UNIVERSITI TEKNIKAL MALAYSIA MELAKA

UNIVERSITI TEKNIKAL MALAYSIA MELAKA
PEPERIKSAAN AKHIR SEMESTER II
FINAL EXAMINATION SEMESTER II
SESI 2020/2021
SESSION 2020/2021
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*	:	**BITS** *BITS*
MASA *TIME*	:	**14.15 PM – 16.15 PM** *14.15 PM – 16.15 PM*
TEMPOH *DURATION*	:	**2 JAM** *2 HOURS*
TARIKH *DATE*	:	**12 07 2021** *12 07 2021*
TEMPAT *VENUE*	:	**HALL 5** *HALL 5*

ARAHAN KEPADA CALON
INSTRUCTION TO CANDIDATES

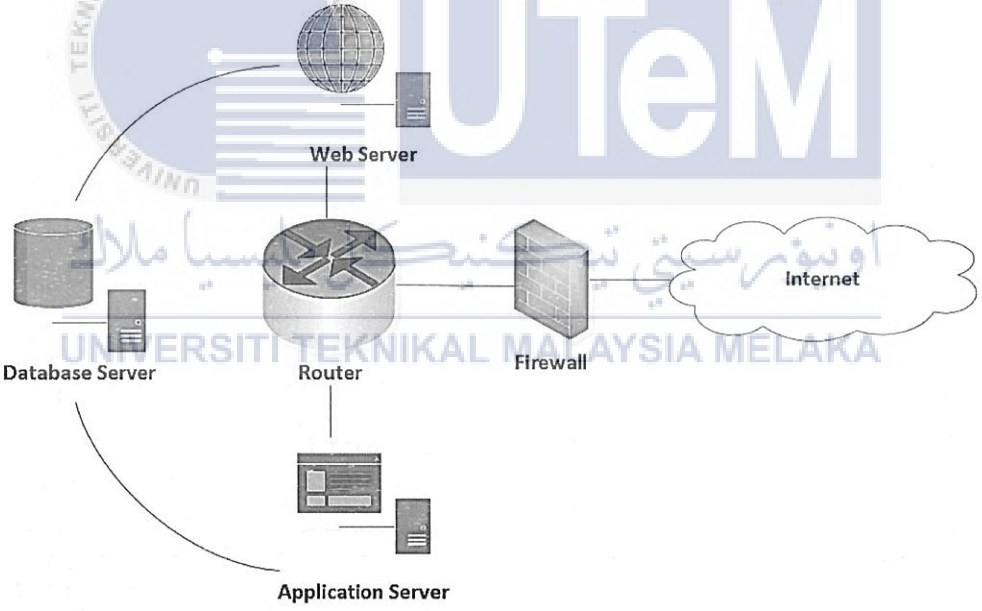
1. **Kertas soalan ini mengandungi EMPAT (4) Soalan.**
   This exam paper contains FOUR (4) Questions.
2. **Sila jawab SEMUA soalan.**
   Please answer ALL questions.
3. **Kertas soalan ini mempunyai 2 versi bahasa. Versi Bahasa Melayu bermula daripada muka surat 2 hingga 7 manakala versi Bahasa Inggeris bermula daripada muka surat 8 hingga 13. Sila jawab di dalam satu versi sahaja.**
   This exam paper has 2 versions. Malay version starts from page 2 to 7 while English version starts from page 8 to 13. Answer in one version only.

KERTAS SOALAN INI TERDIRI DARIPADA (13) MUKA SURAT SAHAJA TERMASUK MUKA SURAT HADAPAN
THIS QUESTION PAPER CONTAINS (13) PRINTED PAGES INCLUSIVE OF FRONT PAGE

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

SOALAN 1 (25 MARKAH)

a) Rajah 1 menggambarkan rajah rangkaian MySite Sdn Bhd. Syarikat ini membekalkan pelbagai jenis produk seperti peralatan rumah tangga, alat elektronik, peralatan sukan dan banyak lagi. Untuk menggunakan perkhidmatan syarikat ini, pengguna perlu mencapai laman web syarikat yang beroperasi 24 jam melalui komputer, telefon bimbit atau aplikasi mudah alih dari internet. Keseluruhan data seperti maklumat pelanggan rekod pembelian dan lain-lain di simpan di dalam pangkalan data. Produk yang dibeli akan dihantar setelah diproses oleh pentadbir sistem melalui pelayan aplikasi. Berdasarkan senario ini, selesaikan soalan **(i)**, **(ii)** dan **(iii)**.



