DUMPSBOSS.COM

EC-Council Certified CISO (CCISO)

ECCouncil 712-50

Version Demo

Total Demo Questions: 20

Total Premium Questions: 458

Buy Premium PDF

https://dumpsboss.com

support@dumpsboss.com

QUESTION NO: 1

Which of the following can the company implement in order to avoid this type of security issue in the future?

A. Network based intrusion detection systems

B. An audit management process

C. A security training program for developers

D. A risk management process

ANSWER: C

QUESTION NO: 2

As a CISO you need to understand the steps that are used to perform an attack against a network.

Put each step into the correct order.

1.Covering tracks

2.Scanning and enumeration

3.Maintaining Access

4.Reconnaissance

5.Gaining Access

A. 4, 3, 5, 2, 1

B. 4, 2, 5, 3, 1

C. 2, 5, 3, 1, 4

D. 4, 5, 2, 3, 1

ANSWER: B

QUESTION NO: 3

How often should the SSAE16 report of your vendors be reviewed?

A. Quarterly

B. Semi-annually

C. Bi-annually

D. Annually

ANSWER: D

QUESTION NO: 4

As the CISO, you need to create an IT security strategy.

Which of the following is the MOST important thing to review before you start writing the plan?

A. The existing IT environment

B. Other corporate technology trends

C. The company business plan

D. The present IT budget

ANSWER: C

QUESTION NO: 5

Step-by-step procedures to regain normalcy in the event of a major earthquake is PRIMARILY covered by which of the following plans?

A. Damage control plan

B. Disaster recovery plan

C. Business Continuity plan

D. Incident response plan

ANSWER: B

QUESTION NO: 6

Which of the following best represents a calculation for Annual Loss Expectancy (ALE)?

A. Value of the asset multiplied by the loss expectancy

B. Replacement cost multiplied by the single loss expectancy

C. Single loss expectancy multiplied by the annual rate of occurrence

D. Total loss expectancy multiplied by the total loss frequency

ANSWER: C

QUESTION NO: 7

An information security department is required to remediate system vulnerabilities when they are discovered. Please select the three primary remediation methods that can be used on an affected system.

A. Install software patch, configuration adjustment, software removal

B. Install software patch, operate system, maintain system

C. Discover software, remove affected software, apply software patch

D. Software removal, install software patch, maintain system

ANSWER: A

QUESTION NO: 8

What is an approach to estimating the strengths and weaknesses of alternatives used to determine options, which provide the BEST approach to achieving benefits while preserving savings called?

A. Business Impact Analysis

B. Economic Impact analysis

C. Return on Investment

D. Cost-benefit analysis

ANSWER: D

Explanation:

Reference: https://artsandculture.google.com/entity/cost%E2%80%93benefit-analysis/m020w0x?hl=en

QUESTION NO: 9

Who in the organization determines access to information?

A. Compliance officer

B. Legal department

C. Data Owner

D. Information security officer

ANSWER: C

QUESTION NO: 10

A severe security threat has been detected on your corporate network. As CISO you quickly assemble key members of the Information Technology team and business operations to determine a modification to security controls in response to the threat.

This is an example of:

A. Change management

B. Thought leadership

C. Business continuity planning

D. Security Incident Response

ANSWER: D

QUESTION NO: 11

You work as a project manager for TYU project. You are planning for risk mitigation. You need to quickly identify high-level risks that will need a more in-depth analysis.

Which one of the following approaches would you use?

A. Risk mitigation

B. Estimate activity duration

C. Quantitative analysis

D. Qualitative analysis

ANSWER: D

QUESTION NO: 12

What is the MAIN reason for conflicts between Information Technology and Information Security programs?

A. The effective implementation of security controls can be viewed as an inhibitor to rapid Information technology implementations.

B. Technology Governance is focused on process risks whereas Security Governance is focused on business risk.

C. Technology governance defines technology policies and standards while security governance does not.

D. Security governance defines technology best practices and Information Technology governance does not.

ANSWER: A

QUESTION NO: 13

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: D

QUESTION NO: 14

Which of the following is the MOST logical method of deploying security controls within an organization?

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

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

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

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

ANSWER: B

QUESTION NO: 15

Who is responsible for verifying that audit directives are implemented?

A. IT Management

B. Internal Audit

C. IT Security

D. BOD Audit Committee

ANSWER: B

Explanation:

Reference: https://www.eccouncil.org/information-security-management/

QUESTION NO: 16

The main purpose of the SOC is:

A. An organization which provides Tier 1 support for technology issues and provides escalation when needed

B. A distributed organization which provides intelligence to governments and private sectors on cyber-criminal activities

C. The coordination of personnel, processes and technology to identify information security events and provide timely response and remediation

D. A device which consolidates event logs and provides real-time analysis of security alerts generated by applications and network hardware

ANSWER: C

Explanation:

Reference: https://www.eccouncil.org/what-is-soc/

QUESTION NO: 17

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: A

QUESTION NO: 18

Which of the following best summarizes the primary goal of a security program?

A. Provide security reporting to all levels of an organization

B. Manage risk within the organization

C. Create effective security awareness to employees

D. Assure regulatory compliance

ANSWER: B

QUESTION NO: 19

The mean time to patch, number of virus outbreaks prevented, and number of vulnerabilities mitigated are examples of what type of performance metrics?

A. Risk metrics

B. Operational metrics

C. Compliance metrics

D. Management metrics

ANSWER: B

QUESTION NO: 20

An organization's firewall technology needs replaced. A specific technology has been selected that is less costly than others and lacking in some important capabilities. The security officer has voiced concerns about sensitive data breaches but the decision is made to purchase.

What does this selection indicate?

A. A high threat environment

B. A low vulnerability environment

C. A high risk tolerance environment

D. A low risk tolerance environment

ANSWER: C