BCS.CISMP-V9.by.Antony.42q

Number: CISMP-V9
Passing Score: 800
Time Limit: 120
File Version: 4.0

Exam Code: CISMP-V9

Exam Name: BCS Foundation Certificate In Information Security Management Principles V9.0

Exam A

QUESTION 1
What form of risk assessment is MOST LIKELY to provide objective support for a security Return on Investment case?

A. ISO/IEC 27001.
B. Qualitative.
C. CPNI.
D. Quantitative

Correct Answer: D
Section:
Explanation:
Quantitative risk assessment is the process of objectively measuring risk by assigning numerical values to the probability of an event occurring and its potential impact. This method is most likely to provide objective support for a security Return on Investment (ROI) case because it allows for the calculation of potential losses in monetary terms, which can be directly compared to the cost of implementing security measures. By quantifying risks and their financial implications, organizations can make informed decisions about where to allocate resources and how to prioritize security investments to maximize ROI. This approach is particularly useful when making a business case to stakeholders who require clear, financial justification for security expenditures.

QUESTION 2
Why might the reporting of security incidents that involve personal data differ from other types of security incident?

A. Personal data is not highly transient so its 1 investigation rarely involves the preservation of volatile memory and full forensic digital investigation.
B. Personal data is normally handled on both IT and non-IT systems so such incidents need to be managed in two streams.
C. Data Protection legislation normally requires the reporting of incidents involving personal data to a Supervisory Authority.
D. Data Protection legislation is process-oriented and focuses on quality assurance of procedures and governance rather than data-focused event investigation

Correct Answer: C
Section:
Explanation:
The reporting of security incidents involving personal data is distinct from other types of incidents primarily due to the legal obligations imposed by data protection legislation. Such laws typically mandate that organizations report certain types of breaches involving personal data to a Supervisory Authority within a specified timeframe. This requirement is in place to ensure prompt and appropriate response to potential privacy risks affecting individuals' rights and freedoms. Failure to comply can result in significant penalties for the organization.The reporting process also often includes notifying affected individuals, especially if there is a high risk of adverse effects on their rights and freedoms12.
The UK GDPR and the Data Protection Act 2018 outline the duty of organizations to report certain personal data breaches to the relevant supervisory authority, such as the ICO, within 72 hours of becoming aware of the breach1.
The ICO's guide on personal data breaches provides detailed instructions on how to recognize a breach, the reporting process, and the importance of having robust breach detection, investigation, and internal reporting procedures12.

QUESTION 3
A system administrator has created the following 'array' as an access control for an organisation.
Developers: create files, update files.
Reviewers: upload files, update files.
Administrators: upload files, delete fifes, update files.
What type of access-control has just been created?

A. Task based access control.
B. Role based access control.
C. Rule based access control.
D. Mandatory access control.

Correct Answer: B
Section:
Explanation:
The access control method described is Role-Based Access Control (RBAC). In RBAC, access permissions are based on the roles within an organization, and users are assigned to these roles based on their responsibilities and qualifications. Each role has a defined set of access permissions to perform certain operations. This method simplifies management and ensures that only authorized users can perform actions relevant to their role. For instance, 'Developers' can create and update files, 'Reviewers' can upload and update files, and 'Administrators' have the rights to upload, delete, and update files. This aligns with the RBAC model where permissions are grouped by role rather than by individual user, making it easier to manage and audit.

QUESTION 4
How does the use of a 'single sign-on' access control policy improve the security for an organisation implementing the policy?

A. Password is better encrypted for system authentication.
B. Access control logs are centrally located.
C. Helps prevent the likelihood of users writing down passwords.
D. Decreases the complexity of passwords users have to remember.

Correct Answer: C
Section:
Explanation:

Single sign-on (SSO) is an access control policy that allows users to authenticate with multiple applications and services by logging in only once. This approach improves security by reducing the number of credentials users must manage, which in turn decreases the likelihood of users writing down passwords. When users have to remember multiple complex passwords, they are more likely to write them down, use simple passwords, or repeat the same password across different services, all of which are security risks. SSO simplifies the login process, which can lead to stronger, unique passwords and reduce the risk of password-related breaches.

QUESTION 5
In terms of security culture, what needs to be carried out as an integral part of security by all members of an organisation and is an essential component to any security regime?

A. The 'need to known principle.
B. Verification of visitor's ID
C. Appropriate behaviours.
D. Access denial measures

Correct Answer: C
Section:
Explanation:
The concept of a security culture within an organization emphasizes that security is not solely a technical issue but also a behavioral one. Appropriate behaviors are essential because they embody the organization's values and beliefs about security. These behaviors ensure that all members of the organization understand and adhere to security policies and procedures, thereby reducing risk and reinforcing the security regime. This includes following the 'need to know' principle, verifying IDs, and implementing access denial measures, but it is the appropriate behaviors that integrate these actions into a coherent and effective security culture.

QUESTION 6
What advantage does the delivery of online security training material have over the distribution of printed media?