Rajah 1: Rajah Rangkaian MySite Sdn Bhd

(i) Bagaiman boleh mengira Cost Benefit Analysis (BCA), Annualized Loss Expectancy (ALE) dan Single Loss Expectancy (SLE) bagi senario di Rajah 1.

(6 markah)

(ii) Laman web syarikat mungkin mengalami kerosakan akibat serangan siber dan boleh menyebabkan kerugian besar. Sebagai juruaudit dalaman MySite Sdn Bhd, anda telah menganggarkan nilai pelayan web pada harga RM10,000 dan faktor pendedahan pelayan tersebut rosak mungkin berjumlah 20%. Kirakan S*ingle Loss Expectancy (SLE), Annualized Rate of Occurrence (ARO)* dan *Annualized Loss Expectancy (ALE)* jika tindakan serangan siber dijangka berjaya berlaku sekali setiap dua tahun.

(9 markah)

(iii) *Return of Investment (ROI)* boleh dikira dengan menentukan kos risiko dan kawalan yang berpotensi. Lazimnya pihak organisasi menggunakannya untuk mengukur keuntungan. Andaikan system e-mel MySite Sdn Bhd dijangka akan mengalami serangan *phishing* sebanyak 3 kali setahun dengan anggaran kos RM25,000 bagi setiap serangan yang berjaya. Kos untuk melatih pekerja dan mengelak dari serangan e-mel *phishing* adalah sebanyak RM15,000, sementara pengurangan kemungkinan berlakunya risiko dengan kawalan yang dilaksanakan diandaikan pada 75%. Oleh itu, kirakan *Return of Investment (ROI)* dan tentukan berapa banyak organisasi anda dapat jimat setiap tahun dengan mengadakan latihan kesedaran kepada pekerjanya.

(10 markah)

SOALAN 2 (25 MARKAH)

a) Andaikan anda bekerja sebagai juruaudit dalaman di sektor perbankan. Baru-baru ini, anda diminta untuk dilakukan pengujian penembusan dalaman untuk mengimbas sistem perbankan yang terdiri daripada sistem kehadiran pekerja, sistem rangkaian, dan beberapa pelayan di pusat data. Sepanjang analisis, anda telah menemui beberapa kelemahan yang berkaitan dengan persekitaran sistem perbankan. Jadual 1 mengandungi contoh kegoyahan, sumber ancaman dan tindakan ancaman yang telah dibentuk berdasarkan pemerhatian anda sebagai juruaudit dalaman. Apakah sumber ancaman dan tindakan ancaman yang berpotensi untuk setiap kegoyaan yang terdapat di dalam Jadual 1?

Jadual 1: Kegiyahan, Sumber Ancaman and Tindakan Ancaman

Kegoyahan	Sumber Ancaman	Tindakan Ancaman
ID pekerja yang telah diberhentikan tidak dikeluarkan dari pangkalan data		
ID tetamu dibolehkan pada pelayan aplikasi dan *firewall* salah dikonfigurasikan untuk membolehkan Telnet		
Penguji penembusan tidak menemui *patch* baru yang diperbaharui untuk semua sistem perbankan		

(6 markah)

b) Lazimnya laporan pengurusan risiko dibangunkan untuk menyokong pihak pengurusan dalam membuat keputusan yang tepat mengenai anggaran, polisi dan prosedur. Jadual 2 memaparkan contoh laporan penilaian risiko yang terdiri dari informasi aset yang berisiko,

kegoyahan dan ancaman yang sesuai, impak ke atas infrastruktur IT dan cadangan kawalan. Apakah cadangan ancaman, impak dan kawalan yang paling sesuai untuk setiap aset dan kegoyahan?

Jadual 2: Laporan Penilaian Risiko

Aset Syarikat	Kegoyahan	Ancaman	Impak	Cadangan Ancaman
Pelayan	Sistem penyaman udara yang berusia 10 tahun			
Lamam Sesawang	*Firewall* tidak dikonfigurasi dengan betul			
Sistem Perkongsian Fail	Tidak ada *backup* secara berkala			

(9 markah)

c) Berikan definisi bagi terma-terma berikut:

i. Analisis Risiko
ii. Pengurusan Risiko Keselamatan
iii. Penerimaan Risiko
iv. Pelan Kontingensi
v. Pelan Pemulihan Bencana

(10 markah)

SOALAN 3 (25 MARKAH)

a) Profesor Adam adalah Ketua Pegawai Teknologi (CTO) di Cyber Intelligent 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. Rekabentuk senarai semak yang dikehendaki dan anda diminta untuk memberikan **LIMA (5)** item paling penting yang boleh dipertimbangkan untuk diaudit dengan memberikan **TIGA (3)** contoh untuk **SETIAP** item yang dipilih..

