



UNIVERSITI TEKNIKAL MALAYSIA MELAKA
PEPERIKSAAN AKHIR SEMESTER I
FINAL EXAMINATION SEMESTER I
SESI 2021/2022
SESSION 2021/2022
FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

KOD KURSUS <i>COURSE CODE</i>	:	BITS 3523 <i>BITS 3523</i>
KURSUS <i>COURSE</i>	:	AUDIT KOMPUTER & PENGURUSAN RISIKO <i>COMPUTER AUDIT & RISK MANAGEMENT</i>
PENYELARAS <i>COORDINATOR</i>	:	DR. WARUSIA MOHAMED YASSIN
PROGRAM <i>PROGRAMME</i>	:	3 BITZ <i>3 BITZ</i>
MASA <i>TIME</i>	:	09.00 AM – 11.00 AM <i>09.00 AM – 11.00 AM</i>
TEMPOH <i>DURATION</i>	:	2 JAM <i>2 HOURS</i>
TARIKH <i>DATE</i>	:	27 JAN 2022 <i>27 JAN 2022</i>
TEMPAT <i>VENUE</i>	:	HALL 5 <i>HALL 5</i>

ARAHAN KEPADA CALON
INSTRUCTION TO CANDIDATES

1. Kertas soalan ini mengandungi TIGA (3) Soalan.
This exam paper contains THREE (3) Questions.
2. Sila jawab SEMUA soalan.
Please answer ALL questions.
3. Kertas soalan ini mempunyai 2 versi bahasa. Versi Bahasa Melayu bermula daripada muka surat 2 hingga 6 manakala versi Bahasa Inggeris bermula daripada muka surat 7 hingga 11. Sila jawab di dalam satu versi sahaja.
This exam paper has 2 versions. Malay version starts from page 2 to 6 while English version starts from page 7 to 11. Answer in one version only.

**KERTAS SOALAN INI TERDIRI DARIPADA (11) MUKA SURAT SAHAJA TERMASUK
MUKA SURAT HADAPAN**
THIS QUESTION PAPER CONTAINS (11) PRINTED PAGES INCLUSIVE OF FRONT PAGE

SOALAN 1 (50 MARKAH)

The diagram illustrates a DMZ configuration for a university network. It shows the following components and connections:

- External Network:** Includes a **Student** and a **Staff** user, each with a computer, connected to the **INTERNET** (represented by a cloud).
- Internal Network:** Includes a **CAMPUS NETWORK** with a switch and a **Staff** user with a computer.
- DMZ (Application & Database):** A central area containing three server icons.
- Firewalls:** Two **FIREWALL** units are positioned on either side of the DMZ.
- Web Servers:** Two **WEB SERVER** units are located at the bottom, each connected to a **Firewall** and the **DMZ**.
- IPS (Intrusion Prevention System):** Two **IPS** units are located at the bottom, each connected to a **Web Server** and the **DMZ**.
- IDS (Intrusion Detection System):** Two **IDS** units are located above the DMZ, each connected to the **INTERNET** and the **DMZ**.

The diagram shows the flow of traffic from the Internet through the IDS and Firewall to the Web Servers and IPS, and then to the DMZ. The DMZ is also connected to the Campus Network.

-2-

- a) Sebagai juruaudit dalaman, kenal pasti **TIGA(3)** jenis kawalan prinsip yang diperlukan di infrastruktur rangkaian sistem maklumat MyUniversity.

(3 markah)

- b) Tentukan **TIGA(3)** fungsi kawalan dan berikan **DUA(2)** contoh untuk **SETIAP** fungsi kawalan yang boleh dipertimbangkan ke atas infrastruktur rangkaian sistem maklumat MyUniversity.

(9 markah)

- c) Jika anda juruaudit luar bagi sistem maklumat MyUniversity, nyatakan **LIMA(5)** kawalan keselamatan kritikal yang anda boleh temui.

(5 markah)

- d) Nyatakan **LAPAN(8)** rasional mengapa kawalan keselamatan kritikal yang dikenalpasti dalam soalan (c) adalah penting.

