UNIVERSITI TEKNIKAL MALAYSIA MELAKA

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 ***COURSE CODE***	**:**	**BITS3353**
KURSUS ***SUBJECT***	**:**	**PENGURUSAN DAN PENTADBIRAN KESELAMATAN RANGKAIAN** ***NETWORK SECURITY ADMINISTRATION AND MANAGEMENT***
PENYELARAS ***COORDINATOR***	**:**	**NUR FADZILAH BINTI OTHMAN**
PROGRAM ***PROGRAMME***	**:**	**BITZ**
MASA ***TIME***	**:**	**9:00 PAGI** ***9:00 AM***
TEMPOH ***DURATION***	**:**	**2 JAM** ***2 HOURS***
TARIKH ***DATE***	**:**	**30 JANUARI 2022** ***30 JANUARY 2021***
TEMPAT ***VENUE***	**:**	**HALL 5** ***HALL 5***

ARAHAN KEPADA CALON
INSTRUCTION TO CANDIDATES

1. **Kertas soalan ini mengandungi EMPAT (4) soalan. Sila jawab SEMUA soalan.**
   The exam paper consists of FOUR(4) questions. Please answer ALL questions.

2. **Kertas soalan ini mempunyai versi dwi-bahasa. Versi Bahasa Melayu bermula daripada mukasurat 2 hingga 5, manakala versi Bahasa Inggeris bermula daripada mukasurat 6 hingga 9.**
   The exam paper consists of dual-language version. The Malay version starts from page 2 to 5, whereas the English version starts from page 6 to 9.

KERTAS SOALAN INI TERDIRI DARIPADA LAPAN (9) MUKA SURAT SAHAJA TERMASUK MUKA SURAT HADAPAN
THIS QUESTION PAPER CONTAINS EIGHT (9) PAGES INCLUSIVE OF FRONT PAGE

ARAHAN: *Jawab **SEMUA** soalan*

SOALAN 1 (25 MARKAH)

Mitigasi risiko ditakrifkan sebagai pengambilan langkah-langkah untuk mengurangkan kesan buruk. Adalah penting untuk membangunkan strategi pengurangan risiko yang berkait rapat dan sepadan dengan profil syarikat anda.

a) Takrifkan istilah berikut yang berkaitan dengan pengurangan risiko. Berikan contoh yang sesuai dan penerangan mesti mempertimbangkan hubungan antara semua istilah.
   i. Ejen ancaman
   ii. Kerentanan
   iii. Ancaman
   iv. Risiko

(8 markah)

b) Tentukan kategori risiko yang betul bagi setiap contoh yang ditunjukkan dalam Jadual 1.

Jadual 1: Kategori risiko

Contoh	**Kategori Risiko**
Kegagalan rantaian bekalan	
Perubahan dalam pilihan pengguna	
Serangan *Cross-Site Scripting (XSS)*	
Pekerja meletak jawatan	
Gempa bumi	
Rasuah	
Kelewatan menghantar barang	

(7 markah)

c) Organisasi menggunakan penilaian risiko untuk mengkaji ancaman, kerentanan dan risiko yang boleh menjejaskan kerahsiaan, integriti dan ketersediaan sistem dan data mereka. Kenal pasti cara memenuhi prinsip teras triad *CIA* dengan melaksanakan kawalan keselamatan untuk mengurangkan risiko tersebut.

(6 markah)

d) Maklumat daripada kajian pengurusan risiko boleh digunakan untuk membuat polisi. Dengan bantuan gambar rajah, gambarkan kitaran polisi keselamatan yang perlu dipertimbangkan.

(4 markah)

SOALAN 2 (25 MARKAH)

Kawalan capaian ialah dengan memberikan atau menafikan kebenaran untuk menggunakan sumber tertentu. Ia adalah mekanisme sistem maklumat untuk membenarkan atau menyekat capaian kepada data atau peranti.

a) Berdasarkan pemahaman anda, bincangkan hubungan antara pengenalan, pengesahan, keizinan dan capaian.

(4 markah)

b) Jelaskan peranan dan tugas yang terlibat dalam kawalan capaian objek atau sumber.

(6 markah)

Pengesahan ialah proses memastikan seseorang yang ingin mengakses sumber adalah sahih.

c) Berserta contoh, terangkan bukti kelayakan pengesahan yang boleh digunakan untuk mengesahkan identiti pengguna dan nyatakan keburukan setiap bukti kelayakan.

(9 markah)

d) Terangkan secara ringkas strategi yang boleh digunakan untuk membina kata laluan. Berdasarkan pendapat anda, pilih strategi terbaik dan beri justifikasi jawapan anda.

(6 markah)

SOALAN 3 (15 MARKAH)

Rangkaian yang selamat adalah penting untuk postur keselamatan maklumat yang komprehensif. Rangkaian selamat akan menjauhkan penyerang daripada peranti di bahagian dalam.

a) Nyatakan protokol pengesahan rangkaian yang melaksanakan pengesahan berasaskan port. Gambarkan dan terangkan elemen dan langkah-langkah yang terlibat dalam proses pengesahan tersebut.