(20 markah)

b) Maklumat yang tidak tepat dalam laporan penilaian risiko keselamatan boleh menyebabkan akibat yang besar kepada postur keselamatan maklumat organisasi. Sebagai contoh, kekurangan fakta penting dalam laporan tersebut dapat menimbulkan masalah kepatuhan, kerugian besar, kerosakan reputasi dan gangguan beberapa ancaman. Berikan **LIMA (5)** elemen terbaik yang perlu ada di dalam laporan penilaian risiko keselamatan.

(5 markah)

SOALAN 4 (25 MARKAH)

a) Bincang **DUA (2)** objektif yang dapat diterapkan oleh juruaudit pengkomputeraan awan?

(4 markah)

b) Pengkomputeran awan sangat popular kerana teknologi ini memberi banyak faedah seperti penjimatan kos, skalabiliti, fleksibiliti, akses sejagat dan banyak lagi. Menyedari hakikat ini, Profesor Fatimah, Ketua Pegawai Eksekutif (CEO) di MyCloud Associate Berhad menggunakan teknologi ini untuk infrastruktur pengkomputeran syarikatnya. Profesor Fatimah telah mengarahkan anda untuk membuat senarai semak untuk tujuan mengaudit model pengkomputeraan awan pada setiap bidang fokus seperti perisian sebagai perkhidmatan (SaaS), platform sebagai perkhidmatan (PaaS), infrastruktur sebagai perkhidmatan (IaaS), virtualisasi, data pengurusan dan penyimpanan data, senarai kawalan capaian dan saluran komunikasi. Berikan senarai semak yang diperlukan. Senarai semak anda mesti mengandungi **TIGA (3)** contoh untuk **SETIAP** bidang fokus.

(21 markah)

- SOALAN TAMAT-

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

QUESTION 1 (25 MARKS)

a) Figure 1 illustrates the MySite Sdn Bhd network diagram. The company supplying a wide range of products including home appliances, electronics devices, sports equipment's and many more. To use their services, users need to access the company website which is available 24 hours via a computer, mobile phone or mobile device application via the internet. The entire data, such as the client's information, purchasing records, and many more are stored inside the database. The purchased product will be delivered after processing by the system administrator via the application server. Based on this scenario, solve question in **(i)**, **(ii)** and **(iii)**.

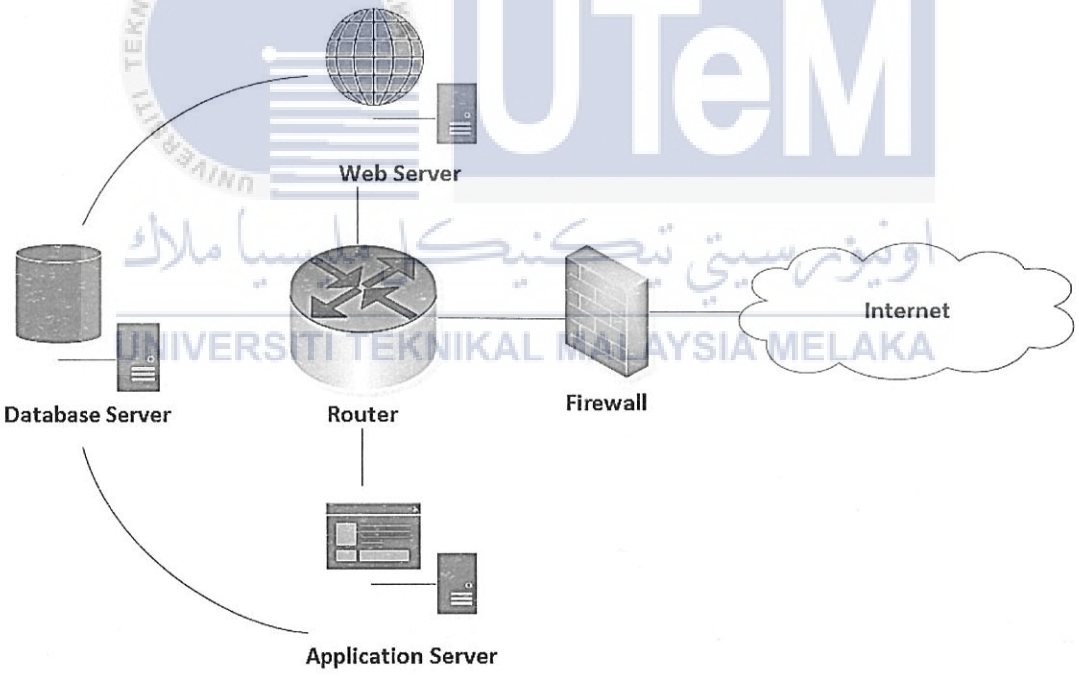


Figure 1: Mysite Sdn Bhd Network Diagram

(i) How can calculate Cost Benefit Analysis (CBA), Annualized Loss Expectancy (ALE) and Single Loss Expectancy (SLE) for Figure 1 scenario.

