SULIT

KEMENTERIAN PENDIDIKAN TINGGI
JABATAN PENDIDIKAN POLITEKNIK DAN KOLEJ KOMUNITI

BAHAGIAN PEPERIKSAAN DAN PENILAIAN
JABATAN PENDIDIKAN POLITEKNIK DAN KOLEJ KOMUNITI
KEMENTERIAN PENDIDIKAN TINGGI

JABATAN TEKNOLOGI MAKLUMAT & KOMUNIKASI

PEPERIKSAAN AKHIR

SESI II : 2024/2025

DFC20313 : CYBERSECURITY FUNDAMENTALS

TARIKH : 21 MEI 2025
MASA : 8.30 PAGI - 10.30 PAGI (2 JAM)

Kertas soalan ini mengandungi **DUA PULUH DUA (22)** halaman bercetak.
Bahagian A: Objektif (30 soalan)
Bahagian B: Struktur (2 soalan)

Dokumen sokongan yang disertakan : Tiada

JANGAN BUKA KERTAS SOALAN INI SEHINGGA DIARAHKAN

(CLO yang tertera hanya sebagai rujukan)

SECTION A : 45 MARKS
BAHAGIAN A : 45 MARKAH

INSTRUCTION:
This section consists of **THIRTY (30)** objective questions. Mark your answers in the OMR form provided.

ARAHAN :
*Bahagian ini mengandungi **TIGA PULUH (30)** soalan objektif. Tandakan jawapan anda di dalam borang OMR yang disediakan.*

CLO1 1. Select the type of cybersecurity that focuses on protecting software applications from external threats such as malware and unauthorized access.
Pilih jenis keselamatan siber yang memberi fokus kepada perlindungan aplikasi perisian daripada ancaman luaran seperti perisian hasad dan akses tanpa kebenaran.

A. Information Security.
Keselamatan maklumat.

B. Network Security.
Keselamatan rangkaian.

C. Application Security.
Keselamatan aplikasi.

D. Operational Security.
Keselamatan Operasi.

CLO1 2. Identify the goal of information security.
Kenal pasti matlamat keselamatan maklumat.

A. Ensuring system availability.
Memastikan ketersediaan sistem.

B. Protecting data confidentiality, integrity, and availability.
Melindungi kerahsiaan, integriti dan ketersediaan data.

C. Preventing unauthorized network access.
Menghalang capaian rangkaian tanpa kebenaran.

D. Securing software application.
Melindungi aplikasi perisian.

CLO1

3. Select the **CORRECT** focus of integrity in cybersecurity.
*Pilih fokus integriti yang **BETUL** dalam keselamatan siber.*

A. Maintaining data confidentiality from unauthorized users.
Mengekalkan kerahsiaan data daripada pengguna yang tidak dibenarkan.

B. Ensuring data accuracy and protection from unauthorized changes.
Memastikan ketepatan dan perlindungan data daripada perubahan yang tidak dibenarkan.

C. Providing continuous system availability to authorized users.
Menyediakan ketersediaan sistem yang berterusan kepada pengguna yang sah.

D. Encrypting communication between connected devices.
Menyulitkan komunikasi antara peranti yang bersambung.

CLO1

4. Identify the hacker who uses his skills to improve security by identifying and mitigating vulnerabilities with permission.
Kenal pasti penggodam yang menggunakan kemahirannya untuk meningkatkan keselamatan dengan mengenal pasti dan mengurangkan kelemahan dengan kebenaran.

A. White hat hacker.
Penggodam topi putih.

B. Black hat hacker.
Penggodam topi hitam.

C. Grey hat hacker.
Penggodam topi kelabu.

D. Script Kiddies.
Script Kiddies

CLO1 5. Select the **CORRECT** security attack that involves unauthorized changes or disruptions to system operations.
*Pilih serangan keselamatan yang **BETUL** yang melibatkan perubahan tanpa kebenaran atau gangguan pada operasi sistem.*

A. Distribution attacks.
Serangan pengedaran.

B. Passive attacks.
Serangan pasif.

C. Active attacks.
Serangan aktif.

D. Insider attacks.
Serangan orang dalam.

CLO1 6. Identify reconnaissance attacks in the context of cyber operation.
Kenal pasti serangan peninjauan dalam konteks operasi siber.

