UNIVERSITI SAINS MALAYSIA

Second Semester Examination
2015/2016 Academic Session

June 2016

CST233 – Information Security & Assurance
[Keselamatan & Jaminan Maklumat]

Duration : 2 hours
[Masa : 2 jam]

INSTRUCTIONS TO CANDIDATE:
[ARAHAN KEPADA CALON:]

- Please ensure that this examination paper contains **FOUR** questions in **SEVEN** printed pages before you begin the examination.

  *[Sila pastikan bahawa kertas peperiksaan ini mengandungi **EMPAT** soalan di dalam **TUJUH** muka surat yang bercetak sebelum anda memulakan peperiksaan ini.]*

- Answer **ALL** questions.

  *[Jawab **SEMUA** soalan.]*

- You may answer the questions either in English or in Bahasa Malaysia.

  [Anda dibenarkan menjawab soalan sama ada dalam bahasa Inggeris atau bahasa Malaysia.]

- In the event of any discrepancies, the English version shall be used.

  [Sekiranya terdapat sebarang percanggahan pada soalan peperiksaan, versi bahasa Inggeris hendaklah diguna pakai.]

1. (a) It is important to balance the information security and access. In order to achieve the balance, the information system must be operated to satisfy the user and the professional security practitioner. In addition, the security level must also allow reasonable access and able to protect against threats.

Adalah penting untuk mengimbangi keselamatan maklumat dan capaian. Untuk mencapai keseimbangan, sistem maklumat hendaklah beroperasi untuk memuaskan pengguna dan pengamal keselamatan profesional. Tambahan pula, tahap keselamatan mestilah membenarkan capaian yang munasabah dan mampu untuk menghalang dari sebarang ancaman.

(i) Briefly explain **two** (**2**) major approaches used in information security implementation.

*Bincangkan dengan ringkas **dua** (**2**) pendekatan utama dalam implementasi keselamatan maklumat.*

(4/100)

(ii) Explain the aspect of logical design in the security systems development life cycle.

Terangkan aspek reka bentuk logik dalam kitar hayat pembangunan sistem.

(4/100)

(iii) What is the difference between champion and team leader in the information security project team?

Apakah perbezaan antara champion dan ketua kumpulan dalam sesebuah pasukan projek keselamatan maklumat?

(4/100)

(b) In today's organizations, protecting information is really important. To perform effectively, organization must ready with secure infrastructure and appropriate services that can cope with the size and scope of enterprise.

Dalam organisasi hari ini, melindungi maklumat adalah sangat penting. Untuk memastikan keberkesanannya, organisasi mesti bersedia dengan infrastruktur selamat dan perkhidmatan yang sesuai serta memenuhi saiz dan skop organisasi.

(i) Give **two** (**2**) reasons why human can be considered as the greatest threats to the organization?

*Nyatakan **dua** (**2**) sebab mengapa manusia boleh dianggap sebagai ancaman terbesar kepada organisasi?*

(4/100)

(ii) Briefly explain competitive intelligence.

Terangkan dengan ringkas kecerdasan kompetitif.

(2/100)

(iii) Differentiate between attack and vulnerability.

Bezakan antara serangan dan kerentanan.

(4/100)

(c) Describe TCP hijacking attack.

Jelaskan serangan rampasan TCP.

(3/100)

2. (a) Rasyid Hussin have total asset value of RM5,500,000 (based on the asset evaluation). It produces computer components to be exported. This company have 100 workers and mostly are foreign workers. The total cost of operation is estimated at RM 1 000 000 per year. Any deliberate act of sabotage or vandalism would take away 1/5 of the capability of his business. Assume that this incident might occur once in every 20 years.

Rasyid Hussin mempunyai jumlah asset yang bernilai RM5,500,000 (Berdasarkan penilaian aset). Ia menghasilkan komponen komputer untuk di eksport. Syarikat ini mempunyai 100 orang pekerja yang majoritinya adalah pekerja asing. Jumlah kos operasi adalah RM 1 000 000 setahun. Sebarang perbuatan sabotaj dengan sengaja atau vandalisme akan menghilangkan 1/5 dari keupayaan perniagaannya. Andaikan yang senario ini mungkin berlaku sekali dalam 20 tahun.

(i) Calculate the single loss expectancy (SLE).

Hitung jangkaan kerugian tunggal (SLE).

(3/100)

(ii) Calculate the annualized loss expectancy (ALE).

Hitung jangkaan kerugian setahun (ALE).

(3/100)

(iii) Given the ALE (post) value at RM25,000 and annualized cost of the safeguard (ACS) at RM15,000, calculate the cost benefit analysis (CBA).

Diberikan ALE (post) bernilai RM25,000 dan kos tahunan perlindungan (ACS) bernilai RM15,000, hitung analisis kos faedah (CBA).