A. Updating online material requires a single edit. Printed material needs to be distributed physically.
B. Online training material is intrinsically more accurate than printed material.

C. Printed material is a 'discoverable record' and could expose the organisation to litigation in the event of an incident.

D. Online material is protected by international digital copyright legislation across most territories.

Correct Answer: A
Section:
Explanation:
The delivery of online security training material offers several advantages over printed media. One of the key benefits is the ease of updating content. When updates are required, online materials can be edited quickly and efficiently, with changes being immediately available to all users.This contrasts with printed materials, which would require a new physical version to be produced and distributed, a process that is both time-consuming and resource-intensive1.
Furthermore, online training materials can be accessed from anywhere at any time, providing flexibility and convenience for learners.They also allow for interactive elements, such as quizzes and simulations, which can enhance the learning experience1.Additionally, online materials can be tracked for usage and completion, enabling organizations to monitor compliance with training requirements2.
While option C mentions a 'discoverable record,' this refers to the legal concept that materials may be used as evidence in litigation. However, this is not an advantage of online over printed media, as both can be discoverable. Option B's claim that online materials are intrinsically more accurate is not necessarily true, as accuracy depends on the content's quality, not the delivery method. Option D is incorrect because while online materials are protected by copyright laws, this is not an exclusive benefit over printed materials, which are also protected.

QUESTION 7
What form of training SHOULD developers be undertaking to understand the security of the code they have written and how it can improve security defence whilst being attacked?

A. Red Team Training.

B. Blue Team Training.

C. Black Hat Training.

D. Awareness Training.

Correct Answer: D
Section:
Explanation:
Developers should undergo Awareness Training to understand the security of the code they have written and how it can improve security defense while being attacked. This type of training educates developers on the importance of security considerations throughout the software development lifecycle (SDLC). It covers best practices for secure coding, common vulnerabilities and how to avoid them, and the impact of code security on the overall security posture of an application. By being aware of security principles and the potential threats, developers can write more secure code, which is crucial for defending against attacks.

QUESTION 8
What type of attack could directly affect the confidentiality of an unencrypted VoIP network?

A. Packet Sniffing.

B. Brute Force Attack.

C. Ransomware.

D. Vishing Attack

Correct Answer: A
Section:
Explanation:
Packet sniffing is a type of network attack that can directly affect the confidentiality of an unencrypted VoIP network. In packet sniffing, an attacker captures data packets as they travel across the network. Since VoIP calls transmit voice data in the form of data packets, an unencrypted VoIP network is particularly vulnerable to this type of attack. The attacker can potentially listen to the conversations or extract sensitive information from these packets.This compromises the confidentiality principle of information security, which aims to protect information from unauthorized disclosure12.
Brute Force Attack (B) and Ransomware are more related to the integrity and availability of systems rather than confidentiality. Vishing Attack (D) is a form of phishing which involves social engineering over telephone systems but does not directly affect the network's confidentiality like packet sniffing does.
Information Security Management Principles, 3rd Edition1.
VoIP Hacking: How It Works & How to Protect Your VoIP Phone3.

QUESTION 9
Geoff wants to ensure the application of consistent security settings to devices used throughout his organisation whether as part of a mobile computing or a BYOD approach.
What technology would be MOST beneficial to his organisation?

A. VPN.
B. IDS.
C. MDM.
D. SIEM.

Correct Answer: C
Section:
Explanation:
Mobile Device Management (MDM) is the most beneficial technology for ensuring consistent security settings across an organization's devices, especially in a Bring Your Own Device (BYOD) or mobile computing environment. MDM allows for the central management of security policies, the enforcement of strong authentication measures, and the protection of corporate data on personal devices. It provides the necessary tools to configure devices remotely, enforce security policies, manage applications, and protect against unauthorized access.This aligns with the Information Security Management Principles, particularly under the domains of Technical Security Controls and Procedural/People Security Controls, as it encompasses both the technology and the policies that govern its use by people within the organization123.Reference: The BCS Foundation Certificate in Information Security Management Principles outlines the importance of understanding the concepts relating to information security management, which includes the knowledge of controls and characteristics that are essential for managing the security of information systems4.Additionally, the benefits of MDM in securing mobile and BYOD environments are well-documented, further supporting its selection as the most appropriate technology for Geoff's requirements123.

QUESTION 10
What Is the first yet MOST simple and important action to take when setting up a new web server?

A. Change default system passwords.
B. Fully encrypt the hard disk.
C. Apply hardening to all applications.
D. Patch the OS to the latest version

Correct Answer: A
Section:
Explanation:
Changing default system passwords is a fundamental step in securing a new web server. Default passwords are often well-known and can be easily found in public documentation or through internet searches, making systems with unchanged default passwords highly vulnerable to unauthorized access. By changing these passwords, an administrator immediately reduces the risk of simple, automated attacks that exploit default credentials.
While the other options listed are also important security measures, they are not typically the first action taken. Encrypting the hard disk (B) is a good practice for protecting data at rest, but it does not protect against unauthorized access via default passwords. Hardening applications and patching the OS (D) are critical for reducing the attack surface and protecting against known vulnerabilities, but they are generally performed after ensuring that the system is not accessible with default passwords.

