EC-Council Certified Security Analyst

1. Credit card information, medical data, and government records are all examples of:

A. Confidential/Protected Information

B. Bodily Information

C. Territorial Information

D. Communications Information

Answer(s): A

---

2. The establishment of a formal risk management framework and system authorization program is essential. The LAST step of the system authorization process is:

A. Contacting the Internet Service Provider for an IP scope

B. Getting authority to operate the system from executive management

C. Changing the default passwords

D. Conducting a final scan of the live system and mitigating all high and medium level vulnerabilities

Answer(s): B

---

3. The single most important consideration to make when developing your security program, policies, and processes is:

A. Budgeting for unforeseen data compromises

B. Streamlining for efficiency

C. Alignment with the business

D. Establishing your authority as the Security Executive

Answer(s): C

---

4. An organization's Information Security Policy is of MOST importance because

A. it communicates management's commitment to protecting information resources

B. it is formally acknowledged by all employees and vendors

C. it defines a process to meet compliance requirements

D. it establishes a framework to protect confidential information

Answer(s): A

---

5. Developing effective security controls is a balance between:

A. Risk Management and Operations

B. Corporate Culture and Job Expectations

C. Operations and Regulations

D. Technology and Vendor Management

Answer(s): A

---

6. The PRIMARY objective for information security program development should be:

A. Reducing the impact of the risk to the business.

B. Establishing strategic alignment with business continuity requirements

C. Establishing incident response programs.

D. Identifying and implementing the best security solutions.

Answer(s): A

---

7. Which of the following should be determined while defining risk management strategies?

A. Organizational objectives and risk tolerance

B. Risk assessment criteria

C. IT architecture complexity

D. Enterprise disaster recovery plans

Answer(s): A

---

8. Who in the organization determines access to information?

A. Legal department

B. Compliance officer

C. Data Owner

D. Information security officer

Answer(s): C

---

9. Which of the following is a benefit of information security governance?

A. Questioning the trust in vendor relationships.

B. Increasing the risk of decisions based on incomplete management information.

C. Direct involvement of senior management in developing control processes

D. Reduction of the potential for civil and legal liability

Answer(s): D

---

10. Which of the following is the MOST important benefit of an effective security governance process?

A. Reduction of liability and overall risk to the organization

B. Better vendor management

C. Reduction of security breaches

D. Senior management participation in the incident response process

Answer(s): A

---

11. The FIRST step in establishing a security governance program is to?

A. Conduct a risk assessment.

B. Obtain senior level sponsorship.

C. Conduct a workshop for all end users.

D. Prepare a security budget.

Answer(s): B

---

12. Which of the following has the GREATEST impact on the implementation of an information security governance model?

A. Organizational budget

B. Distance between physical locations

C. Number of employees

D. Complexity of organizational structure

Answer(s): D

---

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

A. assessed by a business impact analysis.

B. protected under the information classification policy.

C. analyzed under the data ownership policy.

D. analyzed under the retention policy

Answer(s): D

---

14. When briefing senior management on the creation of a governance process, the MOST important aspect should be:

A. information security metrics.

B. knowledge required to analyze each issue.

C. baseline against which metrics are evaluated.

D. linkage to business area objectives.

Answer(s): D

---

15. Which of the following most commonly falls within the scope of an information security governance steering committee?

A. Approving access to critical financial systems

B. Developing content for security awareness programs

C. Interviewing candidates for information security specialist positions

D. Vetting information security policies

Answer(s): D

---

16. A security professional has been promoted to be the CISO of an organization. The first task is to create a security policy for this organization. The CISO creates and publishes the security policy. This policy however, is ignored and not enforced consistently.
Which of the following is the MOST likely reason for the policy shortcomings?

A. Lack of a formal security awareness program

B. Lack of a formal security policy governance process

C. Lack of formal definition of roles and responsibilities

D. Lack of a formal risk management policy

Answer(s): B

---

17. Which of the following is the MAIN reason to follow a formal risk management process in an organization that hosts and uses privately identifiable information (PII) as part of their business models and processes?

A. Need to comply with breach disclosure laws

B. Need to transfer the risk associated with hosting PII data

C. Need to better understand the risk associated with using PII data

D. Fiduciary responsibility to safeguard credit card information

Answer(s): C

---

18. The alerting, monitoring and life-cycle management of security related events is typically handled by the

A. security threat and vulnerability management process

B. risk assessment process

C. risk management process

D. governance, risk, and compliance tools

Answer(s): A

---

19. One of the MAIN goals of a Business Continuity Plan is to

A. Ensure all infrastructure and applications are available in the event of a disaster

B. Allow all technical first-responders to understand their roles in the event of a disaster

C. Provide step by step plans to recover business processes in the event of a disaster

D. Assign responsibilities to the technical teams responsible for the recovery of all data.

Answer(s): C

---

20. When managing an Information Security Program, which of the following is of MOST importance in order to influence the culture of an organization?

A. An independent Governance, Risk and Compliance organization

B. Alignment of security goals with business goals

C. Compliance with local privacy regulations

D. Support from Legal and HR teams

Answer(s): B