(3/100)

(b) Policies are put in place to support the mission, vision and strategic planning of an organization. An information security policy provides rules for the protection of the information assets of the organization.

Polisi diletakkan pada tempatnya untuk menyokong misi, visi dan perancangan strategi bagi organisasi. Polisi keselamatan maklumat menyediakan peraturan untuk melindungi aset maklumat organisasi.

(i) Why best evidence rule is preferred as compared to hearsay rule?

Mengapakah aturan bukti terbaik adalah diutamakan berbanding aturan khabar angin?

(2/100)

(ii) Explain the need of Issue-Specific Security Policy (ISSP) in organization.

Terangkan keperluan Polisi Keselamatan Isu Spesifik (ISSP).

(2/100)

(iii) Describe the **three** (**3**) levels of control in information security safeguards.

*Terangkan **tiga** (**3**) aras kawalan bagi sistem kawal keselamatan maklumat.*

(6/100)

(c) An incident is any identified attack on the organization's information assets that would threaten the assets confidentiality, integrity and availability.

Sesuatu kejadian ialah sebarang serangan yang dikenal pasti terhadap maklumat aset organisasi yang boleh mengancam kerahsiaan, kewibawaan dan kebolehsediaan aset.

(i) Discuss **two** (**2**) suitable mitigation control plans that can be used based on the given scenario.

*Bincang **dua** (**2**) rancangan kawalan mitigasi yang sesuai yang boleh digunakan berdasarkan senario yang dinyatakan.*

(4/100)

(ii) How does tailgating jeopardize the company's security and privacy?

Bagaimana tailgating membahayakan keselamatan dan privasi syarikat?

(2/100)

3. (a) Explain the relationship among the untrusted network, the firewall, and the trusted network.

Terangkan hubungan antara rangkaian yang tak terpercaya, tembok api, dan rangkaian terpercaya.

(3/100)

(b) Explain what stateful inspection is and how is state information maintained during a network connection or transaction?

Terangkan apa yang dimaksudkan dengan pemeriksaan "stateful" dan bagaimana maklumat "state" dikekalkan semasa sambungan atau transaksi rangkaian?

(2/100)

(c) Write the firewall rules as shown in the following diagram.

Tuliskan peraturan tembok api seperti yang ditunjukkan dalam gambar rajah berikut.

		Source	Destination	Service	Interface	Direction	Action
0		firewall net-192.168.1.0	Any	Any	outside	Inbound	Deny
1		net-192.168.1.0	firewall	ssh	All	Both	Accept
2		Any	Any	Any	All	Both	Deny

(6/100)

(d) Explain how a Virtual Private Network (VPN) allows a remote user to securely connect to a business network. You must use a diagram to support your answer.

Terangkan bagaimana Rangkaian Persendirian Maya (VPN) membenarkan pengguna jauh untuk menyambung secara terlindung kepada rangkaian perniagaan. Anda mesti menggunakan gambar rajah untuk menyokong jawapan anda.

(3/100)

(e) Briefly describe how an access control list works with packet filtering.

Huraikan secara ringkas bagaimana senarai kawalan capaian berfungsi dengan penapisan paket.

(5/100)

(f) Describe the kind of data and information that are retrieved by using a packet sniffer.

Huraikan jenis data dan maklumat yang boleh didapati daripada penghidu paket.

(2/100)

(g) List **four** (**4**) types of attacks that can be carried out on a cryptosystems.

*Senaraikan **empat** (**4**) jenis serangan terhadap sistem kripto.*

(4/100)

4. (a) Explain the National Institute of Standards and Technology (NIST) Seven-Step Contingency Planning Process.

Terangkan Tujuh Langkah Proses Perancangan Kemungkinan oleh Institut Piawaian dan Teknologi Kebangsaan (NIST).

(4/100)

(b) Once a project is underway, it is managed using a process known as a negative feedback loop or cybernetic loop. Draw the flowchart for this loop.

Apabila projek sedang dijalankan, ianya diuruskan dengan menggunakan proses yang dikenali sebagai gelung maklum balas negatif atau gelung sibernetik. Lukiskan carta aliran untuk gelung ini.

(4/100)

(c) Describe the Bull's-Eye Model used for Information Security Project Planning.

Huraikan Model "Bull's-Eye" bagi Perancangan Projek Sekuriti Maklumat.

(5/100)

(d) List the functions performed by a security technician, and the key qualifications and requirements for the position.

Senaraikan fungsi keselamatan juruteknik, serta kelayakan utama dan keperluan untuk jawatan tersebut.

(6/100)

(e) Explain how the following domains is affected by security issues.

Terangkan bagaimana domain-domain berikut terjejas akibat isu-isu sekuriti.

(i) Mobile devices

Peranti mobil

(2/100)

(ii) Cloud Computing

Pengkomputeran Awan

(2/100)

(iii) Internet of Things

Internet Benda

(2/100)

- oooOooo -