Free Questions for CISMP-V9 by certsinside

Shared by Kidd on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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?

Options:

A- End-to-end testing.

B- Non-dynamic modeling

C- Desk-top exercise.

D- Fault stressing

Answer:

C

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 2

Question Type: MultipleChoice

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

Options:

A- User security education.

B- Intellectual Property Rights.

C- End-of-service.

D- Liability

Answer:

A

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 3

Question Type: MultipleChoice

Which of the following testing methodologies TYPICALLY involves code analysis in an offline environment without ever actually executing the code?

Options:

A- Dynamic Testing.

B- Static Testing.

C- User Testing.

D- Penetration Testing.

Answer:

B

Explanation:

Static testing is a method where the code is analyzed without being executed. It involves reviewing the code, documentation, and other related artifacts to identify errors at an early stage. Static testing can detect potential issues like syntax errors, variable misuse, and security vulnerabilities. This type of testing is crucial because it helps to find errors before the code is run, which can save time and resources in the development process.It's typically done through various techniques such as code reviews, walkthroughs, and the use of static analysis tools12.

Understanding of static testing and its importance in the software development lifecycle is well-documented in the literature, including the BCS Foundation Certificate in Information Security Management Principles1.

Further details on static testing methodologies and their application can be found in industry-specific guidelines and best practices2.

Question 4

Question Type: MultipleChoice

James is working with a software programme that completely obfuscates the entire source code, often in the form of a binary executable making it difficult to inspect, manipulate or reverse engineer the original source code.

What type of software programme is this?

Options:

A- Free Source.

B- Proprietary Source.

C- Interpreted Source.

D- Open Source.

Answer:

B

Explanation:

The software program described is one that obfuscates the source code, making it difficult to inspect, manipulate, or reverse engineer. This is characteristic of proprietary source software, where the source code is not openly shared or available for public viewing or modification. Proprietary software companies often obfuscate their code to protect intellectual property and prevent unauthorized use or reproduction of their software. Unlike open-source software, where the source code is available for anyone to view, modify, and distribute, proprietary software keeps its source code a secret to maintain control over the software's functions and distribution.

Question 5

Question Type: **MultipleChoice**

Which of the following acronyms covers the real-time analysis of security alerts generated by applications and network hardware?

Options:

A- CERT

B- SIEM.

C- CISM.

D- DDoS.

Answer:

B

Explanation:

SIEM, which stands for Security Information and Event Management, is the correct acronym that covers the real-time analysis of security alerts generated by applications and network hardware. SIEM systems aggregate and analyze activity data from various resources across the IT infrastructure, such as network devices, servers, and domain controllers. They operate on rules-based and statistical correlation algorithms to establish relationships between log entries, providing reports on security-related incidents and events, and sending alerts if the analysis indicates a potential security issue.This enables organizations to gain insights into their security posture, identify trends, and detect threats or anomalies that could indicate a security incident1.

Question 6

Question Type: MultipleChoice

What does a penetration test do that a Vulnerability Scan does NOT?

Options:

A- A penetration test seeks to actively exploit any known or discovered vulnerabilities.

B- A penetration test looks for known vulnerabilities and reports them without further action.

C- A penetration test is always an automated process - a vulnerability scan never is.

D- A penetration test never uses common tools such as Nrnap, Nessus and Metasploit.

Answer:

A

Explanation:

A penetration test, unlike a vulnerability scan, is an in-depth process where security professionals actively attempt to exploit vulnerabilities in a system. The goal is to simulate a real-world attack to understand how an attacker could exploit vulnerabilities and to determine the potential impact. This involves not just identifying vulnerabilities, as a scan does, but also attempting to exploit them to understand the full extent of the risk. Penetration tests are typically manual or semi-automated and involve a variety of tools and techniques to uncover and exploit security weaknesses, which can include common tools like Nmap, Nessus, and Metasploit.

Question 7

Question Type: MultipleChoice

What Is the PRIMARY difference between DevOps and DevSecOps?

Options:

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:

The primary difference between DevOps and DevSecOps lies in the integration of security practices. DevOps is a methodology that emphasizes collaboration between development and operations teams to automate the software development process, including continuous integration (CI) and continuous delivery (CD). However, DevOps does not inherently prioritize security as part of the development process.

DevSecOps, on the other hand, extends the DevOps principles by integrating security into every aspect of the software development lifecycle. This approach is often summarized by the term "shift-left," which means incorporating security from the beginning and throughout the development process, rather than treating it as an afterthought or a final step before deployment. In DevSecOps, security

is considered a shared responsibility among all team members, and it is addressed through continuous security processes that are as integral as CI/CD in the DevOps culture.

Question 8

Question Type: MultipleChoice

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

Options:

A- TOGAF

B- SABSA

C- PCI DSS.

D- OWASP.

Answer:

B

Explanation:

SABSA (Sherwood Applied Business Security Architecture) is a framework and methodology specifically designed for Enterprise Security Architecture and Service Management. It provides a layered approach to security architecture, ensuring that security is aligned with business goals and is driven by risk management principles.SABSA's methodology integrates with business and IT management processes, focusing on the design, delivery, and support of security services within the enterprise environment1.

TOGAF (The Open Group Architecture Framework) is also used in the context of enterprise architecture but is not solely focused on security.It provides a comprehensive approach to the design, planning, implementation, and governance of an enterprise information architecture2.

PCI DSS (Payment Card Industry Data Security Standard) is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment2.

OWASP (Open Web Application Security Project) is an online community that produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security2.

Question 9

Question Type: MultipleChoice

Once data has been created In a standard information lifecycle, what step TYPICALLY happens next?

Options:

A- Data Deletion.

B- Data Archiving.

C- Data Storage.

D- Data Publication

Answer:

C

Explanation:

After data creation, the typical next step in the standard information lifecycle is data storage. This phase involves securing the data in a storage solution where it can be accessed, managed, and protected effectively. Proper data storage ensures that data remains intact and available for future processing and analysis.It is a critical step before data can be used for any operational or analytical purposes, and precedes other stages such as archiving or deletion, which occur later in the lifecycle123.

Question 10

Question Type: MultipleChoice

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

Options:

A- Disposal.

B- Creation.

C- Use.

D- Publication.

Answer:

A

Explanation:

The final stage in the information management lifecycle is often disposal. This stage involves the secure deletion or destruction of information that is no longer needed or has reached the end of its retention period. Proper disposal is crucial to prevent unauthorized access or recovery of sensitive data. It ensures compliance with data protection regulations and organizational policies regarding the retention and destruction of data.

Question 11

Question Type: MultipleChoice

The policies, processes, practices, and tools used to align the business value of information with the most appropriate and cost-effective infrastructure from the time information is conceived through its final disposition.

Which of the below business practices does this statement define?

Options:

A- Information Lifecycle Management.

B- Information Quality Management.

C- Total Quality Management.

D- Business Continuity Management.

Answer:

A

Explanation:

The statement defines Information Lifecycle Management (ILM), which is a set of policies, processes, practices, and tools that manage the flow of an organization's information throughout its life cycle. ILM is concerned with aligning the business value of information with the most appropriate and cost-effective infrastructure from the moment the information is created until its final disposition. This includes how information is created, stored, used, archived, and eventually disposed of. An effective ILM strategy helps organizations manage their data in compliance with business requirements, regulatory obligations, and cost constraints.