PDFDumps

Quality and Value

PDFDumps Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all vce.

Tested and Approved

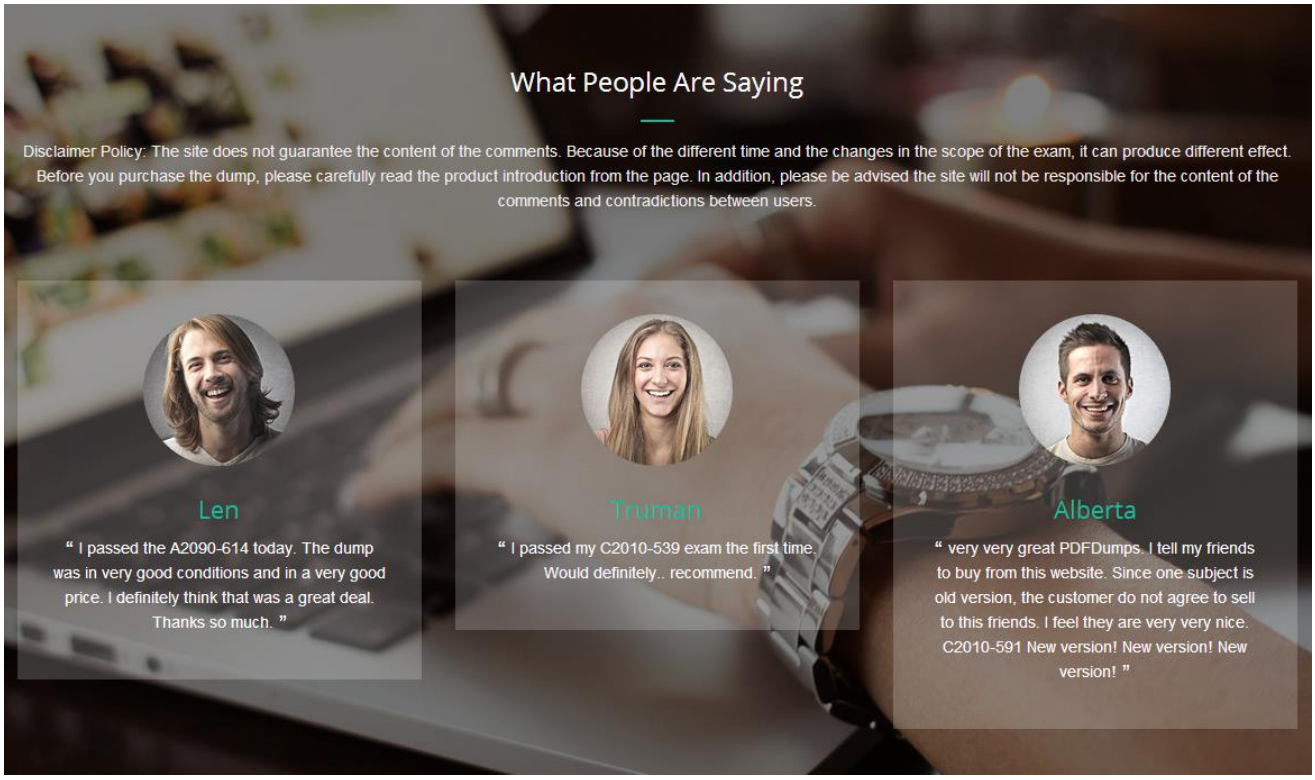
We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.

Easy to Pass

If you prepare for the exams using our PDFDumps testing engine, It is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.

Try Before Buy

PDFDumps offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.



http://www.pdfdumps.com

PDFDumps can solve all your IT exam problems and broaden your knowledge

Exam : **CISSP**

Title : Certified Information Systems Security Professional (CISSP)

Vendor : ISC

Version : DEMO

NO.1 A Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) will provide which of the following?

A. Guaranteed recovery of all business functions

B. Minimization of the need decision making during a crisis

C. Insurance against litigation following a disaster

D. Protection from loss of organization resources

Answer: B

Explanation:

Minimization of the need for decision making during a crisis is the main benefit that a Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) will provide. A BCP/DRP is a set of policies, procedures, and resources that enable an organization to continue or resume its critical functions and operations in the event of a disruption or disaster. A BCP/DRP can provide several benefits, such as:

Improving the resilience and preparedness of the organization and its staff in handling a disruption or disaster Enhancing the performance and efficiency of the organization and its systems in recovering from a disruption or disaster Increasing the compliance and alignment of the organization and its plans with the internal or external requirements and standards Facilitating the monitoring and improvement of the organization and its plans by identifying and addressing any gaps, issues, or risks Minimization of the need for decision making during a crisis is the main benefit that a BCP/DRP will provide, because it can ensure that the organization and its staff have a clear and consistent guidance and direction on how to respond and act during a disruption or disaster, and avoid any confusion, uncertainty, or inconsistency that might worsen the situation or impact. A BCP/DRP can also help to reduce the stress and pressure on the organization and its staff during a crisis, and increase their confidence and competence in executing the plans.

NO.2 When is a Business Continuity Plan (BCP) considered to be valid?

A. When it has been validated by the Business Continuity (BC) manager

B. When it has been validated by the board of directors

C. When it has been validated by all threat scenarios

D. When it has been validated by realistic exercises

Answer: D

Explanation:

A Business Continuity Plan (BCP) is considered to be valid when it has been validated by realistic exercises. A BCP is a part of a BCP/DRP that focuses on ensuring the continuous operation of the organization's critical business functions and processes during and after a disruption or disaster. A BCP should include various components, such as:

