UNIVERSITI TEKNIKAL MALAYSIA MELAKA

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

KOD KURSUS ***COURSE CODE***	**:**	**BITS 3523** ***BITS 3523***
KURSUS ***COURSE***	**:**	**AUDIT KOMPUTER & PENGURUSAN RISIKO** ***COMPUTER AUDIT &RISK MANAGEMENT***
PENYELARAS ***COORDINATOR***	**:**	**DR. WARUSIA MOHAMED YASSIN**
PROGRAM ***PROGRAMME***	**:**	**3 BITZ** ***3 BITZ***
MASA ***TIME***	**:**	**02.30 PM – 05.00 PM** ***02.30 PM – 05.00 PM***
TEMPOH ***DURATION***	**:**	**2 JAM 30 MINIT** ***2 HOURS 30 MINUTES***
TARIKH ***DATE***	**:**	**27 Jun 2022** ***27 June 2022***
TEMPAT ***VENUE***	**:**	**HALL 3** ***HALL 3***

ARAHAN KEPADA CALON
INSTRUCTION TO CANDIDATES

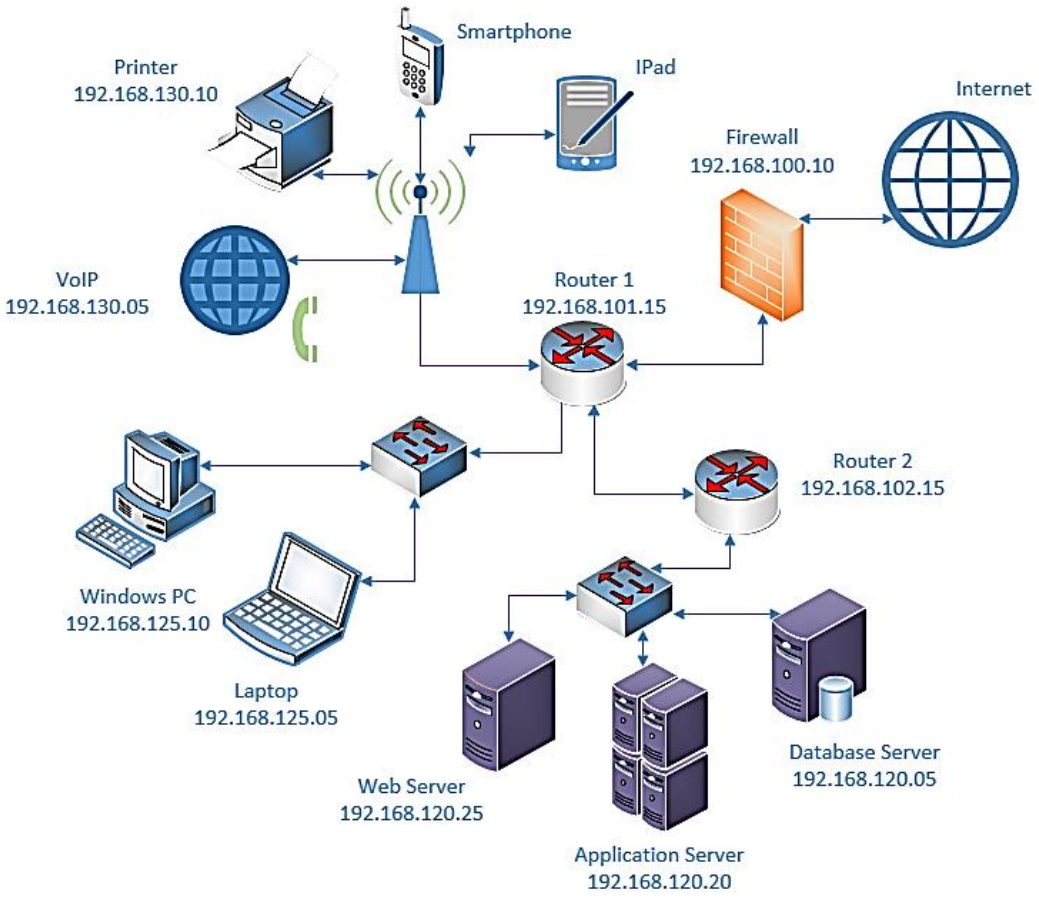
1. **Kertas soalan ini mengandungi TIGA (3) Soalan.**
   This exam paper contains THREE (3) Questions.
2. **Sila jawab SEMUA soalan.**
   Please answer ALL questions.
3. **Kertas soalan ini mempunyai 2 versi bahasa. Versi Bahasa Melayu bermula daripada muka surat 2 hingga 8 manakala versi Bahasa Inggeris bermula daripada muka surat 9 hingga 15. Sila jawab di dalam satu versi sahaja.**
   This exam paper has 2 versions. Malay version starts from page 2 to 8 while English version starts from page 9 to 15. Answer in one version only.

