the recovery time objective (RTO). RTO sets the maximum acceptable downtime for a service after an outage. Once that target is clear and formally agreed, the provider can design the right continuity and disaster recovery approach (people, process, technology, and cost) to meet it.

Data retention policies are important, but they mainly deal with how long data is kept and for compliance—not how fast services must be restored. Server maintenance plans help prevent outages, but they don't define the business-acceptable downtime during a disruption. A reciprocal site agreement could be one possible recovery strategy, but it's a solution choice; you still need the RTO first to know whether that strategy is good enough.

References: https://www.itil-docs.com/blogs/itil-definitions/recovery-time-objective-rto and https://www.nist.gov/privacy-framework/nist-sp-800-34-contingency-planning-guide-federal-information-systems

QUESTION NO: 6

Phishing is BEST mitigated by which of the following?

A. Security monitoring software

B. Encryption

C. Two-factor authentication

D. User awareness

ANSWER: D

Explanation:

Phishing works mainly by tricking people, not by “breaking” technology. That’s why the best mitigation is user awareness: training users to spot suspicious emails, unexpected links, urgent requests, fake login pages, and “too good to be true” messages. When people know what to look for and feel comfortable reporting something odd, you cut off the attacker’s easiest path.

Security monitoring tools can help (for example, flagging malicious domains or attachments), but they’re not perfect and attackers constantly change tactics. Encryption doesn’t stop someone from being fooled into giving away credentials, and two-factor authentication helps reduce the impact of stolen passwords but doesn’t fully prevent phishing (attackers can still steal sessions, trick users into approving prompts, or target other sensitive actions).

So, if you have to pick the single BEST mitigation, it’s building strong user awareness backed by simple reporting and quick follow-up. References: https://www.cisa.gov/topics/cyber-threats-and-advisories/phishing, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/phishing

QUESTION NO: 7

Which of the following is the BEST method for ensuring that security procedures and guidelines are known and understood?

A. Periodic focus group meetings

B. Periodic compliance reviews

C. Computer-based certification training (CBT)

D. Employee's signed acknowledgement

ANSWER: C

Explanation:

The best choice is computer-based certification training (CBT) because it can actually check understanding, not just “expose” people to the content. Good CBT includes short quizzes, scenario questions, and an end-of-module test, so you can confirm users understood key security procedures (and you can track completion and scores).

Compliance reviews are useful, but they mainly tell you whether people followed the rules after the fact—they don’t reliably prove people knew or understood them. Focus groups can give you opinions and feedback, but they’re inconsistent and don’t scale well for verifying understanding across the whole organization. A signed acknowledgement is easy to collect, but it only proves someone signed a form; it doesn’t prove they read or understood the guidance.

References: https://www.nist.gov/privacy-framework/nist-privacy-framework-and-privacy-risk-management (training and awareness as part of organizational governance) and https://www.nist.gov/cyberframework (security awareness and training as a key organizational practice).

QUESTION NO: 8

An online payment provider's computer security incident response team has confirmed that a customer credit card database was breached. Which of the following is MOST important to include in a report to senior management?

A. A summary of the security logs that illustrates the sequence of events

B. An explanation of the potential business impact

C. An analysis of similar attacks and recommended remediation

D. A business case for implementing stronger logical access controls

ANSWER: B

Explanation:

Senior management mainly needs to understand what the breach means for the business so they can make fast, informed decisions. That's why the most important item in the report is the potential business impact—things like regulatory exposure (e.g., PCI DSS implications), legal and notification requirements, customer trust and reputation damage, operational disruption, and likely financial losses.

Technical details like log summaries or deep analysis of attack patterns are useful, but they're better suited for the incident response team and technical stakeholders. Executives typically need a clear picture of impact, urgency, and what decisions or approvals are required (for example, customer notifications, engaging forensics, or involving legal counsel).

This aligns with incident response guidance that emphasizes communicating impact and risk in business terms to leadership. For more background, see https://www.nist.gov/privacy-framework/nist-sp-800-61 and https://www.pcisecuritystandards.org/document_library.

QUESTION NO: 9

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

A. Identify the applications with the shortest recovery time objectives (RTOs)

B. Determine the business recovery strategy

C. Identify critical business processes

D. Determine available resources

ANSWER: C

Explanation:

The first thing you do when building a BCP is figure out what the business actually needs to keep running. That starts with identifying the critical business processes—things like order processing, patient care, payroll, or customer support—because everything else in continuity planning depends on what must be protected and restored.

