ISC2 CISSP - Quiz Questions with Answers

Domain 1: Security and Risk Management

1.

The DREAD rating system pertains to which of the following?

Assessing probability and quantifying potential opportunities for damage

Evaluating and establishing the change management process

Creating a three-layered plan to approach a security plan deployment

Assessing how effective a penetration test was

Correct answer: Assessing probability and quantifying potential opportunities for damage

The DREAD rating system is designed to provide a flexible rating solution that is based on the answers to five main questions about each threat. By answering these questions, it is possible to understand the probability that a threat will occur. If the reproducibility is high and the discoverability is high, it makes it much easier for attackers to exploit that threat.

- *Damage potential (What is the potential damage of this threat?)*
- *Reproducibility (How easy is it to reproduce this attack?)*
- *Exploitability (To what level can this threat be exploited?)*
- *Affected users (How many users are affected when this threat is realized?)*
- *Discoverability (How easy is it to discover the vulnerability that can be exploited with this threat?)*

Through these five questions, it would be understood what the probability of the threat being realized is and how bad the damage would be.

This has nothing to do with the change management process, this is a threat modeling technique. Change management controls changes or alterations to the environment in some way. This has nothing to do with planning security deployment. Security deployment should be carefully controlled. This has nothing to do with penetration testing. Penetration testing is also known as ethical hacking. It is the

process of launching an attack against yourself to find vulnerabilities and figure out if you can exploit them.

2.

Of the following, which BEST describes the objective of ITIL?

Align IT services with the needs of the business

To reduce organizational risk

To produce a culture that welcomes change and delivers results in shorter timeframes

Identify and simplify repeatable tasks

Correct answer: Align IT services with the needs of the business

ITIL (Information Technology Infrastructure Library) is focused on aligning IT services with the needs of the business. ITIL specifies processes and procedures that an organization's IT department can use to serve business needs better. These include processes like change management, configuration management, capacity management, and others.

In a way, it does help to reduce organizational risk. However, the question is asking for the best description of ITIL, and aligning IT to the businesses' needs is a better answer. A culture of change is a good benefit of ITIL, however, it does not necessarily happen in shorter timeframes. Managing IT is not a simple, repeatable task.

3.

Enforcing an Acceptable Use Policy (AUP) BEST helps to avoid what type of misconduct?

Personal use of a system

Opening phishing emails

Disclosure of trade secrets

Hacking

Correct answer: Personal use of a system

An Acceptable Use Policy (AUP) outlines the intended use of a system and what use is acceptable to the organization of any systems that the users are given access to. This use includes what and how systems are used for business purposes, but they should absolutely include personal use restrictions. At a minimum, an organization should require that all employees sign an AUP that outlines what is and is not acceptable behavior when using an information system.

Preventing the opening of phishing emails, or clicking on phishing links requires training. Having a phishing awareness program is essential today. To minimize the chance of the disclosure of trade secrets also requires training. A Non-Disclosure Agreement (NDA) should also be put in place to ensure that the users understand that they must control the disclosure of trade secrets that they know. Hacking should not be a behavior that is experienced by the users within a corporation. Training would be a good idea to ensure the users understand their jobs and the security in place around the corporation's assets to prevent any misbehavior.

4.

Which of the following supports threat modeling by identifying elements common to underlying threats?

Reduction analysis

Tokenization

Deprovisioning

Geofencing

Correct answer: Reduction analysis

A reduction analysis supports threat modeling by identifying elements common to underlying threats. If password attacks are a threat common to several applications but each of those applications relies on Microsoft Active Directory for authentication and authorization, then Microsoft Active Directory need only be evaluated once for password attacks (not for each application).

Tokenization refers to the technique of mapping sensitive data elements to, and replacing them with, an identifying token that is not itself sensitive if revealed. Deprovisioning refers to the deactivation or revocation of a user account. The deprovisioning process is a subset of (and typically completed during) the offboarding process. Geofencing is a security feature commonly utilized in conjunction with mobile devices to restrict access based on location. None of these are activities that directly support threat modeling.

5.

Odelia works for a large manufacturing firm that sells some products directly to customers and the rest wholesale to distributors. When processing credit cards she ensures that she is compliant with her contract with the credit card companies. How many requirements does the Payment Card Industry Data Security Standard (PCI-DSS) have?

12

6

8

20

Correct answer: 12

The Payment Card Industry Data Security Standard (PCI-DSS) has 12 main requirements. Each requirement has additional sub-controls. The 12 requirements are as below:

1. *Install and maintain a firewall configuration to protect cardholder data*
2. *Do not use vendor-supplied defaults for system passwords and other security parameters*
3. *Protect stored cardholder data*
4. *Encrypt transmission of cardholder data across open, public networks*
5. *Use and regularly update anti-virus software or programs*
6. *Develop and maintain secure systems and applications*
7. *Restrict access to cardholder data by business need-to-know*
8. *Assign a unique ID to each person with computer access*
9. *Restrict physical access to cardholder data*
10. *Track and monitor all access to network resources and cardholder data*
11. *Regularly test security systems and processes*
12. *Maintain a policy that addresses information security for employees and contractors*

6.

Which of the following can be used to protect the availability of data as part of the Confidentiality, Integrity, and Availability (CIA) requirements of information security?

Redundant Array of Independent Disks

Advanced Encryption Standard

Secure Hash Algorithm 3

Transport Layer Security

Correct answer: Redundant Array of Independent Disks

The CIA triad is built upon the principles of confidentiality, integrity, and availability, and is at the heart of information security. Confidentiality is the idea that sensitive data should be kept confidential and kept away from unauthorized individuals. Integrity is the idea that data remains authentic and unaltered. Availability ensures reliability and access to system resources.

Examples:

- *Confidentiality: Advanced Encryption Standard (AES), Transport Layer Security (TLS)*
- *Integrity: Secure Hash Algorithm 3 (SHA-3)*
- *Availability: Redundant Array of Independent Disks (RAID)*

7.

Which of the following would MOST LIKELY be categorized as Personally Identifiable Information (PII)?

Criminal record

Time zone

Browser type

Aggregated survey results

Correct answer: Criminal record

An individual's criminal record should be categorized as Personally Identifiable Information (PII).

The National Institute of Standards and Technology (NIST) in Special Publication 800-122 states that PII is any information about an individual maintained by an agency, including the following:

1. *Any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date, and place of birth, mother's maiden name, or biometric records; and*
2. *Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.*
3. *The EU GDPR also includes political views, opinions, religion, gender identification, etc.*

8.

Regardless of the access control model used, what is the FIRST step in granting access?

Identification

Authorization

Verification

Authentication

Correct answer: Identification

In order for any security system to operate, it must first identify the subject. Systems must perform Identification, Authentication, Authorization, and Accountability. These are the four elements of IAAA service. Identification is when a user asserts their identity using their user ID, user name, email, or personal number.

Authentication is the step to prove that identity assertion or verification. Authentication is done using one or more of the factors of authentication. Factor 1 is something that you know, such as a password. Factor 2 is something that you have, such as a token, card, or authentication tool. Factor 3 is something that you are, which would be biometrics such as a fingerprint, retinal pattern, or vocal pattern. Authorization is then granting the user permissions (or not) now that their identification has been verified. Accountability is then tracking the user's activity by creating a log of their activities.

9.

What type of control are mandatory vacation policies considered to be?

Administrative control

Physical control

Technical control

Corrective control

Correct answer: Administrative control

Mandatory vacations are considered to be administrative controls that can help detect fraudulent activity. A mandatory vacation policy allows other department members to discover something that an employee was potentially hiding. It helps uncover employee misconduct and forces cross-training among department members.

Physical controls include walls, fences, locks, guards, dogs, etc. A mandatory vacation is a surprise vacation that lasts a minimum amount of time so that the employees' work can be audited, which is not a physical control. Technical or logical controls include encryption, logical access controls, firewalls, etc. Corrective controls are controls that return the environment to a working condition after an incident of some kind occurs.

10.

Operations security seeks to implement controls that create all EXCEPT which of the following?

Optimization

Availability

Integrity

Confidentiality

Correct answer: Optimization

Optimization is a critical concept in networking design, hardware design, software design as well as other areas of business such as processes.

The three objectives for security systems are confidentiality, integrity, and availability. This is known as the CIA triad. Confidentiality strives to protect assets from unauthorized access, integrity focuses on ensuring the accuracy and reliability of data and systems, and availability focuses on maintaining uninterrupted access for authorized individuals.

11.

Lucy has been asked to create a plan to help her organization continue operations in the event of a natural disaster. Her plan must provide office space and maintain lines of communication with their employees and customers. The plan must also provide the necessary teams and plans to return to repair the affected locations and return everything to a normal condition, including returning the Information Technology (IT) systems to normal. Of the following, what type of plan has Lucy MOST LIKELY been asked to create?

- **Business Continuity Plan**
- Disaster Recovery Plan
- Incident Response Plan
- Crisis Communications Plan

Correct answer: Business Continuity Plan

A Business Continuity Plan (BCP) is a series of procedures and plans that help an organization maintain operations in a long-term disaster. They are often confused with Disaster Recovery Plans (DRPs) but differ in their scope. A BCP is generally focused on the business as a whole, whereas a DRP is generally focused on hardware, software, and facilities, for example, a data center. A BCP and DRP are used together to recover from and maintain operations during a disaster.

An Incident Response Plan (IRP) is incorrect because it focuses on an organization's response to a suspected security event. The IRP is usually the first of the plans that is used when systems are disrupted in some way. In the event of a natural disaster, it is not likely to be used at all. A Crisis Communications Plan (CCP) is incorrect because it focuses on maintaining communications during a disaster.

12.

The US Government agency that has created a lot of useful documentation for information security is NIST. What does NIST stand for?

National Institute of Standards and Technology

National Intelligence Security Team

National Installations for Safety and Transport

National Intelligence Security Taskforce

Correct answer: National Institute of Standards and Technology

NIST stands for the "National Institute of Standards and Technology." NIST is part of the U.S. Department of Commerce and is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems. NIST also helps develop standards and guidelines to be used by private sector companies.

13.

Many departments may be involved in dealing with an employee suspected of fraudulent system use. Which department is almost always involved?

Human Resources

Legal

Physical security

Senior management

Correct answer: Human Resources

Human Resources is responsible for pre-employment screening and termination. They draw up papers and insist IT secures the system during employee termination. They also help with investigations into employee misconduct.

The legal department could become involved if the fraudulent act is a violation of a law or contract the company must be in compliance with, or if the act could result in a lawsuit. Physical security could be involved if there was a breach of physical security controls to perform the fraudulent act. For example, someone coat-tailing or tailgating into a secured area of the building. Senior management could become involved quickly if this is a small company. In a medium to large business, it would depend on the level and the type of fraud that could cause them to become involved.