KERTAS SOALAN INI TERDIRI DARIPADA (15) MUKA SURAT SAHAJA TERMASUK MUKA SURAT HADAPAN
THIS QUESTION PAPER CONTAINS (15) PRINTED PAGES INCLUSIVE OF FRONT PAGE

ARAHAN: *Jawab **SEMUA** soalan.*

SOALAN 1 (50 MARKAH)

Rajah 1 menggambarkan infrastruktur rangkaian dalaman MyOnline Purchase Sdn Bhd yang beroperasi selama 24 jam untuk menyokong perkhidmatan pengurusan pentadbiran dan perniagaan. Perniagaan syarikat berkenaan dijalankan secara dalam talian dan mempunyai data data sulit dan kritikal seperti data pengurusan kewangan, informasi pelanggan dan maklumat pekerja. Ekoran dari serangan malware ke atas infrastruktur ini, pihak syarikat mengambil keputusan untuk menjemput internal auditor untuk mengendalikan penilaian risiko ke atas rangkaian dan aset syarikat. Berdasarkan scenario dan Rajah 1, jawab soalan **(a), (b), (c), (d), (e), (f), (g), (h), (i)** dan **(j)**.



Rajah 1: Rajah Rangkaian Dalaman MyOnline Purchase Sdn Bhd

a) Berikan definasi bagi terma internal auditor.

(2 markah)

b) Berikan definasi bagi terma penilaian risiko.

(2 markah)

c) Berikan definasi bagi terma analisa risiko.

(2 markah)

d) Tentukan dan kenalpasti **SATU(1)** aset kiritikal utama, jenis dan lokasi untuk pemilik berikut.

i) Pentadbir Pangkalan Data

(3 markah)

ii) Pentadbir Sistem

(3 markah)

iii) Pentadbir Keselamatan Rangkaian

(3 markah)

e) Sejurus aset dalaman ditentukan, andaikan anda telah mengenal pasti sumber ancaman yang boleh menjejaskan operasi MyOnline Purchase Sdn Bhd. Tentukan **DUA(2)** tindakan ancaman yang berpotensi untuk **SETIAP** sumber ancaman dalam i, ii, iii, iv dan v. Jawapan anda mungkin berada dalam skop pelanggaran keselamatan, kesilapan teknikal, kesilapan manusia dan kegagalan infrastruktur.

i) Penjenayah Siber

(2 markah)

ii) Pekerja

(2 markah)

iii) Reputasi

(2 markah)

iv) Teknikal

(2 markah)

v) Alam Sekitar

(2 markah)

f) Sebagai juruaudit dalaman, anda dikehendaki melakukan analisis kesan risiko ke atas infrastruktur rangkaian MyOnline Purchase Sdn Bhd. Melalui analisa anda, tentukan kemungkinan *incident* yang boleh berlaku dan terangkan akibatnya untuk **SETIAP** kesan dalam **i, ii dan iii**.

i) Tinggi

(3 markah)

ii) Sederhana

(3 markah)

iii) Rendah

(3 markah)

g) Berdasarkan analisis risiko yang dijalankan, anda sebagai juruaudit telah mengenal pasti beberapa ancaman yang boleh menjejaskan operasi pelayan MyOnline Purchase Sdn Bhd. Nyatakan kelemahan yang berpotensi dan cadangan anda untuk **SETIAP** ancaman dalam **i, ii dan iii.**

i) Taufan

(2 markah)

ii) Kekurangan pelan pemulihan bencana

(2 markah)

iii) Akses tanpa kebenaran ke pelayan

(2 markah)

h) Daripada pemerhatian anda dan hasil penilaian risiko, kebanyakan data didapati tidak direkodkan. Sebagai juruaudit, apakah jenis rawatan yang boleh anda cadangkan kepada organisasi dan berikan contoh yang sesuai untuk mengatasi risiko kehilangan data.

(2 markah)

i) Daripada pemerhatian anda dan hasil penilaian risiko, kebanyakan pekerja didapati menggunakan komputer riba mereka di luar rangkaian organisasi untuk mengakses data sulit. Sebagai juruaudit, jenis rawatan apakah yang anda boleh cadangkan kepada organisasi dan berikan contoh yang sesuai untuk mengatasi akses tanpa kebenaran.

