Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER II
SESSION 2022/2023

COURSE NAME	:	INFORMATION SECURITY STANDARDS
COURSE CODE	:	BIS 33203
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	JULY / AUGUST 2023
DURATION	:	3 HOURS
INSTRUCTION	:	1. ANSWER **ALL** QUESTIONS. 2. THIS FINAL EXAMINATION IS CONDUCTED VIA **CLOSED BOOK.** 3. STUDENTS ARE **PROHIBITED** TO CONSULT THEIR OWN MATERIAL OR ANY EXTERNAL RESOURCES DURING THE EXAMINATION CONDUCTED VIA CLOSED BOOK.

THIS QUESTION PAPER CONSISTS OF **ELEVEN (11)** PAGES

TERBUKA

SECTION A
Choose the **BEST** answer for each of the following questions.

Q1 Recovery point objective is _____.

A. maximum period of data loss from onset of disaster counting backwards
B. maximum period of data loss from onset of disaster counting forwards
C. time period from disaster onset to resumption of business process
D. time period from disaster onset to responding of the cybersecurity event

(1 mark)

Q2 Based on **Figure Q2**:

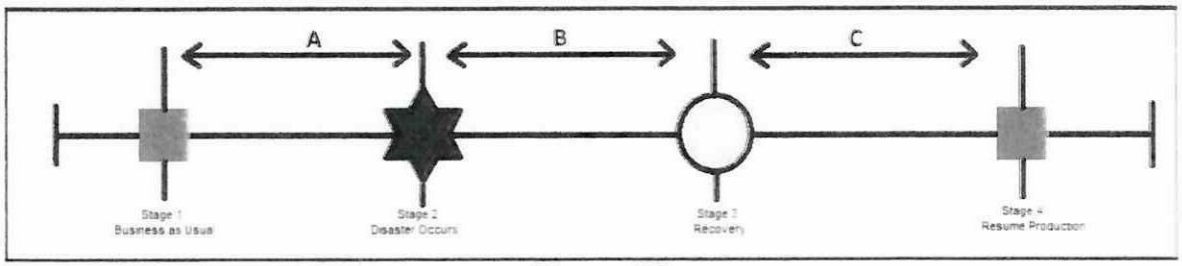

Figure Q2

Choose the **CORRECT** key recovery targets.

A. A=Recovery Time Objective (RTO); B=Recovery Point Objective (RPO); C=Work Recovery Time (WRT).
B. A=Work Recovery Time (WRT); B=Recovery Point Objective (RPO); C=Recovery Time Objective (RTO).
C. A=Recovery Point Objective (RPO); B=Work Recovery Time (WRT); C=Recovery Time Objective (RTO).
D. A=Recovery Point Objective (RPO); B=Recovery Time Objective (RTO); C=Work Recovery Time (WRT).

(1 mark)

Q3 Maximum tolerable downtime is the sum of _____.

A. Recovery Time Objective and Recovery Point Objective
B. Recovery Time Objective and Work Recovery Time
C. Recovery Point Objective and Work Recovery Time
D. Recovery Time Objective and Backup Time Objective

(1 mark)

TERBUKA

Q4 What is the name given to mandatory elements regarding the implementation of a policy?

A. Standards.
B. Guidelines.
C. Regulations.
D. Procedures.

(1 mark)

Q5 _____ are the step-by-step instructions on how to implement policies in the organization.

A. Standards
B. Guidelines
C. Regulations
D. Procedures

(1 mark)

Q6 Which step of the policy lifecycle does the training of users take place?

A. Plan for security.
B. Implement the plans.
C. Monitor the implementation.
D. Evaluate for effectiveness.

(1 mark)

Q7 _____ is the type of users with the responsibility of maintaining a system within its defined requirements.

A. System owner
B. System administrator
C. Privileged user
D. Executive user

(1 mark)

TERBUKA

Q8 _____ is a type of user that has more authority to do a wider range of tasks, but short of full administrative.

A. System owner
B. Executive user
C. Privileged user
D. System administrator

(1 mark)

Q9 Which of the following is **NOT** the benefit of using the ISO 27001-based security controls framework in an organization?

A. Supplemental guidance.
B. Availability of crosswalks.
C. Local accepted standard.
D. Industry accepted standard.

(1 mark)

Q10 _____ is the International Organization for Standardization (ISO) 27001 control that describes information security responsibilities.

