UNIVERSITI KUALA LUMPUR
MALAYSIAN INSTITUTE OF INFORMATION TECHNOLOGY

FINAL TEST
MARCH 2026 SEMESTER

COURSE CODE	:	IKB 42403 & IKB31503
COURSE NAME	:	INFORMATION SECURITY COMPLIANCE & INFORMATION SECURITY MANAGEMENT SYSTEM
PROGRAMME NAME (FOR MPU: PROGRAMME LEVEL)	:	BACHELOR OF INFORMATION TECHNOLOGY IN COMPUTER SYSTEM SECURITY
DATE	:	24 JUNE 2026
TIME	:	2.00 pm – 4.00 pm
DURATION	:	2 HOURS

INSTRUCTIONS TO CANDIDATES

1. Please CAREFULLY read the instructions given in the question paper.
2. This question paper has information printed on both sides of the paper.
3. This question paper consists of TWO (2) sections: Section A and Section B.
4. Answer ALL questions in Section A and Section B.
5. Please write your answers on the answer booklet provided.
6. Answer all questions in English language ONLY.
7. An excerpt of the ISO/IEC 27001:2022 Annex A control list is attached at the end of this question paper for reference.

THERE ARE 11 PAGES OF QUESTIONS, EXCLUDING THIS PAGE.

SECTION A (Total: 30 marks)

INSTRUCTION: Answer ALL questions.
Please answer in the OMR form provided.

1. _____ level breach of security could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
   A. Low
   B. Moderate
   C. Medium
   D. High

2. A social engineer gains access to your colleague's username and password through a phishing mail. Which security property has been compromised?
   A. Availability
   B. Confidentiality
   C. Integrity
   D. Authenticity

3. Which of the following is the **PRIMARY** role of the IS auditor in an organization's information classification process?
   A. Securing information assets in accordance with the classification assigned
   B. Validating that assets are protected according to assigned classification
   C. Ensuring classification levels align with regulatory guidelines
   D. Defining classification levels for information assets within the organization

4. Which of the following would be **MOST** effective to protect information assets in a data center from theft by a vendor?
   A. Conceal data devices and information labels.
   B. Issue an access card to the vendor.
   C. Monitor and restrict vendor activities.
   D. Restrict use of portable and wireless devices.

5. Which of the following issues associated with a data center's closed-circuit television (CCTV) surveillance cameras is of **MOST** concern to an IS auditor?
   A. CCTV recordings are not regularly reviewed.
   B. CCTV records are deleted after one year.
   C. CCTV footage is not recorded 24 x 7.
   D. CCTV cameras are not installed in break rooms.

6. Which of the following is the **GREATEST** risk if two users have concurrent access to the same database record?
   A. Entity integrity
   B. Availability integrity
   C. Referential integrity
   D. Data integrity

7. The Gray-box testing methodology enforces what kind of restriction?
   A. Only the external operation of a system is accessible to the tester.
   B. The internal operation of a system in only partly accessible to the tester.
   C. Only the internal operation of a system is known to the tester.
   D. The internal operation of a system is completely known to the tester.

8. A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?
   A. Perform a vulnerability scan of the system.
   B. Determine the impact of enabling the audit feature.
   C. Perform a cost/benefit analysis of the audit feature.
   D. Allocate funds for staffing of audit log review.

9. What are the limitations of vulnerability scanners?
   A. There are often better at detecting well-known vulnerabilities than more esoteric ones
   B. The scanning speed of their scanners are extremely high
   C. The more vulnerabilities detected; the more tests required
   D. They are expensive and require per host scan license

10. Which of the following type of scanning utilizes automated process of proactively identifying vulnerabilities of the computing systems present on a network?
    A. Port Scanning
    B. Single Scanning
    C. External Scanning
    D. Vulnerability Scanning

11. We can acquire and supply information in several ways. The value of the information depends on its reliability. What factors determine the reliability of information?
    A. Availability, Information Value and Confidentiality
    B. Availability, Integrity, and Confidentiality
    C. Availability, Integrity, and Completeness
    D. Timeliness, Accuracy and Completeness

12. What does ISO/IEC 27001:2022 primarily focus on?
    A. Quality management
    B. Information security management
    C. Environmental management
    D. Occupational health and safety management

13. Which of the following is **NOT** a key component of an Information Security Management System (ISMS) according to ISO/IEC 27001:2022?
    A. Risk assessment
    B. Asset management
    C. Human resource management
    D. Incident management

