Second Semester Examination
2016/2017 Academic Session

June 2017

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 **NINE** printed pages before you begin the examination.

  *[Sila pastikan bahawa kertas peperiksaan ini mengandungi **EMPAT** soalan di dalam **SEMBILAN** 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) (i) Why is information security a management problem?

Mengapa keselamatan maklumat adalah satu masalah pengurusan?

(2/100)

(ii) What can management do that technology cannot?

Apakah yang boleh dilakukan oleh pengurusan yang tidak boleh dibuat oleh teknologi?

(2/100)

(b) (i) Why data is the most important asset an organization possesses?

Mengapa data merupakan aset terpenting yang dimiliki oleh sesebuah organisasi?

(2/100)

(ii) What other assets in the organization require protection?

Apakah aset-aset lain dalam organisasi yang memerlukan perlindungan?

(2/100)

(iii) It is important to protect data in motion (transmission) and data at rest (storage). What **other states of data** are important to be protected?

*Ianya adalah mustahak melindungi data yang bergerak (pemancaran) dan data pegun (storan). Apakah **keadaan data yang lain** yang mustahak dilindungi?*

(1/100)

(iv) Which type of data is the most difficult to protect?

Yang mana satukah yang paling sukar dilindungi?

(1/100)

(c) (i) How does technology obsolescence constitute a threat to information security?

Bagaimanakah kelapukan teknologi menyumbang kepada satu ancaman kepada keselamatan maklumat?

(2/100)

(ii) Based on your answer in (c)(i), how can an organization mitigate the threat?

Berdasarkan jawapan anda di (c)(i), bagaimanakah sesebuah organisasi boleh dilindungi daripada ancaman?

(2/100)

(d) (i) Describe **four** (**4**) risk strategies for controlling risk.

*Terangkan **empat** (**4**) strategi risiko untuk mengawal risiko.*

(8/100)

(ii) Identify **three** (**3**) common methods of risk avoidance.

*Kenal pasti **tiga** (**3**) kaedah-kaedah yang biasa dalam pengelakan risiko.*

(3/100)

2. (a) Consider the information in the following table:

Pertimbangkan maklumat dalam jadual berikut:

XYZ Software Company, major threat categories for new applications development *Syarikat Perisian XYZ, kategori-kategori utama untuk pembangunan aplikasi baru*	Cost per Incident *Kos setiap Insiden*	Frequency of Occurrence *Kekerapan Kejadian*	SLE	ARO	ALE
Programmer mistakes *Kesilapan-kesilapan Pengaturcara*	$5,000	1 per week *1 per minggu*	5,000	52.0	$ 260,000
Loss of intellectual property *Kehilangan Hak milik Intelek*	$75,000	1 per year *1 per tahun*	75,000	1.0	$ 75,000
Software piracy *Cetak rompak Perisian*	$500	1 per week *1 per minggu*	500	52.0	$ 26,000
Theft of information (hacker) *Kecurian Maklumat (penggodam)*	$2,500	1 per quarter *1 per suku tahun*	2,500	4.0	$ 10,000
Theft of information (employee) *Kecurian Maklumat (pekerja)*	$5,000	1 per 6 months *1 per 6 bulan*	5,000	2.0	$ 10,000
Web defacement *Pencacatan Sesawang*	$500	1 per month *1 per bulan*	500	12.0	$ 6,000
Theft of equipment *Kecurian Peralatan*	$5,000	1 per year *1 per tahun*	5,000	1.0	$ 5,000
Virus, worms, Trojan horses *Virus, Cecacing, Kuda Trojan*	$1,500	1 per week *1 per minggu*	1,500	52.0	$ 78,000
Denial-of-service attacks *Serangan Nafi Khidmat*	$2,500	1 per quarter *1 per suku tahun*	2,500	4.0	$ 10,000
Earthquake *Gempa bumi*	$250,000	1 per 20 years *1 per 20 tahun*	250,000	0.05	$ 12,500
Flood *Banjir*	$250,000	1 per 10 years *1 per 10 tahun*	250,000	0.1	$ 25,000
Fire *Kebakaran*	$500,000	1 per 10 years *1 per 10 tahun*	500,000	0.1	$ 50,000

(i) How does XYZ Software Company arrive at the values in the above table?

Bagaimanakah Syarikat Perisian XYZ boleh memperoleh nilai-nilai dalam jadual di atas?

(1/100)

(ii) Describe the process of determining the cost per incident and frequency of occurrence.

Terangkan proses penentuan kos setiap insiden dan kekerapan kejadian.

(4/100)

(b) (i) What is the difference between a policy, a standard, and a practice?