A. To exploit vulnerabilities in a system for unauthorized access.
Untuk mengeksploitasi kelemahan dalam sistem untuk akses tanpa kebenaran.

B. To gather detailed information about a target's systems and network.
Untuk mengumpul maklumat terperinci tentang sistem dan rangkaian sasaran.

C. To disrupt the availability of a network or system.
Untuk mengganggu ketersediaan rangkaian atau sistem.

D. To execute a phishing campaign for credential harvesting.
Untuk melaksanakan kempen pancingan data untuk penuaian kelayakan.

CLO1 | 7. Identify the **MAIN** objective of a shoulder surfing attack.
*Kenal pasti objektif **UTAMA** serangan peluncuran bahu.*

A. To intercept wireless communications.
Untuk memintas komunikasi tanpa wayar.

B. To visually obtain sensitive information without technical tools.
Untuk mendapatkan maklumat sensitif secara visual tanpa alat teknikal.

C. To install keylogging software on a target device.
Untuk memasang perisian keylogging *pada peranti sasaran.*

D. To exploit vulnerabilities in network configurations.
Untuk mengeksploitasi kelemahan dalam konfigurasi rangkaian.

CLO1 | 8. Select the method which computer-based social engineering attack is designed to gain unauthorized access to sensitive systems.
Pilih kaedah serangan kejuruteraan sosial berasaskan komputer yang direka bentuk untuk mendapatkan akses tanpa kebenaran kepada sistem sensitif.

A. Shoulder surfing to view a password
Peluncuran bahu untuk melihat kata laluan.

B. A trojan malware disguised as legitimate software
Satu perisian hasad trojan yang menyamar sebagai perisian yang sah.

C. A fake login page imitating a trusted service
Halaman log masuk palsu meniru perkhidmatan yang dipercayai

D. Listening to public conversations for sensitive details
Mendengar perbualan awam untuk mendapatkan butiran sensitif.

CLO1 9. Select the correct description of the delivery phase function within the Cyber Kill Chain.
Pilih pernyataan yang betul mengenai fungsi fasa penghantaran Cyber Kill Chain.

A. It is the easiest phase to detect and interrupt the attack.
Ia adalah fasa paling mudah untuk mengesan dan mengganggu serangan.

B. It determines the time required for attackers to deploy their payload.
Ia menentukan masa yang diperlukan untuk penyerang menggunakan muatan mereka.

C. It allows attackers to bypass all existing defenses in one attempt.
Ia membolehkan penyerang memintas semua pertahanan sedia ada dalam satu percubaan.

D. It ensures attackers gain immediate access to privileged accounts.
Ia memastikan penyerang mendapat akses segera ke akaun istimewa.

CLO1 10. Identify the advantage of implementing a demilitarized zone (DMZ) in a network topology.
Kenal pasti kelebihan melaksanakan zon demilitarized (DMZ) dalam topologi rangkaian.

A. It provides redundancy to ensure high availability of internal servers.
Ia menyediakan lebihan untuk memastikan ketersediaan tinggi pelayan dalaman.

B. It isolates external-facing services to limit exposure of internal resources.
Ia mengasingkan perkhidmatan yang menghadap luaran untuk menghadkan pendedahan sumber dalaman.

C. It enhances network throughput by prioritizing critical traffic.
Ia meningkatkan daya pemprosesan rangkaian dengan mengutamakan trafik kritikal.

D. It eliminates the need for internal firewalls in a secure network.
Ia menghapuskan keperluan untuk tembok api dalaman dalam rangkaian selamat.

CLO1 | 11. Select the **BEST** method to prevent unauthorized access to other users' workstations in a secured area.
*Pilih kaedah **TERBAIK** untuk menghalang daripada akses ke stesen kerja pengguna lain di dalam kawasan yang selamat.*

A. Require biometric identification for user logins.
Memerlukan pengenalan biometrik untuk log masuk pengguna.

B. Require a username and a password for user logins.
Memerlukan nama pengguna dan kata laluan untuk log masuk pengguna.

C. Enforce a policy that requires passwords to be changed every 30 days.
Menguatkuasakan dasar yang memerlukan kata laluan ditukar setiap 30 hari.