14. How does ISO/IEC 27001:2022 define information security?
    A. The preservation of confidentiality, integrity, and availability of information
    B. The protection of personal data
    C. The prevention of cyber attacks
    D. The compliance with local laws and regulations

15. Which of the following is a requirement for an ISMS to be certified against ISO/IEC 27001:2022?

    A. Completion of a self-assessment questionnaire
    B. Approval from the local government
    C. External audit by a certification body
    D. Implementation of all ISO/IEC 27001 controls

16. What is the purpose of the risk treatment process in ISO/IEC 27001:2022?

    A. To eliminate all risks
    B. To accept all risks
    C. To reduce risks to an acceptable level
    D. To transfer all risks to third parties

17. Which of the following is **NOT** one of the main sections of ISO/IEC 27001:2022?

    A. Context of the organization
    B. Leadership
    C. Operational planning and control
    D. Improvement

18. You work in the IT department of a medium-sized company. Confidential information has got into the wrong hands several times. This has damaged the company's image. You have been asked to propose organizational security measures for laptops at your company. What is the first step that you should take?

    A. Formulate a policy regarding mobile media (PDAs, laptops, smartphones, USB sticks)
    B. Appoint security personnel
    C. Encrypt the hard drives of laptops and USB sticks
    D. Set up an access control policy

19. The Open Source Security Testing Methodology Manual (OSTMM) is a framework and guide for performing security testing and assessments of IT systems. It focuses on:
    A. specific tools or technologies used in security testing.
    B. methodology and techniques used in security testing.
    C. non-risk driven assessment approach.
    D. lesser comprehensive methodology for conducting security testing and assessments.

20. During an ISMS audit, the auditor discovers that management has not defined information security objectives or allocated resources for implementation. Which clause is **MOST** likely non-compliant?
    A. Clause 5 – Leadership
    B. Clause 8 – Operation
    C. Clause 9 – Performance Evaluation
    D. Clause 10 – Improvement

21. Audit evidence must be:
    A. Verifiable
    B. Based on assumptions
    C. Informal
    D. Confidential only

Question 22 -24 refer to scenario 1

Scenario 1 : CyberTech Innovators Sdn Bhd is a cybersecurity company offering managed services, including threat monitoring, vulnerability scanning, and security advisory. The company recently migrated its internal HR and finance systems to a cloud platform.During an internal audit, the following issues were identified:

- Some cloud services had not been included in the last risk assessment.
- Several laptops used by consultants lacked full disk encryption.
- Remote work policy is implemented, but users sometimes use personal devices to access corporate emails.
- Logs of past vulnerability scans were stored on a shared drive without proper access restrictions.
- The IT team has no formal method to evaluate and treat newly discovered risks.

22. Which of the following best describes a key weakness in CyberTech's risk assessment process?
    A. Use of cloud services
    B. Lack of asset inventory
    C. Exclusion of cloud systems in the risk register
    D. Use of shared drives

23. What risk is introduced when personal devices are used to access corporate email without proper controls?
    A. Reduced productivity
    B. Compliance with GDPR
    C. Data leakage or unauthorized access.
    D. Longer incident response times

24. Which of the following is a suitable control to reduce the risk of sensitive audit logs being accessed improperly?
    A. Move logs to a cloud server
    B. Encrypt log files using shared keys
    C. Restrict access using ACLs and role-based controls
    D. Delete old logs regularly

25. Full disk encryption on laptops would reduce the risk of which of the following?
    A. Malware from phishing
    B. Loss of data during internet transfer
    C. Data breach from stolen or lost devices
    D. Insecure cloud login

26. A hospital introduces cloud-based patient record systems. Before selecting security controls, the organization first identifies threats, vulnerabilities, and potential impacts. This activity is part of:
    A. Leadership
    B. Risk Assessment and Treatment
    C. Improvement
    D. Communication

27. What is the purpose of the post-exploitation phase in a penetration test?
    A. To gather information about the target system
    B. To exploit identified vulnerabilities
    C. To maintain access and extract valuable data
    D. To document the findings and provide recommendations

28. Which penetration testing methodology is specifically designed to test the security of web applications?
    A. OSSTMM
    B. NIST SP 800-115
    C. OWASP Testing Guide
    D. ITIL

29. What is a non-conformity in the context of an ISMS audit?
    A. A situation where an organization's practices fully align with its security policies
    B. A minor issue that does not affect the ISMS
    C. A deviation from the requirements of the ISO 27001 standard
    D. An employee's performance review

30. Which phase of the ISMS audit involves the verification of corrective actions taken by the organization?
    A. Planning phase
    B. Fieldwork phase
    C. Reporting phase
    D. Follow-up phase

SECTION B (Total: 50 marks)

INSTRUCTION: Answer ALL questions.