(8 markah)

- e) Berikan formula *Cost Benefit Analysis (CBA)*, *Annualized Loss Expectancy (ALE)* dan *Single Loss Expectancy (SLE)*.

(6 markah)

- f) Sistem e-mel MyUniversity boleh mengalami kerosakan akibat serangan siber dan boleh menyebabkan kerugian besar. Faktor pendedahan untuk kerosakan sistem e-mel adalah berjumlah 30% dan dianggarkan bernilai RM5,000,000. Kirakan *Single Loss Expectancy (SLE)*, *Annualized Rate of Occurrence (ARO)* dan *Annualized Loss Expectancy (ALE)* jika serangan siber dijangka berlaku sekali pada setiap tahun.

(9 markah)

- g) Andaikan anggaran kos untuk satu serangan *phishing* yang berjaya terhadap sistem e-mel MyUniversity adalah sebanyak RM10,000. Sistem e-mel ini dijangka akan dijangkiti oleh aktiviti *phishing* sebanyak 6 kali setahun. Pengurangan kebarangkalian berlakunya risiko jika kawalan dilaksanakan diandaikan pada 75%. Di samping itu, kos untuk melatih pekerja dan mengelak dari serangan e-mel *phishing* adalah sebanyak RM20,000. Kirakan *Return of Investment (ROI)* dan tentukan berapa banyak pihak universiti dapat jimat setiap tahun dengan mengadakan latihan kesedaran kepada pekerjanya.

(10 markah)

SOALAN 2 (25 MARKAH)

- a) Berikan definisi bagi terma-terma berikut:

- i. Audit Keselamatan Aplikasi
- ii. Risiko Aplikasi
- iii. Pengagregatan Risiko
- iv. Pemindahan Risiko
- v. Pengauditan Teknologi Maklumat

(10 markah)

- b) Tentukan jenis aset yang betul untuk setiap aset di Rajah 1.

Jadual 1: Senarai Aset

Asset	Jenis Asset
<i>Laptop</i>	
<i>Student Grades</i>	
<i>Security Analyst</i>	
<i>Microsoft Office Suite</i>	

<i>Microsoft Office License</i>	
<i>Email</i>	
<i>Firewall</i>	
<i>Intrusion Detection System</i>	
<i>Operational Documents</i>	
<i>Memorandum of Agreement</i>	

(10 markah)

- c) Jadual 2 menggambarkan contoh profil penilaian risiko kuantitatif untuk MyUniversity. Tentukan nilai faktor risiko untuk (i), (ii), (iii), (iv) and (v).

Jadual 2: Profil Penilaian Risiko Kuantitatif MyUniversity

<i>Event</i>	<i>Likelihood</i>	<i>Impact</i>	<i>Risk Factor</i>
<i>fire in data center</i>	0.7	0.9	(i)
<i>weak password</i>	0.8	0.5	(ii)
<i>antivirus update weekly</i>	0.8	0.6	(iii)
<i>data encryption breakable</i>	0.8	0.9	(iv)
<i>no backup for data</i>	0.7	0.9	(v)

(5 marks)

SOALAN 3 (25 MARKAH)

- a) Profesor Chong adalah Ketua Pegawai Teknologi (CTO) di Cyber Rescue Sdn Bhd. Baru-baru ini beliau melantik anda sebagai juruaudit dalaman syarikat untuk membangunkan senarai semak audit keselamatan rangkaian. Beliau menugaskan anda untuk menghasilkan senarai semak di dalam bentuk jadual. Lakarkan senarai semak yang dikehendaki dan anda diminta untuk senaraikan **LIMA (5)** item paling penting yang boleh dipertimbangkan untuk diaudit dengan memberikan **TIGA (3)** contoh untuk **SETIAP** item yang dipilih..

(20 markah)

- b) Berikan **LIMA(5)** strategi pengurangan risiko bagi rekabentuk rangkaian pengkomputeraan awan.

(5 markah)



INSTRUCTION: Answer *ALL* questions.