D. Install security cameras in secure areas to monitor logins.
Pasang kamera keselamatan di kawasan selamat untuk memantau log masuk.

CLO1 | 12. Identify an action does that IDS typically take when it detects suspicious activity.
Kenal pasti tindakan yang biasanya diambil oleh IDS apabila ia mengesan aktiviti yang mencurigakan.

A. Automatically blocks the threat.
Menyekat ancaman secara automatik.

B. Disconnect the affected device from the network.
Memutuskan sambungan peranti yang terjejas daripada rangkaian.

C. Install updates to fix the vulnerability.
Memasang kemas kini untuk membetulkan kelemahan.

D. Send an alert to administrators or logs the activity.
Menghantar makluman kepada pentadbir atau merekodkan aktiviti.

CLO1 | 13. Select the solution that best explains how brute-force attack attempts against an organization's system can be detected.
Pilih penyelesaian yang paling tepat menjelaskan cara mengesan percubaan serangan brute-force *terhadap sistem organisasi.*

A. Monitoring by security guards to detect unauthorized physical access attempts.
Pemantauan oleh pengawal keselamatan untuk mengesan percubaan akses fizikal tanpa kebenaran.

B. Installation of locks to physically restrict unauthorized entry.
Pemasangan kunci untuk mengehadkan kemasukan fizikal tanpa kebenaran.

C. Using access cards to control and record entry into secured areas.
Penggunaan kad akses untuk mengawal dan merekod kemasukan ke kawasan terkawal.

D. Deploying an Intrusion Detection System (IDS) to identify repeated login attempts and alert administrators.
Penggunaan Sistem Pengesan Pencerobohan (IDS) *untuk mengenal pasti percubaan log masuk berulang kali dan memberi amaran kepada pentadbir.*

CLO1 | 14. Select the key feature of a VPN.
Pilih ciri utama VPN.

A. Encrypting data transmitted over the network.
Menyulitkan data yang dihantar melalui rangkaian.

B. Blocking all malware automatically.
Menyekat semua perisian hasad secara automatik.

C. Providing free internet access.
Menyediakan akses internet percuma.

D. Improving hardware performance.
Meningkatkan prestasi perkakasan.

CLO1

15. John wants to monitor malicious activity across multiple systems on a network. He sets up systems to capture attack tools and record all attacks. Determine the type of system he has set up.
John ingin memantau aktiviti berniat jahat merentas berbilang sistem pada rangkaian. Dia menyediakan sistem untuk menangkap alat serangan dan ingin merekod semua serangan. Kenal pasti jenis sistem yang telah dia sediakan.

A. Honeypot

B. Firewall

C. Intrusion detection system (IDS)

D. Virtual private network (VPN)

CLO1

16. Identify the key aspect of information security policy governance and management that organizations need to understand.
Kenal pasti aspek utama dalam tadbir urus dan pengurusan dasar keselamatan maklumat yang perlu difahami oleh organisasi.

A. Budgeting for office renovations.
Menganggarkan bajet untuk pengubahsuaian pejabat.

B. Increasing social media presence.
Meningkatkan keberadaan di sosial media.

C. Developing creative marketing campaigns.
Membangunkan kempen pemasaran kreatif.

D. Compliance with information security laws and regulations.
Pematuhan terhadap undang-undang dan peraturan keselamatan maklumat.

CLO1 17. Relate which option is considered a key component of Malaysia's national security framework:
Kenal pasti pilihan yang dianggap sebagai komponen utama dalam kerangka keselamatan negara Malaysia:

A. Cybersecurity.
Keselamatan siber.

B. Environmental protection.
Perlindungan alam sekitar.

C. Cultural preservation.
Pemeliharaan budaya.

D. Economic sanctions.
Sekatan ekonomi.

CLO1 18. Identify the effective measure to protect sensitive information from breaches by selecting the most critical procedure.
Tunjukkan langkah yang paling berkesan untuk melindungi maklumat sensitif daripada pelanggaran dengan memilih prosedur yang paling kritikal.