Once you know the key processes, you can perform (or refine) the business impact analysis (BIA) to understand acceptable downtime, impacts, and priorities. Only after that does it make sense to talk about technical targets like RTOs for applications, pick recovery strategies, or check what resources you have available. If you jump straight to applications or strategies first, you risk protecting the wrong things or spending money in the wrong places.

References: https://www.ready.gov/business/implementation/continuity and https://www.iso.org/standard/75106.html

QUESTION NO: 10

An organization wants to integrate information security into its human resource management processes. Which of the following should be the FIRST step?

A. Evaluate the cost of information security integration

B. Assess the business objectives of the processes

C. Identify information security risk associated with the processes

D. Benchmark the processes with best practice to identify gaps

ANSWER: B

Explanation:

The first thing to do is understand what the HR processes are trying to achieve for the business. If you don't know the business objectives (for example, hiring speed, onboarding effectiveness, regulatory compliance, or employee lifecycle management), it's easy to bolt on controls that slow things down or miss what actually matters. Starting with objectives gives you the right context for deciding what "good security" looks like in HR.

Once the objectives are clear, you can then identify the information assets involved (candidate data, background checks, payroll details, access requests), assess the risks tied to those activities, and choose controls that support the goals instead of fighting them. Cost evaluation and benchmarking can be useful later, but they're not the best starting point because they don't anchor the work to what the business is trying to accomplish.

References: https://www.isaca.org/credentialing/cism and https://www.nist.gov/privacy-framework

QUESTION NO: 11

A PRIMARY purpose of creating security policies is to:

A. implement management's governance strategy.

B. establish the way security tasks should be executed.

C. communicate management's security expectations.

D. define allowable security boundaries.

ANSWER: C

Explanation:

The main reason organizations create security policies is to clearly communicate what management expects when it comes to protecting information. A policy is the "what" and "why" at a high level—things like direction, intent, and rules that everyone is expected to follow. It sets the tone and gives authority to security requirements across the business.

Option B sounds tempting, but it's more about procedures and standards. Those documents explain the step-by-step "how" to do security work (for example, how to configure access, how to run backups, or how to handle incidents). Policies don't usually go into that level of detail.

Option A is too broad (governance strategy is bigger than policy), and option D is more aligned to standards or specific control statements. If you're thinking CISM-style, policies are the top-level statement from management that drives everything else underneath.

References: https://www.nist.gov/privacy-framework/nist-privacy-framework/understanding-policies-standards-guidelines-and-procedures and https://csrc.nist.gov/glossary/term/security_policy

QUESTION NO: 12

Which of the following is the MOST appropriate method for deploying operating system (OS) patches to production application servers?

A. Batch patches into frequent server updates

B. Initially load the patches on a test machine

C. Set up servers to automatically download patches

D. Automatically push all patches to the servers

ANSWER: B

Explanation:

The best approach is to load and test patches in a non-production (test/staging) environment first. OS patches can sometimes break dependencies, change configurations, or conflict with application components, so you want to catch those issues before anything touches production.

Once the patch behaves well in testing, you can roll it into production using your normal change management process (approvals, maintenance window, rollback plan, and monitoring). This is why the "auto-download" and "auto-push everything" choices are risky for application servers—those options can introduce untested changes and cause unexpected outages.

Batching patches into "frequent updates" isn't really a method by itself; it doesn't address the key risk, which is whether the patch will impact the application. Testing first directly reduces that risk and aligns with good patch and change management practices.

References: https://csrc.nist.gov/pubs/sp/800/40/r4/final and https://www.cisa.gov/resources-tools/resources/implementing-patch-management

QUESTION NO: 13

What is the BEST method to confirm that all firewall rules and router configuration settings are adequate?

A. Periodic review of network configuration

B. Review intrusion detection system (IDS) logs for evidence of attacks

C. Periodically perform penetration tests

D. Daily review of server logs for evidence of hacker activity

ANSWER: C

Explanation:

The best way to confirm firewall rules and router settings are truly “adequate” is to test them the way an attacker would. A config review can tell you what the rules say, but it doesn’t always show how they behave in real life (rule order issues, overly broad permits, shadowed rules, unexpected routes, or gaps between devices).