Business impact analysis: a process that identifies and prioritizes the critical business functions and processes, and assesses the potential impacts and risks of a disruption or disaster on them Recovery strategies: a process that defines and selects the appropriate methods and resources to recover the critical business functions and processes, such as alternate sites, backup systems, or recovery teams BCP document: a document that outlines and details the scope, purpose, and features of the BCP, such as the roles and responsibilities, the recovery procedures, and the contact information Testing, training, and exercises: a process that evaluates and validates the effectiveness and readiness of the BCP, and educates and trains the relevant stakeholders, such as the staff, the management, and the customers, on the BCP and their roles and responsibilities Maintenance and review: a process that

monitors and updates the BCP, and addresses any changes or issues that might affect the BCP, such as the business requirements, the threat landscape, or the feedback and lessons learned A BCP is considered to be valid when it has been validated by realistic exercises, because it can ensure that the BCP is practical and applicable, and that it can achieve the desired outcomes and objectives in a real-life scenario. Realistic exercises are a type of testing, training, and exercises that involve performing and practicing the BCP with the relevant stakeholders, using simulated or hypothetical scenarios, such as a fire drill, a power outage, or a cyberattack. Realistic exercises can provide several benefits, such as:
Improving the confidence and competence of the organization and its staff in handling a disruption or disaster Enhancing the performance and efficiency of the organization and its systems in recovering from a disruption or disaster Increasing the compliance and alignment of the organization and its plans with the internal or external requirements and standards Facilitating the monitoring and improvement of the organization and its plans by identifying and addressing any gaps, issues, or risks

NO.3 Recovery strategies of a Disaster Recovery planning (DRIP) MUST be aligned with which of the following?

A. Hardware and software compatibility issues

B. Applications' critically and downtime tolerance

C. Budget constraints and requirements

D. Cost/benefit analysis and business objectives

Answer: D

Explanation:
Recovery strategies of a Disaster Recovery planning (DRP) must be aligned with the cost/benefit analysis and business objectives. A DRP is a part of a BCP/DRP that focuses on restoring the normal operation of the organization's IT systems and infrastructure after a disruption or disaster.
A DRP should include various components, such as:
Risk assessment: a process that identifies and evaluates the potential threats and vulnerabilities that might affect the IT systems and infrastructure, and estimates the likelihood and impact of a disruption or disaster Recovery objectives: a process that defines and quantifies the acceptable levels of recovery for the IT systems and infrastructure, such as the recovery point objective (RPO), which is the maximum amount of data loss that can be tolerated, and the recovery time objective (RTO), which is the maximum amount of downtime that can be tolerated Recovery strategies: a process that selects and implements the appropriate methods and resources to recover the IT systems and infrastructure, such as backup, replication, redundancy, or failover DRP document: a document that outlines and details the scope, purpose, and features of the DRP, such as the roles and responsibilities, the recovery procedures, and the contact information Testing, training, and exercises: a process that evaluates and validates the effectiveness and readiness of the DRP, and educates and trains the relevant stakeholders, such as the IT staff, the management, and the users, on the DRP and their roles and responsibilities Maintenance and review: a process that monitors and updates the DRP, and addresses any changes or issues that might affect the DRP, such as the IT requirements, the threat landscape, or the feedback and lessons learned Recovery strategies of a DRP must be aligned with the cost/benefit analysis and business objectives, because it can ensure that the DRP is feasible and suitable, and that it can achieve the desired outcomes and objectives in a cost-effective and efficient manner. A cost/benefit analysis is a technique that compares the costs and benefits of different recovery strategies, and determines the optimal one that provides the best value for money. A business objective is a goal or a target that the organization wants to achieve

through its IT systems and infrastructure, such as increasing the productivity, profitability, or customer satisfaction. A recovery strategy that is aligned with the cost/benefit analysis and business objectives can help to:
Optimize the use and allocation of the IT resources and funds for the recovery Minimize the negative impacts and risks of a disruption or disaster on the IT systems and infrastructure Maximize the positive outcomes and benefits of the recovery for the IT systems and infrastructure Support and enable the achievement of the organizational goals and targets through the IT systems and infrastructure

NO.4 Which of the following is the FIRST step in the incident response process?
A. Determine the cause of the incident
B. Disconnect the system involved from the network
C. Isolate and contain the system involved
D. Investigate all symptoms to confirm the incident
Answer: D
Explanation:
Investigating all symptoms to confirm the incident is the first step in the incident response process. An incident is an event that violates or threatens the security, availability, integrity, or confidentiality of the IT systems or data. An incident response is a process that involves detecting, analyzing, containing, eradicating, recovering, and learning from an incident, using various methods and tools. An incident response can provide several benefits, such as:
Improving the security and risk management of the IT systems and data by identifying and addressing the security weaknesses and gaps Enhancing the security and decision making of the IT systems and data by providing the evidence and information for the security analysis, evaluation, and reporting Increasing the security and improvement of the IT systems and data by providing the feedback and input for the security response, remediation, and optimization Facilitating the compliance and alignment of the IT systems and data with the internal or external requirements and standards Investigating all symptoms to confirm the incident is the first step in the incident response process, because it can ensure that the incident is verified and validated, and that the incident response is initiated and escalated. A symptom is a sign or an indication that an incident may have occurred or is occurring, such as an alert, a log, or a report. Investigating all symptoms to confirm the incident involves collecting and analyzing the relevant data and information from various sources, such as the IT systems, the network, the users, or the external parties, and determining whether an incident has actually happened or is happening, and how serious or urgent it is. Investigating all symptoms to confirm the incident can also help to:
Prevent the false positives or negatives that might cause the incident response to be delayed or unnecessary Identify the scope and impact of the incident on the IT systems and data Notify and inform the appropriate stakeholders and authorities about the incident Activate and coordinate the incident response team and resources

NO.5 A continuous information security-monitoring program can BEST reduce risk through which of the following?
A. Collecting security events and correlating them to identify anomalies
B. Facilitating system-wide visibility into the activities of critical user accounts
C. Encompassing people, process, and technology

D. Logging both scheduled and unscheduled system changes

Answer: C

Explanation:

A continuous information security monitoring program can best reduce risk through encompassing people, process, and technology. A continuous information security monitoring program is a process that involves maintaining the ongoing awareness of the security status, events, and activities of a system or network, by collecting, analyzing, and reporting the security data and information, using various methods and tools. A continuous information security monitoring program can provide several benefits, such as:

Improving the security and risk management of the system or network by identifying and addressing the security weaknesses and gaps Enhancing the security and decision making of the system or network by providing the evidence and information for the security analysis, evaluation, and reporting Increasing the security and improvement of the system or network by providing the feedback and input for the security response, remediation, and optimization Facilitating the compliance and alignment of the system or network with the internal or external requirements and standards A continuous information security monitoring program can best reduce risk through encompassing people, process, and technology, because it can ensure that the continuous information security monitoring program is holistic and comprehensive, and that it covers all the aspects and elements of the system or network security. People, process, and technology are the three pillars of a continuous information security monitoring program, and they represent the following:

People: the human resources that are involved in the continuous information security monitoring program, such as the security analysts, the system administrators, the management, and the users. People are responsible for defining the security objectives and requirements, implementing and operating the security tools and controls, and monitoring and responding to the security events and incidents.