(6 marks)

(ii) The company website could be damaged by a cyber-attack and could cause huge losses. As an internal auditor for MySite Sdn Bhd, you have estimated the website server value at RM10, 000,000 and the exposure factor of such server could be damaged valued at 20%. Calculate the Single Loss Expectancy (SLE), Annualized Rate of Occurrence (ARO) and Annualized Loss Expectancy (ALE) if the successful act of cyber-attack is expected to occur about once every two years.

(9 marks)

(iii) Return of Investment (ROI) can be calculated by determining the cost of a potential risk and control. Usually an organization applies it for good measure of profitability. Lets assume, Mysite Sdn Bhd email systems is expected to get phished 3 times per year at an estimated cost of RM25,000 per successful attack. The cost to train employees and avoid phishing emails is expected to be RM15,000, while the reduction in probability of risk occurrence with the implemented control assumed at 75%. As such, calculate the ROI and determine how much your organization can be save per year by having awareness training to their employees.

(10 marks)

QUESTION 2 (25 MARKS)

a) Assume you are working as an internal auditor in the banking sector. Recently, you request an internal penetration tester to scan your banking system that comprises an employee attendance system, network system, and several servers at the data center. Throughout your analysis, you have found several vulnerabilities, which is associated with your banking system environment. Table 1 contains an example of vulnerability, threat sources and threat action that has been formed based on your observation as an internal auditor. Identify the potential threat source and threat action for each highlighted vulnerability in Table 1?

Table 1: Vulnerability, Threat Source and Threat Action

Vulnerability	Threat Source	Threat Action
Terminated employees' IDs are not removed from the database.		
Guest IDs enabled on the application server and firewall misconfigured to allow inbound Telnet.		
Penetration tester found no new patches updated for all banking systems.		

(6 marks)

b) Usually a risk management report is developed to support management in making appropriate decisions on budget, policies and procedures. Table 2 represents an example of a risk assessment report, which comprises information on assets at risk, corresponding vulnerabilities and threats, the impact of IT infrastructure and control recommendations.

Identify the potential threat, impact and control recommendations that most appropriate for each asset and exist vulnerability?

Table 2: Risk Assessment Report

Company Asset	Exist Vulnerability	Threat	Impact	Control Recommendations
Server	Air conditioning systems more than 10 years old			
Website	Firewall not configured properly			
Sharing file systems	No backup done regularly			

(9 marks)

c) Define the following terms:

i. Risk Analysis
ii. Security Risk Management
iii. Risk Acceptance
iv. Contingency Plan
v. Disaster Recovery Plan

(10 marks)

QUESTION 3 (25 MARKS)

c) Professor Adam is the Chief Technology Officer (CTO) at Cyber Intelligent 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 the checklist in the form of a table. Sketch the desired checklist and you are required to provide **FIVE (5)** most significant item that can be considered to audit by giving **THREE (3)** examples for **EACH** selected item.

(20 marks)

d) The inaccurate information in the security risk assessment report can cause huge consequences for the organization's information security posture. For instance, lacking an important facts on such report can create compliance issues, expensive losses, reputational damage and distraction of some threats. Give **FIVE (5)** best elements that must contain in the security risk assessment report.

(5 marks)

QUESTION 4 (25 MARKS)

a) Discuss **TWO (2)** objectives that can be applied by cloud computing auditors?

(4 marks)

b) Cloud computing is very popular as this technology provides benefit such as cost saving, scalability, flexibility, universal access and many more. Realizing this fact, Professor Fatimah the Chief Executive Officer (CEO) at MyCloud Associate Berhad adopted these technologies in her company computing infrastructure. Professor Fatimah has instructed you to develop a checklist for the purpose auditing the cloud model on each focus area such as software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS), virtualization, data management and data storage, access control list and communication channels. Provide the required checklist. Your checklist must contain **THREE (3)** examples for **EACH** focus area.

(21 marks)

-END OF QUESTIONS-