A. Data sharing.
Perkongsian Data.

B. Regular security audits.
Audit keselamatan berkala.

C. Data encryption.
Penyulitan data.

D. Access Control.
Kawalan akses.

CLO1 19. Select the key components of an effective security policy to the overall security posture of an organization.
Pilih komponen utama polisi keselamatan yang berkesan kepada keselamatan keseluruhan organisasi.

A. Clearly defined roles and responsibilities
Menetapkan peranan dan tanggungjawab dengan jelas

B. Comprehensive risk assessment procedures
Prosedur penilaian risiko yang menyeluruh

C. Regular policy review and updates
Semakan dan kemas kini polisi keselamatan secara berkala

D. User awareness and training programs
Program kesedaran dan latihan pengguna

CLO1 20. Choose the **CORRECT** principle outlined in the Personal Data Protection Act (PDPA) 2010 in Malaysia:
*Pilih prinsip yang **BETUL** yang dinyatakan dalam Akta Perlindungan Data Peribadi (PDPA) 2010 di Malaysia:*

i. Notice and Choice
Notis dan Pilihan

ii. Data Integrity
Integriti Data

iii. Data Minimization
Pengurangan Data

iv. Big Data
Data Raya

A. iii only / *iii sahaja*

B. i and ii / *i dan ii*

C. i, ii and iii / *i, ii dan iii*

D. i, iii and iv / *i, iii dan iv*

CLO1 21. Identifying a key feature of the Malaysia Cybersecurity Bill.
Kenal pasti ciri utama bagi Malaysia Cybersecurity Bill.

A. Mandatory encryption for all personal data.
Penyulitan mandatori untuk semua data peribadi.

B. Establishment of a national cybersecurity agency.
Penubuhan agensi siber keselamatan kebangsaan.

C. Prohibition of all online communications.
Larangan semua komunikasi dalam talian.

D. Regulation of online gaming.
Peraturan permainan dalam talian.

CLO1 22. In an information security governance framework, user privileges are defined to ensure compliance with organizational policies and security principles. Determine how the principle of least privilege reduces the risks of unauthorized access and consider the potential trade-offs it may bring in terms of operational efficiency and user experience.
Dalam rangka kerja tadbir urus keselamatan maklumat, hak pengguna ditentukan untuk memastikan pematuhan terhadap dasar organisasi dan prinsip keselamatan. *Tentukan bagaimana prinsip keistimewaan minimum dapat mengurangkan risiko akses tanpa kebenaran dan pertimbangkan kemungkinan kompromi yang mungkin timbul dari segi kecekapan operasi dan pengalaman pengguna.*

A. It ensures that only authorized individuals can access sensitive information, but strict access controls might slow down operations
Ia memastikan hanya individu yang diberi kebenaran dapat mengakses maklumat sensitif, tetapi kawalan akses yang ketat mungkin melambatkan operasi

B. It improves system performance by reducing resource loads, but it could compromise the confidentiality of sensitive data
Ia meningkatkan prestasi sistem dengan mengurangkan beban pada sumber, tetapi mungkin menjejaskan kerahsiaan maklumat sensitif

C. It simplifies the user experience by allowing broader access, but this reduces the organization's ability to hold users accountable for data misuse
Ia memudahkan pengalaman pengguna dengan membenarkan akses yang lebih meluas, tetapi ini mengurangkan keupayaan organisasi untuk memastikan pengguna bertanggungjawab terhadap penyalahgunaan data

D. It makes collaboration easier for all users, but granting excessive access rights may increase the risk of data breaches
Ia memudahkan kerjasama untuk semua pengguna, tetapi memberikan hak akses yang berlebihan mungkin meningkatkan risiko pelanggaran data

CLO1

23. Determine the primary objective of Malaysia's National Security Policy. Which of the following best aligns with its goals?
Tentukan objektif utama Dasar Keselamatan Negara Malaysia. Yang manakah antara berikut paling selaras dengan matlamatnya?

