EC-Council Certified CISO

1. Topic #: 1
From an information security perspective, information that no longer supports the main purpose of the business should be:

A. A. protected under the information classification policy

B. B. analyzed under the data ownership policy

C. C. assessed by a business impact analysis.

D. D. analyzed under the retention policy.

Answer(s): A

---

2. Question #: 457
Topic #: 1
From the CISO’s perspective in looking at financial statements, the statement of retained earnings of an organization:

A. A. Has a direct correlation with the CISO’s budget

B. B. Represents, in part, the savings generated by the proper acquisition and implementation of security controls

C. C. Represents the sum of all capital expenditures

D. D. Represents the percentage of earnings that could in part be used to finance future security controls

Answer(s): D

---

3. Question #: 449
Topic #: 1
You have been hired as the CISO for a hospital. The hospital currently deploys a hybrid cloud

model using a Software as a Service (SaaS) product for healthcare clearinghouse services. The Health Insurance Portability and Accountability Act (HIPAA) require an agreement between Cloud Service Providers (CSP) and the covered entity. Based on HIPAA, once the agreement between the covered entity and the CSP signed, the CSP is _____?

A. A. Partially liable for compliance with the applicable requirements of the HIPAA Rules

B. B. Directly liable for compliance with the applicable requirements of the HIPAA Rules

C. C. Not liable for compliance with the applicable requirements of the HIPAA Rules

D. D. Indirectly liable for compliance with the applicable requirements of the HIPAA Rules

Answer(s): B

---

4. Question #: 440
Topic #: 1
As the CISO, you are the project sponsor for a highly visible log management project. The objective of the project is to centralize all the enterprise logs into a security information and event management (SIEM) system. You requested the results of the performance quality audits activity. The performance quality audit activity is done in what project management process group?

A. A. Executing

B. B. Controlling

C. C. Planning

D. D. Closing

Answer(s): B

---

5. Question #: 417
Topic #: 1
To make sure that the actions of all employees, applications, and systems follow the organization’s rules and regulations can BEST be described as which of the following?

A. A. Compliance management

B. B. Asset management

C. C. Risk management

D. D. Security management

Answer(s): A

---

6. Question #: 415
Topic #: 1
A key cybersecurity feature of a Personal Identification Verification (PIV) Card is:

A. A. Inability to export the private certificate/key

B. B. It can double as physical identification at the DMV

C. C. It has the user’s photograph to help ID them

D. D. It can be used as a secure flash drive

Answer(s): A

---

7. Question #: 384
Topic #: 1
Michael starts a new job and discovers that he has unnecessary access to a variety of systems. Which of the following best describes the problem he has encountered?

A. A. Rights collision

B. B. Excessive privileges

C. C. Privilege creep

D. D. Least privileges

Answer(s): C

---

8. Question #: 373
Topic #: 1
Which of the following defines the boundaries and scope of a risk assessment?

A. A. The risk assessment schedule

B. B. The risk assessment framework

C. C. The risk assessment charter

D. D. The assessment context

Answer(s): D

---

9. Question #: 371
Topic #: 1
A newly-hired CISO needs to understand the organization’s financial management standards for business units and operations. Which of the following would be the best source of this information?

A. A. The internal accounting department

B. B. The Chief Financial Officer (CFO)

C. C. The external financial audit service

D. D. The managers of the accounts payables and accounts receivables teams

Answer(s): B

---

10. Question #: 370
Topic #: 1
Which of the following is an accurate statement regarding capital expenses?

A. A. They are easily reduced through the elimination of usage, such as reducing power for lighting of work areas during off-hours

B. B. Capital expenses can never be replaced by operational expenses

C. C. Capital expenses are typically long-term investments with value being realized through their use

D. D. The organization is typically able to regain the initial cost by selling this type of asset

Answer(s): C

---

11. Question #: 367
Topic #: 1
What is meant by password aging?

A. A. An expiration date set for passwords

B. B. A Single Sign-On requirement

C. C. Time in seconds a user is allocated to change a password

D. D. The amount of time it takes for a password to activate

Answer(s): A

---

12. Question #: 363
Topic #: 1
During the 3rd quarter of a budget cycle, the CISO noticed she spent more than was originally planned in her annual budget. What is the condition of her current budgetary posture?

A. A. The budget is in a temporary state of imbalance

B. B. The budget is operating at a deficit

C. C. She can realign the budget through moderate capital expense (CAPEX) allocation

D. D. She has a surplus of operational expenses (OPEX)

Answer(s): B

---

13. Question #: 360
Topic #: 1
Which of the following best describes revenue?

A. A. Non-operating financial liabilities minus expenses

B. B. The true profit-making potential of an organization

C. C. The sum value of all assets and cash flow into the business

D. D. The economic benefit derived by operating a business

Answer(s): D

---

14. Question #: 359
Topic #: 1
Where does bottom-up financial planning primarily gain information for creating budgets?

A. A. By adding all capital and operational costs from the prior budgetary cycle, and determining potential financial shortages

B. B. By reviewing last year’s program-level costs and adding a percentage of expected additional portfolio costs

C. C. By adding the cost of all known individual tasks and projects that are planned for the next budgetary cycle

D. D. By adding all planned operational expenses per quarter then summarizing them in a budget request

Answer(s): C

---

15. Question #: 357
Topic #: 1
Which of the following is the MOST logical method of deploying security controls within an organization?

A. A. Obtain funding for all desired controls and then create project plans for implementation

B. B. Apply the simpler controls as quickly as possible and use a risk-based approach for the more difficult and costly controls

C. C. Apply the least costly controls to demonstrate positive program activity

D. D. Obtain business unit buy-in through close communication and coordination

Answer(s): D

---

16. Question #: 356
Topic #: 1
The network administrator wants to strengthen physical security in the organization. Specifically, to implement a solution stopping people from entering certain restricted zones without proper credentials. Which of following physical security measures should the administrator use?

A. A. Video surveillance

B. B. Mantrap

C. C. Bollards

D. D. Fence

Answer(s): B

---

17. Question #: 376
Topic #: 1
At what level of governance are individual projects monitored and managed?

A. A. Program

B. B. Milestone

C. C. Enterprise

D. D. Portfolio

Answer(s): D

---

18. Question #: 326
Topic #: 1
Scenario: Most industries require compliance with multiple government regulations and/or industry standards to meet data protection and privacy mandates.
When multiple regulations or standards apply to your industry you should set controls to meet the_____.

A. A. Most complex standard

B. B. Recommendations of your Legal Staff

C. C. Easiest regulation or standard to implement

D. D. Stricter regulation or standard

Answer(s): D

---

19. Question #: 322
Topic #: 1
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. A. Scope

B. B. Constraints

C. C. Resources

D. D. Budget

Answer(s): A

20. Question #: 305
Topic #: 1
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. A. Set your firewall permissions aggressively and monitor logs regularly.

B. B. Develop an Information Security Awareness program

C. C. Conduct background checks on individuals before hiring them

D. D. Monitor employee drowsing and surfing habits

Answer(s): C