QUESTION 1 (50 MARKS)

- a) Figure 1 illustrates the network infrastructure for MyUniversity Information System that operates 24 hours to support an academic programmes and administrative services. The information systems uses confidential data from the database such as student information, grades, financial related information and many more. Such critical information can be accessed by validated student and staff via web browser. Moreover, the entire hardware and applications that are used to support this system are located in MyUniversity Data Center which is monitored by CCTV. Furthermore, fingerprint identification is implemented to record the attendance of staff in the server plant. Based on this scenario and Figure 1, solve question in (a), (b), (c), (d), (e), (f) and (g).

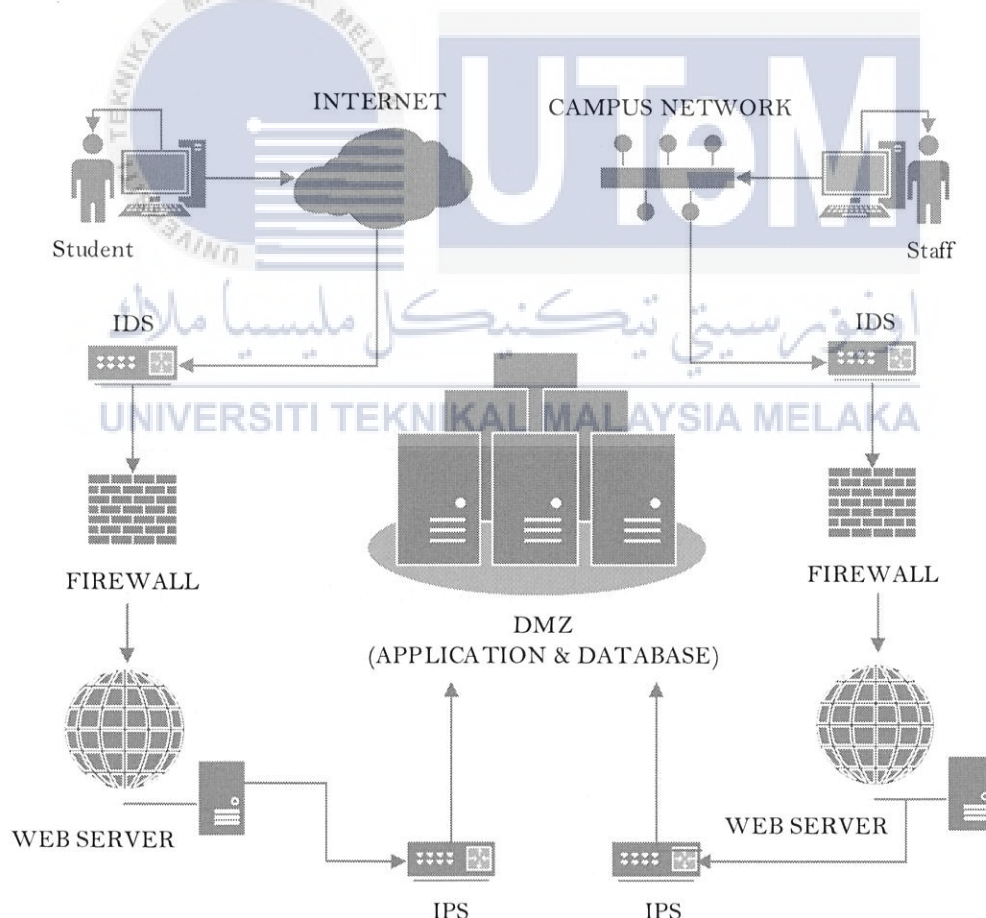







Figure 1: MyUniversity Information System Network Infrastructure

- a) If you are an internal auditor, identify **THREE(3)** types of principle control that required for MyUniversity information system network infrastructure.  (3 marks)
- b) Determine **THREE(3)** control functions and give **TWO(2)** examples for **EACH** control function that can be considered for MyUniversity information system network infrastructure. (9 marks)
- c) List **FIVE(5)** critical security control that can be suggested in a context of an external auditor.  (5 marks)
- d) Give **EIGHT(8)** rationale on the importance of the critical security controls stated in question (c).  (8 marks)
- e) Define the formula for Cost Benefit Analysis (CBA), Annualized Loss Expectancy (ALE) and Single Loss Expectancy (SLE).  (6 marks)
- f) The email system of MyUniversity could be damaged by a cyber attack which can cause huge losses. The exposure factor for email system to be damaged is valued at 30% and the value is estimated at RM5,000,000. Calculate the Single Loss Expectancy (SLE), Annualized Rate of Occurrence (ARO) and Annualized Loss Expectancy (ALE) if cyber attack is expected to be happen once every year.  (9 marks)