14.

The purpose of a Business Impact Analysis (BIA) is to determine the impact of the loss of a critical business function in both quantitative and qualitative measures. Which of these choices is a qualitative loss?

Decrease in service quality

Loss of asset value

Increase in expenses

Loss of revenue

Correct answer: Decrease in service quality

Service quality would be measured in the degree to which the quality was lessened. Quantitative loss can be measured numerically, but qualitative loss is measured subjectively.

An increase in expenses, loss of revenue, and loss of asset value are all quantitative measurements.

15.

Which of the following types of agreements might an employee sign before being permitted to use company-owned devices?

AUP

NDA

NCA

SLA

Correct answer: AUP

An Acceptable Use Policy (AUP) describes how an employee is permitted to use company-owned IT assets. Employees may be required to sign one before being permitted to use these devices.

A Service Level Agreement (SLA) is a contract between a service provider and customer defining acceptable, contracted levels of service.

A Non-Disclosure Agreement (NDA) requires someone to protect sensitive company data against exposure to unauthorized parties.

A Non-Compete Agreement (NCA) specifies that a former employee cannot work for a competitor for a certain number of years after leaving the company.

16.

Kathryn is the human resources manager for a hospital. She proceeds to log in to her workstation by first tapping her smart card against a reader connected to the workstation and then entering her Personal Identification Number (PIN) on the keyboard. What BEST describes the role of the PIN?

Authentication

Identification

Accountability

Authorization

Correct answer: Authentication

A Personal Identification Number (PIN) is a sequence of numbers that verifies or authenticates a user's identity. Examples of authentication mechanisms are passwords, biometrics, and encryption keys. In this scenario, the smart card provides the user's identification, and the PIN provides authentication.

Identification is the act of claiming to be someone or something. It is the equivalent of stating your name when you meet someone. Authentication is the act of proving that claimed identity. There are three factors that can be used to prove identity, they are something you know (factor 1), something you have (factor 2), and something you are (factor 3). Authorization is the granting of permissions such as read, write, full control, tag, or list. Accountability is the logging of the activities that have occurred, for example, mistyped passwords or logging in. It allows the corporation to hold the user accountable for the actions they take.

17.

According to the basic concepts of security controls, which type is BEST at reducing risk?

Preventive controls

Detective controls

Corrective controls

Deterrent controls

Correct answer: Preventive controls

Preventive controls are the best at reducing risk since they directly stop an unwanted action. Detective, corrective, deterrent, recovery, and compensating controls also reduce risk but work in a complementary manner with preventive controls that help create an organization's overall security posture. Preventive controls include gates, fences, anti-virus software, and smart cards.

Detective controls inform by recording or notifying the operations center that there are problems somewhere. Corrective controls return broken systems or services to a functional state. This state is likely not a normal state, but it does allow the business to continue. Recovery controls would return the system back to a normal state. Deterrent controls have the effect that the threat actor would be dissuaded from launching an attack.

18.

When discussing risk analysis, which of the following BEST describes weakness?

Vulnerability

Risk

Safeguard

Threat

Correct answer: Vulnerability

A vulnerability is a weakness in a system. When a threat agent exploits a vulnerability, it can cause loss. Vulnerabilities could be flaws in a system or flaws in a process.

Risk is defined, most commonly, with the two ideas of Likelihood and Impact. Risk is the likelihood, or chance of a threat being realized and the impact it would have on that system/business. A threat is any circumstance or event that has the possibility of impacting the confidentiality, integrity, and/or availability of a system, and therefore a business. For example the theft of a laptop.

A safeguard is defined in two ways. One school of thought says that safeguards, countermeasures, and controls are all the same thing. So, a safeguard is a control that is added to reduce the likelihood and/or the impact of a potential threat. The second school of thought defines safeguards and countermeasures as two different types of controls: safeguards as preventive in nature and countermeasures as reactive in nature. For example, a cable lock on a laptop has the intention of preventing the theft of the laptop (emphasis on intention). In the event the laptop is stolen, Mobile Device Management (MDM) could be used to locate the device or send a command to overwrite the existing data on the drive in that laptop.

19.

Which of the following terms refers to the technique of adding a term or phrase to the header of a communication to enhance its effectiveness as a social engineering attack?

Prepending

Smishing

Shoulder surfing

Baiting

Correct answer: Prepending

Prepending refers to the technique of adding a term or phrase to the header of a communication to enhance its effectiveness as a social engineering attack. Prepending is commonly employed in phishing e-mails. Examples include spoofed subject tags such as "RE:" or "[INTERNAL]" to support pretexts, or spoofed header tags in the content body (e.g. "X-SPAM-STATUS: NO") to trick spam filters.

Smishing refers to a phishing attack that is attempted or executed over SMS (Short Message Service) text messaging. Shoulder surfing refers to the technique of obtaining privileged information through observation from a position of proximity (e.g. watching a password or PIN being typed through an office window or reading the laptop display of someone adjacently seated on an airplane). Baiting refers to the practice of leaving compromised portable media in a public location in a manner that entices its use from a secure, nonpublic location (for example, leaving an infected USB drive labeled "staff salaries" in the lobby of an office building).

20.

Which technical form of assessing risk deals with the more elusive theoretical evaluations?

Qualitative risk analysis

Quantitative risk analysis

Theoretical mathematical review

Objective risk analysis

Correct answer: Qualitative risk analysis

Qualitative risk analysis does exactly as it sounds: it takes in the qualities, or theories of value and risk, to evaluate risk. It is a subjective form of risk analysis. There are two main approaches to performing a risk assessment: quantitative and qualitative.

Quantitative takes a calculated value of an asset and the projected percentage of loss of an asset to calculate the projected loss if an incident were to occur. It then further calculates the projected annual loss by adding in the number of incidents that would be expected within a single year. Theoretical mathematical review and objective risk analysis are not real risk management terms.

21.

Which disaster recovery site provides the most rapid recovery capability, but also requires the most effort to maintain its readiness?

Hot site

Cold site

Warm site

Reciprocal site

Correct answer: Hot site

A hot site provides the most rapid recovery capability because it is complemented by the full resources required for instant function and connectivity of IT systems. A hot site is only missing people and some data.

A cold site is incorrect because a cold site is an empty computer room with environmental facilities such as heating, ventilation, and air conditioning, but no computing equipment. A warm site is incorrect because a warm site is basically a cold site, but with computers and communication links already in place ready to be loaded with operating systems and data. Reciprocal site is incorrect because, in a reciprocal agreement, two organizations pledge the availability of their organization's data center in the event of a disaster but it could take a while to get over to that site and get working. This is not faster because the other company's site would not have any of the data and it can take a while to get the other company to let them in and release access to some of the systems.

22.

What security process is used to identify and understand potential threats and mitigations regarding an asset?

Threat modeling

Threat hunting

Penetration testing

Control testing

Correct answer: Threat modeling

Threat modeling is the security process wherein potential threats and mitigations to assets are identified and analyzed. It can be used for software, hardware, business processes, Internet of Things (IoT), and more.

Threat hunting refers to a technique used in security operations in which production environments are actively scrutinized by an experienced analyst for threats and indications of compromise. Penetration testing attempts to discover and exploit potential vulnerabilities. Penetration testing does not analyze mitigations for the threats it discovers. After the penetration test has been performed and the report submitted the company can then look for mitigations. Control testing is performed to evaluate controls for sufficiency. It can be used to test the quality of a control before being sold to the public using something like Common Criteria (ISO 15408), or it can be used to test the control within a business.

23.

A medium-sized business that provides services for the government is building its Disaster Recovery Plan. Their lead information security manager is working with the team to determine the threats that they must address with their plan. Which of the following BEST helps an organization to identify and prioritize risks?

A Business Impact Analysis (BIA)

A quantitative risk analysis

A qualitative risk analysis

Threat modeling

Correct answer: A Business Impact Analysis (BIA)

A BIA, or Business Impact Analysis, is a critical process used by organizations to assess the potential impacts of disruptions on their operations. It identifies and quantifies the financial, operational, and reputational consequences of various threats such as natural disasters, cyber-attacks, or supply chain disruptions. During a BIA, key business processes and their dependencies are analyzed, and the potential downtime, data loss, and recovery time objectives are determined. The findings help organizations prioritize their resources, develop business continuity and disaster recovery plans, and make informed decisions to mitigate risks and ensure continuity during adverse events.

Quantitative risk analysis is a method used to assess and measure risks in numerical terms, typically involving probabilities and potential impact. It involves data-driven approaches to quantify the likelihood of risks occurring and the potential magnitude of their consequences, enabling better-informed decision-making and risk prioritization.

Qualitative risk analysis is an assessment method that focuses on identifying and prioritizing risks based on their qualitative characteristics. It involves subjective evaluation, such as high, medium, or low, to determine the likelihood and potential impact of risks. This approach helps in understanding risks qualitatively and aids in risk management planning. Both quantitative and qualitative risk analyses are included in a BIA.

Threat modeling is a structured approach used to identify and assess potential threats and vulnerabilities in a system or application. It helps organizations understand potential attack scenarios and prioritize security measures to proactively mitigate risks.

24.

Daisy has been working with the Business Continuity (BC) teams to identify potential threats that have not been addressed appropriately or at all by the corporation. They have just identified a threat that has a low likelihood of occurrence and a low impact score. What would be the best response to this threat?

Risk acceptance

Risk transfer

Risk reduction

Risk avoidance

Correct answer: Risk acceptance

When a threat is not likely to be realized and will have little impact, an organization should document and accept the risk. Risk acceptance does not mean choosing to ignore the risk but rather concluding that doing something about the risk is more costly than the risk itself.

Risk transfer involves the sharing of the burden of the threat with another. The most common example given is insurance policies, but it can also include contracts and End User Licensing Agreements (EULA) to name a couple more. Risk reduction or risk mitigation includes tools or actions taken to reduce the change or impact. This could be a tool like an Intrusion Prevention System (IPS), encryption, policies, and so on. Risk avoidance would not be used in a risky activity to begin with, or to stop one when identified.

25.

Which of the following documents would MOST LIKELY reference the importance of following institutional policies and outline sanctions for violating them?

Compliance policy

Service Level Agreement (SLA)

Playbook

Runbook

Correct answer: Compliance policy

A compliance policy would most likely reference the importance of following institutional policies and outline sanctions for violating them. Compliance policies are an essential addition to policy portfolios. Employees' compliance with institutional policies is vital for organizations to maintain consistency in the goods and services they provide while further ensuring that the organization itself remains compliant with laws, regulations, and contractual obligations.