QUESTION 11
By what means SHOULD a cloud service provider prevent one client accessing data belonging to another in a shared server environment?

A. By ensuring appropriate data isolation and logical storage segregation.
B. By using a hypervisor in all shared severs.
C. By increasing deterrent controls through warning messages.
D. By employing intrusion detection systems in a VMs.

Correct Answer: A
Section:
Explanation:

In a shared server environment, such as cloud services, it's crucial to maintain the confidentiality and integrity of client data. The most effective way to prevent one client from accessing another's data is through data isolation and logical storage segregation. This approach aligns with the Information Security Management Principles, specifically under the domain of Technical Security Controls. Data isolation ensures that each client's data is processed and stored separately, while logical storage segregation uses software controls to keep data separate even when stored on the same physical server. This method is part of a broader set of security controls that include encryption, access controls, and regular audits to ensure compliance with security policies.

QUESTION 12
In a virtualised cloud environment, what component is responsible for the secure separation between guest machines?

A. Guest Manager
B. Hypervisor.
C. Security Engine.
D. OS Kernal

Correct Answer: B
Section:
Explanation:
In a virtualized cloud environment, the hypervisor, also known as the virtual machine monitor (VMM), is the software, firmware, or hardware that creates and runs virtual machines. It is responsible for managing the system's hardware resources so they are distributed efficiently among multiple virtual environments. The hypervisor provides the secure separation between guest machines by ensuring that each guest machine operates independently and is unaware of the other guests' existence. This isolation prevents one guest from accessing or interfering with another guest's resources, which is crucial for maintaining security in a multi-tenant environment where multiple virtual machines are hosted on a single physical server.

QUESTION 13
Which of the following cloud delivery models is NOT intrinsically 'trusted' in terms of security by clients using the service?

A. Public.
B. Private.
C. Hybrid.
D. Community

Correct Answer: A
Section:
Explanation:
In the context of cloud delivery models, the term ''trusted'' typically refers to the level of security control and assurance that clients can expect. Among the options provided, thePubliccloud delivery model is generally considered to be the least ''trusted'' in terms of security by clients using the service. This is because public clouds are shared environments where the infrastructure and services are owned and operated by a third-party provider and shared among multiple tenants. The multi-tenant nature of public clouds can introduce risks such as data breaches or other security incidents that might not be as prevalent in more controlled environments.
In contrast,Privateclouds are dedicated to a single organization, providing more control over data, security, and compliance.Hybridclouds combine both public and private elements, offering a balance of control and flexibility.Communityclouds are shared between organizations with common goals and compliance requirements, offering a level of trust tailored to the group's needs.
Therefore, while all cloud models come with their own security considerations and potential risks, the public cloud model is typically the one where clients have to place more trust in the provider's security measures, as they have less control over the environment.

QUESTION 14
Which of the following subjects is UNLIKELY to form part of a cloud service provision laaS contract?

A. User security education.
B. Intellectual Property Rights.
C. End-of-service.
D. Liability

Correct Answer: A
Section:
Explanation:
In the context of a cloud service provision, particularly Infrastructure as a Service (IaaS), the focus is typically on providing the physical or virtual infrastructure to the customer. The responsibility for user security education generally falls within the domain of the customer, as it pertains to their internal operations and how their employees or users interact with the IaaS. The IaaS provider's responsibilities are more aligned with ensuring the security of the infrastructure itself, rather than the education of users on security practices.
Intellectual Property Rights (B), End-of-service , and Liability (D) are all common considerations in cloud service contracts. Intellectual Property Rights would cover the ownership of data and software used within the service. End-of-service terms would outline the process and responsibilities when the service term ends, including data retrieval or transfer. Liability clauses would define the extent to which the provider is responsible for damages or losses incurred due to service issues.

QUESTION 15
When an organisation decides to operate on the public cloud, what does it lose?

A. The right to audit and monitor access to its information.
B. Control over Intellectual Property Rights relating to its applications.
C. Physical access to the servers hosting its information.
D. The ability to determine in which geographies the information is stored.

Correct Answer: C
Section:
Explanation:
When an organization opts for public cloud services, it relinquishes direct control over many aspects of security and privacy. While the cloud service provider maintains the physical servers, the organization loses the ability to physically access these servers. This is a significant shift from traditional on-premises data centers where the organization would have complete control over and access to the physical infrastructure. In the context of the public cloud, the organization must rely on the cloud provider's security measures and protocols to protect its data.However, it's important to note that while physical access is lost, cloud providers typically offer robust security features and compliance certifications that can compensate for this loss12.

QUESTION 16
One traditional use of a SIEM appliance is to monitor for exceptions received via syslog.
What system from the following does NOT natively support syslog events?

A. Enterprise Wireless Access Point.
B. Windows Desktop Systems.
C. Linux Web Server Appliances.
D. Enterprise Stateful Firewall.

