BCS

Exam Questions CISMP-V9

BCS Foundation Certificate in Information Security Management Principles V9.0

NEW QUESTION 1
The policies, processes, practices, and tools used to align the business value of information with the most appropriate and cost-effectiveinfrastructure from the time information is conceived through its final disposition.
Which of the below business practices does this statement define?

A. Information Lifecycle Management.
B. Information Quality Management.
C. Total Quality Management.
D. Business Continuity Management.

Answer: A

Explanation:
https://www.stitchdata.com/resources/glossary/information-lifecycle-management/#:~:text=%E2%80%9CILM%

NEW QUESTION 2
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 knownprinciple.
B. Verification of visitor's ID
C. Appropriate behaviours.
D. Access denial measures

Answer: D

NEW QUESTION 3
What Is the PRIMARY security concern associated with the practice known as Bring Your Own Device (BYOD) that might affect a largeorganisation?

A. Most BYOD involves the use of non-Windows hardware which is intrinsically insecure and open to abuse.
B. The organisation has significantly less control over the device than over a corporately provided and managed device.
C. Privately owned end user devices are not provided with the same volume nor frequency of security patch updates as a corporation.
D. Under GDPR it is illegal for an individual to use a personal device when handling personal information under corporate control.

Answer: A

NEW QUESTION 4
Which security framework impacts on organisations that accept credit cards, process credit card transactions, store relevant data or transmitcredit card data?

A. PCI DSS.
B. TOGAF.
C. ENISA NIS.
D. Sarbanes-Oxiey

Answer: A

Explanation:
https://digitalguardian.com/blog/what-pci-compliance

NEW QUESTION 5
Which of the following is often the final stage in the information management lifecycle?

A. Disposal.
B. Creation.
C. Use.
D. Publication.

Answer: A

Explanation:
https://timg.co.nz/blog-the-information-management-life-cycle/

NEW QUESTION 6
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.

Answer: D

Explanation:
https://www.ncjrs.gov/pdffiles1/nij/219941.pdf

NEW QUESTION 7
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.

Answer: B

NEW QUESTION 8
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.

Answer: D

NEW QUESTION 9
Which of the following is considered to be the GREATEST risk to information systems that results from deploying end-to-end Internet of Things(IoT) solutions?

A. Use of 'cheap" microcontroller based sensors.
B. Much larger attack surface than traditional IT systems.
C. Use of proprietary networking protocols between nodes.
D. Use of cloud based systems to collect loT data.

Answer: D

NEW QUESTION 10
What Is the PRIMARY difference between DevOps and DevSecOps?

A. Within DevSecOps security is introduced at the end of development immediately prior to deployment.
B. DevSecOps focuses solely on iterative development cycles.
C. DevSecOps includes security on the same level as continuous integration and delivery.
D. DevOps mandates that security is integrated at the beginning of the development lifecycle.

Answer: C

Explanation:
https://www.viva64.com/en/b/0710/#:~:text=DevOps%20is%20a%20methodology%20aiming,in%20the%20sof

NEW QUESTION 10
When securing a wireless network, which of the following is NOT best practice?

A. Using WPA encryption on the wireless network.
B. Use MAC tittering on a SOHO network with a smart group of clients.
C. Dedicating an access point on a dedicated VLAN connected to a firewall.
D. Turning on SSID broadcasts to advertise security levels.

Answer: C

NEW QUESTION 12
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.

Answer: C

NEW QUESTION 16
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.

Answer: A

NEW QUESTION 20
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

Answer: A

NEW QUESTION 23
What term is used to describe the testing of a continuity plan through a written scenario being used as the basis for discussion and simulation?

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

Answer: E

NEW QUESTION 27
Which of the following is LEASTLIKELY to be the result of a global pandemic impacting on information security?

A. A large increase in remote workers operating in insecure premises.
B. Additional physical security requirements at data centres and corporate headquarters.
C. Increased demand on service desks as users need additional tools such as VPNs.
D. An upsurge in activity by attackers seeking vulnerabilities caused by operational changes.

