will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan. Answer: B is incorrect. A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen. Contingency plans include specific strategies and actions to deal with specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also include a monitoring process and "triggers" for initiating planned actions. They are required to help governments, businesses, or individuals to recover from serious incidents in the minimum time with minimum cost and disruption. Answer: C is incorrect. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking), and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication, and reputation protection, and should refer to the disaster recovery plan (DRP) for IT-related infrastructure recovery/continuity. Answer: A is incorrect. The Continuity Of Operation Plan (COOP) refers to the preparations and institutions maintained by the United States government, providing survival of federal government operations in the case of catastrophic events. It provides procedures and capabilities to sustain an organization's essential. COOP is the procedure documented to ensure persistent critical operations throughout any period where normal operations are unattainable.

QUESTION 97

Which of the following ISO standards provides guidelines for accreditation of an organization that is concerned with certification and registration related to ISMS?

A. ISO 27006
B. ISO 27005
C. ISO 27003
D. ISO 27004

Answer: A

Explanation:

ISO 27006 is an information security standard developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is entitled as "Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems". The ISO 27006 standard provides guidelines for accreditation of an organization which is concerned with certification and registration related to ISMS. The ISO 27006 standard contains the following elements: Scope Normative references Terms and definitions Principles General requirements Structural requirements Resource requirements Information requirements Process requirements Management system requirements for certification bodies Information security risk communication Information security risk monitoring and review Annex A. Defining the scope of process Annex B. Asset valuation and impact assessment Annex C. Examples of typical threats Annex D. Vulnerabilities and vulnerability assessment methods Annex E. Information security risk assessment (ISRA) approaches Answer C is incorrect. The ISO 27003 standard provides guidelines for implementing an ISMS (Information Security Management System). Answer D is incorrect. The ISO 27004 standard provides guidelines on specifications and use of measurement techniques for the assessment of the effectiveness of an implemented information security management system and controls. Answer B is incorrect. The ISO 27005 standard provides guidelines for information security risk management.

QUESTION 98

You are advising a school district on disaster recovery plans. In case a disaster affects the main

IT centers for the district they will need to be able to work from an alternate location. However, budget is an issue. Which of the following is most appropriate for this client?

A. Cold site
B. Off site
C. Warm site
D. Hot site

Answer: A
Explanation:
A cold site provides an office space, and in some cases basic equipment. However, you will need to restore your data to that equipment in order to use it. This is a much less expensive solution than the hot site. Answer: D is incorrect. A hot site has equipment installed, configured and ready to use. This may make disaster recovery much faster, but will also be more expensive. And a school district can afford to be down for several hours before resuming IT operations, so the less expensive option is more appropriate. Answer: C is incorrect. A warm site is between a hot and cold site. It has some equipment ready and connectivity ready. However, it is still significantly more expensive than a cold site, and not necessary for this scenario. Answer: B is incorrect. Off site is not any type of backup site terminology.

QUESTION 99
Which of the following authentication methods is used to access public areas of a Web site?

A. Anonymous authentication
B. Biometrics authentication
C. Mutual authentication
D. Multi-factor authentication

Answer: A
Explanation:
Anonymous authentication is an authentication method used for Internet communication. It provides limited access to specific public folders and directory information or public areas of a Web site. It is supported by all clients and is used to access unsecured content in public folders. An administrator must create a user account in IIS to enable the user to connect anonymously. Answer: D is incorrect. Multi-factor authentication involves a combination of multiple methods of authentication. For example, an authentication method that uses smart cards as well as usernames and passwords can be referred to as multi-factor authentication. Answer: C is incorrect. Mutual authentication is a process in which a client process and server are required to prove their identities to each other before performing any application function. The client and server identities can be verified through a trusted third party and use shared secrets as in the case of Kerberos v5. The MS-CHAP v2 and EAP-TLS authentication methods support mutual authentication.
Answer: B is incorrect. Biometrics authentication uses physical characteristics, such as fingerprints, scars, retinal patterns, and other forms of biophysical qualities to identify a user.

QUESTION 100
Stella works as a system engineer for BlueWell Inc. She wants to identify the performance thresholds of each build. Which of the following tests will help Stella to achieve her task?

A. Reliability test
B. Performance test
C. Regression test
D. Functional test

Answer: B
Explanation:
The various types of internal tests performed on builds are as follows: Regression tests: It is also known as the verification testing. These tests are developed to confirm that capabilities in earlier builds continue to work correctly in the subsequent builds. Functional test: These tests emphasizes on verifying that the build meets its functional and data requirements and correctly generates each expected display and report. Performance tests: These tests are used to identify the performance thresholds of each build. Reliability tests: These tests are used to identify the reliability thresholds of each build.

QUESTION 101
Continuous Monitoring is the fourth phase of the security certification and accreditation process. What activities are performed in the Continuous Monitoring process? Each correct answer represents a complete solution. Choose all that apply.

A. Security accreditation decision
B. Security control monitoring and impact analyses of changes to the information system
C. Security accreditation documentation
D. Configuration management and control
E. Status reporting and documentation

Answer: BDE
Explanation:
Continuous Monitoring is the fourth phase of the security certification and accreditation process. The Continuous Monitoring process consists of the following three main activities: Configuration management and control Security control monitoring and impact analyses of changes to the information system Status reporting and documentation The objective of these tasks is to observe and evaluate the information system security controls during the system life cycle. These tasks determine whether the changes that have occurred will negatively impact the system security. Answer: A and C are incorrect. Security accreditation decision and security accreditation documentation are the two tasks of the security accreditation phase.