Process: the procedures and policies that are followed in the continuous information security monitoring program, such as the security standards and guidelines, the security roles and responsibilities, the security workflows and tasks, and the security metrics and indicators. Process is responsible for establishing and maintaining the security governance and compliance, ensuring the security consistency and efficiency, and measuring and evaluating the security performance and effectiveness.

Technology: the tools and systems that are used in the continuous information security monitoring program, such as the security sensors and agents, the security loggers and collectors, the security analyzers and correlators, and the security dashboards and reports. Technology is responsible for supporting and enabling the security functions and capabilities, providing the security visibility and awareness, and delivering the security data and information.

NO.6 What would be the MOST cost effective solution for a Disaster Recovery (DR) site given that the organization's systems cannot be unavailable for more than 24 hours?

A. Warm site

B. Hot site

C. Mirror site

D. Cold site

Answer: A

Explanation:
A warm site is the most cost effective solution for a disaster recovery (DR) site given that the organization's systems cannot be unavailable for more than 24 hours. A DR site is a backup facility that can be used to restore the normal operation of the organization's IT systems and infrastructure after a disruption or disaster. A DR site can have different levels of readiness and functionality, depending on the organization's recovery objectives and budget. The main types of DR sites are:
Hot site: a DR site that is fully operational and equipped with the necessary hardware, software, telecommunication lines, and network connectivity to allow the organization to be up and running almost immediately. A hot site has all the required servers, workstations, and communications links, and can function as a branch office or data center that is online and connected to the production network. A hot site also has a backup of the data from the systems at the primary site, which may be replicated in real time or near real time. A hot site greatly reduces or eliminates downtime for the organization, but it is also very expensive to maintain and operate.
Warm site: a DR site that is partially operational and equipped with some of the hardware, software, telecommunication lines, and network connectivity to allow the organization to be up and running within a short time. A warm site has some of the required servers, workstations, and communications links, and can function as a temporary office or data center that is offline or partially connected to the production network. A warm site may have a backup of the data from the systems at the primary site, but it is not updated or synchronized as frequently as a hot site. A warm site reduces downtime for the organization, but it is also less expensive than a hot site.
Cold site: a DR site that is not operational and equipped with only the basic infrastructure and environmental support systems to allow the organization to be up and running within a long time. A cold site has none of the required servers, workstations, and communications links, and cannot function as an office or data center until they are installed and configured. A cold site does not have a backup of the data from the systems at the primary site, and it has to be restored from other sources, such as tapes or disks. A cold site increases downtime for the organization, but it is also the cheapest option among the DR sites.
Mirror site: a DR site that is an exact replica of the primary site, with the same hardware, software, telecommunication lines, and network connectivity, and with the same data and applications. A mirror site is always online and synchronized with the primary site, and can take over the operation of the organization seamlessly in the event of a disruption or disaster. A mirror site eliminates downtime for the organization, but it is also the most expensive option among the DR sites.
A warm site is the most cost effective solution for a disaster recovery (DR) site given that the organization's systems cannot be unavailable for more than 24 hours, because it can provide a balance between the recovery time and the recovery cost. A warm site can enable the organization to resume its critical functions and operations within a reasonable time frame, without spending too much on the DR site maintenance and operation. A warm site can also provide some flexibility and scalability for the organization to adjust its recovery strategies and resources according to its needs and priorities.

NO.7 A Java program is being developed to read a file from computer A and write it to computer B, using a third computer C. The program is not working as expected. What is the MOST probable security feature of Java preventing the program from operating as intended?

A. Least privilege

B. Privilege escalation

C. Defense in depth

D. Privilege bracketing

Answer: A

Explanation:

The most probable security feature of Java preventing the program from operating as intended is least privilege. Least privilege is a principle that states that a subject (such as a user, a process, or a program) should only have the minimum amount of access or permissions that are necessary to perform its function or task. Least privilege can help to reduce the attack surface and the potential damage of a system or network, by limiting the exposure and impact of a subject in case of a compromise or misuse.

Java implements the principle of least privilege through its security model, which consists of several components, such as:

The Java Virtual Machine (JVM): a software layer that executes the Java bytecode and provides an abstraction from the underlying hardware and operating system. The JVM enforces the security rules and restrictions on the Java programs, such as the memory protection, the bytecode verification, and the exception handling.

The Java Security Manager: a class that defines and controls the security policy and permissions for the Java programs. The Java Security Manager can be configured and customized by the system administrator or the user, and can grant or deny the access or actions of the Java programs, such as the file I/O, the network communication, or the system properties.

The Java Security Policy: a file that specifies the security permissions for the Java programs, based on the code source and the code signer. The Java Security Policy can be defined and modified by the system administrator or the user, and can assign different levels of permissions to different Java programs, such as the trusted or the untrusted ones.

The Java Security Sandbox: a mechanism that isolates and restricts the Java programs that are downloaded or executed from untrusted sources, such as the web or the network. The Java Security Sandbox applies the default or the minimal security permissions to the untrusted Java programs, and prevents them from accessing or modifying the local resources or data, such as the files, the databases, or the registry.