Apakah perbezaan antara polisi, standard, dan amalan?

(3/100)

(ii) Based on The National Institute of Standards and Technology's (NIST) Special Publication 800-14, there are three types of information security policies.

Choose **one** (**1**) type of the information security policies, and **describe how** that type of the security policy will be used.

Berdasarkan kepada "The National Institute of Standards and Technology's (NIST) Special Publication 800-14", terdapat tiga jenis polisi keselamatan maklumat.

*Pilih **satu** (**1**) jenis daripada polisi-polisi keselamatan maklumat tersebut, dan **jelaskan bagaimana** jenis polisi keselamatan maklumat berkenaan akan digunakan.*

(3/100)

(iii) What type of policy would be needed to guide use of the Web, E-mail, and Office equipment for personal use?

Apakah jenis polisi yang diperlukan untuk membimbing penggunaan Sesawang, E-mel, dan peralatan Pejabat untuk kegunaan peribadi?

(2/100)

(c) SFRGCorp has asked you to recommend a strategy for detecting possible attacks on the network. SFRGCorp has hired a two-person security team. Part of their jobs will be to watch for signs that indicate an attack. SFRGCorp's development team builds web applications for customers and deploys them in a perimeter network. Each application will have a different network access pattern. One of SFRGCorp's concerns is that a detection system will trigger false alarms when a new customer application is deployed.

SFRGCorp meminta anda mencadangkan satu strategi untuk mengesan kemungkinan-kemungkinan serangan ke atas rangkaian. SFRGCorp telah melantik satu pasukan keselamatan yang terdiri dengan dua anggota. Sebahagian daripada kerja mereka adalah memantau tanda-tanda yang menunjukkan sesuatu serangan. Pasukan pembangun SFRGCorp membina aplikasi sesawang untuk pelanggan-pelanggan dan meletakkannya dalam satu perimeter rangkaian. Setiap aplikasi akan mempunyai satu corak capaian rangkaian yang berbeza. Salah satu daripada perkara yang diambil berat oleh SFRGCorp adalah satu sistem pengesan yang akan mencetus penggera-penggera palsu apabila suatu aplikasi pelanggan yang baru dipasang.

(i) What type of intrusion detection will you recommend? Explain why.

Apakah jenis pengesan pencerobohan yang akan anda cadangkan? Terangkan mengapa.

(2/100)

(ii) What would be the maintenance concern for this type of IDS?

Apakah yang akan menjadi pertimbangan penyelenggaraan untuk IDS jenis ini?

(1/100)

(iii) Would you recommend the use of a honeypot? If so, where would you position it?

Apakah anda akan mencadangkan penggunaan komputer madu? Jika demikian, di mana akan anda tempatkannya?

(2/100)

(d) You are a security consultant who has been called in to investigate an attack against a company's client database. The company will most likely prosecute the attacker if the identity of the attacker is discovered.

Anda adalah konsultan keselamatan yang telah dipanggil untuk menyiasat satu serangan terhadap pangkalan data satu syarikat pelanggan. Syarikat berkenaan hampir pasti akan mendakwa penyerang tersebut jika identitinya dapat dikenal pasti.

(i) Describe the importance of maintaining a chain of custody for all evidence.

Huraikan kepentingan memelihara rantaian penjagaan untuk kesemua bukti.

(2/100)

(ii) What precautions will you take prior to find evidence on the hard disk?

Apakah langkah-langkah beringat yang akan anda ambil sebelum cuba mencari bukti yang terdapat pada cakera keras?

(2/100)

(iii) When you arrive at the site, you find the customer has already shut down the system. What evidence have you lost?

Apabila anda sampai di tempat kejadian, anda dapati pelanggan telahpun membuat penutupan system. Apakah bukti yang anda hilang?

(1/100)

(iv) State areas you might check in determining if there is a rootkit or other type of malicious software hidden on the computer.

Nyatakan beberapa kawasan yang anda boleh semak untuk menentukan sama ada terdapat kit akar atau perisian perosak yang tersembunyi pada komputer berkenaan.

(2/100)

3. (a) Technical computer solutions that is properly implemented can improve on organization's ability to balance the frequent conflicting objectives of making information readily and to preserve the information confidentiality and integrity.

Penyelesaian komputer teknikal yang dilaksanakan secara teratur boleh mempertingkatkan keupayaan organisasi untuk mengimbangi objektif konflik yang kerap berlaku untuk memastikan maklumat tersedia serta memelihara kerahsiaan dan integriti.

(i) List **three (3)** types of authentication mechanisms that are widely used.