Service Level Agreements (SLAs) use agreed-upon standards of measurement to establish minimum thresholds for acceptable service performance. SLAs are typically made between service providers and clients, whether internal (e.g. between different business units in an organization) or external (i.e. between the organization and a third-party provider), to ensure the quality of the services they have contracted to receive. While SLAs sometimes define sanctions if acceptable performance isn't met, they do not highlight the importance of following other policies. Playbooks & runbooks do not relate to policy compliance but are utilized to support incident response automation. Playbooks and runbooks document the step-by-step activities required to verify whether a detected security event is an actual incident and the step-by-step response activities needed to contain any such incidents.

26.

Which action is performed at the beginning of business continuity planning to identify areas that would suffer the greatest financial or operational loss in the event of a disaster?

Business Impact Analysis

Determine max downtime

Annualized loss expectancy calculation

Quantitative risk assessment

Correct answer: Business Impact Analysis

The Business Impact Analysis (BIA) is performed to determine which areas would sustain the greatest impact in the event of a disaster or disruption. One purpose of this analysis is to identify critical systems and prioritize assets that are most critical to the business. A BIA involves quantitative risk assessments, qualitative risk assessments, and determining the Maximum Tolerable Downtime (MTD), Recovery Point Objective (RPO), and more.

A quantitative risk assessment involves calculating the Single Loss Expectancy (SLE), Annual Rate of Occurrence (ARO), and Annualized Loss Expectancy (ALE).

27.

Quantitative risk management has which of the following in its favor compared to qualitative risk management?

Measures risk consistently and objectively according to a set formula

Prioritizes the most critical risk

Reviews where the most harm has been done

Portrays which risks are more serious

Correct answer: Measures risk consistently and objectively according to a set formula

Quantitative risk management deals with the exact quantities of factors involved in risk. It measures the anticipated loss numerically using the Single Loss Expectancy (SLE), Annual Rate of Occurrence (ARO), and Annualized Loss Expectancy (ALE) formulas. Quantitative risk management assessments can utilize past data and information for details that might help predict the future.

Qualitative risk management attempts to assign priorities of importance, distinguishing lower risk from higher risk factors. This allows scenarios to be created to portray which risk is the most serious and needs the most attention. Quantitative loss can be measured numerically, but qualitative loss is measured subjectively.

28.

Of the following, which is NOT a type of law that exists within the Common legal category of law?

Congressional law

Tort law

Criminal law

Administrative law

Correct answer: Congressional law

Congressional law is a fabricated term. In the United States, Congress writes laws.

The three sub-categories or types of law within the Common legal category of law are criminal, tort (often referred to as civil), and administrative. These categories cover different actions and their corresponding consequences. For instance, civil action requires punitive damages, but criminal offenses can lead to imprisonment. Administrative law is created by government agencies to address areas including international trade, manufacturing, the environment, and immigration. Administrative law must comply with existing civil and criminal laws and cannot contradict laws passed by the legislature. Other major categories of law include Civilist (Napoleonic code or Roman law), Religious, and Customary law. Civilist (sometimes referred to as civil which causes confusion with the tort subcategory here) is the most predominant on the planet.

29.

Payroll managers must follow a policy where one creates and prints the checks and the other signs them. There is no authorization for one manager to both print and sign a check. This is an example of which of the following?

Separation of duties

Dual control

Job rotation

Security policy

Correct answer: Separation of duties

Separation of duties segregates critical job roles between individuals and prevents any one person from subverting critical security controls. In this case, one individual isn't allowed to both print and sign checks, leading to the ability to steal money. With the separation of duties system, stealing would require collusion between the two resources, which is much less likely.

Dual control is when both people must be present at the same time to accomplish something. This is different from the question because it is not necessary to have both people present when the check is printed or when it is signed.

Job rotation is something that should actually be considered when a separation of duties is in place. In job rotation, employees change to a different role on occasion. If they switch between these two jobs, printing and signing of the checks, the benefit of separation of duties is lost. It is possible for someone to print a false check, switch jobs overnight, and then come in and sign that check the next day.

It is good to have all of these ideas specified in the security policies when appropriate, but the question is looking for the specific name for the separation between the managers and that is the separation of duties.

30.

The European Union's (EU) Data Protection Directive (DPD) law sets requirements for protecting personal information. In May 2018, this law was replaced by what?

General Data Protection Regulation (GDPR)

Safe Harbor

Privacy Act of 1988

Gramm Leach Bliley Act (GLBA)

Correct answer: General Data Protection Regulation (GDPR)

The EU's General Data Protection Regulation (GDPR) is intended to protect an individual's personal information and set specific rules for how it can be transferred and used.

Safe harbor is a defunct American regulation that required American companies to protect data according to the EU's requirement. The EU court system found it to be insufficient. It was replaced by the EU-US Privacy Shield. It too has been found by European courts to be insufficient. The Privacy Act of 1988 is an Australian law that requires the protection of personal information. The Gramm Leach Bliley Act (GLBA) is the American regulation that requires the protection of personal information that is tied to the financial accounts protected under Sarbanes Oxley (SOX).

31.

An IT administrator reviews all the servers in the organization and notices that a server is missing crucial patches against a recently discovered exploit. Which BEST describes what the administrator has just found?

A vulnerability

An exposure

A threat

A breach

Correct answer: A vulnerability

The weakness in an asset or the absence or weakness of a safeguard or countermeasure is a vulnerability. A vulnerability is a flaw, loophole, oversight, error, limitation, frailty, or susceptibility in the IT infrastructure or any other process.

A threat is something that could cause damage, alteration, loss, disclosure, etc. It is something that will impact the confidentiality, integrity, or availability of an asset. Exposures are when an asset is susceptible to a threat. If there is no exposure, there is no threat to deal with. A breach is a specific threat that is the exposure of sensitive, confidential, or personally identifiable information to the outside world.

32.

Jim is a facility manager for a national hotel chain. His organization outsources Heating, Ventilation, and Air Conditioning (HVAC) maintenance to different vendors across the country. Some of the vendors request to have monitoring equipment installed at the location they support. What is the MOST critical step that must be done before allowing the vendors to install monitoring equipment?

Establish a supply chain risk management program

Segment the network using Virtual Local Area Networks (VLANs)

Establish policies and procedures that each vendor must follow

Require each vendor sign a non-disclosure agreement

Correct answer: Establish a supply chain risk management program

Establishing a supply chain risk management program is an essential step before allowing third parties access to internal systems. Each vendor must be assessed to ensure they do not introduce more risk than the organization's risk appetite allows. Organizations often use Security Organization Control 1 (SOC-1), SOC-2, and SOC-3 audit reports to show compliance with internal security controls that can be used when assessing vendor risk.

The risk management program would include the other three answers, where appropriate. It would include control over the network using Virtual Local Area Networks (VLANs). Policies and procedures would be created, and the vendor would be notified of their compliance requirements. A Non-Disclosure Agreement (NDA) would also be included and should be one of the first steps in managing the risks the vendors bring with them.

33.

COBIT 2019 has five principles for governance. Of the following, which is NOT a COBIT principle?

Aligning security objectives with business objectives

Meeting stakeholder needs

Covering the enterprise end to end

Separating governance from management

Correct answer: Aligning security objectives with business objectives

COBIT (formerly Control Objectives for Information and related Technology) is a framework for governance developed by the Information Systems Audit and Control Association (ISACA). The five COBIT 2019 principles are:

- *Meeting stakeholder needs*
- *Covering the enterprise end to end*
- *Applying a single integrated framework*
- *Enabling a holistic approach*
- *Separating governance from management*

The other three answers are statements that information security professionals would make. It is essential to meet stakeholder needs. It is necessary to cover the enterprise's security needs from one end to the other. It is also true that governance and management are not the same and both need to be addressed, but they are not the stated principles within COBIT 2019. The outline for the exam starting in 2024 does include COBIT as an item that is testable.

34.

What is the FIRST step in quantitative risk analysis?

Assign asset value

Calculate exposure factor

Calculate single loss expectancy

Assess the annualized rate of occurrence

Correct answer: Assign asset value

Before you can determine the loss due to risk, you first need to know each Asset's Value (AV). The first step in quantitative risk analysis is to perform an asset valuation for each asset, which identifies the asset's cost and value.

It is necessary to understand the asset that is at risk. This includes calculating its asset value. Only once the asset value is known, the Exposure Factor (EF) can be calculated. With the asset value and the exposure factor, the Single Loss Expectancy (SLE) can be calculated. SLE = AV x EF

The Annualized Rate of Occurrence (ARO) is the next thing to be determined. The ARO is how many times a threat can be expected to occur within a year (x/1) or how many years between the threat being realized (1/X). If it is expected that a threat will be realized 5 times in a year, it would be 5/1 and if it is once every 8 years it would be 1/8.

35.

An organization is undergoing an investigation controlled by a third party that doesn't have the goal of proving wrongdoing. Which of the following does this BEST describe?

Regulatory

Criminal

Civil

Administrative

Correct answer: Regulatory

Security investigations fall into one of four types:

- ***Regulatory:*** *Regulatory investigations are conducted by regulators to prove non-compliance with laws and standards. Their requirements depend on the type of case to be brought against a non-compliant company. This type of investigation is controlled by a third party and may be intended to find out what went wrong rather than prove wrongdoing.*
- ***Administrative:*** *Administrative investigations are internal affairs and may be intended to troubleshoot a problem or address an HR issue. Operational (troubleshooting) investigations have the loosest standards, while ones conducted for HR purposes may have a higher requirement for proof.*
- ***Criminal:*** *Criminal investigations involve law enforcement, must follow strict evidence collection requirements, and are intended to prove a crime "beyond a reasonable doubt."*
- ***Civil:*** *Civil investigations do not involve law enforcement and may be conducted internally or with external consultants. They are conducted to collect evidence to bring charges in civil court. They have less stringent evidence standards than criminal investigations because they only have to prove that the "preponderance of the evidence" supports the case.*

36.

A Business Impact Analysis (BIA) is MOST LIKELY to include which of the following tasks?

Identify organizational risks

Form a mission statement

Develop a process Gantt chart

Estimate year-end earnings

Correct answer: Identify organizational risks

The Business Impact Analysis must identify organizational risks. Identifying risks allows the business to understand the risk and security needed for a specific system. It also assigns priority and asset value to a system to help determine costs associated with implementing the additional controls.