Answer: C

NEW QUESTION 31
Why have MOST European countries developed specific legislation that permits police and security services to monitor communications trafficfor specific purposes, such as the detection of crime?

A. Under the European Convention of Human Rights, the interception of telecommunications represents aninterference with the right toprivacy.
B. GDPR overrides all previous legislation on information handling, so new laws were needed to ensure authorities did not inadvertentlybreak the law.
C. Police could previously intercept without lawful authority any communications in the course of transmission through a public post ortelecoms system.
D. Surveillance of a conversation or an online message by law enforcement agents was previously illegaldue to the 1950 version of theHuman Rights Convention.

Answer: C

NEW QUESTION 35
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.

Answer: A

NEW QUESTION 38
What are the different methods that can be used as access controls?
* 1. Detective.
* 2. Physical.
* 3. Reactive.
* 4. Virtual.
* 5. Preventive.

A. 1, 2 and 4.
B. 1, 2 and 3.
C. 1, 2 and 5.
D. 3, 4 and 5.

Answer: C

NEW QUESTION 43
When considering the disposal of confidential data, equipment and storage devices, what social engineering technique SHOULD always betaken into consideration?

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

Answer: A

NEW QUESTION 46

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

Answer: D

NEW QUESTION 51
What term refers to the shared set of values within an organisation that determine how people are expected tobehave in regard to informationsecurity?

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

Answer: B

Explanation:
https://www.cpni.gov.uk/developing-security-culture#:~:text=Developing%20a%20Security%20Culture,-What

NEW QUESTION 55
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.

Answer: D

NEW QUESTION 59
You are undertaking a qualitative risk assessment of a likely security threat to an information system. What is the MAIN issue with this type of risk assessment?

A. These risk assessments are largely subjective and require agreement on rankings beforehand.
B. Dealing with statistical and other numeric data can often be hard to interpret.
C. There needs to be a large amount of previous data to "train" a qualitative risk methodology.
D. It requires the use of complex software tools to undertake this risk assessment.

Answer: D

NEW QUESTION 63
Which of the following compliance legal requirements are covered by the ISO/IEC 27000 series?
* 1. Intellectual Property Rights.
* 2. Protection of Organisational Records
* 3. Forensic recovery of data.
* 4. Data Deduplication.
* 5. Data Protection & Privacy.

A. 1, 2 and 3
B. 3, 4 and 5
C. 2, 3 and 4
D. 1, 2 and 5

Answer: D

NEW QUESTION 64
Which standards framework offers a set of IT Service Management best practices to assist organisations in aligning IT service delivery withbusiness goals - including security goals?

A. ITIL.
B. SABSA.
C. COBIT
D. ISAGA.

Answer: A

Explanation:
https://www.cherwell.com/it-service-management/library/essential-guides/essential-guide-to-itil-framework-and

NEW QUESTION 69
Which of the following is a framework and methodology for Enterprise Security Architecture and Service Management?

A. TOGAF
B. SABSA

C. PCI DSS.
D. OWASP.

Answer: B

NEW QUESTION 74
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.

Answer: A

Explanation:
Vulnerability
A vulnerability is a weakness of an asset or control thactould potentially be exploited by one or more threats.
An asset is any tangible or intangible thing or characteristtichat has value to an organization, a control is any administrativme, anagerial, technical, or legal method that can be used to modifyor manage risk,
and a threat is any potential event that coulhdarm an organization or system. https://www.praxiom.com/iso-27000-definitions.htm

NEW QUESTION 76
Which membership based organisation produces international standards, which cover good practice for information assurance?

A. BSI.
B. IETF.
C. OWASP.
D. ISF.

Answer: A

NEW QUESTION 80
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CISMP-V9 Practice Exam Features:

* CISMP-V9 Questions and Answers Updated Frequently

* CISMP-V9 Practice Questions Verified by Expert Senior Certified Staff

* CISMP-V9 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CISMP-V9 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year