Correct Answer: B
Section:
Explanation:
Syslog is a standard for message logging and allows devices to send event notification messages across IP networks to event message collectors - also known as Syslog servers or SIEM (Security Information and Event Management) systems. Native support for syslog is commonly found in various network devices and Unix/Linux-based systems.
Enterprise Wireless Access Points,Linux Web Server Appliances, andEnterprise Stateful Firewallstypically have built-in capabilities to generate and send syslog messages to a SIEM system for monitoring and analysis.
Windows Desktop Systems, on the other hand, do not natively support syslog because Windows uses its own event logging system known as Windows Event Log.While it is possible to configure Windows systems to send logs to a SIEM appliance, this usually requires additional software or agents to translate Windows Event Log messages into syslog format before they can be sent1.

QUESTION 17
What type of diagram used in application threat modeling includes malicious users as well as descriptions like mitigates and threatens?

A. Threat trees.

B. STRIDE charts.

C. Misuse case diagrams.

D. DREAD diagrams.

Correct Answer: C
Section:
Explanation:
Misuse case diagrams are a type of diagram used in application threat modeling that includes malicious users (also known as threat actors) and describes how their potential actions could threaten the system, as well as how the system mitigates those threats. These diagrams are an adaptation of use case diagrams, which are commonly used in software engineering to specify the required usages of a system.Misuse case diagrams, on the other hand, focus on the negative scenarios, illustrating how a system can be used improperly and what measures are in place to prevent or mitigate these actions12.

QUESTION 18
Ensuring the correctness of data inputted to a system is an example of which facet of information security?

A. Confidentiality.

B. Integrity.

C. Availability.

D. Authenticity.

Correct Answer: B
Section:
Explanation:
Ensuring the correctness of data inputted to a system is a fundamental aspect of data integrity within information security. Integrity refers to the trustworthiness and accuracy of data throughout its lifecycle. This means that the data has not been altered in an unauthorized manner and remains consistent, accurate, and trustworthy. It is crucial for the proper functioning of any system that relies on data to make decisions or perform operations. Measures to ensure data integrity include input validation, error checking, and data verification processes that prevent incorrect data entry, unauthorized data alteration, and ensure that the data reflects its intended state.

QUESTION 19
How does network visualisation assist in managing information security?

A. Visualisation can communicate large amounts of data in a manner that is a relatively simple way for people to analyse and interpret.

B. Visualisation provides structured tables and lists that can be analysed using common tools such as MS Excel.

C. Visualisation offers unstructured data that records the entirety of the data in a flat, filterable ftle format.

D. Visualisation software operates in a way that is rarely and thereby it is less prone to malware infection.

Correct Answer: A
Section:
Explanation:
Network visualization is a powerful tool in managing information security as it can transform complex data sets into visual formats that are easier to understand and analyze. This is particularly useful in cybersecurity, where large volumes of data need to be monitored for potential security threats.Effective data visualization can provide meaningful insights into network security data, helping analysts to quickly identify patterns, anomalies, and trends that may indicate security incidents12.
While options B and C are methods of data analysis, they do not leverage the unique capabilities of visualization for rapid interpretation of security data.Option D is incorrect because the operation of visualization software does not inherently reduce malware infection risks; it's the insights gained from visualization that can assist in proactive threat detection and management12.
Effective Data Visualization in Cybersecurity, IEEE Conference1.
A Survey of Visualization Systems for Network Security, IEEE Transactions2.

QUESTION 20
When considering the disposal of confidential data, equipment and storage devices, what social engineering technique SHOULD always be taken into consideration?

A. Spear Phishing.
B. Shoulder Surfing.
C. Dumpster Diving.
D. Tailgating.

Correct Answer: C
Section:
Explanation:
Dumpster diving refers to the practice of sifting through commercial or residential waste to find items that have been discarded but can still be of value, particularly information. In the context of information security, dumpster diving is a significant threat because it can lead to the recovery of sensitive documents, storage devices, or other materials that contain confidential data. When disposing of such items, it's crucial to ensure they are destroyed or sanitized in a manner that prevents data reconstruction or retrieval.This aligns with the BCS Information Security Management Principles, which emphasize the importance of secure disposal methods to protect against unauthorized access to or recovery of sensitive information1234.

QUESTION 21
What term is used to describe the testing of a continuity plan through a written scenario being used as the basis for discussion and simul-ation?

A. End-to-end testing.
B. Non-dynamic modeling
C. Desk-top exercise.
D. Fault stressing

Correct Answer: C
Section:
Explanation:

A desk-top exercise is a form of testing for a continuity plan that involves a structured discussion around a written scenario. This scenario is used as the basis for simulation, without the activation of actual resources. It typically involves key personnel discussing the steps they would take in response to a particular set of circumstances, as outlined in the scenario. This type of exercise is designed to validate the theoretical aspects of a plan and ensure that those involved understand their roles and responsibilities. It can also highlight any gaps or issues within the plan that need to be addressed.

QUESTION 22
In business continuity, what is a battle box?

