FIPS 199 defines the three levels of potential impact on organizations. Which of the following potential impact levels shows limited adverse effects on organizational operations, organizational assets, or individuals?

A. Moderate
B. Low
C. Medium
D. High

Answer: B
Explanation:
The potential impact is called low if the loss of confidentiality, integrity, or availability is expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. Answer: C is incorrect. Such a type of potential impact level does not exist Answer: A is incorrect. The potential impact is known to be moderate if the loss of confidentiality, integrity, or availability is expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. Answer: D is incorrect. The potential impact is called high if the loss of confidentiality, integrity, or availability is expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

QUESTION 43
You work as the senior project manager in SoftTech Inc. You are working on a software project using configuration management. Through configuration management you are decomposing the verification system into identifiable, understandable, manageable, traceable units that are known as Configuration Items (CIs). According to you, which of the following processes is known as the decomposition process of a verification system into Configuration Items?

A. Configuration status accounting
B. Configuration identification
C. Configuration auditing
D. Configuration control

Answer: B
Explanation:
Configuration identification is known as the decomposition process of a verification system into Configuration Items. Configuration identification is the process of identifying the attributes that define every aspect of a configuration item. A configuration item is a product (hardware and/or software) that has an end-user purpose. These attributes are recorded in configuration documentation and baselined. Baselining an attribute forces formal configuration change control processes to be effected in the event that these attributes are changed. Answer: D is incorrect. Configuration control is a procedure of the Configuration management. Configuration control is a set of processes and approval stages required to change a configuration item's attributes and to re-baseline them. It supports the change of the functional and physical attributes of software at various points in time, and performs systematic control of changes to the identified attributes. Configuration control is a means of ensuring that system changes are approved before being implemented. Only the proposed and approved changes are implemented, and the implementation is complete and accurate. Answer: A is incorrect. The configuration status accounting procedure is the ability to record and report on the configuration baselines associated with each configuration item at any moment of time. It supports the functional and physical attributes of software at various points in time, and performs systematic control of accounting to the identified attributes for the purpose of maintaining software integrity and traceability throughout the software development life cycle. Answer: C is incorrect. Configuration auditing is the quality assurance element of configuration management. It is occupied in the process of periodic checks to establish the consistency and completeness of accounting information and to

validate that all configuration management policies are being followed. Configuration audits are broken into functional and physical configuration audits. They occur either at delivery or at the moment of effecting the change. A functional configuration audit ensures that functional and performance attributes of a configuration item are achieved, while a physical configuration audit ensures that a configuration item is installed in accordance with the requirements of its detailed design documentation.

QUESTION 44

Bill is the project manager of the JKH Project. He and the project team have identified a risk event in the project with a high probability of occurrence and the risk event has a high cost impact on the project. Bill discusses the risk event with Virginia, the primary project customer, and she decides that the requirements surrounding the risk event should be removed from the project. The removal of the requirements does affect the project scope, but it can release the project from the high risk exposure. What risk response has been enacted in this project?

A. Mitigation
B. Transference
C. Acceptance
D. Avoidance

Answer: D
Explanation:
This is an example of the avoidance risk response. Because the project plan has been changed to avoid the risk event, so it is considered the avoidance risk response. Risk avoidance is a technique used for threats. It creates changes to the project management plan that are meant to either eliminate the risk completely or to protect the project objectives from its impact. Risk avoidance removes the risk event entirely either by adding additional steps to avoid the event or reducing the project scope requirements. It may seem the answer to all possible risks, but avoiding risks also means losing out on the potential gains that accepting (retaining) the risk might have allowed. Answer: C is incorrect. Acceptance is when the stakeholders acknowledge the risk event and they accept that the event could happen and could have an impact on the project. Acceptance is usually used for risk events that have low risk exposure or risk events in which the project has no control, such as a pending law or weather threats. Answer: A is incorrect. Mitigation is involved with the actions to reduce an included risk's probability and/or impact on the project's objectives. As the risk was removed from the project, this scenario describes avoidance, not mitigation. Answer: B is incorrect. Transference is when the risk is still within the project, but the ownership and management of the risk event is transferred to a third party - usually for a fee.

QUESTION 45

Martha registers a domain named Microsoft.in. She tries to sell it to Microsoft Corporation. The infringement of which of the following has she made?

A. Copyright
B. Trademark
C. Patent
D. Intellectual property

Answer: B

Explanation:
According to the Lanham Act, domain names fall under trademarks law. A new section 43(d) of the Trademark Act (Lanham Act) states that anyone who in bad faith registers, traffics in, or uses a domain name that infringes or dilutes another's trademark has committed trademark infringement. Factors involved in assessing bad faith focus on activities typically associated with cyberpiracy or cybersquatting, such as whether the registrant has offered to sell the domain name to the trademark holder for financial gain without having used or intended to use it for a bona fide business; whether the domain-name registrant registered multiple domain names that are confusingly similar to the trademarks of others; and whether the trademark incorporated in the domain name is distinctive and famous. Other factors are whether the domain name consists of the legal name or common handle of the domain-name registrant and whether the domain-name registrant previously used the mark in connection with a bona fide business.