In this question, the Java program is being developed to read a file from computer A and write it to computer B, using a third computer C. This means that the Java program needs to have the permissions to perform the file I/O and the network communication operations, which are considered as sensitive or risky actions by the Java security model. However, if the Java program is running on computer C with the default or the minimal security permissions, such as in the Java Security Sandbox, then it will not be able to perform these operations, and the program will not work as expected. Therefore, the most probable security feature of Java preventing the program from operating as intended is least privilege, which limits the access or permissions of the Java program based on its source, signer, or policy.

NO.8 Which of the following is the PRIMARY risk with using open source software in a commercial software construction?

A. Lack of software documentation

B. License agreements requiring release of modified code

C. Expiration of the license agreement

D. Costs associated with support of the software

Answer: B

Explanation:
The primary risk with using open source software in a commercial software construction is license agreements requiring release of modified code. Open source software is software that uses publicly available source code, which can be seen, modified, and distributed by anyone. Open source software has some advantages, such as being affordable and flexible, but it also has some disadvantages, such as being potentially insecure or unsupported.
One of the main disadvantages of using open source software in a commercial software construction is the license agreements that govern the use and distribution of the open source software. License agreements are legal contracts that specify the rights and obligations of the parties involved in the software, such as the original authors, the developers, and the users.
License agreements can vary in terms of their terms and conditions, such as the scope, the duration, or the fees of the software.
Some of the common types of license agreements for open source software are:
Permissive licenses: license agreements that allow the developers and users to freely use, modify, and distribute the open source software, with minimal or no restrictions. Examples of permissive licenses are the MIT License, the Apache License, or the BSD License.
Copyleft licenses: license agreements that require the developers and users to share and distribute the open source software and any modifications or derivatives of it, under the same or compatible license terms and conditions. Examples of copyleft licenses are the GNU General Public License (GPL), the GNU Lesser General Public License (LGPL), or the Mozilla Public License (MPL).
Mixed licenses: license agreements that combine the elements of permissive and copyleft licenses, and may apply different license terms and conditions to different parts or components of the open source software. Examples of mixed licenses are the Eclipse Public License (EPL), the Common Development and Distribution License (CDDL), or the GNU Affero General Public License (AGPL).
The primary risk with using open source software in a commercial software construction is license agreements requiring release of modified code, which are usually associated with copyleft licenses. This means that if a commercial software construction uses or incorporates open source software that is licensed under a copyleft license, then it must also release its own source code and any modifications or derivatives of it, under the same or compatible copyleft license. This can pose a significant risk for the commercial software construction, as it may lose its competitive advantage, intellectual property, or revenue, by disclosing its source code and allowing others to use, modify, or distribute it.

NO.9 When in the Software Development Life Cycle (SDLC) MUST software security functional requirements be defined?

A. After the system preliminary design has been developed and the data security categorization has been performed

B. After the vulnerability analysis has been performed and before the system detailed design begins

C. After the system preliminary design has been developed and before the data security categorization begins

D. After the business functional analysis and the data security categorization have been performed

Answer: D

Explanation:
Software security functional requirements must be defined after the business functional analysis and the data security categorization have been performed in the Software Development Life Cycle (SDLC). The SDLC is a process that involves planning, designing, developing, testing, deploying, operating, and

maintaining a system, using various models and methodologies, such as waterfall, spiral, agile, or DevSecOps. The SDLC can be divided into several phases, each with its own objectives and activities, such as:
System initiation: This phase involves defining the scope, purpose, and objectives of the system, identifying the stakeholders and their needs and expectations, and establishing the project plan and budget.
System acquisition and development: This phase involves designing the architecture and components of the system, selecting and procuring the hardware and software resources, developing and coding the system functionality and features, and integrating and testing the system modules and interfaces.
System implementation: This phase involves deploying and installing the system to the production environment, migrating and converting the data and applications from the legacy system, training and educating the users and staff on the system operation and maintenance, and evaluating and validating the system performance and effectiveness.
System operations and maintenance: This phase involves operating and monitoring the system functionality and availability, maintaining and updating the system hardware and software, resolving and troubleshooting any issues or problems, and enhancing and optimizing the system features and capabilities.
Software security functional requirements are the specific and measurable security features and capabilities that the system must provide to meet the security objectives and requirements. Software security functional requirements are derived from the business functional analysis and the data security categorization, which are two tasks that are performed in the system initiation phase of the SDLC. The business functional analysis is the process of identifying and documenting the business functions and processes that the system must support and enable, such as the inputs, outputs, workflows, and tasks. The data security categorization is the process of determining the security level and impact of the system and its data, based on the confidentiality, integrity, and availability criteria, and applying the appropriate security controls and measures. Software security functional requirements must be defined after the business functional analysis and the data security categorization have been performed, because they can ensure that the system design and development are consistent and compliant with the security objectives and requirements, and that the system security is aligned and integrated with the business functions and processes.

NO.10 Which of the following is the BEST method to prevent malware from being introduced into a production environment?

A. Purchase software from a limited list of retailers

B. Verify the hash key or certificate key of all updates

C. Do not permit programs, patches, or updates from the Internet

D. Test all new software in a segregated environment

Answer: D

Explanation:
Testing all new software in a segregated environment is the best method to prevent malware from being introduced into a production environment. Malware is any malicious software that can harm or compromise the security, availability, integrity, or confidentiality of a system or data. Malware can be introduced into a production environment through various sources, such as software downloads, updates, patches, or installations. Testing all new software in a segregated environment involves verifying and validating the functionality and security of the software before deploying it to the production environment, using a separate system or network that is isolated and protected from the

production environment. Testing all new software in a segregated environment can provide several benefits, such as:
Preventing the infection or propagation of malware to the production environment Detecting and resolving any issues or risks caused by the software Ensuring the compatibility and interoperability of the software with the production environment Supporting and enabling the quality assurance and improvement of the software

NO.11 The configuration management and control task of the certification and accreditation process is incorporated in which phase of the System Development Life Cycle (SDLC)?