A. To promote economic growth.
Untuk mempromosikan pertumbuhan ekonomi.

B. To ensure national sovereignty and territorial integrity.
Untuk memastikan kedaulatan negara dan integriti wilayah.

C. To enhance international relations.
Untuk meningkatkan hubungan antarabangsa.

D. To support cultural diversity.
Untuk menyokong kepelbagaian budaya.

CLO1

24. National security efforts require effective coordination among various government agencies to address threats and ensure the safety of the nation. Based on the National Security Policy, analyze the role of different agencies and determine which one holds the primary responsibility for leading and coordinating these efforts. Choose your answer by considering their scope of authority and responsibilities.
Usaha keselamatan negara memerlukan penyelarasan yang berkesan di antara pelbagai agensi kerajaan untuk menangani ancaman dan memastikan keselamatan negara terjamin. Berdasarkan Dasar Keselamatan Negara, analisis peranan pelbagai agensi dan tentukan agensi manakah yang memegang tanggungjawab utama untuk mengetuai dan menyelaras usaha-usaha ini. Pilih jawapan anda dengan mempertimbangkan skop kuasa dan tanggungjawab mereka.

A. Ministry of Finance – Responsible for managing the nation's financial resources, but its role in national security is limited to budget allocations and economic stability
Kementerian Kewangan – Bertanggungjawab dalam mengurus sumber kewangan negara, tetapi peranannya dalam keselamatan negara terhad kepada peruntukan bajet dan kestabilan ekonomi

B. Royal Malaysian Police – Plays a key role in maintaining public order and enforcing laws but does not lead national-level security coordination
Polis Diraja Malaysia – Memainkan peranan penting dalam mengekalkan ketenteraman awam dan penguatkuasaan undang-undang, tetapi tidak mengetuai penyelarasan keselamatan di peringkat kebangsaan

C. National Security Council – Functions as the main agency responsible for planning, coordinating, and implementing national security strategies across various sectors
Majlis Keselamatan Negara – Berfungsi sebagai agensi utama yang bertanggungjawab dalam merancang, menyelaras, dan melaksanakan strategi keselamatan negara merentasi pelbagai sektor

D. CyberSecurity Malaysia – Focuses on cybersecurity threats and initiatives but does not oversee overall national security coordination
CyberSecurity Malaysia – *Memberi tumpuan kepada ancaman dan inisiatif keselamatan siber tetapi tidak menyelia penyelarasan keselamatan negara secara keseluruhan.*

CLO1

25. A financial institution in Malaysia has recently faced a cyberattack that compromised customer data. As a risk management officer, you are tasked with assessing the situation using the Risk Management in Technology (RMIT) framework by Bank Negara Malaysia. Determine the specific step you would take to identify the vulnerabilities that contributed to the breach.
Sebuah institusi kewangan di Malaysia baru-baru ini menghadapi serangan siber yang membahayakan data pelanggan. Sebagai pegawai pengurusan risiko, anda ditugaskan untuk menilai situasi tersebut menggunakan rangka kerja Pengurusan Risiko dalam Teknologi (RMIT) oleh Bank Negara Malaysia. Tentukan langkah khusus yang akan anda ambil untuk mengenal pasti kerentanan yang menyumbang kepada pelanggaran tersebut.

A. Conduct a post-incident review and analyze the attack vector.
Melakukan semakan selepas insiden dan menganalisis vektor serangan.

B. Increase marketing efforts to regain customer trust.
Meningkatkan usaha pemasaran untuk mendapatkan kembali kepercayaan pelanggan.

C. Implement a new customer service protocol.
Melaksanakan protokol perkhidmatan pelanggan yang baru.

D. Focus solely on improving physical security measures.
Memfokuskan sepenuhnya kepada peningkatan langkah keselamatan fizikal.

CLO1

26. The XYZ university has implemented end-to-end encryption for communications between its central database and the student portal. Choose the **CORRECT** method of this encryption.
*Universiti XYZ telah melaksanakan penyulitan hujung ke hujung untuk komunikasi antara pangkalan data pusatnya dan portal pelajar. Pilih aplikasi yang **BETUL** bagi kaedah penyulitan ini.*

A. Encrypting all student data stored on the university's servers to prevent unauthorized access.
Menyulitkan semua data pelajar yang disimpan pada pelayan-pelayan universiti untuk mengelakkan akses tanpa kebenaran.