Please use the answer booklet provided.

Question 1

Refer to following case study

Case Study: Bersatu Jaya Sdn Bhd (BJSB)

Bersatu Jaya Sdn Bhd (BJSB) is a mid-sized Malaysian fintech company based in Kuala Lumpur. The company provides a digital payment platform and micro-lending services to SMEs and individual users. Its platform integrates with local banks, e-wallet providers, and third-party credit scoring APIs. Over the past year, BJSB has experienced rapid growth, expanding its services across Southeast Asia. However, several critical issues have recently emerged:

Recent Developments

A major management restructuring took place, including the replacement of the Chief Information Security Officer (CISO) and several senior IT managers. The company suffered a data loss incident, where customer transaction records were accidentally deleted during a cloud migration. Although partial recovery was possible, some records were permanently lost. BJSB has increasingly relied on third-party vendors, including cloud hosting providers and external developers, to accelerate product delivery. Due to competitive pressure, the company is planning to launch a new AI-based credit scoring feature within the next 3 months. An internal audit revealed that security policies exist but are inconsistently enforced across departments.

Operational Situation:

Customer data handled includes:

- Personally Identifiable Information (PII)
- Financial transaction data
- Credit scoring data

The company must comply with Malaysian regulations such as Personal Data Protection Act 2010 and financial guidelines from Bank Negara Malaysia. Employees work in a hybrid environment, with remote access to internal systems via VPN.

Development teams follow agile practices, often prioritizing speed over documentation and formal security checks.

Senior management is concerned that:

1) Information security risks are increasing faster than controls
2) There is a lack of alignment between business strategy and security practices
3) External threats (e.g., cyberattacks, fraud) are becoming more sophisticated
4) Internal awareness of security responsibilities is inconsistent

Questions below will be based on the case study above.

a) State **TWO (2)** internal issues and **TWO (2)** external issues that may affect the implementation of ISMS in BJSB.

(4 Marks)

b) Bersatu Jaya Sdn Bhd (BJSB) recently experienced rapid expansion, cloud migration activities, inconsistent security policy enforcement, and increased dependency on third-party vendors. As part of the ISMS implementation team, you are required to perform an information security risk assessment based on ISO/IEC 27001:2022 Clause 6.1.2.

Use the following scale:

- **Likelihood:** Low (1), Medium (2), High (3)
- **Impact:** Low (1), Medium (2), High (3)
- **Risk Level = Likelihood × Impact**

Complete the following risk assessment table:

i. Identify **THREE (3)** main critical assets. (1.5 marks)
ii. Identify suitable threats and vulnerabilities for each assets. (3 marks)
iii. Assign likelihood and impact ratings. (1.5 marks)
iv. Determine the overall risk score and risk level. (1 mark)
v. Recommend an appropriate risk treatment option. (3 marks)

c) Suggest and explain why **THREE (3)** appropriate ISO/IEC 27001:2022 Annex A controls that can reduce the risk of data loss during cloud migration. Use the Annex A control list provided.

(6 marks)

d) Bersatu Jaya Sdn. Bhd. is considering implementing an Information Security Management System (ISMS) based on ISO/IEC 27001:2022. List **FIVE (5)** benefits the organization may achieve from obtaining ISO/IEC 27001:2022 certification.

(5 marks)

(Total: 25 marks)

Question 2

Refer to following case study

Case Study: MedCare Specialist Clinic Sdn. Bhd.

MedCare Specialist Clinic Sdn. Bhd. is a private healthcare provider located in Kuala Lumpur, Malaysia. The clinic recently introduced an online patient portal that allows patients to:

- Book medical appointments
- View laboratory results
- Download medical reports
- Make online payments
- Communicate with doctors through an online messaging system

The web application is hosted on a cloud server and developed by a third-party software vendor. Due to limited cybersecurity budget and pressure to launch the system quickly, the clinic did not conduct a full penetration test before deployment.

Recently, several suspicious activities were detected:

1. Patients reported being logged into other users' accounts after login.
2. The IT administrator discovered unusual SQL queries in the web server logs.
3. A vulnerability scan identified:
    - Open port 3306 (MySQL database service exposed to the Internet)
    - Weak administrator password
    - Outdated Apache web server version
4. Security monitoring also revealed repeated failed login attempts from foreign IP addresses.
5. During testing, a security consultant successfully injected the following payload into the login form: `' OR '1'='1`

The consultant was able to bypass authentication and access patient records. The clinic management is concerned because the system stores: Patient Personally Identifiable Information (PII), Medical records , Payment information, Staff credentials

The organization must also comply with Personal Data Protection Act (PDPA) 2010 AND Malaysian healthcare data privacy requirements

The clinic has now hired a cybersecurity team to perform Vulnerability Assessment and Penetration Testing (VAPT) to identify weaknesses and recommend mitigation strategies.