A. System acquisition and development

B. System operations and maintenance

C. System initiation

D. System implementation

Answer: A

Explanation:
The configuration management and control task of the certification and accreditation process is incorporated in the system acquisition and development phase of the System Development Life Cycle (SDLC). The SDLC is a process that involves planning, designing, developing, testing, deploying, operating, and maintaining a system, using various models and methodologies, such as waterfall, spiral, agile, or DevSecOps. The SDLC can be divided into several phases, each with its own objectives and activities, such as:
System initiation: This phase involves defining the scope, purpose, and objectives of the system, identifying the stakeholders and their needs and expectations, and establishing the project plan and budget.
System acquisition and development: This phase involves designing the architecture and components of the system, selecting and procuring the hardware and software resources, developing and coding the system functionality and features, and integrating and testing the system modules and interfaces.
System implementation: This phase involves deploying and installing the system to the production environment, migrating and converting the data and applications from the legacy system, training and educating the users and staff on the system operation and maintenance, and evaluating and validating the system performance and effectiveness.
System operations and maintenance: This phase involves operating and monitoring the system functionality and availability, maintaining and updating the system hardware and software, resolving and troubleshooting any issues or problems, and enhancing and optimizing the system features and capabilities.
The certification and accreditation process is a process that involves assessing and verifying the security and compliance of a system, and authorizing and approving the system operation and maintenance, using various standards and frameworks, such as NIST SP 800-37 or ISO/IEC 27001. The certification and accreditation process can be divided into several tasks, each with its own objectives and activities, such as:
Security categorization: This task involves determining the security level and impact of the system and its data, based on the confidentiality, integrity, and availability criteria, and applying the appropriate security controls and measures.
Security planning: This task involves defining the security objectives and requirements of the system, identifying the roles and responsibilities of the security stakeholders, and developing and documenting the security plan and policy.

Security implementation: This task involves implementing and enforcing the security controls and measures for the system, according to the security plan and policy, and ensuring the security functionality and compatibility of the system.
Security assessment: This task involves evaluating and testing the security effectiveness and compliance of the system, using various techniques and tools, such as audits, reviews, scans, or penetration tests, and identifying and reporting any security weaknesses or gaps.
Security authorization: This task involves reviewing and approving the security assessment results and recommendations, and granting or denying the authorization for the system operation and maintenance, based on the risk and impact analysis and the security objectives and requirements.
Security monitoring: This task involves monitoring and updating the security status and activities of the system, using various methods and tools, such as logs, alerts, or reports, and addressing and resolving any security issues or changes.
The configuration management and control task of the certification and accreditation process is incorporated in the system acquisition and development phase of the SDLC, because it can ensure that the system design and development are consistent and compliant with the security objectives and requirements, and that the system changes are controlled and documented.
Configuration management and control is a process that involves establishing and maintaining the baseline and the inventory of the system components and resources, such as hardware, software, data, or documentation, and tracking and recording any modifications or updates to the system components and resources, using various techniques and tools, such as version control, change control, or configuration audits. Configuration management and control can provide several benefits, such as:
Improving the quality and security of the system design and development by identifying and addressing any errors or inconsistencies Enhancing the performance and efficiency of the system design and development by optimizing the use and allocation of the system components and resources Increasing the compliance and alignment of the system design and development with the security objectives and requirements by applying and enforcing the security controls and measures Facilitating the monitoring and improvement of the system design and development by providing the evidence and information for the security assessment and authorization

NO.12 What is the BEST approach to addressing security issues in legacy web applications?
A. Debug the security issues
B. Migrate to newer, supported applications where possible
C. Conduct a security assessment
D. Protect the legacy application with a web application firewall
Answer: B
Explanation:
Migrating to newer, supported applications where possible is the best approach to addressing security issues in legacy web applications. Legacy web applications are web applications that are outdated, unsupported, or incompatible with the current technologies and standards. Legacy web applications may have various security issues, such as:
Vulnerabilities and bugs that are not fixed or patched by the developers or vendors Weak or obsolete encryption and authentication mechanisms that are easily broken or bypassed by attackers Lack of compliance with the security policies and regulations that are applicable to the web applications Incompatibility or interoperability issues with the newer web browsers, operating systems, or platforms that are used by the users or clients Migrating to newer, supported applications where

possible is the best approach to addressing security issues in legacy web applications, because it can provide several benefits, such as:
Enhancing the security and performance of the web applications by using the latest technologies and standards that are more secure and efficient Reducing the risk and impact of the web application attacks by eliminating or minimizing the vulnerabilities and bugs that are present in the legacy web applications Increasing the compliance and alignment of the web applications with the security policies and regulations that are applicable to the web applications Improving the compatibility and interoperability of the web applications with the newer web browsers, operating systems, or platforms that are used by the users or clients

NO.13 Which of the following is a web application control that should be put into place to prevent exploitation of Operating System (OS) bugs?
A. Check arguments in function calls
B. Test for the security patch level of the environment
C. Include logging functions
D. Digitally sign each application module
Answer: B
Explanation:
Testing for the security patch level of the environment is the web application control that should be put into place to prevent exploitation of Operating System (OS) bugs. OS bugs are errors or defects in the code or logic of the OS that can cause the OS to malfunction or behave unexpectedly. OS bugs can be exploited by attackers to gain unauthorized access, disrupt business operations, or steal or leak sensitive data. Testing for the security patch level of the environment is the web application control that should be put into place to prevent exploitation of OS bugs, because it can provide several benefits, such as:
Detecting and resolving any vulnerabilities or issues caused by the OS bugs by applying the latest security patches or updates from the OS developers or vendors Enhancing the security and performance of the web applications by using the most secure and efficient version of the OS that supports the web applications Increasing the compliance and alignment of the web applications with the security policies and regulations that are applicable to the web applications Improving the compatibility and interoperability of the web applications with the other systems or platforms that interact with the web applications

NO.14 Which of the following methods protects Personally Identifiable Information (PII) by use of a full replacement of the data element?
A. Transparent Database Encryption (TDE)
B. Column level database encryption
C. Volume encryption
D. Data tokenization
Answer: D
Explanation:
Data tokenization is a method of protecting PII by replacing the sensitive data element with a non-sensitive equivalent, called a token, that has no extrinsic or exploitable meaning or value. The token is then mapped back to the original data element in a secure database. This way, the PII is not exposed in the data processing or storage, and only authorized parties can access the original data

element. Data tokenization is different from encryption, which transforms the data element into a ciphertext that can be decrypted with a key. Data tokenization does not require a key, and the token cannot be reversed to reveal the original data element.

