Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

712-50 MCQs
712-50 TestPrep
712-50 Study Guide
712-50 Practice Test
712-50 Exam Questions

killexams.com

EC-Council

712-50

EC-Council Certified CISO (CCISO)

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/712-50

QUESTION: 330
Scenario: You are the newly hired Chief Information Security Officer for a company that has not previously had a senior level security practitioner. The company lacks a defined security policy and framework for their Information Security Program. Your new boss, the Chief Financial Officer, has asked you to draft an outline of a security policy and recommend an industry/sector neutral information security control framework for implementation. Which of the following industry / sector neutral information security control frameworks should you recommend for implementation?

A. National Institute of Standards and Technology (NIST) Special Publication 800-53
B. Payment Card Industry Digital Security Standard (PCI DSS)
C. International Organization for Standardization – ISO 27001/2
D. British Standard 7799 (BS7799)

Answer: C

QUESTION: 331
Scenario: You are the CISO and have just completed your first risk assessment for your organization. You find many risks with no security controls, and some risks with inadequate controls. You assign work to your staff to create or adjust existing security controls to ensure they are adequate for risk mitigation needs. You have identified potential solutions for all of your risks that do not have security controls. What is the NEXT step?

A. Get approval from the board of directors
B. Screen potential vendor solutions
C. Verify that the cost of mitigation is less than the risk
D. Create a risk metrics for all unmitigated risks

Answer: C

QUESTION: 332
Access Control lists (ACLs), Firewalls, and Intrusion Prevention Systems are examples of

A. Network based security preventative controls
B. Software segmentation controls
C. Network based security detective controls
D. User segmentation controls

Answer: A

QUESTION: 333
Scenario: You are the newly hired Chief Information Security Officer for a company that has not previously had a senior level security practitioner. The company lacks a defined security policy and framework for their Information Security Program. Your new boss, the Chief Financial Officer, has asked you to draft an outline of a security policy and recommend an industry/sector neutral information security control framework for implementation. Your Corporate Information Security Policy should include which of the following?

A. Information security theory
B. Roles and responsibilities
C. Incident response contacts
D. Desktop configuration standards

Answer: B

QUESTION: 334
Scenario: You are the CISO and have just completed your first risk assessment for your organization. You find many risks with no security controls, and some risks with inadequate controls. You assign work to your staff to create or adjust existing security controls to ensure they are adequate for risk mitigation needs. When adjusting the controls to mitigate the risks, how often should the CISO perform an audit to verify the controls?

A. Annually
B. Semi-annually
C. Quarterly
D. Never

Answer: D

QUESTION: 335
The process for management approval of the security certification process which states the risks and mitigation of such risks of a given IT system is called

A. Security certification
B. Security system analysis

C. Security accreditation
D. Alignment with business practices and goals.

Answer: C

QUESTION: 336
Scenario: Your program is developed around minimizing risk to information by focusing on people, technology, and operations. You have decided to deal with risk to information from people first. How can you minimize risk to your most sensitive information before granting access?

A. Conduct background checks on individuals before hiring them
B. Develop an Information Security Awareness program
C. Monitor employee browsing and surfing habits
D. Set your firewall permissions aggressively and monitor logs regularly.

Answer: A

QUESTION: 337
Scenario: The new CISO was informed of all the Information Security projects that the section has in progress. Two projects are over a year behind schedule and way over budget. Using the best business practices for project management, you determine that the project correctly aligns with the organization goals. What should be verified next?

A. Scope
B. Budget
C. Resources
D. Constraints

Answer: A

QUESTION: 338
What are the primary reasons for the development of a business case for a security project?

A. To estimate risk and negate liability to the company
B. To understand the attack vectors and attack sources

C. To communicate risk and forecast resource needs
D. To forecast usage and cost per software licensing

Answer: C

QUESTION: 339
File Integrity Monitoring (FIM) is considered a

A. Network based security preventative control
B. Software segmentation control
C. Security detective control
D. User segmentation control

Answer: C

QUESTION: 340
Scenario: As you begin to develop the program for your organization, you assess the corporate culture and determine that there is a pervasive opinion that the security program only slows things down and limits the performance of the "real workers." What must you do first in order to shift the prevailing opinion and reshape corporate culture to understand the value of information security to the organization?

A. Cite compliance with laws, statutes, and regulations – explaining the financial implications for the company for non-compliance
B. Understand the business and focus your efforts on enabling operations securely
C. Draw from your experience and recount stories of how other companies have been compromised
D. Cite corporate policy and insist on compliance with audit findings

Answer: B

QUESTION: 341
Acceptable levels of information security risk tolerance in an organization should be determined by?

A. Corporate legal counsel
B. CISO with reference to the company goals
C. CEO and board of director

D. Corporate compliance committee

Answer: C

QUESTION: 342
When dealing with risk, the information security practitioner may choose to:

A. assign
B. transfer
C. acknowledge
D. defer

Answer: C

QUESTION: 343
Scenario: Your organization employs single sign-on (user name and password only) as a convenience to your employees to access organizational systems and data. Permission to individual systems and databases is vetted and approved through supervisors and data owners to ensure that only approved personnel can use particular applications or retrieve information. All employees have access to their own human resource information, including the ability to change their bank routing and account information and other personal details through the Employee Self-Service application. All employees have access to the organizational VPN. What type of control is being implemented by supervisors and data owners?

A. Management
B. Operational
C. Technical
D. Administrative

Answer: B

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.