BRAINWARE UNIVERSITY

Term End Examination 2023
Programme – M.Sc.(ANCS)-2022
Course Name – Cyber Risk Management
Course Code - MNCS204
(Semester II)

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) Compare the types of controls focused on stopping a security breach from occurring in the first place are termed _____

a) Containment b) Preventive
c) Detection d) Recovery

(ii) Estimate an audit log is an example of what type of control _____

a) Containment b) Preventive
c) Detection d) Recovery

(iii) To allocate resources and constructing cost-effective controls, organizations, after identifying all possible controls and evaluating their feasibility and effectiveness, should perform what form of additional analysis _____

a) Vulnerability analysis b) Cost-benefit analysis
c) Qualitative d) Quantitative

(iv) Define a policy for the physical component of the information technology infrastructure could work with all of the following except _____

a) Firewalls b) ID badges
c) Cameras d) Security guards

(v) Define the primary responsibility of the information security steering committee is _____

a) Direction setting and performance monitoring b) Information security policy development
c) Information security control implementation d) Provision of information security training for employees

(vi) Classify to ensure that an organization's password policy is effective, it must provide two key elements: difficult to guess; and _____

a) Be encrypted at all times
b) Contain a number of characters
c) Must be changed periodically
d) Controlled by security administration

(vii) Define the purpose of change control is to _____

a) Track changes to system hardware, software, firmware, and documentation.
b) Maintain visibility of changes to the system.
c) Ensure that changes to the system are approved.
d) To track and approve changes to system hardware, software, firmware, and documentation.

(viii) Ask the four deliverables from a risk assessment process are threats identified, controls selected, action plan complete, and _____

a) Risk level established
b) Technical issues quantified
c) Vulnerability assessment completed
d) Risk mitigation established

(ix) Compare a financial estimate designed to help consumers and enterprise managers assess direct and indirect costs related to the purchase of any capital investment, such as (but not limited to) computer software or hardware is termed _____

a) Return on investment
b) Return on security investment
c) Total value of asset compensation
d) Total cost of ownership

(x) Apply this recent piece of legislation requires annual affirmation of management's responsibility for internal controls over financial reporting. Management must attest to effectiveness based on an evaluation and the auditor must attest and report on management's evaluation _____

a) Foreign Corrupt Practices Act
b) Sarbanes–Oxley
c) Model Business Corporation Act
d) Gramm–Leach–Bliley Act

(xi) Define an annual report of the state of information security should be presented to the information security steering committee. This reporting requirement has been established in the current legislation and information security international standards. This report should not be confused with a standard feature audit performed by the audit staff nor is it part of some third-party certification process. Who is responsible for presenting this annual report _____

a) CISO
b) CTO
c) CEO
d) CFO

(xii) Apply any information security program must get its direction from executive management. The requirements of today's laws and regulations have identified either the organization's board of directors or what other body as responsible for instituting an effective program?

a) Information security steering committee
b) Business operations approval team
c) Crisis management team
d) Cyber incident response board

(xiii) Compare the group who is charged with the responsibility to "assess the adequacy of and compliance with management, operating, and financial controls, as well as the administrative and operational effectiveness of organizational units" is who _____

a) Information security
b) Auditing staff
c) Corporate council
d) Government and regulatory affairs

(xiv) In providing risk reporting to management, choose the most appropriate vehicle for the initial reporting of a major security incident would be to include it in a:

a) Quarterly report
b) Special report
c) Monthly report
d) Weekly report

(xv) Classify senior management depends on an effective risk analysis process to make informed business decisions. This management responsibility is called _____

a) Due diligence
b) Due proxy
c) Due date
d) DEW line

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Analyze the risk management process and identify its key components. (3)
3. Demonstrate the process of asset classification. (3)
4. Differentiate between inherent risk and control risk. (3)
5. How do network components interact with each other to form an IT system? (3)
6. Analyze the components of an IT asset management system, including asset identification, tracking, and disposal. (3)

OR

Develop an IT asset management plan for a small business that includes the identification, valuation, and classification of assets. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Illustrate how to perform a physical data gathering for a security risk assessment. (5)
8. Evaluate the advantages and disadvantages of using a quantitative risk analysis method versus a qualitative risk analysis method. (5)
9. Illustrate the process of identifying and assessing risks in IT systems. How does risk tolerance play a role in the process? (5)
10. Explain the level of risk in security risk assessment (5)
11. Analyze how can Disaster Recovery plans help ensure the continuity of critical business functions and processes? (5)
12. Analyze the various types of security risks that can affect an organization. (5)

OR

Analyze the different components of a risk management plan, and explain how they can be used to manage and mitigate risks within an organization. (5)

****