NO.15 Which of the following elements MUST a compliant EU-US Safe Harbor Privacy Policy contain?

A. An explanation of how long the data subject's collected information will be retained for and how it will be eventually disposed.

B. An explanation of who can be contacted at the organization collecting the information if corrections are required by the data subject.

C. An explanation of the regulatory frameworks and compliance standards the information collecting organization adheres to.

D. An explanation of all the technologies employed by the collecting organization in gathering information on the data subject.

Answer: B

Explanation:

The EU-US Safe Harbor Privacy Policy is a framework that was established in 2000 to enable the transfer of personal data from the European Union to the United States, while ensuring adequate protection of the data subject's privacy rights. The framework was invalidated by the European Court of Justice in 2015, and replaced by the EU-US Privacy Shield in 2016. However, the Safe Harbor Privacy Policy still serves as a reference for the principles and requirements of data protection across the Atlantic. One of the elements that a compliant Safe Harbor Privacy Policy must contain is an explanation of who can be contacted at the organization collecting the information if corrections are required by the data subject. This is part of the principle of access, which states that individuals must have access to their personal information and be able to correct, amend, or delete it where it is inaccurate.

NO.16 What is the MOST effective countermeasure to a malicious code attack against a mobile system?

A. Sandbox

B. Change control

C. Memory management

D. Public-Key Infrastructure (PKI)

Answer: A

Explanation:

A sandbox is a security mechanism that isolates a potentially malicious code or application from the rest of the system, preventing it from accessing or modifying any sensitive data or resources.
A sandbox can be implemented at the operating system, application, or network level, and can provide a safe environment for testing, debugging, or executing untrusted code. A sandbox is the most effective countermeasure to a malicious code attack against a mobile system, as it can prevent the code from spreading, stealing, or destroying any information on the device. Change control, memory management, and PKI are not directly related to preventing or mitigating malicious code attacks on mobile systems.

NO.17 Which of the following is the BEST mitigation from phishing attacks?

A. Network activity monitoring
B. Security awareness training
C. Corporate policy and procedures
D. Strong file and directory permissions
Answer: B
Explanation:
Security awareness training is the process of educating users on the potential threats and risks they may face online, and the best practices and behaviors they should adopt to protect themselves and the organization. Security awareness training is the best mitigation from phishing attacks, as it can help users recognize and avoid malicious emails, links, or attachments that may compromise their credentials, data, or devices. Network activity monitoring, corporate policy and procedures, and strong file and directory permissions are also important security measures, but they are not as effective as security awareness training in preventing phishing attacks, as they rely on technical controls rather than human factors.

NO.18 Which of the following is a physical security control that protects Automated Teller Machines (ATM) from skimming?
A. Anti-tampering
B. Secure card reader
C. Radio Frequency (RF) scanner
D. Intrusion Prevention System (IPS)
Answer: B
Explanation:
A secure card reader is a physical security control that protects ATM from skimming, which is a type of fraud where a device is attached to the card slot of an ATM to capture the data from the magnetic stripe of the card. A secure card reader can prevent skimming by encrypting the data at the point of entry, making it unreadable by the skimming device. Anti-tampering, RF scanner, and IPS are not physical security controls that protect ATM from skimming, as they do not prevent the capture of the card data by the skimming device.

NO.19 Which of the following is an essential element of a privileged identity lifecycle management?
A. Regularly perform account re-validation and approval
B. Account provisioning based on multi-factor authentication
C. Frequently review performed activities and request justification
D. Account information to be provided by supervisor or line manager
Answer: A
Explanation:
A privileged identity lifecycle management is a process of managing the access rights and activities of users who have elevated permissions to access sensitive data or resources in an organization. An essential element of a privileged identity lifecycle management is to regularly perform account re-validation and approval, which means verifying that the privileged users still need their access rights and have them approved by the appropriate authority. This can help prevent unauthorized or excessive access, reduce the risk of insider threats, and ensure compliance with policies and regulations. Account provisioning based on multi-factor authentication, frequently review performed activities and request justification, and account information to be provided by supervisor or line

manager are also important aspects of a privileged identity lifecycle management, but they are not as essential as account re-validation and approval.

NO.20 Which of the following is ensured when hashing files during chain of custody handling?

A. Availability

B. Accountability

C. Integrity

D. Non-repudiation

Answer: C

Explanation:

Hashing files during chain of custody handling ensures integrity, which means that the files have not been altered or tampered with during the collection, preservation, or analysis of digital evidence. Hashing is a process of applying a mathematical function to a file to generate a unique value, called a hash or a digest, that represents the file's content. By comparing the hash values of the original and the copied files, the integrity of the files can be verified. Availability, accountability, and non-repudiation are not ensured by hashing files during chain of custody handling, as they are related to different aspects of information security.

NO.21 Which Hyper Text Markup Language 5 (HTML5) option presents a security challenge for network data leakage prevention and/or monitoring?

A. Cross Origin Resource Sharing (CORS)

B. WebSockets

C. Document Object Model (DOM) trees

D. Web Interface Definition Language (IDL)

Answer: B

Explanation:

WebSockets is an HTML5 option that presents a security challenge for network data leakage prevention and/or monitoring, as it enables a bidirectional, full-duplex communication channel between a web browser and a server. WebSockets can bypass the traditional HTTP request- response model and establish a persistent connection that can exchange data in real time. This can pose a risk of data leakage, as the data transmitted over WebSockets may not be inspected or filtered by the network security devices, such as firewalls, proxies, or data loss prevention systems. Cross Origin Resource Sharing (CORS), Document Object Model (DOM) trees, and Web Interface Definition Language (IDL) are not HTML5 options that present a security challenge for network data leakage prevention and/or monitoring, as they are not related to the communication channel between the web browser and the server.