A. A portable container that holds Items and information useful in the event of an organisational disaster.
B. An armoured box that holds all an organisation's backup databases.
C. A collection of tools and protective equipment to be used in the event of civil disturbance.
D. A list of names and addresses of staff to be utilised should industrial action prevent access to a building.

Correct Answer: A
Section:
Explanation:
A battle box, in the context of business continuity, is a portable container that holds items and information essential for an organization to continue critical operations during and after a disaster. This may include contact lists, key documents, backup media, and other resources necessary for decision-making and recovery efforts. The concept of a battle box aligns with theDisaster Recovery and Business Continuity Managementdomain of Information Security Management Principles, which emphasizes the importance of preparedness and the ability to respond effectively to incidents that disrupt business operations.
http://www.battlebox.biz/why.asp

QUESTION 23
When undertaking disaster recovery planning, which of the following would NEVER be considered a 'natural' disaster?

A. Arson.

B. Electromagnetic pulse

C. Tsunami.

D. Lightning Strike

Correct Answer: A
Section:
Explanation:
Arson is an act of intentionally setting fire to property for malicious reasons. It is a criminal act and is not classified as a natural disaster. Natural disasters are events that occur due to natural processes of the Earth, such as tsunamis, lightning strikes, and other weather-related events. An electromagnetic pulse can be a natural event if it is caused by solar flares or a man-made event if it is the result of a nuclear explosion.However, arson is always the result of human activity and is not caused by natural processes1.

QUESTION 24
Why have MOST European countries developed specific legislation that permits police and security services to monitor communications traffic for specific purposes, such as the detection of crime?

A. Under the European Convention of Human Rights, the interception of telecommunications represents an interference with the right to privacy.

B. GDPR overrides all previous legislation on information handling, so new laws were needed to ensure authorities did not inadvertently break the law.

C. Police could previously intercept without lawful authority any communications in the course of transmission through a public post or telecoms system.

D. Surveillance of a conversation or an online message by law enforcement agents was previously illegal due to the 1950 version of the Human Rights Convention.

Correct Answer: A
Section:
Explanation:
The European Convention on Human Rights (ECHR) protects the right to privacy, which includes the security of personal data and protection against surveillance1. This right is not absolute and can be limited under certain conditions, such as for the protection of national security or public safety. Most European countries have developed specific legislation that allows police and security services to monitor communications traffic, but this must be done within the boundaries set by the ECHR and subsequent legislation like the GDPR.The GDPR itself does not override the ECHR but complements it by providing detailed regulations on the processing of personal data, including provisions for law enforcement authorities to process data for criminal investigations in a way that respects fundamental rights23.

QUESTION 25
Which of the following statements relating to digital signatures is TRUE?

A. Digital signatures are rarely legally enforceable even if the signers know they are signing a legal document.

B. Digital signatures are valid and enforceable in law in most countries in the world.

C. Digital signatures are legal unless there is a statutory requirement that predates the digital age.

D. A digital signature that uses a signer's private key is illegal.

Correct Answer: B
Section:
Explanation:
Digital signatures are a form of electronic signature that uses cryptographic techniques to provide secure and verifiable means of signing electronic documents. They are widely recognized and accepted as legally binding in many jurisdictions around the world. The enforceability of digital signatures is backed by various laws and regulations that recognize electronic signatures as equivalent to handwritten signatures, provided they meet certain criteria for authenticity and integrity.For instance, in the United States, the ESIGN Act establishes the legal validity of electronic signatures, including digital signatures1.Similarly, the eIDAS regulation in the European Union provides a legal framework for electronic signatures and trust services, including digital signatures2.

QUESTION 26
Which type of facility is enabled by a contract with an alternative data processing facility which will provide HVAC, power and communications infrastructure as well computing hardware and a duplication of organisations existing 'live' data?

A. Cold site.

B. Warm site.
C. Hot site.
D. Spare site

Correct Answer: C
Section:
Explanation:
A hot site is a type of disaster recovery facility that is fully equipped and ready to take over operation at a moment's notice. It includes HVAC, power, communications infrastructure, computing hardware, and a real-time duplication of the organization's existing ''live'' data. This enables an organization to resume operations quickly after a disaster with minimal downtime. Hot sites are typically maintained at a state of readiness and can become operational almost immediately after an incident occurs. This contrasts with cold sites, which provide space and infrastructure but require installation and configuration of equipment, and warm sites, which are partially equipped with some operational resources.

QUESTION 27
In business continuity (BC) terms, what is the name of the individual responsible for recording all pertinent information associated with a BC exercise or real plan invocation?

A. Recorder.
B. Desk secretary.
C. Scribe.
D. Scrum Master.

Correct Answer: C
Section:
Explanation:
In the context of business continuity (BC), the individual tasked with documenting all relevant details during a BC exercise or actual plan activation is known as theScribe. The Scribe's role is crucial as they ensure that all actions, decisions, and changes are recorded accurately, which is essential for post-incident reviews and audits. This position supports the BC process by providing a clear and chronological account of events, which is vital for assessing the effectiveness of the BC plan and for making improvements.