Forming a mission statement is something that the senior leaders of the business are responsible for. It would be part of governance within GRC (Governance, Risk Management, and Compliance). A Gantt chart is a visual representation of a project schedule. It displays tasks or activities along a timeline, showing their start and end dates. Horizontal bars represent each task, providing a clear overview of project progress, dependencies, and timelines. Estimating year-end earnings is something for the finance department to do, not for the security department.

37.

Of the following, which is one of the first steps to conducting a Business Impact Analysis (BIA)?

Identifying the organization's critical business functions

Identifying threats

Calculating the maximum tolerable downtime

Calculating the annualized loss expectancy

Correct answer: Identifying the organization's critical business functions

One of the first Business Impact Analysis (BIA) tasks should be identifying the organization's critical business functions. The priority identification task, or criticality prioritization, involves creating a comprehensive list of critical business functions and ranking them in order of importance.

Once the Critical Business Functions (CBF) are identified, then it is possible to do a risk assessment. The risk assessment includes identifying threats and vulnerabilities. With that information, it is then possible to perform both a quantitative and qualitative analysis. The Maximum Tolerable Downtime (MTD) and the Annualized Loss Expectancy (ALE) are calculated after learning the organization's critical business functions.

38.

Of the following, which BEST describes a script kiddie?

An unskilled attacker who uses tools to exploit vulnerabilities

Software that simplifies the process of writing a complicated script

Malware that propagates using scripting languages

A zombie node of a botnet

Correct answer: An unskilled attacker who uses tools to exploit vulnerabilities

A script kiddie is generally an unskilled attacker who uses tools to exploit vulnerabilities. Script kiddies lack the technical skill to write software and must rely on simple-to-use programs.

There could be many programs that can help write scripts but there is no special term that applies. The programs are likely created for good purposes, but they could be used for evil purposes by someone. Script kiddies likely do not have the skills to use those programs even. Malware that propagates would normally be called a worm. A zombie is a small program that lies in wait on end devices. They wait for the Command and Control (CnC) to send instructions on how and when to attack. Traditionally, they are used to participate in Denial of Service (DoS) attacks. They could be used by script kiddies.

39.

A malicious actor uses bots to improve the rating (and popularity) of a friend's restaurant. What type of social engineering attack is this an example of?

Influence campaign

Clickjacking

Vishing

Baiting

Correct answer: Influence campaign

The use of bots by a malicious actor to improve the rating (and popularity) of a friend's restaurant is an example of an influence campaign. Influence campaigns are a type of social engineering attack that attempts to alter public opinion through dishonest means. In addition to bots, influence campaigns sometimes employ fake or deepfake content and fake accounts to amplify their reach/effect.

Clickjacking (i.e. the hijacking of a user's intended click) occurs when the user interface of a website is manipulated to misdirect intended click-throughs (for example, embedding a URL whose HTML display misrepresents its actual destination). Vishing refers to voice-based (rather than email-based) phishing. Baiting refers to the practice of leaving compromised portable media in a public location in a manner that entices its use from a secure, nonpublic location (for example, leaving an infected USB drive labeled "staff salaries" in the lobby of an office building).

40.

When discussing risk analysis, which of the following is the likelihood of an exploit taken into consideration with the impact of that exploit?

Risk

Vulnerability

Safeguard

Threat

Correct answer: Risk

When discussing risk, it can be defined as the possibility or likelihood that a vulnerability will be exploited, and the resulting impact. The word risk can be used in many different ways when combined with another word such as risk appetite. Risk appetite is the amount of risk an 'entity' is willing to take on in pursuit of its mission.

A threat is defined by the United States (US) National Institute of Standards and Technology (NIST) as, "Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service."

A vulnerability is a weakness or flaw that can be exploited by the threat actor to bring about the threat or damage. It must be an exploitable weakness. These could be flawed lines of code or an unpatched device, default configurations, default or weak passwords, and so on.

A safeguard is a type of control. There are definitions (NIST for example) that state that a safeguard is the same thing as a control or countermeasure. Other definitions say that those three items are different. If that definition is used control is the generic term, it is inclusive of both countermeasures and safeguards. A control is something that is done to reduce the impact or the likelihood of a threat being realized. A safeguard is preventive in nature and a countermeasure is reactive in nature.

41.

Of the following, which requires a United States federal agency to implement an information security program to cover its operations?

Federal Information Security Management Act

Computer Security Act

Government Information Security Reform Act

Paperwork Reduction Act

Correct answer: Federal Information Security Management Act

The Federal Information Security Management Act (FISMA), passed in 2002, requires that federal agencies implement an information security program that covers their operations. FISMA also requires that government agencies include the activities of their contractors in the security management programs.

The Computer Security Act of 1987 is a US federal law that was enacted to improve the security and privacy of sensitive information in federal computer systems. The Government Information Security Reform Act is not real. The Paperwork Reduction Act is a United States federal law enacted in 1980 with the primary goal of reducing the burden of federal paperwork on individuals, businesses, and government agencies.

42.

Tom is performing a Business Impact Analysis (BIA) for Acme Inc. and needs to calculate the Annualized Loss Expectancy (ALE) if a tornado hits their building. He estimates the building is worth $500,000 and that if a tornado hit the building, it would lose 80% of its value. In the past 100 years, five tornadoes have touched down in the town where the building is located. Based on this information, what is the ALE?

$20,000

$400,000

$25,000

$320,000

Correct answer: $20,000

Annualized Loss Expectancy (ALE) measures exactly a one-year financial loss an asset may suffer from a specifically identified threat. The formula for ALE is SLE (single loss expectancy) x ARO (annualized rate of occurrence), and it is used to determine risk and insurance requirements based on the potential for failure.

The formula for SLE is AV (asset value) x EF (Exposure Factor). The AV is the full monetary value of the asset. The EF is the percentage of expected loss if a threat is realized.

- *AV = $500,000*
- *EF = .80*
- *ARO = .05*
- *SLE = $500,000 x .80 = $400,000*
- *ALE = 400,000 x .05 = $20,000*

43.

What BEST defines the minimum level of security a system must meet?

- **Baselines**
- Procedures
- Guidelines
- System security charter

Correct answer: Baselines

Baselines are reference points used for system security configuration. This is important in establishing consistent security standards across the entire organization. Any systems that do not meet the baseline should be taken out of production and patched to meet the baseline's security level.

Procedures are documentation of the step-by-step process that a user should follow for specific tasks. Guidelines are suggested courses of action. It is not a requirement to follow guidelines, but they would be recommended. There is no system security charter.

44.

Data on media should be erased when it is no longer required. Of the following, what is the BEST method to ensure sensitive data cannot be recovered from magnetic media?

Degaussing

Deleting

Re-formatting the media

Overwriting

Correct answer: Degaussing

A degausser creates a magnetic field that realigns the magnetic fields on media. It's one way to remove data remanence on media such as a hard drive or tape drive. It is very difficult to recover data from media if it has been correctly degaussed. Degaussing is only effective on magnetic media, so it can't be used on media such as Digital Video Discs (DVD) or Compact Discs (CD).

Deleting is incorrect because it does not remove the data from the media; it only removes the record from the data's file system. Re-formatting the media is incorrect because it does not adequately overwrite the data and it may still be recoverable. Overwriting is incorrect because unless it has been overwritten multiple times, the data can still be recovered.

45.

The new information security manager, Ugo, has been exploring how risk is being handled within the company. He has recently been discussing the concept of risk with the Chief Executive Officer (CEO). Since Ugo prefers the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137, he knows that risk is defined using which two critical concepts?

Likelihood and Impact

Vulnerability and Threat

Threat and Safeguard

Vulnerability and Safeguard

Correct answer: Likelihood and Impact

NIST defines risk in many different documents that are all very similar. NIST SP 80-137 defines risk as, "A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse IMPACTS that would arise if the circumstance or event occurs; and (ii) the LIKELIHOOD of occurrence."

A vulnerability is a weakness or flaw that allows the threat to be realized. The threat is the harm or damage that could be experienced and impact the confidentiality, integrity, or availability of an asset. A safeguard is a control that is added to protect the asset. NIST considers the terms safeguard, control, and countermeasure as equal. Some people consider safeguarding as a preventive control. For example, putting a laptop in a safe will safeguard it, making it very difficult for someone to steal.

46.

Which technical form of assessing risk deals with direct mathematical evaluations?

Quantitative risk analysis

Qualitative risk analysis

Risk evaluation

Mathematical probability of risk

Correct answer: Quantitative risk analysis

Quantitative risk analysis does exactly what it sounds like it does: it takes in the quantities, or mathematically exact totals, to evaluate risk. It is an objective form of risk analysis. There are two main approaches to performing a risk assessment: quantitative and qualitative.

Qualitative risk analysis assesses risks based on subjective criteria like probability and impact. It doesn't rely on numerical data but rather on expert judgment, categorizing risks as low, medium, or high. This helps prioritize risks for further assessment and mitigation planning. Risk evaluation is the process of assessing identified risks in terms of their impact, likelihood, and significance. It helps organizations determine which risks require mitigation or acceptance, aiding in informed decision-making and resource allocation. The mathematical probability of risk quantifies the likelihood of an event or threat occurring. It's expressed as a numerical value between 0 and 1, with 0 indicating impossibility and 1 indicating certainty. This probability informs risk assessment and management strategies.

47.

Which of the following developed a security standard specifically designed to protect against theft of financial data?

PCI Council

NIST

ISO

COBIT

Correct answer: PCI Council

PCI DSS is a standard developed by the Payment Card Industry (PCI) Council focused specifically on protecting cardholders' data and preventing fraud.

The International Organization for Standardization (ISO) is an international agency that creates standards defining best practices in various areas. Among these are several information security standards, such as ISO 27001.

NIST is a US government agency that publishes various standards, including cybersecurity ones such as NIST 800-53.

COBIT is a framework developed by ISACA to describe goals for security controls.

48.

A threat actor has attacked a web server and disabled its ability to serve a company's customers. What category of crime would this be?

The computer is the target of the crime

The computer is incidental in the commission of the crime

The computer assisted the crime

Computer misuse crime

Correct answer: The computer is the target of the crime

There are basically three categories of crime involving computers. The computer could be the target of the crime, the computer could be of assistance in the commission of the crime, and finally, the computer could be incidental to the commission of the crime. When a computer is the target of the crime, the attack would be something like what is given as an example in the question, as the server is what was attacked.

If the computer is of assistance in the commission of the crime, then the threat actor used the computer and its capabilities to launch the attack. For example, the computer can be used to decrypt a protected file. Without the computer, this would be very difficult to do.

If the computer is incidental in the commission of the crime, then the threat actor used a computer but it was something that could have been done without a computer. For example, documenting the sales of their illicit drug trading in a Word document or spreadsheet when it could just as easily have been done on paper.