NO.22 Which of the following statements is TRUE of black box testing?

A. Only the functional specifications are known to the test planner.

B. Only the source code and the design documents are known to the test planner.

C. Only the source code and functional specifications are known to the test planner.

D. Only the design documents and the functional specifications are known to the test planner.

Answer: A

Explanation:

Black box testing is a method of software testing that does not require any knowledge of the internal

structure or code of the software. The test planner only knows the functional specifications, which describe what the software is supposed to do, and tests the software based on the expected inputs and outputs. Black box testing is useful for finding errors in the functionality, usability, or performance of the software, but it cannot detect errors in the code or design. White box testing, on the other hand, requires the test planner to have access to the source code and the design documents, and tests the software based on the internal logic and structure.

NO.23 A software scanner identifies a region within a binary image having high entropy. What does this MOST likely indicate?

A. Encryption routines

B. Random number generator

C. Obfuscated code

D. Botnet command and control

Answer: C

Explanation:

Obfuscated code is a type of code that is deliberately written or modified to make it difficult to understand or reverse engineer. Obfuscation techniques can include changing variable names, removing comments, adding irrelevant code, or encrypting parts of the code. Obfuscated code can have high entropy, which means that it has a high degree of randomness or unpredictability.

A software scanner can identify a region within a binary image having high entropy as a possible indication of obfuscated code. Encryption routines, random number generators, and botnet command and control are not necessarily related to obfuscated code, and may not have high entropy.

NO.24 Which of the following is a limitation of the Common Vulnerability Scoring System (CVSS) as it relates to conducting code review?

A. It has normalized severity ratings.

B. It has many worksheets and practices to implement.

C. It aims to calculate the risk of published vulnerabilities.

D. It requires a robust risk management framework to be put in place.

Answer: C

Explanation:

The Common Vulnerability Scoring System (CVSS) is a framework that provides a standardized and consistent way of measuring and communicating the severity and risk of published vulnerabilities. CVSS assigns a numerical score and a vector string to each vulnerability, based on various metrics and formulas. CVSS is a useful tool for prioritizing the remediation of vulnerabilities, but it has some limitations as it relates to conducting code review. One of the limitations is that CVSS aims to calculate the risk of published vulnerabilities, which means that it does not cover the vulnerabilities that are not yet discovered or disclosed. Code review, on the other hand, is a process of examining the source code of a software to identify and fix any errors, bugs, or vulnerabilities that may exist in the code. Code review can help find vulnerabilities that are not yet published, and therefore not scored by CVSS.

NO.25 Which of the following is the MOST important consideration when storing and processing Personally Identifiable Information (PII)?

A. Encrypt and hash all PII to avoid disclosure and tampering.
B. Store PII for no more than one year.
C. Avoid storing PII in a Cloud Service Provider.
D. Adherence to collection limitation laws and regulations.
Answer: D
Explanation:
The most important consideration when storing and processing PII is to adhere to the collection limitation laws and regulations that apply to the jurisdiction and context of the data processing. Collection limitation is a principle that states that PII should be collected only for a specific, legitimate, and lawful purpose, and only to the extent that is necessary for that purpose. By following this principle, the data processor can minimize the amount of PII that is stored and processed, and reduce the risk of data breaches, misuse, or unauthorized access. Encrypting and hashing all PII, storing PII for no more than one year, and avoiding storing PII in a cloud service provider are also good practices for protecting PII, but they are not as important as adhering to the collection limitation laws and regulations.

NO.26 Which of the following assessment metrics is BEST used to understand a system's vulnerability to potential exploits?
A. Determining the probability that the system functions safely during any time period
B. Quantifying the system's available services
C. Identifying the number of security flaws within the system
D. Measuring the system's integrity in the presence of failure
Answer: C
Explanation:
Identifying the number of security flaws within the system is the best assessment metric to understand a system's vulnerability to potential exploits. A security flaw is a weakness or a defect in the system's design, implementation, or operation that could be exploited by an attacker to compromise the system's confidentiality, integrity, or availability. By identifying the number of security flaws within the system, the assessor can measure the system's vulnerability, which is the degree to which the system is susceptible or exposed to attacks. Determining the probability that the system functions safely during any time period, quantifying the system's available services, and measuring the system's integrity in the presence of failure are not assessment metrics that directly relate to the system's vulnerability to potential exploits, as they are more concerned with the system's reliability, availability, and resilience.

NO.27 Which of the following is an effective method for avoiding magnetic media data remanence?
A. Degaussing
B. Encryption
C. Data Loss Prevention (DLP)
D. Authentication
Answer: A
Explanation:
Degaussing is an effective method for avoiding magnetic media data remanence, which is the residual representation of data that remains on a storage device after it has been erased or overwritten. Degaussing is a process of applying a strong magnetic field to the storage device, such as a hard disk

or a tape, to erase the data and destroy the magnetic alignment of the media.
Degaussing can ensure that the data is unrecoverable, even by forensic tools or techniques.
Encryption, DLP, and authentication are not methods for avoiding magnetic media data remanence, as they do not erase the data from the storage device, but rather protect it from unauthorized access or disclosure.

NO.28 Which of the following MUST be part of a contract to support electronic discovery of data stored in a cloud environment?

A. Integration with organizational directory services for authentication

B. Tokenization of data

C. Accommodation of hybrid deployment models

D. Identification of data location

Answer: D

Explanation:
Identification of data location is a must-have clause in a contract to support electronic discovery of data stored in a cloud environment. Electronic discovery, or e-discovery, is the process of identifying, preserving, collecting, processing, reviewing, and producing electronically stored information (ESI) that is relevant to a legal case or investigation. In a cloud environment, where data may be stored in multiple locations, jurisdictions, or servers, it is essential to have a clear and contractual agreement on how and where the data can be accessed, retrieved, and produced for e-discovery purposes. Identification of data location can help ensure the availability, integrity, and admissibility of the data as evidence. Integration with organizational directory services for authentication, tokenization of data, and accommodation of hybrid deployment models are not mandatory clauses for e-discovery support, as they are more related to the security, privacy, and flexibility of the cloud service, rather than the legal aspects of data discovery.