IDS and server logs are useful for detecting and investigating activity, but they’re reactive—you’re waiting for something to happen (or to be detected) before you learn there’s a problem. They also won’t reliably prove that the rule base blocks what it should block.

Penetration testing (and related attack simulation) gives direct evidence that the current controls actually stop unauthorized access and allow legitimate traffic. Done periodically and after major changes, it’s a strong confirmation that the combined firewall/router configuration works as intended in practice. References: https://www.nist.gov/privacy-framework/nist-sp-800-115 and https://owasp.org/www-project-web-security-testing-guide/

QUESTION NO: 14

An organization establishes an internal document collaboration site. To ensure data confidentiality of each project group, it is MOST important to:

A. prohibit remote access to the site.

B. periodically recertify access rights.

C. enforce document lifecycle management.

D. conduct a vulnerability assessment.

ANSWER: B

Explanation:

For a collaboration site, the biggest confidentiality risk is usually that the wrong people can see the wrong project’s documents. The most direct control for that is making sure access rights are correct and stay correct over time. That’s why periodically recertifying access rights is the best answer—it catches “access creep” when people change roles, move to a new project, or leave the company but still keep old permissions.

Prohibiting remote access doesn’t really solve the core issue, because an internal user could still access another group’s content if permissions are too broad. Document lifecycle management is helpful for retention and disposal, but it doesn’t prevent unauthorized viewing today. A vulnerability assessment is important for security hygiene, but even a perfectly patched site can leak data if the access model is wrong.

Regular access reviews (recertification) are a classic CISM-style control for confidentiality because they enforce least privilege and make project owners confirm who should have access. References: https://en.wikipedia.org/wiki/Principle_of_least_privilege and https://csrc.nist.gov/glossary/term/access_control

QUESTION NO: 15

An incident response team recently encountered an unfamiliar type of cyber event. Though the team was able to resolve the issue, it took a significant amount of time to identify. What is the BEST way to help ensure similar incidents are identified more quickly in the future?

A. Perform a threat analysis.

B. Perform a post-incident review.

C. Establish performance metrics for the team.

D. Implement a SIEM solution.

ANSWER: B

Explanation:

The best move is to do a solid post-incident review (often called “lessons learned”) and turn what happened into something reusable—new detection rules, updated playbooks, better triage steps, and improved escalation criteria. Since the team already fixed the issue, the real gap was recognizing it fast. A post-incident review is the step that captures indicators of compromise, log sources that mattered, what signals were missed, and what should be monitored next time.

A SIEM can help, but it’s not automatically the “best” answer here because buying or implementing a tool doesn’t guarantee faster identification unless you feed it the right use cases and detection content. The post-incident review is where those SIEM use cases (or other monitoring rules) get defined based on what you just learned, making future identification quicker and more reliable.

References: https://www.nist.gov/privacy-framework/nist-sp-800-61 and https://www.cisa.gov/resources-tools/resources/incident-handling-overview

QUESTION NO: 16

What should be an information security manager's PRIMARY objective in the event of a security incident?

A. Contain the threat and restore operations in a timely manner.

B. Ensure that normal operations are not disrupted.

C. Identify the source of the breach and how it was perpetrated.

D. Identify lapses in operational control effectiveness.

ANSWER: A

Explanation:

In an actual security incident, the information security manager’s first priority is to limit damage and get the business back on its feet. That means focusing on containment (stopping the spread or ongoing impact) and restoring critical services safely and quickly. If you don’t contain the issue first, the incident can keep growing—more systems get affected, more data may be lost, and recovery becomes harder and more expensive.

The other choices matter, but they come after the immediate fire is under control. Keeping “normal operations” undisrupted (B) isn’t realistic during a real incident—some disruption is often necessary to stop the bleeding. Finding the attacker and how it happened (C) is part of investigation and forensics, which is important, but it’s not the first objective when the organization is actively being impacted. Identifying control lapses (D) is valuable for lessons learned and long-term improvement, but it’s a post-incident activity.

This aligns with standard incident response guidance: contain and eradicate the threat, then recover operations, and only then complete deeper analysis and improvements. References: https://csrc.nist.gov/pubs/sp/800/61/r2/final and https://www.cisa.gov/resources-tools/resources/incident-response-playbooks

QUESTION NO: 17

Management decisions concerning information security investments will be MOST effective when they are based on:

A. an annual loss expectancy (ALE) determined from the history of security events.

B. the formalized acceptance of risk analysis by management.

C. the reporting of consistent and periodic assessments of risks.

D. a process for identifying and analyzing threats and vulnerabilities.

ANSWER: C

Explanation:

The best security investment decisions come from understanding risk in a steady, repeatable way over time. That's why **consistent and periodic risk assessments** are the most effective basis: they give management a reliable view of what's changing, what's getting better or worse, and where money will actually reduce risk the most.