A. Human resource security
B. Operations security
C. Asset management
D. Supplier relationship

(1 mark)

Q11 COBIT is _____.

A. Control Objectives for Information and Technology
B. Control Organizations for Business and Information Technology
C. Control Objectives for Information and Related Technology
D. Control Objectives for Business and Information Technology

(1 mark)

TERBUKA

Q12 Select the **CORRECT** orders of the COBIT domains.

I. Plan and organize.
II. Deliver and support.
III. Monitor and evaluate.
IV. Acquire and implement.

A. IV, I, III, II
B. I, IV, III, II
C. IV, I, II, III
D. I, IV, II, III

(1 mark)

Q13 Which of the following is the COBIT process for Acquire and Implement domain?

A. Determine technological directions.
B. Install and accredit solutions and changes.
C. Manage service desk and incidents.
D. Ensure compliance with external requirements.

(1 mark)

Q14 Which of the following is **NOT** the technology intrusion ethical dilemma?

A. Employee monitoring.
B. Computer surveillance.
C. Privacy internal to the firm.
D. Ergonomics and human factors.

(1 mark)

Q15 Which of the following is **NOT** the cybercrime using computer as storage devices?

A. Using a laptop to store stolen password files.
B. Using a WhatsApp application to spread scam messages.
C. Using a cloud storage account to share cracked software.
D. Using a smartphone memory to keep pornographic images files.

(1 mark)

TERBUKA

Q16 Which of the following is **NOT** the benefit of Codes of Conduct?

A. A code can be educational.
B. A code can be a means of deterrence and discipline.
C. A code can disrupt the profession's public image.
D. A code can be a positive stimulus for ethical conduct.

(1 mark)

Q17 Which of the following ISO standard refers to Common Criteria?

A. ISO/IEC 27001.
B. ISO/IEC 15408.
C. ISO/IEC 27043.
D. ISO/IEC 27035.

(1 mark)

Q18 In Common Criteria (CC), _____ is the specific product or system that is being evaluated.

A. Security Target
B. Protection Profile
C. Target of Evaluation
D. Evaluation Assurance Level

(1 mark)

Q19 In Common Criteria (CC), _____ is the specific functional and assurance requirements.

A. Protection Profile
B. Security Target
C. Target of Evaluation
D. Evaluation Assurance Level

(1 mark)

TERBUKA

Q20 Evaluation Assurance Level (EAL) _____ refers to a security product that is semi formally verified, designed, and tested.

A. 6
B. 5
C. 4
D. 3

(1 mark)

SECTION B

Q21 Your team is consulting RapidKL Light Right Transit (LRT) Operational Division to prepare information security policy and best practices to their Internet of Things (IoT) transportation devices. The value of threats probability and impact level are 1 for Minor, 2 for Medium, and 3 for Major. **Table Q21** presents the initial assessment of the IoT devices. Your team proposes to use the ISO/IEC 27001:2013 framework to guide the development of RapidKL Information Security Policy.

Table Q21

No.	Threats to the IoT devices	Probability	Impact
1	Password attack	3	3
2	Human error	1	3
3	Malicious insider	1	3
4	Malfunction device	2	2
5	Outdated devices	2	3

Based on the scenario, answer the following questions:

(a) (i) Illustrate a risk evaluation map based on **Table Q21** with acceptable risk level is 1.5.

(7 marks)

(ii) List **THREE (3)** threats in the unacceptable risk area based on your answer in **Q21(a)(i)**.

(3 marks)

(iii) Propose a Statement of Applicability for unacceptable risks in **Q21(a)(ii)** by referring to the ISO 27001 Annex A Controls in Appendix A.

(10 marks)

TERBUKA

(b) (i) Describe **ONE (1)** encryption protocol to protect data in-transit for RapidKL IoT transportation devices.

(4 marks)

(ii) Would you encourage RapidKL to use the same key in **Q21(b)(i)** digital signatures?

(1 mark)

(iii) Discuss your answer in **Q21(b)(ii)** based on the National Institute Standard and Technology (NIST) Recommendation for Key Management - Part 1: General.