NO.29 When transmitting information over public networks, the decision to encrypt it should be based on

A. the estimated monetary value of the information.

B. whether there are transient nodes relaying the transmission.

C. the level of confidentiality of the information.

D. the volume of the information.

Answer: C

Explanation:
The level of confidentiality of the information is the most important factor to consider when deciding whether to encrypt it or not when transmitting it over public networks. Confidentiality is the property of preventing unauthorized disclosure of information, and encryption is a technique of transforming information into an unreadable format that can only be decrypted by authorized parties. Public networks, such as the internet, are inherently insecure and vulnerable to interception, eavesdropping, or modification of the transmitted data. Therefore, encryption is necessary to protect the confidentiality of sensitive or classified information that may have legal, financial, or personal implications if disclosed. The estimated monetary value, the presence of transient nodes, and the volume of the information are not as relevant as the level of confidentiality, as they do not directly reflect the impact or risk of data exposure.

NO.30 Logical access control programs are MOST effective when they are

A. approved by external auditors.

B. combined with security token technology.

C. maintained by computer security officers.

D. made part of the operating system.

Answer: D

Explanation:

Logical access control programs are most effective when they are made part of the operating system. Logical access control is the process of granting or denying access to information or resources based on the identity, role, or credentials of the user or device. Logical access control programs, such as authentication, authorization, and auditing mechanisms, can be implemented at different levels of the system, such as the application, the database, or the network. However, the most effective level is the operating system, as it provides the lowest and most comprehensive layer of access control, and can enforce the principle of least privilege and the separation of duties for all users and processes. Approval by external auditors, combination with security token technology, and maintenance by computer security officers are not factors that affect the effectiveness of logical access control programs, as they are more related to the compliance, assurance, and administration of the access control policies.

NO.31 Which one of the following considerations has the LEAST impact when considering transmission security?

A. Network availability

B. Data integrity

C. Network bandwidth

D. Node locations

Answer: C

Explanation:

Network bandwidth is the least important consideration when considering transmission security, as it is more related to the performance or efficiency of the network, rather than the security or protection of the data. Network bandwidth is the amount of data that can be transmitted or received over a network in a given time period, and it can affect the speed or quality of the communication. However, network bandwidth does not directly impact the confidentiality, integrity, or availability of the data, which are the main goals of transmission security. Network availability, data integrity, and node locations are more important considerations when considering transmission security, as they can affect the ability to access, verify, or protect the data from unauthorized or malicious parties.

NO.32 What principle requires that changes to the plaintext affect many parts of the ciphertext?

A. Diffusion

B. Encapsulation

C. Obfuscation

D. Permutation

Answer: A

Explanation:

Diffusion is the principle that requires that changes to the plaintext affect many parts of the

ciphertext. Diffusion is a property of a good encryption algorithm that aims to spread the influence of each plaintext bit over many ciphertext bits, so that a small change in the plaintext results in a large change in the ciphertext. Diffusion can increase the security of the encryption by making it harder for an attacker to analyze the statistical patterns or correlations between the plaintext and the ciphertext. Encapsulation, obfuscation, and permutation are not principles that require that changes to the plaintext affect many parts of the ciphertext, as they are related to different aspects of encryption or security.

NO.33 Which one of these risk factors would be the LEAST important consideration in choosing a building site for a new computer facility?

A. Vulnerability to crime

B. Adjacent buildings and businesses

C. Proximity to an airline flight path

D. Vulnerability to natural disasters

Answer: C

Explanation:

Proximity to an airline flight path is the least important consideration in choosing a building site for a new computer facility, as it poses the lowest risk factor compared to the other options. Proximity to an airline flight path may cause some noise or interference issues, but it is unlikely to result in a major disaster or damage to the computer facility, unless there is a rare case of a plane crash or a terrorist attack. Vulnerability to crime, adjacent buildings and businesses, and vulnerability to natural disasters are more important considerations in choosing a building site for a new computer facility, as they can pose significant threats to the physical security, availability, and integrity of the facility and its assets. Vulnerability to crime can expose the facility to theft, vandalism, or sabotage. Adjacent buildings and businesses can affect the fire safety, power supply, or environmental conditions of the facility. Vulnerability to natural disasters can cause the facility to suffer from floods, earthquakes, storms, or fires.

NO.34 Which one of the following transmission media is MOST effective in preventing data interception?

A. Microwave

B. Twisted-pair

C. Fiber optic

D. Coaxial cable

Answer: C

Explanation:

Fiber optic is the most effective transmission media in preventing data interception, as it uses light signals to transmit data over thin glass or plastic fibers. Fiber optic cables are immune to electromagnetic interference, which means that they cannot be tapped or eavesdropped by external devices or signals. Fiber optic cables also have a low attenuation rate, which means that they can transmit data over long distances without losing much signal strength or quality.

Microwave, twisted-pair, and coaxial cable are less effective transmission media in preventing data interception, as they use electromagnetic waves or electrical signals to transmit data over metal wires or air. These media are susceptible to interference, noise, or tapping, which can compromise the confidentiality or integrity of the data.

NO.35 Which security action should be taken FIRST when computer personnel are terminated from their jobs?

A. Remove their computer access

B. Require them to turn in their badge

C. Conduct an exit interview

D. Reduce their physical access level to the facility

Answer: A

Explanation:

The first security action that should be taken when computer personnel are terminated from their jobs is to remove their computer access. Computer access is the ability to log in, use, or modify the computer systems, networks, or data of the organization. Removing computer access can prevent the terminated personnel from accessing or harming the organization's information assets, or from stealing or leaking sensitive or confidential data. Removing computer access can also reduce the risk of insider threats, such as sabotage, fraud, or espionage. Requiring them to turn in their badge, conducting an exit interview, and reducing their physical access level to the facility are also important security actions that should be taken when computer personnel are terminated from their jobs, but they are not as urgent or critical as removing their computer access.