(2 markah)

j) Berikan **TIGA(3)** kemungkinan kegagalan yang boleh mengakibatkan status ketidakakuran kepada MyOnline Purchase Sdn Bhd.

(2 markah)

SOALAN 2 (25 MARKAH)

a) Berikan definasi bagi terma-terma berikut:

i) Analisis Impak Perniagaan (BIA)

(2 markah)

ii) Pelan Kesinambungan Perniagaan (BCP)

(2 markah)

b) Pelayan pangkalan data MyOnline Purchase Sdn Bhd boleh rosak akibat serangan siber yang akan menyebabkan kerugian besar. Faktor pendedahan bagi sistem pangkalan data yang boleh rosak adalah bernilai 25% dan nilainya dianggarkan berjumlah RM10,000,000. Serangan siber itu dijangka berlaku lima kali dalam dua tahun. Berdasarkan kes ini, selesaikan soalan dalam **i, ii, iii, iv dan v**. Tunjukkan langkah kerja bagi setiap soalan.

i) Kenalpasti nilai aset (AV)

(1 markah)

ii) Kenalpasti nilai faktor pendedahan

(1 markah)

iii) Kira jangka kerugian tunggal (SLE)

(2 markah)

iv) Kira kadar kejadian tahunan

(2 markah)

v) Kira jangkaan kerugian tahunan

(2 markah)

c) Anggaran kos untuk satu serangan vishing yang berjaya terhadap sistem VoIP MyOnline Purchase Sdn Bhd ialah RM250,000. Sistem VoIP MyOnline Purchase Sdn Bhd dijangka akan dijangkiti vishing 1 kali dalam setahun. Pengurangan kebarangkalian berlakunya risiko diandaikan pada 80% jika kawalan dilaksanakan. Di samping itu, kos untuk menjalankan program kesedaran bagi mengelak vhishing dijangka sebanyak RM50,000. Berdasarkan kes ini, selesaikan soalan dalam **i, ii, iii, iv, v, vi, vii dan viii**. Tunjukkan langkah kerja bagi setiap soalan.

i. Kenalpasti kos kawalan

(1 markah)

ii. Kenalpasti kadar kejadian tahunan

(1 markah)

iii. Kenalpasti kerugian kewangan yang dijangkakan untuk satu peristiwa

(1 markah)

iv. Kenalpasti pengurangan dalam kebarangkalain kejadian dengan kawalan yang dilaksanakan

(1 markah)

v. Kira pengurangan risiko

(2 markah)

vi. Kira pulangan pelaburan.

(2 markah)

vii. Tentukan jumlah penjimatan MyOnline Purchase Sdn Bhd untuk setiap tahun dengan menjalan program kesedaran.

(2 markah)

viii. Berdasarkan pendapat anda, adakah kos pengurangan tahunan boleh diterima? Terangkan hujah anda.

(3 markah)

SOALAN 3 (25 MARKAH)

a) Takrifkan istilah Sistem Pengurusan Keselamatan Maklumat (ISMS).

(2 markah)

b) Ternagkan objective keselamatan maklumat seperti yang ditakrifkan dalam ISO/IEC 27002.

(2 markah)

c) Huraikan **DUA(2)** faedah yang boleh dicapai oleh sesebuah organisasi apabila berjaya mengguna pakai Sistem Pengurusan Keselamatan Maklumat (ISMS).

(4 markah)

d) Terangkan **SATU(1)** perbezaan antara ISO 19011 dan ISO 3100.

(4 markah)

e) Pensijilan ISO/IEC 27001 biasanya melibatkan tiga peringkat proses audit luaran. Terangkan dua peringkat pertama proses tersebut seperti yang ditakrifkan oleh ISO/IEC 17021 dan ISO/IEC 27006.

(4 markah)

f) Tentukan **EMPAT(4)** komponen prinsip yang terlibat dalam kitaran Sistem Pengurusan Keselamatan Maklumat (ISMS).

(4 markah)

g) Nyatakan **EMPAT(4)** pilihan yang boleh dipertimbangkan untuk ancaman risiko apabila risiko telah dikenal pasti.

(4 markah)

h) Nyatakan **SATU(1)** peranan juruaudit teknologi maklumat.