Option A (ALE from history) can help, but it's often incomplete because many security events are underreported, and past losses don't always predict future attacks. Option B (formal acceptance of risk analysis) is more about governance and sign-off than about making good investment choices. Option D (identifying threats and vulnerabilities) is important, but by itself it doesn't prioritize or quantify risk well enough to guide spending.

With regular assessments, leaders can compare risks across business areas, track trends, and justify investments using current exposure—not just one-time studies or gut feel. This aligns with the idea that risk management should be ongoing and measurable.

References: https://www.nist.gov/privacy-framework/nist-risk-management-framework
https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

QUESTION NO: 18

Which of the following BEST illustrates residual risk within an organization?

A. Risk management framework

B. Risk register

C. Business impact analysis

D. Heat map

ANSWER: B

Explanation:

Residual risk is the amount of risk that's still left over after you've put controls and treatments in place. The best place to "illustrate" that remaining exposure is the risk register, because it typically records the inherent risk, the controls/mitigations applied, and the remaining (residual) risk rating that management accepts or further treats.

A risk management framework is more like the rulebook for how you do risk management; it doesn't show the remaining risk for specific scenarios. A business impact analysis focuses on impact to business processes from disruptions, not the leftover

risk after controls. A heat map can visualize risk levels, but it usually shows a snapshot of risk ratings and may not explicitly distinguish residual vs. inherent unless it's specifically designed that way. In practice, the risk register is the clearest, most direct artifact for documenting and demonstrating residual risk per risk item.

References: https://en.wikipedia.org/wiki/Risk_register and https://en.wikipedia.org/wiki/Residual_risk

QUESTION NO: 19

Business units within an organization are resistant to proposed changes to the information security program. Which of the following is the BEST way to address this issue?

A. Implementing additional security awareness training

B. Communicating critical risk assessment results to business unit managers

C. Including business unit representation on the security steering committee

D. Publishing updated information security policies

ANSWER: B

Explanation:

The best way to reduce resistance is to make the change feel relevant to the business. Communicating the key results of risk assessments to business unit managers (in business language) helps them see what could realistically happen—financial loss, operational downtime, customer impact, regulatory exposure—and why the proposed security changes are worth the effort.

Security awareness training (A) and publishing policies (D) may help later, but they don't directly address the "why should we change?" question that drives resistance. Including business representation on a steering committee (C) is useful for long-term alignment, but it can be slower and may not immediately overcome pushback unless leaders first understand the risk and urgency.

When managers understand the critical risks and how the changes reduce those risks, they're much more likely to sponsor the effort, prioritize resources, and influence their teams to cooperate. This is classic CISM thinking: tie security decisions to risk management and business objectives rather than pushing security changes as a purely technical or compliance exercise.

References: https://www.isaca.org/resources/cism and https://www.nist.gov/privacy-framework/nist-privacy-framework

QUESTION NO: 20

Which of the following is the BEST way to address risk associated with using an outsourced technology service provider?

A. Review cyber liability insurance.

B. Implement a vendor management program.

C. Require management approval for vendor selection.

D. Perform due diligence on the provider at contract time.

ANSWER: B

Explanation:

The best answer is to implement a vendor management program because it covers the full life cycle of the outsourced relationship—not just the moment you sign the contract. Outsourcing risk isn't a one-time problem; it changes over time as the provider's controls, staff, subcontractors, and even financial health change.

A solid vendor management program typically includes ongoing due diligence, security and compliance requirements in contracts, SLAs, right-to-audit clauses, continuous monitoring (for example, SOC reports), issue management, and periodic risk reassessments. That broad, ongoing coverage is what makes it the "best" choice.

By comparison, cyber liability insurance can help transfer some financial impact, but it doesn't prevent failures or ensure the provider is actually managing security well. Management approval for vendor selection is a governance step, but it's too narrow to manage day-to-day and ongoing risk. And due diligence only at contract time is important, but it's incomplete without continuous oversight.

References: https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/supply-chain-risk-management and https://www.cisa.gov/supply-chain