QUESTION 28
When a digital forensics investigator is conducting art investigation and handling the original data, what KEY principle must they adhere to?

A. Ensure they are competent to be able to do so and be able to justify their actions.
B. Ensure they are being observed by a senior investigator in all actions.
C. Ensure they do not handle the evidence as that must be done by law enforcement officers.
D. Ensure the data has been adjusted to meet the investigation requirements.

Correct Answer: A
Section:
Explanation:
The key principle a digital forensics investigator must adhere to is ensuring competence and the ability to justify their actions. This is crucial because the integrity of the investigation and the evidence must be maintained. Competence ensures that the investigator has the necessary skills and knowledge to handle and analyze the data correctly. Being able to justify their actions is important for the legal process, as every step of the investigation may be scrutinized in court.This principle aligns with the Information Security Management Principles, which emphasize the importance of procedural/people security controls and technical security controls to maintain the confidentiality, integrity, and availability of information.Reference: BCS Foundation Certificate in Information Security Management Principles1.

QUESTION 29
When preserving a crime scene for digital evidence, what actions SHOULD a first responder initially make?

A. Remove power from all digital devices at the scene to stop the data changing.
B. Photograph all evidence and triage to determine whether live data capture is necessary.

C. Remove all digital evidence from the scene to prevent unintentional damage.

D. Don't touch any evidence until a senior digital investigator arrives.

Correct Answer: B
Section:
Explanation:
When preserving a crime scene for digital evidence, it is crucial to maintain the integrity of the evidence while also ensuring that volatile data is not lost. The initial actions should include photographing all evidence, which helps document the scene and the location of digital devices. This is important for later analysis and may be required for legal proceedings. Triage is the process of determining the importance of digital evidence and whether live data capture is necessary.Live data capture can be essential because some data can be lost if a device is powered down, such as encryption keys or active network connections1.

QUESTION 30
Which of the following is NOT an accepted classification of security controls?

A. Nominative.

B. Preventive.

C. Detective.

D. Corrective.

Correct Answer: A
Section:
Explanation:
Security controls are measures taken to safeguard an information system from attacks or to mitigate the impact of a breach. They are commonly classified into three main categories: preventive, detective, and corrective. Preventive controls aim to prevent incidents before they occur, detective controls are designed to discover and detect security events, and corrective controls are intended to restore systems to normal operation after an incident. The term ''nominative'' is not recognized as a standard classification of security controls within the principles of information security management.Instead, the accepted classifications align with the objectives of protecting the confidentiality, integrity, and availability of information.Reference: The BCS Foundation Certificate in Information Security Management Principles outlines the categorization, operation, and effectiveness of controls of different types and characteristics, which does not include ''nominative'' as a classification1.

QUESTION 31
Which three of the following characteristics form the AAA Triad in Information Security?
1. Authentication
2. Availability
3. Accounting
4. Asymmetry
5. Authorisation

A. 1, 2 and 3.

B. 2, 4, and 5.

C. 1, 3 and 4.

D. 1, 3 and 5.

Correct Answer: D
Section:
Explanation:
The AAA Triad in Information Security stands for Authentication, Authorization (also known as Authorisation), and Accounting. These three components are fundamental to ensuring that access to systems is controlled and monitored:
Authenticationis the process of verifying the identity of a user or entity. It ensures that individuals are who they claim to be. This can involve methods such as passwords, biometrics, or tokens.
Authorizationdetermines what an authenticated user is allowed to do. It involves granting or denying rights to access resources and perform actions within a system based on the user's identity.
Accountingkeeps track of user activities. This includes logging when users log in and out, what actions they perform, and what resources they access. It's essential for auditing purposes and can also be used for billing or

analyzing resource usage.
These principles are designed to protect information by managing potential risks and controlling access to data. They are part of a broader framework that includes physical, technical, and procedural controls to safeguard information assets.

QUESTION 32
According to ISO/IEC 27000, which of the following is the definition of a vulnerability?

A. A weakness of an asset or group of assets that can be exploited by one or more threats.
B. The impact of a cyber attack on an asset or group of assets.
C. The threat that an asset or group of assets may be damaged by an exploit.
D. The damage that has been caused by a weakness iin a system.

Correct Answer: A
Section:
Explanation:
The term 'vulnerability' within the context of ISO/IEC 27000 refers to any weakness present in an asset or group of assets that could potentially be exploited by one or more threats. This definition aligns with the concept of vulnerability as a gap in protection efforts that, if not addressed, could allow a threat to compromise the confidentiality, integrity, or availability of an asset. It is important to note that vulnerabilities can be identified in various components of an organization's infrastructure, including hardware, software, processes, and even personnel. Effective information security management involves identifying these vulnerabilities through risk assessments and implementing appropriate controls to mitigate the risk of exploitation.

QUESTION 33
Which term describes the acknowledgement and acceptance of ownership of actions, decisions, policies and deliverables?