(1 markah)

- SOALAN TAMAT-

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

QUESTION 1 (50 MARKS)

Figure 1 illustrates the internal network infrastructure of MyOnline Purchase Sdn Bhd which operates for 24 hours to support administrative and business management services. The company's business is conducted online and has confidential and critical data such as financial, customer and employee information. Due to malware attacks against this infrastructure, the company decided to invite internal auditors to conduct risk assessments on the company's network and assets. Based on this scenario and Figure 1, solve question in **(a)**, **(b)**, **(c), (d), (e), (f)**, **(g), (h), (i) and (j)**.

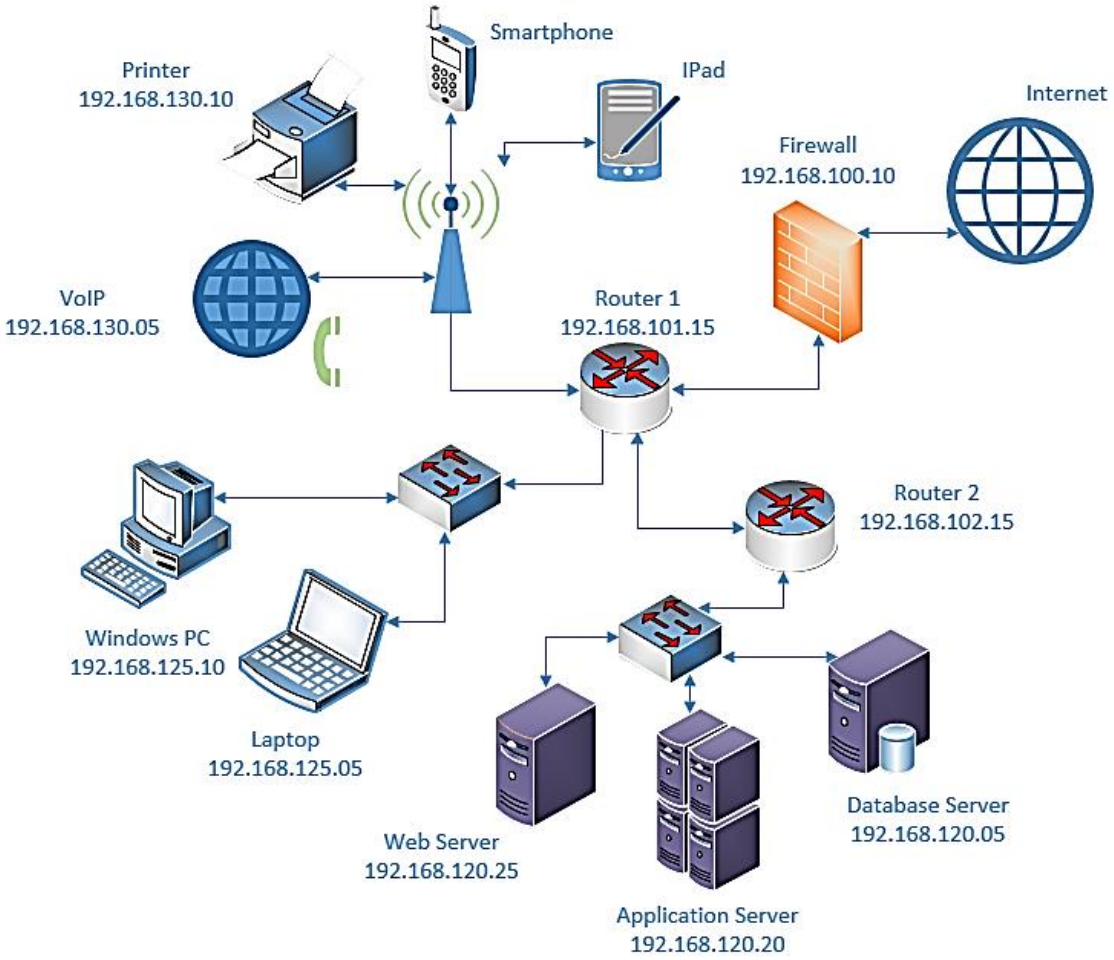


Figure 1: MyOnline Purchase Sdn Bhd Internal Network Infrastructure

a) Define the term internal auditor.

(2 marks)

b) Define the term risk assessment.

(2 marks)

c) Define the term risk analysis.