B. Implementing encryption keys at both the database and student portal to secure transmitted data.
Melaksanakan kekunci-kekunci penyulitan pada kedua-dua pangkalan data dan portal pelajar untuk melindungi data yang dihantar.

C. Limiting access to the student portal using two-factor authentication for students and faculty.
Mengehadkan akses kepada portal pelajar menggunakan pengesahan dua faktor untuk pelajar-pelajar dan fakulti.

D. Monitoring network traffic for suspicious activity to detect potential intrusions.
Memantau trafik rangkaian bagi aktiviti yang mencurigakan untuk mengesan kemungkinan pencerobohan.

CLO1

27. Identify the **ACCURATE** definition of regulations.
*Kenal pasti definisi peraturan yang **TEPAT**.*

A. General principles for behaviour.
Prinsip-prinsip umum untuk tingkah laku.

B. Detailed rules and guidelines for implementing laws.
Peraturan-peraturan dan garis panduan terperinci untuk melaksanakan undang-undang.

C. A framework for chaos.
Rangka kerja untuk huru-hara.

D. A list of prohibited actions.
Senarai tindakan- tindakan yang dilarang.

CLO1 28. Select the purpose of data minimization in Privacy Law.
Pilih tujuan pengecilan data dalam Undang-undang Privasi.

A. To ignore data security.
Untuk mengabaikan keselamatan data.

B. To collect as much data as possible.
Untuk mengumpul data sebanyak mungkin.

C. To only collect necessary personal information.
Hanya mengumpul maklumat peribadi yang diperlukan.

D. To share data with third parties.
Untuk berkongsi data dengan pihak- pihak ketiga.

CLO1 29. Identify the role of the World Trade Organization (WTO).
Kenal pasti peranan Pertubuhan Perdagangan Dunia (WTO).

A. To regulate government agencies.
Untuk mengawal selia agensi kerajaan.

B. To protect intellectual property.
Untuk melindungi harta intelek.

C. To govern international trade.
Untuk mentadbir perdagangan antarabangsa.

D. To enforce criminal laws.
Untuk menguatkuasakan undang-undang jenayah.

CLO1

30. Select the statement that best describes the purpose of conducting information security awareness and training programs within an organization.
Pilih pernyataan yang paling tepat menjelaskan tujuan melaksanakan program kesedaran dan latihan keselamatan maklumat dalam sesebuah organisasi.

A. To provide insights into the latest security technologies and techniques. To introduce employees to the latest security technologies and methods available in the market.
Untuk memperkenalkan pekerja kepada teknologi dan kaedah keselamatan terkini yang terdapat di pasaran.

B. To safeguard organizations' information systems and resources from threats. To protect the organization's information systems and resources against security threats.
Untuk melindungi sistem maklumat dan sumber organisasi daripada ancaman keselamatan.

C. To foster a cybersecurity culture within organization. To encourage employees to adopt cybersecurity practices and attitudes as part of their daily routine.
Untuk menggalakkan pekerja mengamalkan sikap dan amalan keselamatan siber sebagai sebahagian daripada rutin harian mereka.

D. To ensure IT personnel are competent in working with sensitive data. To ensure IT personnel have adequate skills to handle sensitive organizational data securely.
Untuk memastikan kakitangan IT mempunyai kemahiran mencukupi dalam mengendalikan data sensitif organisasi secara selamat.

SECTION B : 55 MARKS

BAHAGIAN B : 55 MARKAH

INSTRUCTION:
This section consists of **TWO (2)** structured questions. Answer **ALL** questions.