(5 marks)

Q22 Based on **Figure Q22**:

```
Case 1: A scammer used a Dell laptop to conduct social
engineering attacks to Malaysia's Shopee customers. The laptop
was used to store victims' personal information and to distribute
phishing emails. The illicit acts took place at unit 3-9,
Condominium ABC, Jalan Cyber, Cyberjaya, Selangor.

Case 2: A Malaysian student in Melbourne, Australia was arrested
by Australia Federal Office for possessing pornographic images.
The suspect stored pornography materials on XX cloud storage
application. The XX cloud data center is in Malaysia.

Case 3: A Malaysian, who resides in Singapore, was found guilty
of possessing and distributing child pornography materials to
his Singaporean colleagues. The materials were stored in Google
Drive. Google's data centers are in the United States, China,
and Singapore.
```

Figure Q22

(a) (i) Identify the types of cybercrime for each of the cases in **Figure Q22**.

(3 marks)

(ii) Discuss your answer in **Q22(a)(i)**.

(6 marks)

(b) Justify if the Territorial Scope of Malaysia Computer Crime Act 1997 is applicable for each of the case in **Figure Q22**.

(15 marks)

TERBUKA

Q23 (a) Discuss the differences between product-oriented and process-oriented product evaluation.

(5 marks)

(b) Discuss the structure of an effective evaluation process, and provide **ONE (1)** example for each of the following:

(i) Functionality

(3 marks)

(ii) Effectiveness

(3 marks)

(iii) Assurance

(3 marks)

(c) (i) List **FOUR (4)** purposes of security evaluations based on the Trusted Computer System Evaluation Criteria (Orange Book).

(4 marks)

(ii) Discuss each of the security evaluations in **Q23(c)(i)**.

(8 marks)

- END OF QUESTIONS -

TERBUKA

FINAL EXAMINATION
APPENDIX A

SEMESTER / SESSION : SEM II 2022/2023
COURSE NAME : INFORMATION SECURITY STANDARDS
PROGRAMME CODE : BIS
COURSE CODE : BIS 33203

NO	ISO 27001 CONTROL	FRAMEWORK POLICY
A5	Information security policies	Information security policy set [A.5.1.1]
A6	Information security organization	Information security responsibilities [A.6.1.1] Mobile device security policy [A.6.2.1] Telework security policy [A.6.2.2]
A7	Human resource security	Employee and contractor security responsibility agreements [A.7.1.1] Disciplinary process [A.7.2.3] Termination process [A.7.3.1]
A8	Asset management	Asset inventory [A.8.1.1] Acceptable use of assets [A.8.1.3] Classification labeling procedures [A.8.2.2] Asset handling procedures [A.8.2.3] Removable media management procedures [A.8.3.1] Media disposal procedures [A.8.3.2]
A9	Access control	Access control policy [A.9.1.1] User registration process [A.9.2.1] User access provisioning process [A.9.2.2] Authentication information management process [A.9.2.4] Secure login procedure [A.9.4.2]
A10	Cryptography	Cryptographic controls policy [A.10.1.1] Key management policy [A.10.1.2]
A11	Physical security	Physical security perimeter diagrams [A.11.1.1] Physical office security designs [A.11.1.3] Natural disaster protection designs [A.11.1.4] Secure working area procedures [A.11.1.5] Clear desk policy [A.11.2.9]
A12	Operations security	Operating procedures [A.12.1.1] Backup policy [A.12.3.1] Software installation procedures [A.12.5.1] User software installation rules [A.12.6.2] System audit policy [A.12.7.1]
A13	Communications security	Network service security requirements [A.13.1.2] Information transfer policy and procedures [A.13.2.2] Secure transfer agreements [A.13.2.2] Nondisclosure agreements [A.13.2.4]

TERBUKA

FINAL EXAMINATION
APPENDIX A

SEMESTER / SESSION : SEM II 2022/2023
COURSE NAME : INFORMATION SECURITY STANDARDS
PROGRAMME CODE : BIS
COURSE CODE : BIS 33203

NO	ISO 27001 CONTROL	FRAMEWORK POLICY
A14	System acquisition, development, and maintenance	Information security requirements specification [A.14.1.1] Secure coding rules [A.14.2.1] Change control procedures [A. 14.2.2] Secure system engineering principles [A.14.2.5] System acceptance testing program and criteria [A.14.2.9]
A15	Supplier relationship	Supplier information security requirements [A.15.1.1]
A16	Information security incident management	Incident management responsibilities [A.16.1.1] Incident management procedures [A.16.1.1] Evidence collection procedures [A.16.1.7]
A17	Business continuity management	Business continuity requirements [A.17.1.1] Business continuity processes and procedures [A.17.1.2]
A18	Compliance	Applicable regulations and requirements [A.18.1.1] Compliance procedures [A.18.1.2]

TERBUKA