(2 marks)

d) Determine and identify **ONE(1)** primary critical assets, type and location for the following possible owners.

i. Database Administrator

(3 marks)

ii. System Administrator

(3 marks)

iii. Web Administrator

(3 marks)

iv. Network Security Administrator

(3 marks)

e) Upon internal assets has been determined, assume you has identified threat sources that could affect MyOnline Purchase Sdn Bhd operations. Determine **TWO(2)** potential threat actions for **EACH** threat sources in **i, ii, iii, iv and v**. Your answer could be within the scope of security breaches, technical missteps, human errors and infrastructure failure.

i. Cyber Criminal

(2 marks)

ii. Employees

(2 marks)

iii. Reputation

(2 marks)

iv. Technical

(2 marks)

v. Environmental

(2 marks)

f) As an internal auditor, you are required to perform risk impact analysis for MyOnline Purchase Sdn Bhd network infrastructure. Throughout your analysis, determine the potential incidents and explain their consequences for **EACH** impact in **i, ii and iii**.

i. High

(3 marks)

ii. Moderate

(3 marks)

iii. Low

(3 marks)

g) Based on the conducted risk analysis, you as an auditor have identified several threats that could affect the operation of MyOnline Purchase Sdn Bhd servers. Outline the potential vulnerabilities and recommendations for **EACH** threat in **i, ii and iii**.

i. Hurricane

(2 marks)

ii. Lack of disaster recovery plan

(2 marks)

iii. Unauthorized access to the server

(2 marks)

h) From your observations and the results of the risk assessment, it was found that most of the data were not recorded. As an auditor, which type of treatment that you can suggest to the organization and give an appropriate example to overcome the risk of data loss.

(2 marks)

i) From your observations and the results of the risk assessment, it was found that most of the employees use their laptops outside an organization's network to access confidential data. As an auditor, which type of treatment that you can suggest to the organization and give an appropriate example to overcome unauthorized access.

(2 marks)

j) State **THREE(3)** possible failures that can result in nonconformity status to MyOnline Purchase Sdn Bhd.

(3 marks)

QUESTION 2 (25 MARKS)

a) Explain the following terms:

i. Business impact analysis (BIA)

(2 marks)

ii. Business continuity plan (BCP)

(2 marks)

b) The database server of MyOnline Purchase Sdn Bhd could be damaged by a cyber-attack which can cause huge losses. The exposure factor for a database system to be damaged is valued at 25% and the value is estimated at RM10,000,000. The cyberattack is expected to happen five times in two years. Based on this case, solve questions in **i, ii, iii, iv and v**. Show the working steps for each question.

i. Identify the asset value (AV)

(1 marks)

ii. Identify the exposure factor value

(1 marks)

iii. Calculate the Single Loss Expectancy (SLE).

(2 marks)

iv. Calculate the Annualized Rate of Occurrence (ARO).

(2 marks)

v. Calculate the Annualized Loss Expectancy (ALE).

(2 marks)

c) The estimated cost for a single successful vishing attack against the MyOnline Purchase Sdn Bhd VoIP system is RM250,000. MyOnline Purchase Sdn Bhd VoIP system is expected to be infected due to vishing 1 time in a year. The reduction of probability of risk occurrence is assumed at 80% if the control is implemented. In addition, the cost to conduct an awareness program to avoid vhishing calls is expected to be RM50,000. Based on this case, solve questions in **i, ii, iii, iv, v, vi, vii and viii**. Show the working steps for each question.

i. Identify the Cost of Control

(1 marks)

ii. Identify the annualized rate of occurrence

(1 marks)

iii. Identify the expected monetary loss for a single event

(1 marks)

iv. Identify the reduction in probability occurrence with the implemented control

(1 marks)

v. Calculate the Reduction in Risk

(2 marks)

vi. Calculate the Return of Investment

(2 marks)

vii. Evaluate how much the MyOnline Purchase Sdn Bhd can save per year by conducting an awareness program.

(2 marks)

viii. Based on your opinion, is the annual reduction cost acceptable? Justify your answer.

(3 marks)

QUESTION 3 (25 MARKS)

a) Define the term Information Security Management System (ISMS).

(2 marks)

b) Explain the objective of information security as defined in ISO/IEC 27002.

(2 marks)

c) Describe **TWO(2)** benefits that can be achieved by an organization upon successfully adopting Information Security Management System (ISMS).

(4 marks)

d) Explain **ONE (1)** the differences between ISO 19011 and ISO 3100.

(4 marks)

e) The ISO/IEC 27001 certification usually involves three stages of external audit processes. Explain the first two stages as define by ISO/IEC 17021 and ISO/IEC 27006.

(4 marks)

f) Define **FOUR(4)** principle components involve in Information Security Management System (ISMS) cycle.

(4 marks)

g) State **FOUR(4)** options that can be considered for risk threatment upon the risk has been identified.

(4 marks)

h) State **ONE (1)** information technology auditor role.

(1 marks)

-END OF QUESTIONS-