ARAHAN:
*Bahagian ini mengandungi **DUA (2)** soalan berstruktur. Jawab **semua** soalan.*

QUESTION 1

SOALAN 1

CLO1 (a)(i) List **FOUR (4)** sources of security threats.
*Senaraikan **EMPAT (4)** sumber ancaman keselamatan.*

[4 marks]
[4 markah]

CLO1 (a)(ii) Describe **TWO (2)** types of security threats.
*Terangkan **DUA (2)** jenis ancaman keselamatan.*

[3 marks]
[3 markah]

CLO1 (b)(i) List **THREE (3)** types of attack. [3 marks]
Senaraikan 3 jenis serangan. *[3 markah]*

CLO1 (b)(ii) Explain **TWO (2)** types of social engineering with an example. [5 mark]
*Terangkan **DUA (2)** jenis kejuruteraan sosial beserta contoh.* *[5 markah]*

CLO1 (c)(i) List **TWO (2)** roles of a firewall in network security.
*Senaraikan **DUA (2)** peranan firewall dalam keselamatan rangkaian.*

[2 marks]
[2 markah]

CLO1 (c)(ii) Explain about **TWO (2)** security hardening in application
*Terangkan tentang **DUA (2)** pengerasan keselamatan dalam aplikasi*

[4 marks]
[4 markah]

CLO1 (c)(iii) Discuss the cybersecurity implications and law enforcement challenges related to the misuse of VPNs that can be exploited for malicious activities, such as cybercrime.
Bincangkan implikasi keselamatan siber dan cabaran penguatkuasaan undang-undang berkaitan dengan penyalahgunaan VPN yang boleh dieksploitasi untuk aktiviti jahat, seperti jenayah siber.

[4 marks]
[4 markah]

QUESTION 2

SOALAN 2

(a) A company, WebPanel Solutions, provides a web panel service that allows customers to manage their online accounts and access various features. As part of their security assessment, the company needs to identify potential risks that could affect their service and customer data.

Syarikat WebPanel Solutions, menyediakan perkhidmatan panel web bagi membolehkan pelanggan untuk menguruskan akaun di atas talian dan juga capaian kepada pelbagai ciri. Dalam sebahagian daripada penilaian keselamatan, syarikat tersebut perlu mengenalpasti potensi risiko yang boleh mempengaruhi perkhidmatan dan data pelanggan mereka.

CLO1 (a)(i) Identify the **TWO (2)** methods the company could use to identify risks.
*Kenal pasti **DUA (2)** kaedah yang boleh digunakan oleh syarikat untuk mengenal pasti risiko.*

[7 marks]
[7 markah]

CLO1 (a)(ii) Summarize **TWO (2)** types of risks that WebPanel Solutions might encounter in their operations.
*Rumuskan **DUA (2)** jenis risiko yang mungkin dihadapi oleh WebPanel Solutions dalam operasi mereka.* [7 marks]
[7 markah]

CLO1 (a)(iii) Construct the necessity of continuous security assessments for WebPanel Solutions in the face of evolving cyber threats. In your response, discuss how the company can adapt its security measures based on assessment outcomes, focusing on the following aspects: the dynamic threat landscape, proactive risk management, regulatory compliance, and cost-effectiveness.

Bina keperluan untuk penilaian keselamatan berterusan bagi WebPanel Solutions dalam menghadapi ancaman siber yang semakin berkembang. Dalam jawapan anda, bincangkan bagaimana syarikat dapat menyesuaikan langkah-langkah keselamatannya berdasarkan hasil penilaian, dengan memberi tumpuan kepada aspek berikut: landskap ancaman yang dinamik, pengurusan risiko proaktif, pematuhan peraturan, dan keberkesanan kos.

[8 marks]

[8 markah]

CLO1 (b) A mid-sized organization has recently experienced a data breach caused by employee negligence and insufficient understanding of cybersecurity protocols. The breach exposed sensitive customer information, raising concerns about compliance with data protection laws and the need for a robust information assurance strategy. Explain **FOUR (4)** security awareness and training programs to mitigate future risks.

Sebuah organisasi bersaiz sederhana baru-baru ini mengalami pelanggaran data yang disebabkan oleh kecuaian pekerja dan pemahaman yang tidak mencukupi tentang protokol keselamatan siber. Pelanggaran itu mendedahkan maklumat pelanggan yang sensitif, menimbulkan kebimbangan tentang pematuhan undang-undang perlindungan data dan keperluan untuk strategi jaminan maklumat yang mantap.

*Terangkan **EMPAT (4)** program kesedaran dan latihan keselamatan untuk mengurangkan risiko- risiko pada masa hadapan.*

[8 marks]

[8 markah]

SOALAN TAMAT