*Senaraikan **tiga** (**3**) jenis mekanisme pengesahan yang biasanya digunakan.*

(3/100)

(ii) Describe the functionalities of Network Address Translation (NAT) to provide layers of security.

Huraikan fungsi-fungsi Terjemahan Alamat Rangkaian (NAT) yang menyediakan lapisan-lapisan sekuriti.

(2/100)

(b) Firewall works by examining a data packet and performing a comparison with some predetermined logical rules. Based on the given table, answer the following questions.

Tembok api berfungsi untuk memeriksa paket data dan melakukan perbandingan dengan peraturan logik. Berdasarkan jadual yang diberi, jawab soalan-soalan yang berikut.

Source Address	Source port	Destination Address	Destination Port	Action
Any	Any	10.10.10.1	Any	Deny
Any	Any	10.10.10.2	Any	Deny
10.10.10.1	Any	Any	Any	Deny
10.10.10.2	Any	Any	Any	Deny

(i) State which firewall rule set can be applied.

Nyatakan peraturan tembok api yang boleh diaplikasikan.

(1/100)

(ii) Describe your answer based on the given answer in question 3(b)(i),

Huraikan jawapan anda berdasarkan jawapan yang diberikan dalam soalan 3(b)(i).

(2/100)

(iii) Explain the reasons on the need of a separate rule for each IP address.

Terangkan sebab-sebab keperluan terhadap peraturan pengasingan bagi setiap alamat IP.

(2/100)

(c) Biometric technologies are evaluated based on the three basic criteria. List **all three**.

*Teknologi biometrik dinilai berdasarkan tiga kriteria asas. Senaraikan **ketiga-tiganya**.*

(3/100)

(d) Cryptography is the process of making and using codes to secure the information transmission.

Kriptografi merupakan proses menjadikan dan menggunakan kod-kod untuk keselamatan penghantaran maklumat.

(i) Briefly explain the process of Public Key Infrastructure (PKI) to protect the information assets in the context of authentication and privacy.

Terangkan dengan ringkas proses Infrastruktur Kunci Awam (PKI) untuk menjaga aset maklumat dari konteks pengesahan dan kerahsiaan.

(4/100)

(ii) Briefly describe **two** (**2**) protocols that have been designed to enable secure network communications over the Internet.

*Huraikan secara ringkas **dua** (2) protokol yang telah direka bentuk untuk membolehkan komunikasi rangkaian keselamatan dalam talian.*

(4/100)

(iii) There are four layers of processes involve in the Bull's-Eye Model. Describe the policy layer and systems layer.

Terdapat empat lapisan dalam proses yang melibatkan "Bull's-Eye Model". Huraikan lapisan polisi dan lapisan sistem.

(4/100)

4. (a) Information security governance is an effective program that requires constant review.

Tadbir urus sekuriti maklumat merupakan program berkesan yang memerlukan kajian semula secara tetap.

(i) State **three** (**3**) reasons for the need for agencies to monitor the status of their program.

*Nyatakan **tiga** (**3**) sebab dari segi keperluan agensi untuk memantau status program yang direncanakan.*

(3/100)

(ii) Briefly describe the non-technical changes and technical changes in configuration and change management.

Huraikan secara ringkas perubahan bukan teknikal dan perubahan teknikal dalam konfigurasi dan pengurusan perubahan.

(2/100)

(iii) Draw a chart to illustrate the Security Maintenance Model.

Lukis satu carta untuk menggambarkan Model Penyenggaraan Sekuriti.

(5/100)

(b) Security training involves in providing members of the organization with detailed information and hands-on instruction to enable them to perform their duties securely.

Latihan sekuriti melibatkan penyediaan ahli-ahli dalam organisasi dengan maklumat yang terperinci dan arahan amali yang membolehkan mereka melaksanakan kerja secara selamat.

(i) Explain under what circumstances or conditions training become the most effective.

Terangkan dalam situasi atau keadaan yang menjadikan latihan sebagai kaedah yang paling berkesan.

(2/100)

(ii) Differentiate between Preventive Controls and Deterrent Controls.

Bezakan antara Kawalan Pencegahan dan Kawalan Halangan.

(4/100)

(c) Among all possible biometrics, only three can be considered as truly unique. State **all three**.

Antara semua kemungkinan biometrik, hanya tiga yang boleh dikategorikan benar-benar unik. Nyatakan **ketiga-tiganya**.

(3/100)

(d) Briefly explain the following terminologies.

Terangkan secara ringkas terminologi-terminologi yang berikut.

(i) Hash algorithms.

Algoritma cincangan.

(2/100)

(ii) Steganography.

Steganografi.

(2/100)

(iii) Encipher.

Ensifer.

(2/100)