BRAINWARE UNIVERSITY

Term End Examination 2025-2026
Programme – B.Tech.(CSE)-DS-2022/B.Tech.(CSE)-DS-2023
Course Name – Information Security Analysis and Audit
Course Code - OEC-CSD601B
(Semester VI)

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) Where are security performance metrics commonly reported.
- a) Employee newsletters
- b) Executive dashboards
- c) Social media platforms
- d) Marketing brochures

(ii) Which phase of an information security audit involves evidence collection.
- a) Planning
- b) Execution
- c) Reporting
- d) Follow-up

(iii) Compare black-box and white-box testing methodologies.
- a) Black-box testing requires internal knowledge; white-box does not
- b) White-box testing involves full system knowledge; black-box does not
- c) Both require complete access to system code
- d) Neither is used in security audits

(iv) Summarize the role of compliance in security auditing.
- a) Ensures adherence to regulatory standards
- b) Increases employee satisfaction
- c) Reduces network latency
- d) Prevents software crashes

(v) Select the most effective logging system for security incident detection.
- a) A system that logs all events but lacks real-time monitoring
- b) A system with automated anomaly detection and alerting
- c) A system that only records login attempts
- d) A system with no logging capability

(vi) Apply security methodologies to a cloud computing environment by.
- a) Ignoring encryption since cloud providers handle security
- b) Implementing data encryption, access control, and continuous monitoring
- c) Allowing public access to sensitive files
- d) Avoiding regular security updates

(vii) How does a pre-audit checklist help in an information security audit?
- a) It ensures all audit steps are followed
- b) It replaces the need for vulnerability scanning
- c) It only focuses on firewall settings
- d) It helps in developing new security policies

(viii) Find the correct definition of an internal network security audit.

a) A security review of systems inside an organization's network
b) A test conducted only for cloud-based services
c) A process of blocking all incoming emails
d) A way to enhance physical security measures

(ix) Illustrate how vulnerability analysis is performed.

a) By identifying, classifying, and mitigating security weaknesses in a system
b) By installing more RAM in servers
c) By blocking all incoming network traffic
d) By disabling firewalls

(x) Classify different types of post-audit actions.

a) Corrective actions, Preventive measures, Continuous monitoring
b) Deleting reports, Ignoring vulnerabilities, Disabling security policies
c) Increasing social media presence, Buying new computers, Hiring developers
d) Reducing work hours, Extending deadlines, Removing employee access

(xi) Select the best approach to mitigate risks found in an external security audit.

a) Implement recommended security patches and policy changes
b) Ignore the audit results if there are no immediate issues
c) Disable antivirus programs to improve system speed
d) Share audit reports publicly without review

(xii) Apply firewall and IDS audit techniques to prevent unauthorized access.

a) Configure firewall rules based on security policies and analyze IDS alerts
b) Disable all security features to increase network speed
c) Allow all traffic to bypass security checks
d) Turn off IDS notifications to reduce workload

(xiii) Choose a type of Social Engineering attack.

a) Phishing
b) SQL Injection
c) DDoS Attack
d) Brute Force

(xiv) Explain the role of Threat Management.

a) Running antivirus programs
b) Only scanning for vulnerabilities
c) Ignoring minor threats
d) Identifying, analyzing, and mitigating threats

(xv) Solve a security issue caused by a Zero-Day Attack.

a) Apply the latest patches
b) Reset all passwords
c) Block all users
d) Disable antivirus

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Classify the different types of Information Security Audit methodologies. (3)
3. Explain the role of security audit reports in risk management. (3)
4. Find the purpose of a vulnerability assessment. (3)
5. Classify different types of security risks. (3)
6. Describe the importance of remediation in the vulnerability management process. (3)

OR

Describe the importance of configuration control policies in IT governance. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Compare manual and automated configuration management processes. (5)
8. Explain the importance of security log management in forensic investigations. (5)
9. Select an effective encryption method for cloud data security and justify why. (5)
10. Explain the role of vulnerability analysis in an information security audit. (5)
11. Choose the most effective security auditing technique for detecting insider threats and justify your choice. (5)

12. Suggest solutions to improve remediation strategies in vulnerability management. (5)

OR

Design a configuration management policy for securing cloud environments. (5)

****