QUESTION 46
Which of the following is a variant with regard to Configuration Management?

A. A CI that has the same name as another CI but shares no relationship.
B. A CI that particularly refers to a software version.
C. A CI that has the same essential functionality as another CI but a bit different in some small manner.
D. A CI that particularly refers to a hardware specification.

Answer: C
Explanation:
A CI that has the same essential functionality as another CI but a bit different in some small manner, and therefore, might be required to be analyzed along with its generic group. A Configuration item (CI) is an IT asset or a combination of IT assets that may depend and have relationships with other IT processes. A CI will have attributes which may be hierarchical and relationships that will be assigned by the configuration manager in the CM database. The Configuration Item (CI) attributes are as follows: 1.Technical: It is data that describes the CI's capabilities which include software version and model numbers, hardware and manufacturer specifications, and other technical details like networking speeds, and data storage size. Keyboards, mice and cables are considered consumables. 2.Ownership: It is part of financial asset management, ownership attributes, warranty, location, and responsible person for the CI. 3.Relationship: It is the relationship among hardware items, software, and users. Answer: B, D, and A are incorrect. These are incorrect definitions of a variant with regard to Configuration Management.

QUESTION 47
The organization level is the Tier 1 and it addresses risks from an organizational perspective. What are the various Tier 1 activities? Each correct answer represents a complete solution. Choose all that apply.

A. The organization plans to use the degree and type of oversight, to ensure that the risk management strategy is being effectively carried out.
B. The level of risk tolerance.
C. The techniques and methodologies an organization plans to employ, to evaluate information system-related security risks.

D. The RMF primarily operates at Tier 1.

Answer: ABC
Explanation:
The Organization Level is the Tier 1, and it addresses risks from an organizational perspective. It includes the following points: The techniques and methodologies an organization plans to employ, to evaluate information system-related security risks. During risk assessment, the methods and procedures the organization plans to use, to evaluate the significance of the risks identified. The types and extent of risk mitigation measures the organization plans to employ, to address identified risks. The level of risk tolerance. According to the environment of operation, how the organization plans to monitor risks on an ongoing basis, given the inevitable changes to organizational information system.

The organization plans to use the degree and type of oversight, in order to ensure that the risk management strategy is being effectively carried out.Answer: D is incorrect. The RMF primarily operates at Tier 3.

QUESTION 48
An asset with a value of $600,000 is subject to a successful malicious attack threat twice a year. The asset has an exposure of 30 percent to the threat. What will be the annualized loss expectancy?

A. $360,000
B. $180,000
C. $280,000
D. $540,000

Answer: A
Explanation:
The annualized loss expectancy will be $360,000. Annualized loss expectancy (ALE) is the annually expected financial loss to an organization from a threat. The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). It is mathematically expressed as follows:

ALE = Single Loss Expectancy (SLE) * Annualized Rate of Occurrence (ARO)

Here, it is as follows:

SLE = Asset value * EF (Exposure factor)

= 600,000 * (30/100)

= 600,000 * 0.30

= 180,000

ALE = SLE * ARO

= 180,000 * 2

= 360,000

Answer: C, B, and D are incorrect. These are not valid answers.

QUESTION 49

Which of the following are the common roles with regard to data in an information classification program? Each correct answer represents a complete solution. Choose all that apply.

A. Editor
B. Custodian
C. Owner
D. User
E. Security auditor

Answer: BCDE

Explanation:

The following are the common roles with regard to data in an information classification program: Owner Custodian User Security auditor The following are the responsibilities of the owner with regard to data in an information classification program: Determining what level of classification the information requires. Reviewing the classification assignments at regular time intervals and making changes as the business needs change. Delegating the responsibility of the data protection duties to the custodian. The following are the responsibilities of the custodian with regard to data in an information classification program: Running regular backups and routinely testing the validity of the backup data Performing data restoration from the backups when necessary Controlling access, adding and removing privileges for individual users The users must comply with the requirements laid out in policies and procedures. They must also exercise due care. A security auditor examines an organization's security procedures and mechanisms.

QUESTION 50

Which of the following life cycle modeling activities establishes service relationships and message exchange paths?

A. Service-oriented logical design modeling
B. Service-oriented conceptual architecture modeling
C. Service-oriented discovery and analysis modeling
D. Service-oriented business integration modeling

Answer: A

Explanation:

The service-oriented logical design modeling establishes service relationships and message exchange paths. It also addresses service visibility and crafts service logical compositions.

QUESTION 51

You have a storage media with some data and you make efforts to remove this data. After performing this, you analyze that the data remains present on the media. Which of the following refers to the above mentioned condition?

A. Object reuse
B. Degaussing
C. Residual
D. Data remanence

Answer: D