There are just those three categories, so 'computer misuse crime' is not a category.

49.

An organization is looking for a threat modeling framework that enables it to consider risk while taking into account the fact that certain corporate IT assets are more important than others. Which of the following is the BEST fit?

PASTA

DREAD

STRIDE

VAST

Correct answer: PASTA

PASTA is a seven-step threat modeling framework that considers both risks and the importance of various corporate assets.

DREAD classifies threats based on the Damage, Reproducibility, Exploitability, Affected users, and Discoverability of a threat.

STRIDE is a Microsoft-developed threat modeling framework named for the six types of threats that an attacker may pose to the organization.

VAST is a threat modeling framework customized for Agile environments.

50.

What are the three overarching objectives for a systems security program?

Confidentiality, Integrity, Availability (CIA)

Fast, Business-capable, Intelligent (FBI)

Secure, Encrypted, Customizable (SEC)

Secure, Administrative, Manageable (SAM)

Correct answer: Confidentiality, Integrity, Availability (CIA)

The three objectives for security systems are confidentiality, integrity, and availability. This is known as the CIA triad. Confidentiality strives to protect assets from unauthorized access, integrity focuses on ensuring the accuracy and reliability of data and systems, and availability focuses on maintaining uninterrupted access for authorized individuals.

All of the other options provided are good things to have. However, the question is pretty basic and it is looking for an objective for a security program. The basics of security are CIA.

51.

In a Common Law system, "Tort" law is another term for what category of law?

Civil law

Criminal law

Administrative law

Customary law

Correct answer: Civil law

Tort law is another name for civil law. Examples include divorces and lawsuits. Civil or Tort cases occur because someone has caused harm or injury to another. That harm could be simply saying something that injures someone's reputation (e.g. slander).

The main categories of law on the planet include but are not limited to Common law, Civil law (also known as Civilist, Napoleonic, or Roman law), Religious law, and Customary law. Common law dates back to historical England. Civil law dates back to ancient Roman times. Both civilist and common law are based on the idea that laws are created to tell people what they are not allowed to do. Once it is a law, people can be held accountable for their actions. Both common law and civilist law are broken down into three primary subcategories.

The first subcategory is criminal law. This includes laws that make physically harming another illegal (e.g. assault and battery laws). The second subcategory is where you find lawsuits. Tort law is a good name to use here. In the US, it is commonly called civil law which causes confusion with a test like CISSP. The third subcategory is administrative (or regulatory) laws. These are laws that are intended to protect the population from corporations. Health Information Protection and Accountability Act (HIPAA) in the US is a good example here.

Religious laws are legal systems that are based on what the religion considers correct behavior. In the Middle East, Sharia law (Muslim law) is an example. Vatican City is another location where religious law is found. The pope is the head of the state because he is the head of the religion in Vatican City, which means that what is legal is up to the pope and the bible.

Customary law is also usually found in the Middle East. The customs are what is considered the law. For example, if women have never driven cars it would be illegal for them to start, simply because it has been the custom.

52.

The (ISC)² Code of Ethics Canons includes all EXCEPT which of the following?

Use sound judgment and report inappropriate activity to the proper authorities.

Protect society, the common good, necessary public trust and confidence, and the infrastructure.

Provide diligent and competent service to principals.

Advance and protect the profession.

Correct answer: Use sound judgment and report inappropriate activity to the proper authorities

The Code of Ethics Preamble states:

The safety and welfare of society and the common good, duty to our principals, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.

Therefore, strict adherence to this Code is a condition of certification.

Code of Ethics Canons:

- *Protect society, the common good, necessary public trust and confidence, and the infrastructure.*
- *Act honorably, honestly, justly, responsibly, and legally.*
- *Provide diligent and competent service to principals.*
- *Advance and protect the profession.*

53.

Of the following, which BEST describes The Open Group Architecture Framework (TOGAF)?

An enterprise architecture development methodology

An open standard used to maintain compatibility between different software types

A series of controls that an organization must meet to maintain compliance with various regulations

A framework used to develop a security program within an organization

---

Correct answer: An enterprise architecture development methodology

The Open Group Architecture Framework (TOGAF) is a standard that helps organizations design, plan, implement, and govern information technology architecture. TOGAF uses the Architecture Development Method (ADM) to create architectures for business, data, applications, and technology.

ISO 27001 is an example of a framework that can be used to develop a security program. A series of controls that an organization could use to achieve and maintain compliance could be ISO 27002 or NIST SP 800-53. There is no open standard used to maintain compatibility between software types. There are things that are used consistently such as ASCII encoding so that computers can exchange and read information easily.

54.

An organization is attempting to quantify the threat of ransomware to one of its servers. The server has a value of $2,000 and an exposure factor of 0.1.

With an ARO of 0.2, what is the ALE?

- **40**
- 1000
- 600
- 2000

Correct answer: 40

The Annualized Loss Expectancy (ALE) is calculated as the product of its Annualized Rate of Occurrence (ARO) and its Single Loss Expectancy (SLE). The SLE is the product of the Asset's Value (AV) and the percentage of that value lost due to an incident or the Exposure Factor (EF).

ALE = ARO x SLE = ARO x AV x EF = $2,000 x 0.1 x 0.2 = $40

55.

In qualitative risk assessment, which technique takes anonymous feedback from participants to reach a consensus?

Delphi

Bowtie

Bayeisan

Interviews

Correct answer: Delphi

The Delphi technique is one of the less common techniques and involves bringing focus groups into a room where they anonymously provide feedback. Each group compiles its feedback on a piece of paper and submits it. The feedback is then presented to the groups and repeated until a consensus has been reached.

A bowtie analysis is a risk assessment methodology that visually represents potential incidents, their causes, preventive barriers, and mitigations, offering a comprehensive view of risk management and control measures in a bowtie-shaped diagram. Bayesian assessment is a statistical method for updating beliefs or probabilities based on new evidence. It applies Bayes' theorem to iteratively refine predictions or hypotheses, incorporating prior knowledge and adjusting as additional information becomes available. In risk assessment interviews, experts engage stakeholders to gather information on potential risks. They explore scenarios, assess vulnerabilities, and discuss controls. These interactive sessions provide qualitative insights, enhance understanding of risk landscapes, and inform comprehensive risk management strategies for organizations across various sectors.

56.

Of the following, what quantitative risk analysis term is used to define the estimated cost an organization will experience if a threat is realized for a particular asset?

Single loss expectancy

Annualized loss expectancy

Exposure factor

Annualized rate of occurrence

Correct answer: Single loss expectancy

The Single Loss Expectancy (SLE) is the monetary loss that an organization can expect if a specific threat is realized for a particular asset. The formula is SLE = AV (Asset Value) x EF (Exposure Factor). The AV is the full monetary value of the asset. The EF is the percentage of expected loss if a threat is realized.

As an example, if a building is worth $100,000, the AV = $100,000. If the EF for a fire is 50%, the EF = (.50). Using these values, the SLE would equal $50,000.

$100,000 x .50 = $50,000.

The Annualized Rate of Occurrence (ARO) is the estimate of how many times this will happen in a year. For example, if a fire is likely to happen once every two years, the ARO would be 1/2.

The Annualized Loss Expectancy (ALE) is the spreading of the SLE over the years of the ARO, or multiplied by the number of times in a year. ALE = SLE x ARO.

So, for the fire, the ALE would be $50,000 x 1/2, which would be $25,000.

57.

Risk mitigation decisions are made once an organization has performed a risk assessment. Which of the following is NOT a standard risk decision?

Risk tolerance

Risk reduction

Risk transfer

Risk acceptance

Correct answer: Risk tolerance

Risk tolerance is usually defined as the level of risk that a business can survive. For example, Research In Motion (RIM) had the Blackberry product many years ago. There was a weekend where no emails were delivered to anyone with a Blackberry over a period of approximately four days. They sold the Blackberry product off within four and a half years. That was a greater loss than the business could tolerate. Such loss like this will likely cause a business to immediately fold, or go out of business within five years.

There are four risk mitigation options: risk reduction (or sometimes stated as mitigation), risk avoidance, risk transfer (or share), and risk acceptance. Risk reduction is used if an organization decides to lower the risk using controls. Risk transfer is used if an organization decides to transfer the risk to another entity; this is commonly used with insurance. Risk acceptance is used if an organization chooses not to lower the risk and accept it as is. The other option is risk avoidance. To avoid is to not enter into or to stop specific behavior.

58.

Ultimately, who is accountable for the security of a company or organization?

Senior management

Information security officer

Functional management

IT department

Correct answer: Senior management

Senior management is ultimately responsible for establishing and enforcing security policies. The security policies and standards are usually developed by a committee that involves managers from each department.

It is the word accountable that identifies senior management as opposed to the information security officer or functional management. The IT department may implement a lot of the security controls but they would be responsible for that, not accountable. Accountability cannot be delegated, where responsibility can be.

59.

Which type of document is used to reinforce trust between an organization and the security assessment supplier?

Nondisclosure agreement

Statement of work

Work commencement

Noncompete agreement

Correct answer: Nondisclosure agreement

Security assessments often require several legal documents in the delivery of a final product. A nondisclosure agreement reinforces trust between the organization and the security assessment supplier by ensuring that the confidential materials and ideas used by both parties are not disclosed to others without consent.

A statement of work is incorrect because this simply outlines the tasks and deliverables the assessment supplier will provide. Work commencement is incorrect because it is an authorization to commence work. A noncompete agreement is incorrect because it does not restrict the security assessor from disclosure.

60.

Of the following, what BEST describes the process in which senior management directs an organization to meet its objectives?

Governance

Internal audits

Top-down approach

A business continuity plan

Correct answer: Governance

Governance is the process in which senior management directs an organization to meet its objectives. Governance must involve oversight to ensure that the goals set by senior management have been met. When performing security governance, IT managers need to keep security objectives in alignment with business objectives.

An internal audit is an independent, objective assurance and consulting activity within an organization. It evaluates and improves the effectiveness of risk management, internal controls, and governance processes. Internal auditors provide valuable insights, recommendations, and assurance to management and stakeholders, helping organizations achieve their objectives, enhance efficiency, and mitigate risks.

The top-down approach is a problem-solving or design method that starts with a broad view and then breaks it down into smaller, more manageable components. It involves identifying the overall objectives or goals first and then progressively refining the details and specifics to achieve those goals.

A Business Continuity Plan (BCP) is a comprehensive strategy outlining how an organization will continue essential operations during and after disruptive events like natural disasters, cyber-attacks, or pandemics. It includes contingency measures, data backups, and recovery procedures to minimize downtime, protect critical assets, and ensure the organization can quickly recover and resume normal operations in adverse circumstances.