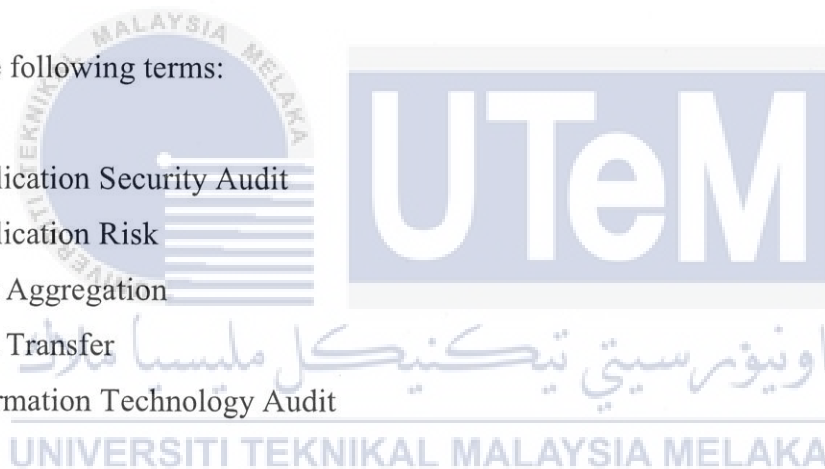
- g) Assume, the estimated cost for a single successful phishing attack against MyUniversity email system is at RM10,000. MyUniversity e-mail system is expected to be infected due to phishing for 6 times in a year. The reduction of probability of risk occurrence is assumed at 75% if the control is implemented.. In addition, the cost to train employees and avoid phishing emails is expected to be RM20,000. Calculate the Return of Investment (ROI) and determine how much the university can save per year by conducting awareness training for its employees.

(10 marks)

QUESTION 2 (25 MARKS)

- a) Define the following terms:

- i. Application Security Audit
- ii. Application Risk
- iii. Risk Aggregation
- iv. Risk Transfer
- v. Information Technology Audit



(10 marks)

- b) Determine the correct asset types for each asset represented in Table 1.

Table 1: Asset List

Asset	Asset Types
Laptop	
Student Grades	
Security Analyst	

Microsoft Office Suite	
Microsoft Office License	
Email	
Firewall	
Intrusion Detection System	
Operational Documents	
Memorandum of Agreement	

(10 marks)

- c) Table 2 illustrates an example of quantitative risk assessment profile for MyUniversity. Determine the value of risk factor for (i), (ii), (iii), (iv) and (v).

Table 2: MyUniversity Quantitative Risk Assessment Profile

Event	Likelihood	Impact	Risk Factor
fire in data center	0.7	0.9	(i)
weak password	0.8	0.5	(ii)
antivirus update weekly	0.8	0.6	(iii)
data encryption breakable	0.8	0.9	(iv)
no backup for data	0.7	0.9	(v)

(5 marks)

QUESTION 3 (25 MARKS)

- a) Professor Chong is the Chief Technology Officer (CTO) at Cyber Rescue Sdn Bhd. He recently appointed you as the company's internal auditor to develop a network security audit checklist for the organization. He instructed you to design a checklist in the form of a table. Design the desired checklist and you are required to provide **FIVE (5)** most



significant items that can be considered to audit by giving **THREE (3)** examples for **EACH** selected item.

(20 marks)

b) Give **FIVE(5)** risk mitigation strategies for the cloud computing network design.

(5 marks)





UTeM

اونيورسيتي تيكنيكل مليسيا ملاك

UNIVERSITI TEKNIKAL MALAYSIA MELAKA