QUESTION 102
Which of the following terms ensures that no intentional or unintentional unauthorized modification is made to data?

A. Non-repudiation
B. Integrity
C. Authentication
D. Confidentiality

Answer: B
Explanation:
Integrity ensures that no intentional or unintentional unauthorized modification is made to data. Answer: D is incorrect. Confidentiality refers to the protection of data against unauthorized access. Administrators can provide confidentiality by encrypting data. Answer: A is incorrect. Non- repudiation is a mechanism to prove that the sender really sent this message. Answer: C is incorrect. Authentication is the process of verifying the identity of a person or network host.

QUESTION 103
Which of the following provides an easy way to programmers for writing lower-risk applications

and retrofitting security into an existing application?

A. Watermarking
B. ESAPI
C. Encryption wrapper
D. Code obfuscation

Answer: B
Explanation:
ESAPI (Enterprise Security API) is a group of classes that encapsulate the key security operations, needed by most of the applications. It is a free, open source, Web application security control library. ESAPI provides an easy way to programmers for writing lower-risk applications and retrofitting security into an existing application. It offers a solid foundation for new development. Answer: A is incorrect. Watermarking is the process of embedding information into software in a way that is difficult to remove. Answer: C is incorrect. Encryption wrapper dynamically encrypts and decrypts all the software code at runtime. Answer: D is incorrect. Code obfuscation is designed to protect code from decompilation.

QUESTION 104
Which of the following testing methods tests the system efficiency by systematically selecting the suitable and minimum set of tests that are required to effectively cover the affected changes?

A. Unit testing
B. Integration testing
C. Acceptance testing
D. Regression testing

Answer: D
Explanation:
Regression testing focuses on finding defects after a major code change has occurred. Specifically, it seeks to uncover software regressions, or old bugs that have come back. Such regressions occur whenever software functionality that was previously working correctly stops working as intended. Typically, regressions occur as an unintended consequence of program changes, when the newly developed part of the software collides with the previously existing code. Regression testing tests the system efficiency by systematically selecting the suitable and minimum set of tests that are required to effectively cover the affected changes. Answer: A is incorrect. Unit testing is a type of testing in which each independent unit of an application is tested separately. During unit testing, a developer takes the smallest unit of an application, isolates it from the rest of the application code, and tests it to determine whether it works as expected. Unit testing is performed before integrating these independent units into modules. The most common approach to unit testing requires drivers and stubs to be written. Drivers and stubs are programs. A driver simulates a calling unit, and a stub simulates a called unit. Answer: C is incorrect. Acceptance testing is performed on the application before its implementation into the production environment. It is done either by a client or an application specialist to ensure that the software meets the requirement for which it was made. Answer: B is incorrect. Integration testing is a software testing that seeks to verify the interfaces between components against a software design. Software components may be integrated in an iterative way or all together ("big bang"). Normally the former is considered a better practice since it allows interface issues to be localized more quickly and fixed. Integration testing works to expose defects in the interfaces and interaction between the integrated components (modules). Progressively larger groups of tested software components corresponding to elements of the architectural design are integrated and tested until the software works as a system.

QUESTION 105
Which of the following specifies access privileges to a collection of resources by using the URL mapping?

A. Code Access Security
B. Security constraint
C. Configuration Management
D. Access Management

Answer: B
Explanation:
Security constraint is a type of declarative security, which specifies the protection of web content. It also specifies access privileges to a collection of resources by using the URL mapping. A deployment descriptor is used to define the security constraint. Security constraint includes the following elements: Web resource collection Authorization constraint User data constraint Answer: A is incorrect. Code Access Security (CAS), in the Microsoft .NET framework, is Microsoft's solution to prevent untrusted code from performing privileged actions. When the CLR (common language runtime) loads an assembly it will obtain evidence for the assembly and use this to identify the code group that the assembly belongs to. A code group contains a permission set (one or more permissions). Code that performs a privileged action will perform a code access demand, which will cause the CLR to walk up the call stack and examine the permission set granted to the assembly of each method in the call stack. The code groups and permission sets are determined by the administrator of the machine who defines the security policy. Answer: D is incorrect. Access Management is used to grant authorized users the right to use a service, while preventing access to non- authorized users. The Access Management process essentially executes policies defined in IT Security Management. It is sometimes also referred to as Rights Management or Identity Management. It is part of Service Operation and the owner of Access Management is the Access Manager. Access Management is added as a new process to ITIL V3. The sub-processes of Access Management are as follows: Maintain Catalogue of User Roles and Access Profiles Manage User Access Requests Answer: C is incorrect. Configuration Management (CM) is an Information Technology Infrastructure Library (ITIL) IT Service Management (ITSM) process. It tracks all of the individual Configuration Items (CI) in an IT system, which may be as simple as a single server, or as complex as the entire IT department. In large organizations a configuration manager may be appointed to oversee and manage the CM process.

QUESTION 106
You are the project manager of QSL project for your organization. You are working you're your project team and several key stakeholders to create a diagram that shows how various elements of a system interrelate and the mechanism of causation within the system. What diagramming technique are you using as a part of the risk identification process?

A. Cause and effect diagrams
B. Influence diagrams
C. Predecessor and successor diagramming
D. System or process flowcharts

Answer: D
Explanation:
In this example you are using a system or process flowchart. These can help identify risks within the process flow, such as bottlenecks or redundancy. Answer: A is incorrect. A cause and effect diagram, also known as an Ishikawa or fishbone diagram, can reveal causal factors to the effect to be solved. Answer: B is incorrect. An influence diagram shows causal influences, time ordering of events and relationships among variables and outcomes. Answer: C is incorrect. Predecessor