

Dr. Babasaheb Ambedkar Open University
Term End Examination January-2026

Course	: MSCCS	Date	: 17/02/2026
Subject Code	: MSCCS-302	Time	: 03:00PM TO 05:15PM
Subject Name	: Information Security Assurance: Framework, Standards and Industry best practices	Duration	: 2.15 Hours
		Max. Marks	: 70

Section A

Answer the following (Attempt any three) (30)

1. Explain in great details about standard ISO/IEC 27001.
2. Write a short note on Sarbanes-Oxley Act(SOX).
3. What do you mean by security audit? Explain about it in details.
4. Describe in details about Open Web Application Security Project (OWASP).
5. Discuss in details about Business Continuity Planning.

Section B

Answer the following (Attempt any four) (20)

1. Discuss in brief about SANS Institute.
2. Give your suggestions on how to improve security posture of organization?
3. Write a note on Information Security Management System (ISMS) Internal Audit.
4. Discuss in brief about access control of information.
5. Explain in short about international standard (ISO/IEC 15408) for evaluating criteria for IT security.
6. What is a PLAN-DO-CHECK-DO (PDCA) Cycle ?

Section C

Part – A (Multiple Choice Questions) (10)

1. _____ flaws occur whenever an application takes un-trusted data and sends it to a web browser without proper validation and escaping.
A Failure to Restrict URL Access B XSS
C Insecure Direct Object D Cross Site Request Forgery
2. ISO _____ supersedes ISO/IEC 27001:2005, and is published by the ISO and the IEC under the joint ISO and IEC subcommittee.
A 27001:2013 B 27001:2022
C 27002 D None of them
3. _____ is a US government computer security standard used to accredit cryptographic modules.
A FISMA B HIPAA
C FIPS D GLBA
4. _____ standard provides guidelines for information security risk management.
A ISO/IEC 27001 B ISO/IEC 27010
C ISO/IEC 27002 D ISO/IEC 27005

- 5 A _____ audit is performed by an audit organization independent of the customer-supplier relationship and is free of any conflict of interest.
A First-party B Second-party
C Third-party D All of them
- 6 Data _____ means maintaining and assuring the accuracy and completeness of data over its entire life-cycle.
A Integrity B Availability
C Confidentiality D Repudiation
- 7 Generally computer security audits are performed by _____.
A Federal or State Regulators B Corporate Internal auditors
C External auditors and Consultants D All of them
- 8 Employees accessing office resources from home should be using _____.
A Static IP B VPN
C Firewall D Antivirus
- 9 Primary goal of Information Security Management System (ISMS) is to ensure the, _____ of the information in the organization.
A Confidentiality B Availability
C Integrity D All of them
- 10 Section _____ gave authorities the power of "interception or monitoring or decryption of any information through any computer resource".
A 66A B 69
C 302 D 340

Part – B (Do as Directed)

(10)

- 1 The Children's Online Privacy Protection Act of 1998 (COPPA) is a US federal law. True / False
- 2 ITIL stands for Information Technology International Library. True / False
- 3 A policy is a high level document that outlines specific requirements or rules that must be met. True / False
- 4 ISO 3166 is the International Standard for country codes and codes for their subdivisions. True / False
- 5 Proxy servers shows the true address of the client workstation and can also act as a firewall. True / False
- 6 Nuclear explosions and bio-terrorism are the example of man-made Disasters. True / False
- 7 A business continuity plan enables critical services or products to be continually delivered to clients. True / False
- 8 Full form of COBIT is Control Objectives for Information and related Technology. True / False
- 9 A security audit is a manual or systematic Examination of a system or application. True / False
- 10 Common Criteria (CC) is an international standard (ISO/IEC 15408) for certifying computer security software. True / False