(10 markah)

b) Tentukan protokol selamat yang disyorkan untuk setiap aplikasi atau teknologi yang ditunjukkan dalam Jadual 2.

Jadual 2: Protokol selamat yang disyorkan oleh aplikasi atau teknologi

Applikasi atau teknologi	**Protokol selamat yang disyorkan**
Melayari web	
Perutenan dan pensuisan	
Pemindahan fail	
Email	
Akses jauh	

(5 markah)

SOALAN 4 (35 MARKAH)

Situasi Covid-19 telah mengubah cara kerja yang sebelum ini melibatkan pertemuan fizikal kepada interaksi maya dan digital. Oleh itu, ia meningkatkan aktiviti rangkaian organisasi dan bilangan peranti yang disambungkan pada rangkaian tersebut. Walau bagaimanapun, mengalihkan sebahagian besar tenaga kerja kepada model kerja dari rumah, mendedahkan kelemahan infrastruktur dan alatan IT awam asas yang digunakan, serta mencipta serangan besar peranti yang digunakan dengan pantas dan membuka pintu kepada kompromi keselamatan .

a) Berdasarkan situasi di atas, kenal pasti **LIMA (5)** pendedahan ancaman yang mungkin berlaku.

(5 markah)

b) Tentukan prosedur pencegahan bagi setiap ancaman yang dinyatakan dalam Soalan 4 (a).

(10 markah)

c) Senaraikan dan terangkan ciri-ciri yang paling biasa terlibat dalam Pelan Pemulihan Bencana (*DRP*).

(10 markah)

d) Pemulihan bencana adalah salah satu faktor yang mempengaruhi keputusan untuk melindungi dan memulihkan fungsi. Terangkan **LIMA (5)** isu yang berkaitan dengan senario penemuan bencana.

(10 markah)

-SOALAN TAMAT-

INSTRUCTION: *Answer **ALL** questions.*

QUESTION 1 (25 MARKS)

Risk mitigation is defined as steps to reduce adverse effects. It is important to develop a risk mitigation strategy that closely relates to and matches your company's profile.

a) Define the following terms associated with risk mitigation. Give the appropriate example and the explanation must consider the relationship between all the terms.

i. Threat agent
ii. Vulnerability
iii. Threat
iv. Risk

(8 marks)

b) Determine the correct risk category for each example which represented in Table 1.

Table 1: Risk Classification

Example	**Risk Category**
Supply chain failure	
Changes in consumer preferences	
Cross-Site Scripting (XSS) attacks	
Employee resign	
Earthquakes	
Bribery	
Delay in delivering goods	

(7 marks)

c) Organizations use risk assessments to examine the threats, vulnerabilities, and risks that could affect the confidentiality, integrity, and availability of their systems and data. Identify how to fulfill CIA triad's core principles by implementing security controls to mitigate those risks.

(6 marks)

d) Information from the risk management study can be used to create the policy. With the aid of diagram, identify security policy cycle that need to be considered.

(4 marks)

QUESTION 2 (25 MARKS)

Access control is granting or denying approval to use specific resources. It is an information system's mechanism to allow or restrict access to data or devices.

a) Based on your understanding, discuss the relationship between identification, authentication, authorization and access.

(4 marks)

b) Explain roles and duties involves in access control objects or resources.

(6 marks)

Authentication is the process of ensuring a person desiring to access resources is authentic.

c) With an example, describe authentication credential that can be used to verify a user identity and state the disadvantages of each credential.

(9 marks)

d) Explain briefly the strategies that can be used to construct a password. Based on your opinion, choose the best strategies and justify your answer.

(6 marks)

QUESTION 3 (15 MARKS)

Secure network is essential to a comprehensive information security posture. A secure network would keep attackers away from the devices on the inside.

a) Specify the network authentication protocol that implement port-based authentication. Illustrated and explain the elements and steps involves in the authentication process.

(10 marks)

b) Determine the recommended secure protocol for each application or technology which represented in Table 2.

Table 2: Application or technology recommended secure protocol

Application or technology	**Recommended secure protocol**
Web browsing	
Routing and switching	
File transfer	
Email	
Remote Access	

(5 marks)

QUESTION 4 (35 MARKS)

Covid-19 situation has changed the way of work that previously involved physical meeting to virtual and digital interactions. Hence, it increases an organization network activity and the number of connected devices on those networks. However, shifting large parts workforce to a work-from-home model, exposes the vulnerabilities of the underlying public IT infrastructure and tools used, as well as creates a huge attack surface of devices that were rapidly deployed and are opening the door to security compromises.

a) Based on the above situation, identify **FIVE (5)** exposure of threats that may occur.

(5 marks)

b) Determine preventive procedures for each threat stated in Question 4 (a)**.**

(10 marks)

c) List and explain most common features involves in Disaster Recovery Plan (DRP).

(10 marks)

d) Disaster recovery is one of the factors that influence the decisions on protecting and restoring the function. Explain **FIVE (5)** issue which related to disaster discovery scenario.

(10 marks)

- END OF QUESTIONS –