61.

Which law or policy protects US citizens by setting limits on the federal government's use of their personal information?

Privacy Act of 1974

Safe Harbor

Data Protection Directive

Personal Information Protection and Electronic Documents Act (PIPEDA)

Correct answer: Privacy Act of 1974

The Privacy Act of 1974 restricts the way the government can use private information. It also defines exceptions, such as the census, law enforcement, and health and safety.

Personal Information Protection and Electronic Documents Act (PIPEDA) is a Canadian privacy law requiring the protection of personal data. The Data Protection Directive (DPD) is the European Union (EU) law that preceded the General Data Protection Regulation (GDPR) requiring the protection of personal data. Safe harbor was an American attempt at protecting personal data, as required by the EU laws. It was declared defunct by a European court and replaced by the Privacy Shield, which was also declared defunct by a European court.

62.

Jim signs a document using a unique key assigned to him. Of the following, which BEST describes the purpose of signing the document?

Nonrepudiation

Confidentiality

Integrity

Accounting

Correct answer: Nonrepudiation

Nonrepudiation prevents an individual from claiming not to have done a particular action. In this example, Jim cannot deny he signed the document since he is the only individual with the digital signature's private key. To repudiate is to deny or argue. Nonrepudiation leaves a user who cannot deny or argue their action.

A signature does not provide any confidentiality. A signature is achieved when the user encrypts something with their private key. To verify the signature, it is verified by decrypting it with the user's public key. The public key is public, anyone can get a hold of that key. Integrity is achieved through the use of the hashing algorithm. The message digest, the result of the hashing algorithm, is what is usually encrypted by the private key. So there is an element of integrity to the digital signature, but that is not the purpose of the digital signature. Accounting is the third "A" in IAAA. It requires that a log is created so that the user can be held accountable. But accounting is only a record of their actions, not a digital signature.

63.

Which of the following statements is NOT true regarding procedures and guidelines?

Procedures and guidelines both provide detailed specific instructions.

Procedures and guidelines both outline actions a user is expected to take.

Procedures and guidelines work together to improve security.

Procedures and guidelines are both essential to a capable security system.

Correct answer: Procedures and guidelines both provide detailed specific instructions.

Procedures and guidelines both provide direction for a user, but procedures detail a step-by-step process to accomplish the desired results, whereas guidelines cover broad general areas or recommendations.

Procedures and guidelines both work with standards and baselines to fulfill corporate policies. Guidelines are optional suggestions for employees. So, the user is not expected to follow guidelines, although they can if they wish to. Guidelines can be used to answer Frequently Asked Questions (FAQ) with information that assists users in complying with the policies, procedures, standards, or baselines.

64.

Of the following, which BEST describes the purpose of a Business Impact Analysis (BIA)?

Identify critical systems and prioritize assets that are most critical to the business

Estimate year-end earnings

Define the legal and regulatory requirements of an organization

Mitigate risk

Correct answer: Identify critical systems and prioritize assets that are most critical to the business

A Business Impact Analysis (BIA) is used to help identify critical systems and prioritize assets that are most critical to the business. The BIA also identifies organizational risks. Identifying risks allows the business to understand the risk and security needed for a specific system. It also assigns priority and asset value to a system to help determine costs associated with implementing the additional controls.

Estimating year-end earnings would be the responsibility of the accountants/finance department. Defining the legal and regulatory requirements should be done through the Governance, Risk management, and Compliance (GRC) process. Once the BIA is complete, the process will head toward mitigating risk. It is the BIA that provides a great deal of info that makes appropriate mitigation.

65.

The STRIDE threat model is used for assessing threats against applications or operating systems. Which of the following is part of STRIDE?

Spoofing

Spamming

Replay

Discover

Correct answer: Spoofing

Microsoft developed STRIDE, a way of categorizing threats. STRIDE stands for Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service (DoS), and Elevation of privilege. A spoofing attack tries to imitate a trusted user, thereby fooling the system into accepting the imposter as the original entity. An example is an Internet Protocol (IP) spoofing attack. In IP spoofing, hackers replace a valid IP address with a phony one to impersonate a genuine system or keep their identity a secret.

The other options are not part of the STRIDE threat model. Spamming is a continual form of security risk that uses repetition by way of email. Replay attacks involve capturing a legitimate authentication attempt and replaying it for malicious purposes. Discover is not relevant.

66.

Chloe and Andy are planning an attack on Chloe's organization. Chloe is a disgruntled employee who sits next to the IT department and has insider knowledge of the environment. Every time she learns the IT department is away on a work outing, she eats her sandwich at a specific table next to a window that Andy can see. Andy wants to conduct the attack when the IT department is away to reduce the likelihood of being caught. Of the following, this information exchange is BEST described as what?

Covert channel

Overt channel

Information flow

Storage channel

Correct answer: Covert channel

A covert channel is the disclosure of information in an unauthorized manner. Covert channels can be very sophisticated and difficult to detect. In this scenario, Chloe and Andy are conducting a timed covert channel.

There are two types of covert channels:

- *Storage: exchange of information by writing data to a common storage medium that another process can read.*
- *Timing: exchange of information through the use of timing. An example of this could be that a shared resource is used or not used.*

A storage channel is a type of covert channel, however, she is using a timing channel. Sitting at the window at lunchtime is the timing of the event of her eating her sandwich.

Information flow is a model used to discover where information is actually flowing within a business. Overt channel is fabricated.

67.

An organization is performing a forensic investigation to prove that a particular employee took malicious action against the company's IT assets. Which of the following principles is MOST applicable?

Non-repudiation

Confidentiality

Integrity

Authenticity

Correct answer: Non-repudiation

Non-repudiation refers to the inability to deny that someone took a particular action. Achieving this is the goal of the forensic investigation.

The principle of confidentiality refers to protecting sensitive information from being disclosed to an unauthorized party.

Integrity refers to ensuring that data hasn't been modified by an unauthorized party.

Authenticity refers to ensuring that data was created by its alleged author.

68.

A Redundant Array of Independent Disks (RAID) is used to ensure which of the following?

- **Availability**
- Confidentiality
- Integrity
- Accountability

Correct answer: Availability

Availability is used to ensure reliability and access to system resources or data. A Redundant Array of Independent Disks (RAID) is used to ensure the system is still accessible if a drive fails.

RAID 0 has two drives that stripe data between them. If one drive fails, the data is lost. So, RAID 1 was created. There are still two drives, but the data is written simultaneously to both, so if one fails, no data is lost. RAID 2 was designed to be more efficient than storing two copies of each piece of data. It requires more drives and was never really used. RAID 3 and 4 both use three drives and they stripe data across two of them. Then they write parity information for each byte/block of data to the third drive. Bytes are written in RAID 3 and blocks for RAID 4. RAID 5 is much more common than RAID 3 or 4 because it interleaves the data and parity to all drives.

Confidentiality is not achieved because there is no encryption. Accountability is not achieved because there are no logs generated that account for the user activity. RAID concerns writing data to the drives only. Integrity is not achieved because there is no check on the validity or accuracy of the data. The data is simply stored in RAID with a focus on having the data available tomorrow in the event of a drive failure.

69.

Which of the following types of plans describes how an organization's general security goals can be accomplished?

Tactical

Strategic

Operational

Contingency

Correct answer: Tactical

Organizations can have three types of security plans:

- *Strategic plans are the longest type of security management plan. They describe overall security goals and can be viable for up to five years.*
- *Tactical plans are the next longest and describe how particular goals can be accomplished. They're usually good for about a year.*
- *Operational plans have an extremely short duration. They provide in-depth detail on how the organization will accomplish tasks to support their strategic or tactical plans.*

Contingency plans are not one of the three types of security management plans.

70.

Which of the following is generally considered the weakest component of any organizational security program?

Personnel

Security procedures

Firewalls

Passwords

Correct answer: Personnel

Humans are generally considered the weakest component of most organizational security plans. Social engineering threats, for example, pose a high risk due to their effectiveness against the human element of an organization. Humans can discover ways to circumvent, avoid, subvert, or disable any physical and logical controls that have been deployed. Annual reports show that phishing is the most common entry method for bad actors into a corporation. Phishing is a social engineering technique.

Security procedures can cause problems if they are not complete or are incorrect, however, this is not the weakest component. Firewalls can be misconfigured and cause problems for a corporation, and passwords can be weak and easy to guess.

71.

Haruto has to send some legal communications. He sends the documents through certified mail and requests a signature on delivery from the recipient so he will have paperwork confirming the documents were delivered. This is an example of which of the following?

Nonrepudiation

Layering

Confidentiality

Authentication

Correct answer: Nonrepudiation

Nonrepudiation ensures that the subject of an activity or event cannot deny that the event occurred. In this case, the letter was delivered and signed for, leaving a paper trail. Therefore, the subject who received and signed for the mail cannot deny that they received it. This is what digital signatures replicate.

Confidentiality means to keep something a secret. Physical signatures or digital signatures do not keep something secret. Digital signatures could be encrypted for confidentiality purposes. Authentication is the process of verifying someone's identity. Layering is used in two ways. One is in discussing layered security (defense in depth), which is a recommended process. However, the question is just asking what a signature on a delivery form is. Layering would be the topic of having fences, then guards, then locked doors, and so on.

72.

Of the following, which is a United States law that was the first to implement penalties against those who perpetrate and spread viruses, worms, and other malicious software intended to harm computing systems?

Computer Fraud and Abuse Act

Sarbanes-Oxley Act

Computer Security Act

National Infrastructure Protection Plan

Correct answer: Computer Fraud and Abuse Act

Congress first enacted computer crime law as part of the Comprehensive Crime Control Act (CCCA) of 1984, and it remains enforced today, with several amendments. The Computer Fraud and Abuse Act amendment was enacted in 1986 and was carefully worded to only cover computer crimes that cross state boundaries to avoid infringing on states' rights.

The Sarbanes-Oxley (SOX) Act was created as a response to the actions taken by Enron. They lied about their financial status and cost their customers a huge amount of money. SOX requires companies to ensure that their financial status is accurate and the files are protected. The Computer Security Act of 1987 is a US federal law that was enacted to improve the security and privacy of sensitive information in federal computer systems. The National Infrastructure Protection Plan (NIPP) outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes.

73.

Software programmers should not be the only people to test code because they may have a predetermined view of how the testing results should appear. This is classified under which administrative access control?