A. Accountability.
B. Responsibility.
C. Credibility.
D. Confidentiality.

Correct Answer: A
Section:
Explanation:
Accountability is the term that describes the acknowledgement and acceptance of ownership of actions, decisions, policies, and deliverables. It implies that an individual or organization is willing to take responsibility for their actions and the outcomes of those actions, and is answerable to the relevant stakeholders. This concept is fundamental in information security management, as it ensures that individuals and teams are aware of their roles and the expectations placed upon them, particularly in relation to the protection of information assets. Accountability cannot be delegated; while tasks can be assigned to others, the ultimate ownership and obligation to report and justify the outcomes remain with the accountable party.

QUESTION 34
Which security concept provides redundancy in the event a security control failure or the exploitation of a vulnerability?

A. System Integrity.
B. Sandboxing.
C. Intrusion Prevention System.
D. Defence in depth.

Correct Answer: D
Section:
Explanation:
Defence in depth is a security concept that involves implementing multiple layers of security controls throughout an information system. The idea is that if one control fails or a vulnerability is exploited, other controls will

provide redundancy and continue to protect the system. This approach is analogous to a physical fortress with multiple walls; if an attacker breaches one wall, additional barriers exist to stop them from progressing further. In the context of information security, this could include a combination of firewalls, intrusion detection systems, antivirus software, and strict access controls, among others. Defence in depth is designed to address security vulnerabilities not only in technology but also in processes and people, acknowledging that human error or negligence can often lead to security breaches.

Online retailers are the most at risk for the theft of electronic-based credit card data due to the nature of their business, which involves processing a large volume of transactions over the internet. This exposes them to various cyber threats, including hacking, phishing, and other forms of cyber-attacks that can compromise credit card information. Traditional market traders, mail delivery businesses, and agricultural producers typically do not handle credit card transactions to the same extent or in the same electronic manner as online retailers, making them less likely targets for this specific type of data theft.

The principles of Information Security Management emphasize the importance of protecting sensitive data, such as credit card information, through technical security controls and risk management practices.Online retailers must implement robust security measures, including encryption, secure payment gateways, and regular security audits, to mitigate the risks associated with electronic transactions12.

BCS Information Security Management Principles, particularly the sections on Technical Security Controls and Information Risk, provide guidance on protecting electronic data and managing the associated risks1.

Additional insights can be found in the Information Security Management Principles, 3rd Edition by Andy Taylor, David Alexander, Amanda Finch, David Sutton2.

QUESTION 35

What form of attack against an employee has the MOST impact on their compliance with the organisation's 'code of conduct'?

A. Brute Force Attack.

B. Social Engineering.

C. Ransomware.

D. Denial of Service.

Correct Answer: B
Section:
Explanation:

Social engineering attacks are designed to exploit human psychology and manipulate individuals into breaking normal security procedures and best practices. These attacks have the most impact on an employee's compliance with an organization's code of conduct because they directly target the employee's behavior and decision-making process. By using deception, persuasion, or influence, attackers can coerce employees into divulging confidential information, providing access to restricted areas, or performing actions that go against the company's policies and ethical standards. This form of attack can lead to violations of the code of conduct, as employees may unknowingly or unwillingly engage in activities that compromise the organization's values and principles.

QUESTION 36

When considering outsourcing the processing of data, which two legal 'duty of care' considerations SHOULD the original data owner make?

1 Third party is competent to process the data securely.
2. Observes the same high standards as data owner.
3. Processes the data wherever the data can be transferred.
4. Archive the data for long term third party's own usage.

A. 2 and 3.

B. 3 and 4.

C. 1 and 4.

D. 1 and 2.

Correct Answer: D
Section:
Explanation:

When outsourcing data processing, the original data owner has a legal duty of care to ensure that the third party is competent to process the data securely (1) and observes the same high standards as the data owner (2). This means that the third party must have the necessary skills, knowledge, and security measures in place to protect the data, and they must adhere to the same level of data protection and privacy standards as the original owner. Processing the data wherever it can be transferred (3) and archiving the data for the third party's own long-term usage (4) are not primary legal considerations and may, in fact, contravene data protection laws if done without proper safeguards and compliance with regulations.

QUESTION 37

Select the document that is MOST LIKELY to contain direction covering the security and utilisation of all an organisation's information and IT equipment, as well as email, internet and telephony.

A. Cryptographic Statement.
B. Security Policy Framework.
C. Acceptable Usage Policy.
D. Business Continuity Plan.

Correct Answer: C
Section:
Explanation:
The Acceptable Usage Policy (AUP) is the document most likely to contain directives on the security and utilization of an organization's information and IT equipment, including email, internet, and telephony. An AUP outlines the acceptable and unacceptable behaviors for users of the organization's IT systems and services. It typically includes rules and guidelines on the proper use of IT resources, security practices, and the consequences of non-compliance.The AUP is designed to protect both the organization and its users by mitigating risks associated with the misuse of IT resources and ensuring that the use of these resources aligns with the organization's security policies and objectives123.

