Certified Ethical Hacker (CEH)

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

A. knowledge required to analyze each issue

B. information security metrics

C. linkage to business area objectives

D. baseline against which metrics are evaluated

Answer(s): C

---

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

A. Organizational objectives and risk tolerance

B. Enterprise disaster recovery plans

C. Risk assessment criteria

D. IT architecture complexity

Answer(s): A

---

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

A. Senior management participation in the incident response process

B. Better vendor management

C. Reduction of security breaches

D. Reduction of liability and overall risk to the organization

Answer(s): D

---

4. A global retail organization is looking to implement a consistent Disaster Recovery and Business Continuity Process across all of its business units.
Which of the following standards and guidelines can BEST address this organization’s need?

A. International Organization for Standardizations – 22301 (ISO-22301)

B. Information Technology Infrastructure Library (ITIL)

C. Payment Card Industry Data Security Standards (PCI-DSS)

D. International Organization for Standardizations – 27005 (ISO-27005)

Answer(s): A

---

5. A security manager regularly checks work areas after business hours for security violations; such as unsecured files or unattended computers with active sessions.
This activity BEST demonstrates what part of a security program?

A. Compliance management

B. Audit validation

C. Physical control testing

D. Security awareness training

Answer(s): A

---

6. 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. Fiduciary responsibility to safeguard credit information

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

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

Answer(s): D

---

7. A method to transfer risk is to_____________.

A. Implement redundancy

B. Move operations to another region

C. Align to business operations

D. Purchase breach insurance

Answer(s): D

---

8. An organization licenses and uses personal information for business operations, and a server containing that information has been compromised.
What kind of law would require notifying the owner or licensee of this incident?

A. Consumer right disclosure

B. Data breach disclosure

C. Special circumstance disclosure

D. Security incident disclosure

Answer(s): B

---

9. Why is it vitally important that senior management endorse a security policy?

A. So that employees will follow the policy directives.

B. So that they can be held legally accountable.

C. So that external bodies will recognize the organizations commitment to security.

D. So that they will accept ownership for security within the organization.

Answer(s): D

---

10. Which of the following is of MOST importance when security leaders of an organization are required to align security to influence the culture of an organization?

A. Understand the business goals of the organization

B. Poses a strong technical background

C. Poses a strong auditing background

D. Understand all regulations affecting the organization

Answer(s): A

---

11. The PRIMARY objective of security awareness is to:

A. Encourage security-conscious employee behavior

B. Put employees on notice in case follow-up action for noncompliance is necessary

C. Ensure that security policies are read

D. Meet legal and regulatory requirements

Answer(s): A

---

12. Which of the following is MOST likely to be discretionary?

A. Policies

B. Procedures

C. Guidelines

D. Standards

Answer(s): C

---

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

A. Complexity of organizational structure

B. Distance between physical locations

C. Organizational budget

D. Number of employees

Answer(s): A

---

14. When dealing with Security Incident Response procedures, which of the following steps come FIRST when reacting to an incident?

A. Eradication

B. Escalation

C. Containment

D. Recovery

Answer(s): C

15. What is the relationship between information protection and regulatory compliance?

A. That all information in an organization must be protected equally.

B. The information required to be protected by regulatory mandate does not have to be identified in the organizations data classification policy.

C. There is no relationship between the two.

D. That the protection of some information such as National ID information is mandated by regulation and other information such as trade secrets are protected based on business need.

Answer(s): D

---

16. Who in the organization determines access to information?

A. Compliance officer

B. Legal department

C. Data Owner

D. Information security officer

Answer(s): C

---

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

A. Compliance with local privacy regulations

B. An independent Governance, Risk and Compliance organization

C. Support Legal and HR teams

D. Alignment of security goals with business goals

Answer(s): D

---

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

A. Obtain senior level sponsorship

B. Conduct a workshop for all end users.

C. Conduct a risk assessment.

D. Prepare a security budget.

Answer(s): A

---

19. When an organization claims it is secure because it is PCI-DSS certified, what is a good first question to ask towards assessing the effectiveness of their security program?

A. How many credit records are stored?

B. What is the value of the assets at risk?

C. What is the scope of the certification?

D. How many servers do you have?

Answer(s): C

---

20. A security manager has created a risk program. Which of the following is a critical part of ensuring the program is successful?

A. Ensuring developers include risk control comments in code

B. Creating risk assessment templates based on specific threats

C. Providing a risk program governance structure

D. Allowing for the acceptance of risk for regulatory compliance requirements

Answer(s): C