Separation of duties

Job rotation

Least privilege

Mandatory vacations

Correct answer: Separation of duties

Separation of duties is a control measure used to ensure that a different person or department performs functionality and integrity testing for internal software. Software should be tested by developers as they are developing their code. For the formal step of testing software, it is essential to have it tested by people other than the ones who created it. There are many testing methodologies such as code walkthroughs that are performed by developers, just not the ones who wrote it. It is like trying to edit your own email. Seeing the typos and grammatical mistakes is very difficult because you know what you meant to say, even if that is not exactly what is on your screen.

Job rotation is a human resource strategy where employees periodically switch roles or departments within an organization. It aims to develop skills, reduce monotony, enhance adaptability, and promote a broader understanding of the company. Least privilege is a security principle where individuals or systems are only granted the minimum access permissions necessary to perform their tasks. It reduces the attack surface and minimizes risks. Mandatory vacations are a surprise vacation that allows the corporation to audit a user's work and is very commonly used in the finance world.

74.

What BEST describes the purpose of separation of duties?

To prevent any one person from having the ability to subvert security controls

To provide an efficient corporate structure of personnel

To provide confidentiality for sensitive information

To reduce negative impact on the organization if the employee leaves

---

Correct answer: To prevent any one person from having the ability to subvert security controls

Separation of Duties (SoD) segregates critical job roles between individuals and prevents any one person from subverting critical security controls. For example, if an Identity Access Management (IAM) admin wanted to plant a network sniffer but didn't have access to the monitoring system to disable the security alerts, they would be less likely to attempt planting the sniffer.

SoD does not provide an efficient corporate structure of personnel. In fact, it complicates it by requiring more than one person to be involved in completing a task where it would be easier for one person to do the work. Its job is to prevent one user from committing fraud. It does not protect the confidentiality of information, it prevents one user from completing all the steps of a particular process. It does not protect the sensitivity since both of the users see some of the data, if not all of it. It also reduces the negative impact of an employee misbehaving while being employed, not after they leave the organization.

75.

Which of the following is NOT a valid step in creating a Business Continuity Plan (BCP) as established by the United States (US) National Institute of Standards and Technology (NIST)?

Project budgeting

Developing the continuity policy planning statement

Business Impact Analysis

Scope the project

Correct answer: Project budgeting

Project budgeting is not considered to be one of the standard high-profile steps set forth by NIST for disaster recovery. NIST helps businesses establish standards and procedures to protect assets and avoid risk. It is also not a step according to many other documents that guide businesses through the building of the BCP. It is necessary, it is not just a standard step identified. It would be within one of the initial steps.

The core steps of planning for business continuity issues or disasters are:

1. *Policy*
2. *Project scope and planning*
3. *Business Impact Analysis (BIA)*
4. *Continuity planning*
5. *Implementation and Testing*

Budgeting would come before the planning and might have to be revised during the planning process. The continuity policy planning statement is step one.

76.

Which of the following will MOST LIKELY reduce an organization's liability should a breach happen?

Due care

Due process

Liability assessment

Standard of care

Correct answer: Due care

Due care is best defined as taking and making decisions that a reasonable and competent person would make. Due care helps shield an organization from liability should a breach happen. If an organization can prove they practiced due care, they are less likely to be found liable for the incident.

Due process is a fundamental principle of law that ensures fair treatment and protection of individuals' rights when facing legal actions. It involves the right to notice, a fair and impartial hearing, and an opportunity to be heard before any government action may affect one's life, liberty, or property.

A liability assessment involves evaluating an individual's, organization's, or entity's legal responsibility for potential harms, losses, or damages. This assessment typically considers factors such as legal obligations, adherence to standards, and the reasonable standard of care applicable to a specific situation. This is good for a corporation to perform to understand where they stand in terms of liabilities.

The standard of care refers to the level of skill, diligence, and care that a reasonably prudent person in similar circumstances would exercise. In various fields such as medicine, law, engineering, and others, professionals are expected to adhere to a certain standard of care when providing services or performing duties.

77.

Which of the following is based on providing a system where access duration is limited and is given to others at a later time?

Job rotation

Least privilege

Preferred user

Separation of duties

Correct answer: Job rotation

Job rotation among employees helps break up potential risks where users may be hiding inappropriate work within their own private access roles. It acts as a deterrent and a detection tool. If one knows that someone will be taking over their job functions soon, they are less likely to participate in fraudulent activities. If someone does do something fraudulent, job rotation increases the likelihood it will be discovered.

Least privilege is incorrect because the least privilege access control provides system users only the minimum level of access required to do their job. Preferred user is incorrect because it is not an identifier for access control. Separation of duties is incorrect because it restricts user access to specific identified tasks, preventing them from accessing tasks that are unrelated to their work or duties.

78.

Tina is an accountant for a financial institution and has been committing fraud for years by secretly skimming money from unused budgets. Of the following, what detective control could Tina's organization have implemented to detect her fraud?

Mandatory vacations

Separation of duties

Split knowledge

M of N control

Correct answer: Mandatory vacations

Mandatory vacations are used to detect fraud within an organization. Employees who commit fraud often do not take vacations in order to minimize other employees' chances of discovering their fraud. Mandatory vacation length is recommended for a minimum of two weeks to be considered effective. During the mandatory vacation, the employees' work is audited.

Separation of duties is a control used to prevent fraud because it limits the ability of a user to complete a transaction or task on their own. For example, if an employee is trying to receive money in response to a fake invoice, the employee should only be able to perform part of the work, as accounts receivable should verify the work was done. Or they can perform the accounts payable, which should also confirm the work was done, or that the goods were received (whatever the 'fake' invoice was for).

Split knowledge is the concept that a critical piece of information, e.g., a combination for a safe, or the password for a critical private key, is split into at least two pieces and given to that number of people. It would then be necessary for all of those pieces to be brought together to be used. This is used to prevent a user from committing fraud.

The M of N control states that there are N number of parts and M of them must be brought together to work. For example, 4 (M) of 8 (N) parts must be brought together for something to work. Without all of those parts, a user is prevented from committing fraud.

Separation of duties, split knowledge, and M of N are all designed to prevent something from happening and would have prevented the fraud if implemented

correctly, while a mandatory vacation would have helped the company actually detect the fraud.

79.

Which of the following BEST describes integrity?

Ensure the accuracy and reliability of data and systems

Keep information from being disclosed to unauthorized individuals

Ensure data is made available in a timely manner

Ensure systems are resilient to single points of failure

Correct answer: Ensure the accuracy and reliability of data and systems

Integrity ensures the accuracy and reliability of data and systems. The purpose of integrity is to maintain confidence that data is accurate and has not been modified by unauthorized users. Integrity mechanisms include Authentication, Authorization, Accounting (AAA), hashing, and digital signatures.

Keeping information from being disclosed to unauthorized individuals is the concept of confidentiality. Ensuring the data is made available in a timely manner is the concept of availability. This a redundant statement, but in security, the core triad is Confidentiality, Integrity, and Availability (CIA). That being said, availability is the concept of ensuring that users are able to gain access to the systems and data that they require when they require it. Ensuring systems are resilient to single points of failure is also a concept found within availability.

80.

The Sarbanes Oxley (SOX) Act primarily applies to what type of organization?

Publicly held

Privately held

Government departments and agencies

Non-profit

Correct answer: Publicly held

The Sarbanes Oxley (SOX) Act primarily applies to publicly held organizations and is enforced by the Securities and Exchange Commission (SEC). SOX holds executives accountable if they are found to submit fraudulent accounting findings to the SEC. SOX is based on the Committee of Sponsoring Organizations (COSO) framework. A publicly held company is traded on the stock exchange.

Portions of SOX do apply to privately held and non-profit companies. Since the question says 'primarily,' that results in publicly held as the answer to this question. SOX does not apply to government departments or agencies.

81.

Which of the following are considered required or critical steps in developing a Business Continuity Plan (BCP) as established by the National Institute of Standards and Technology (NIST)?

1. Form a tiger team
2. Develop the contingency planning policy statement
3. Identify preventive controls
4. Business Impact Analysis
5. Ensure plan maintenance

2, 3, 4, 5

1, 2, 3, 4

1, 3, 4, 5

2, 3, 4

Correct answer: 2, 3, 4, 5

Although forming a tiger team may be done, it's not considered a critical step in a Business Continuity Plan. An IT tiger team, also known as a red team, is a specialized group of skilled professionals within an organization, or hired externally, with the primary purpose of simulating real-world cyberattacks or security breaches. The team's objective is to assess and test the organization's cybersecurity measures, infrastructure, and response capabilities. The name "tiger team" is derived from the idea of having a highly agile and aggressive team that actively hunts for vulnerabilities and weaknesses in the organization's security posture.

The National Institute of Standards and Technology (NIST) outlines the following steps in SP 800-34:

1. ***Develop the contingency planning policy statement.*** *A formal policy provides the authority and guidance necessary to develop an effective contingency plan.*
2. ***Conduct the Business Impact Analysis (BIA).*** *The BIA helps identify and prioritize information systems and components critical to supporting the organization's mission/business functions. A template for developing the BIA is provided to assist the user.*
3. ***Identify preventive controls.*** *Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs.*

4. ***Create contingency strategies.*** *Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.*
5. ***Develop an information system contingency plan.*** *The contingency plan should contain detailed guidance and procedures for restoring a damaged system unique to the system's security impact level and recovery requirements.*
6. ***Ensure plan testing, training, and exercises.*** *Testing validates recovery capabilities, whereas training prepares recovery personnel for plan activation and exercising the plan identifies planning gaps; combined, the activities improve plan effectiveness and overall organization preparedness.*
7. ***Ensure plan maintenance.*** *The plan should be a living document that is updated regularly to remain current with system enhancements and organizational changes.*

82.

Acting in a way that a reasonable and competent person would act is BEST described as what?

Due diligence

Due care

Ethics standards

Human reasonability

Correct answer: Due diligence

Due diligence is defined in Black's law dictionary as "Such a measure of prudence, activity, or assiduity, as is properly to be expected from, and ordinarily exercised by, a reasonable and prudent man under the particular circumstances; not measured by any." Taking reasonable actions that a jury of your peers (if there is a jury) would agree are reasonable actions is due diligence.

Due care is defined in Black's law dictionary as "Just, proper, and sufficient care, so far as the circumstances demand it; the absence of negligence. This term, as usually understood in cases where the gist of the action is the defendant's negligence, implies not." Negligence occurs when harm or injury occurs because of the companies' actions or inaction. Both due diligence and due care are defined in a variety of ways as people try to find a way to explain thoughts. Going to the source is always a good idea when that happens. ISC2 has referred to Black's law dictionary many times over the years. Ethics are personal ideas as to what is right and wrong. There are also corporate ethics that businesses will want the employees to uphold or ethics agreements like the one from ISC2. Human reasonability is similar in thought to ethics but is not a common term.