QUESTION 38
What term refers to the shared set of values within an organisation that determine how people are expected to behave in regard to information security?

A. Code of Ethics.
B. Security Culture.
C. System Operating Procedures.
D. Security Policy Framework.

Correct Answer: B
Section:
Explanation:

The term that refers to the shared set of values within an organization that determines how people are expected to behave in regard to information security is known asSecurity Culture. This encompasses the attitudes, beliefs, and behaviors of individuals within the organization towards the protection of data and information assets. A strong security culture is vital for the effective implementation of security policies and controls, as it influences how employees interact with the organization's information systems and handle sensitive information.It's the collective mindset that prioritizes security as a fundamental aspect of all business operations and decisions1.
ACode of Ethicstypically outlines the principles and moral values that guide the behavior of individuals within an organization but does not specifically address information security behaviors.
System Operating Proceduresare detailed written instructions to achieve uniformity of the performance of a specific function, which is more about the operational aspect rather than the underlying values or behaviors.
ASecurity Policy Frameworkprovides a structured set of policies that dictate the security measures and controls that are to be applied across the organization.While it sets the formal requirements for security, it does not inherently define the cultural aspect of how individuals within the organization value and engage with these requirements1.

QUESTION 39
Which of the following controls would be the MOST relevant and effective in detecting zero day attacks?

A. Strong OS patch management
B. Vulnerability assessment
C. Signature-based intrusion detection.
D. Anomaly based intrusion detection.

Correct Answer: D
Section:
Explanation:
Anomaly-based intrusion detection systems (IDS) are particularly effective in detecting zero-day attacks because they do not rely on known signatures, which zero-day attacks would not have. Instead, they monitor network behavior for deviations from a baseline of normal activity.This approach can identify suspicious activities that could indicate a novel or unknown threat, such as a zero-day exploit12345.These systems use various methods, including machine learning and deep learning, to detect patterns that could signify an attack, making them a robust solution against the unpredictable nature of zero-day threats12345.

QUESTION 40
What physical security control would be used to broadcast false emanations to mask the presence of true electromagentic emanations from genuine computing equipment?

A. Faraday cage.
B. Unshielded cabling.
C. Copper infused windows.
D. White noise generation.

Correct Answer: D
Section:
Explanation:
The use of white noise generation is a countermeasure to protect against the threat of eavesdropping on electromagnetic emanations from computing equipment. This method involves broadcasting random electromagnetic signals, which are referred to as 'white noise', to mask the genuine signals emitted by electronic devices. This makes it significantly more difficult for unauthorized parties to intercept and decipher the information being processed by the genuine equipment.
A Faraday cage (A) is designed to block external electromagnetic fields but does not specifically broadcast false signals to mask emanations. Unshielded cabling (B) would actually increase the risk of emanation interception rather than protect against it. Copper infused windows can shield against electromagnetic signals but, like the Faraday cage, do not broadcast false emanations.

QUESTION 41
Which of the following types of organisation could be considered the MOST at risk from the theft of electronic based credit card data?

A. Online retailer.
B. Traditional market trader.
C. Mail delivery business.
D. Agricultural producer.

Correct Answer: A
Section:
Explanation:
Online retailers are the most at risk for the theft of electronic-based credit card data due to the nature of their business, which involves processing a large volume of transactions over the internet. This exposes them to various cyber threats, including hacking, phishing, and other forms of cyber-attacks that can compromise credit card information. Traditional market traders, mail delivery businesses, and agricultural producers typically do not handle credit card transactions to the same extent or in the same electronic manner as online retailers, making them less likely targets for this specific type of data theft.
The principles of Information Security Management emphasize the importance of protecting sensitive data, such as credit card information, through technical security controls and risk management practices.Online retailers must implement robust security measures, including encryption, secure payment gateways, and regular security audits, to mitigate the risks associated with electronic transactions12.
BCS Information Security Management Principles, particularly the sections on Technical Security Controls and Information Risk, provide guidance on protecting electronic data and managing the associated risks1.
Additional insights can be found in the Information Security Management Principles, 3rd Edition by Andy Taylor, David Alexander, Amanda Finch, David Sutton2.

QUESTION 42
Which types of organisations are likely to be the target of DDoS attacks?

A. Cloud service providers.
B. Any financial sector organisations.
C. Online retail based organisations.
D. Any organisation with an online presence.

Correct Answer: D
Section:
Explanation:
Distributed Denial of Service (DDoS) attacks are a threat to any organization that maintains an online presence. This is because DDoS attacks are designed to overwhelm an organization's network with traffic, rendering it

inaccessible to legitimate users. While cloud service providers, financial sector organizations, and online retail companies can be attractive targets due to their high-profile nature and the critical nature of their services, the reality is that any organization with an online presence can be targeted. This includes small businesses, educational institutions, government agencies, and non-profits. The motivation behind such attacks can vary from financial gain, to disruption of service, to political statements. Therefore, it's crucial for all organizations to implement robust security measures to mitigate the risk of DDoS attacks.