BRAINWARE UNIVERSITY

Term End Examination 2024-2025
Programme – B.Sc.(ANCS)-Hons-2023
Course Name – Information Security Management
Course Code - BNC30109
(Semester III)

Full Marks : 60 **Time : 2:30 Hours**

[The figure in the margin indicates full marks. Candidates are required to give their answers in their own words as far as practicable.]

Group-A
(Multiple Choice Type Question) 1 x 15=15

1. *Choose the correct alternative from the following :*

(i) Select the appropriate definition for information security governance.

a) A set of policies to manage data privacy
b) A framework to manage and protect information assets
c) A technology to encrypt sensitive data
d) A method to train employees on security protocols

(ii) Name the purpose of an information security management structure.

a) To design new software
b) To handle customer complaints
c) To oversee and implement security policies
d) To create marketing strategies

(iii) Find the term describes the organizational structures used to manage information security.

a) Hierarchy
b) Framework
c) Matrix
d) Network

(iv) Identify the purpose of a risk assessment checklist.

a) To ensure all potential risks are identified and evaluated consistently
b) To track employee performance
c) To develop marketing strategies
d) To enhance customer service

(v) When should a risk register be reviewed and updated?

a) Once every five years
b) Regularly and after significant changes
c) Only during audits
d) Never

(vi) Select the best practice in maintaining a relevant and effective risk register.

a) Regularly reviewing and updating the risks and mitigation measures
b) Limiting access to senior management only
c) Including only financial risks
d) Reviewing and updating annually

(vii) How can organizations identify resources required for control implementation?

a) Omit all non-technical resources from the assessment.
b) Consider human capital, information, infrastructure, and architecture.

c) Focus solely on the availability of security software.
d) Prioritize resources readily available within the IT department.

(viii) Choose how organizations can measure the effectiveness of security awareness training.

a) Focus solely on employee satisfaction with the training program
b) Rely solely on the number of security awareness training sessions conducted
c) Delegate measurement entirely to external security auditors
d) Conduct simulations or phishing tests to assess employee behavior

(ix) What factors should be considered when evaluating audit results?

a) Speed and efficiency of the audit process
b) Level of employee satisfaction with the audit process
c) Cost-effectiveness of the audit compared to the budget
d) Relevancy, accuracy, and perspective of the conclusions

(x) Identify the two MAIN types of IT audits.

a) Internal and external
b) Network and application
c) Financial and compliance
d) Formal and Informal

(xi) Identify the PRIMARY objective of IT audit follow-up activities.

a) To assign blame for identified security weaknesses.
b) To ensure that management implements recommended corrective actions.
c) To close out the IT audit project formally.
d) To conduct additional testing to validate the effectiveness of implemented controls.

(xii) Select the advantages of outsourcing IT audits to an external firm.

a) Lack of familiarity with the organization's specific IT environment.
b) Reduced cost of conducting IT audits compared to internal audit teams.
c) Access to a wider range of expertise and specialized skills.
d) Potential for bias or conflicts of interest due to internal relationships.

(xiii) Identify the challenges associated with using internal audit teams for IT audits.

a) Potential for lack of objectivity due to familiarity with the IT environment.
b) The high cost of hiring and training qualified internal audit staff.
c) The in-depth industry knowledge required for effective IT audits.
d) The limited access to specialized IT audit tools and resources.

(xiv) Identify the role of continuous monitoring in improving an organization's overall security posture.

a) Replacing the need for periodic IT audits altogether.
b) Providing a one-time assessment of the IT environment's security posture.
c) Enabling real-time detection and response to security threats and incidents.
d) Simplifying the process of conducting comprehensive IT audits.

(xv) Identify the PRIMARY objective of information security.

a) To ensure the smooth operation of IT systems.
b) To protect the confidentiality, integrity, and availability of information.
c) To minimize the cost of IT security controls.
d) To improve user experience with IT systems.

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Define an information security governance program and its key components (leadership, structures, processes). (3)
3. Explain the ROI in information security governance monitoring. (3)
4. Explain the importance of ISO 27000 in risk management and compliance. (3)
5. Write one metric and its corresponding KPI that can be used to measure the effectiveness of user access controls. (3)
6. Classify the best practices for deploying anti-virus software. (3)

OR

Explain the importance of security awareness training in mitigating social engineering attacks. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Define information security governance. (5)
8. Distinguish between risk assessment and risk management in the context of information security. (5)
9. Explain how to design information security controls that are aligned with the operational needs and goals of an organization. (5)
10. Estimate the benefits and limitations of a risk-based IT audit strategy. (5)
11. Summarize the importance of relevancy, accuracy, and perspective in audit management. (5)
12. Write about the risk management concept for selecting and implementing information security controls. (5)

OR

Write in detail about metrics and key performance indicators. (5)

****