Questions below will based on the case study above.

a) Analyze **FOUR (4)** vulnerabilities identified in the MedCare Specialist Clinic case study and explain the potential impact of each vulnerability on the organization's information assets.

(10 Marks)

b) Discuss **TWO (2)** objectives of conducting penetration testing and explain how each objective helps protect the clinic's sensitive healthcare information.

(8 Marks)

c) During a penetration test, a security consultant gained unauthorized access to the MedCare Clinic system through the login form. Identify the attack used and explain the underlying vulnerability that made the attack possible.

(5 Marks)

d) List **TWO (2)** strategic recommendations that MedCare Specialist Clinic should adopt to improve its cybersecurity resilience and protect its critical information assets.

(2 Marks)

(Total: 25 marks)

END OF EXAMINATION PAPER

Annex A Controls List

A.5 Organizational Controls (37 Controls)

Control No.	Control Name
5.1	Policies for information security
5.2	Information security roles and responsibilities
5.3	Segregation of duties
5.4	Management responsibilities
5.5	Contact with authorities
5.6	Contact with special interest groups
5.7	Threat intelligence
5.8	Information security in project management
5.9	Inventory of information and other associated assets
5.10	Acceptable use of information and other associated assets
5.11	Return of assets
5.12	Classification of information
5.13	Labelling of information
5.14	Information transfer
5.15	Access control
5.16	Identity management
5.17	Authentication information
5.18	Access rights
5.19	Information security in supplier relationships
5.20	Addressing information security within supplier agreements
5.21	Managing information security in the ICT supply chain
5.22	Monitoring, review and change management of supplier services
5.23	Information security for use of cloud services
5.24	Information security incident management planning and preparation
5.25	Assessment and decision on information security events
5.26	Response to information security incidents
5.27	Learning from information security incidents
5.28	Collection of evidence
5.29	Information security during disruption
5.30	ICT readiness for business continuity
5.31	Legal, statutory, regulatory and contractual requirements

Control No.	Control Name
5.32	Intellectual property rights
5.33	Protection of records
5.34	Privacy and protection of PII
5.35	Independent review of information security
5.36	Compliance with policies, rules and standards for information security
5.37	Documented operating procedures

A.6 People Controls (8 Controls)

Control No.	Control Name
6.1	Screening
6.2	Terms and conditions of employment
6.3	Information security awareness, education and training
6.4	Disciplinary process
6.5	Responsibilities after termination or change of employment
6.6	Confidentiality or non-disclosure agreements
6.7	Remote working
6.8	Information security event reporting

A.7 Physical Controls (14 Controls)

Control No.	Control Name
7.1	Physical security perimeters
7.2	Physical entry
7.3	Securing offices, rooms and facilities
7.4	Physical security monitoring
7.5	Protecting against physical and environmental threats
7.6	Working in secure areas
7.7	Clear desk and clear screen
7.8	Equipment siting and protection
7.9	Security of assets off-premises
7.10	Storage media
7.11	Supporting utilities
7.12	Cabling security
7.13	Equipment maintenance
7.14	Secure disposal or re-use of equipment

A.8 Technological Controls (34 Controls)

Control No.	Control Name
8.1	User endpoint devices
8.2	Privileged access rights
8.3	Information access restriction
8.4	Access to source code
8.5	Secure authentication
8.6	Capacity management
8.7	Protection against malware
8.8	Management of technical vulnerabilities
8.9	Configuration management
8.10	Information deletion
8.11	Data masking
8.12	Data leakage prevention
8.13	Information backup
8.14	Redundancy of information processing facilities
8.15	Logging
8.16	Monitoring activities
8.17	Clock synchronization
8.18	Use of privileged utility programs
8.19	Installation of software on operational systems
8.20	Networks security
8.21	Security of network services
8.22	Segregation of networks
8.23	Web filtering
8.24	Use of cryptography
8.25	Secure development life cycle
8.26	Application security requirements
8.27	Secure system architecture and engineering principles
8.28	Secure coding
8.29	Security testing in development and acceptance
8.30	Outsourced development
8.31	Separation of development, test and production environments
8.32	Change management
8.33	Test information
8.34	Protection of information systems during audit testing