83.

A sequence of numbers used by a user to verify a user's identity is MOST COMMONLY called which of the following?

Personal Identification Number (PIN)

User Identification

Retinal scan

Password

Correct answer: Personal Identification Number (PIN)

A Personal Identification Number (PIN) is a sequence of numbers that verifies or authenticates a user's identity. PINs are usually numerical, as opposed to passwords, which are generally alphanumeric with numbers and special characters.

User identification is usually something like an email address that is used by a user to claim to be someone who has an account. That claim is then validated by using one of the three factors of identification. Something you know, something you have, and something you are. PINs and passwords are considered something you know, or factor 1. A retinal scan is something you are, or factor 3. The retina is analyzed by looking at the blood vessel pattern at the back of the eye.

84.

Of the following, which is the BEST example of risk transfer?

Cybersecurity insurance

Software patching

Taking no action

Performing a Business Impact Analysis (BIA)

Correct answer: Cybersecurity insurance

Risk transfer is when risk is transferred to someone else. For example, when you pay an insurance company, they become responsible for paying out if the risk is realized.

Software patching is an example of risk mitigation. Taking no action is an example of risk acceptance, however, a cost-benefit analysis should be performed prior to accepting risk. Conducting a Business Impact Analysis (BIA) is a step in building a Business Continuity Plan (BCP) which would assess risk.

85.

Which of the following is characterized legally by securing protections on data critical to an organization's operations?

Trade secrets

Trademarks

Copyrights

Patents

Correct answer: Trade secrets

Trade secrets legally secure protections on data critical to an organization's operations. This intellectual property usually requires other legal support, such as Non-Disclosure Agreements (NDA) and non-compete clauses. An example of a trade secret is the Coca-Cola formula.

Trademarks represent the goodwill that the customers have for a company and their products. For example the shape of the Coca-Cola bottle, the flying windows logo for Microsoft Windows, and any car emblem, among so many others. Trademarks can be registered, but it is not a requirement. If there is a conflict later on, it will be necessary to prove when that logo was first used.

Copyrights protect content for movies, music, books, and software among other things. Copyright covers the expression of an idea. For example, the exact layout of this question and the unique explanation. This too can be registered, but does not have to be registered. The same would be true for the copyright if not registered, it will be necessary to prove when the content was created.

Patents must be registered. Patents can be applied to ideas that are novel, useful, and non-obvious. The idea is registered and is the property of the person/company that the patent has been granted to. The holder of the patent has control over the idea and its use for a period of approximately 20 years. The RSA algorithm is an example of something that was granted a patent. It was the first algorithm that had two distinct keys, the public and private key pair.

86.

Which of the following is NOT a goal of a Security Control Assessment (SCA)?

Recommend solutions for weaknesses of an organization's security infrastructure

Verify the capability of security mechanisms

Assess the effectiveness of an organization's risk management processes

Identify the strengths and weaknesses of an organization's security

---

Correct answer: Recommend solutions for weaknesses of an organization's security infrastructure

A Security Control Assessment (SCA) does not recommend solutions.

An SCA's goals are to verify security, assess the effectiveness of security, and identify the strengths and weaknesses of security through its risk management processes.

87.

A senior security officer is training several new employees on the Confidentiality, Integrity, and Availability (CIA) triad and how to apply it at their organization. They are discussing which principle corresponds to authorized subjects having timely and uninterrupted access to objects. Which principle is being reviewed?

Availability

Authorization

Confidentiality

Accountability

Correct answer: Availability

The third principle of the Confidentiality, Integrity, and Availability (CIA) triad is availability. The focus of availability is to ensure reliability and access to system resources or data. An example of an attack that disrupts availability is a Denial-of-Service (DoS) attack. Planning for power outages and using Uninterruptible Power Supplies (UPS) helps ensure the availability of a given system.

Authorization is the granting of permissions to verified users such as read, write, execute, etc. Confidentiality is about keeping secrets secret. It is necessary to protect company data, phone conversations, and so on. Accountability is usually used in Identity and Access Management (IAM) as the act of logging user activity so that they can be held accountable for their actions.

88.

The U.S. Department of Defense organizes its security classifications into which of the following?

Unclassified, Sensitive but Unclassified, Confidential, Secret, and Top Secret

Public, Confidential, Secret, Top Secret, and Sealed

Open, Closed, and Sealed

Open, Sensitive but Unclassified, Secret, and Top Secret

Correct answer: Unclassified, Sensitive but Unclassified, Confidential, Secret, and Top Secret

The U.S. Department of Defense organizes its security into five principal classes, including Unclassified, Sensitive but Unclassified, Confidential, Secret, and Top Secret. Individuals are then awarded classification levels based on this system to grant and restrict access. Access is given on a need-to-know basis.

The other answers are fabricated lists.

89.

When performing strategic alignment, all of the following types of plans are created EXCEPT:

Auditing plans

Strategic plans

Tactical plans

Operational plans

Correct answer: Auditing plans

Strategic alignment means that security policy aligns and supports the business's objectives, goals, and mission. This is done through the use of strategic plans, tactical plans, and operational plans. Auditing plans are used when it is time to determine compliance levels of the implemented security functions within the business. This occurs much later than strategic alignment.

Strategic plans are long-term plans. For example, creating a disaster recovery location within five years. Tactical plans are more detailed than strategic plans and cover a shorter amount of time. For example, installing servers in the third quarter and setting up backups in the fourth quarter. Operational plans are short, detailed plans. For example, using a Network File System (NFS) with a Storage Area Network (SAN) to attach storage to the servers next week.

90.

An attacker attempts to break into a building by cutting the padlock off the roof's access hatch but is unable to access anything because the door leading to the hatch is locked from the inside. This event is BEST described as what?

Security incident

Data breach

Security failure

A violation of policy

Correct answer: Security incident

A security incident is any event that negatively impacts an organization's security posture or may lead to the eventual disclosure of sensitive information.

A data breach is an incident that results in the disclosure of sensitive information. All data breaches are security incidents, but not all security incidents are data breaches. This is a security failure, but security incidents are the more common language. As a security incident, the incident response process is started. It is plausible that this was a violation of the security policy if this was an employee breaking in, but that is not stated explicitly in the question.

91.

Despite proper planning and implementation, an information security program will remain weak without which of the following?

Approval and buy-in from senior management

Funding

A hierarchical organizational structure

Reviewing the plan with department leaders

Correct answer: Approval and buy-in from senior management

Without senior management's approval of and commitment to an information security program, it will remain weak and provide little benefit. The security team's responsibility is to sufficiently educate senior management to understand the risks, liabilities, and vulnerabilities that remain even after the policies and security measures are deployed.

Without senior management's approval, funding for security projects will not happen. As projects are planned and funded it would be necessary to review those plans with department leaders to ensure that the business and its mission can continue. It is normal in business to establish a hierarchical organizational structure. It is possible to build a business in a different format. It is not necessary for security to have a hierarchical structure to be effective.

92.

Which of the following BEST protects original works of authorship from unauthorized duplication?

Copyrights

Patents

Trademarks

Licenses

Correct answer: Copyrights

Copyrights are used to protect creative works from unauthorized duplication. Copyright protection can be used for music, books, videos, and any other original work created by an author.

Trademarks are used to protect slogans, logos, and brand names. Anything that represents the company and the goodwill of their customers. Patents are used to protect inventions. For an invention to be awarded a patent, it must be considered novel, useful, and nonobvious. Novel, meaning a new and never-before-seen idea. Useful for people somewhere at some time. And nonobvious to the rest of the country/world until they are introduced to it through the patent. Licenses are used to protect software.

93.

Of the following, which BEST encompasses the primary goals and objectives of security?

Confidentiality, integrity, availability

Organizational hierarchy

Privacy and use case policies

Organizational roadmap

Correct answer: Confidentiality, integrity, availability

Confidentiality, integrity, and availability are at the heart of information security. Confidentiality is the idea that sensitive data should be kept confidential and kept away from unauthorized individuals. Integrity is the idea that data remains authentic and unaltered. Availability ensures reliability and access to system resources.

Examples:

- *Confidentiality: Advanced Encryption Standard (AES)*
- *Integrity: Secure Hash Algorithm (SHA-3)*
- *Availability: Redundant Array of Independent Disks (RAID)*

Organizational hierarchy is critical to assessing security. For example, it is normally a conflict of interest to have the security department reporting to the Chief Financial Officer (CFO). In most businesses, the CFO is responsible for audits. If that is the case, it is a conflict to be responsible for the audits of the security that you are also responsible for. This is not a primary goal of security. It is a best practice in security.

Privacy and acceptable use case policies are critical for security and are tools within the department. Privacy today usually refers to the protection of personal data. An organizational roadmap is critical for business. It is necessary for management to have an idea and plan for where they want to take their business. That is not security though. There can be a security roadmap, but that is how you get to the goal, not the goal itself.

94.

Which of the following types of security controls is designed to address an incident but doesn't restore normal operations?

Corrective

Recovery

Compensating

Deterrent

Correct answer: Corrective

The six main types of security controls include the following:

- ***Corrective:*** *Corrective controls fix issues after a security incident but may not fully restore normal operations. Antimalware that removes an infection or an auto-close arm on a door are examples of corrective controls.*
- ***Recovery:*** *Recovery controls restore normal operations after an incident to a greater extent than corrective ones. Backups and server clusters are examples of recovery controls.*
- ***Preventive:*** *Preventive controls are designed to stop an incident from happening. Fences, locks, and access controls are examples of preventive controls.*
- ***Detective:*** *Detective controls help to identify that an incident is occurring. CCTV, audit trails, and honeypots are examples of detective controls.*
- ***Deterrent:*** *Deterrent controls attempt to discourage an incident from occurring. Corporate policies and security cameras are examples of deterrent controls.*
- ***Compensating:*** *Compensating controls are used as a replacement when the preferred control is unusable. For example, a company renting an office in a building may put locks on the doors when it can't build a fence.*

95.

When referring to the Business Continuity Plan (BCP) or Disaster Recovery Plan (DRP), the Business Impact Analysis (BIA) does which of the following?

Identify critical functions and calculate risk

Mitigate risk

Test and recommend changes to the BCP and DRP

Review the financial impact of a disaster

Correct answer: Identify critical functions and calculate risk

Performing a Business Impact Analysis (BIA) is critical in developing a Business Continuity Plan (BCP). The BIA identifies all critical functions and processes so the organization can prioritize them based on criticality. The BIA also involves calculating risk for the identified business functions so that vulnerabilities are prioritized appropriately.

Mitigating risk occurs after a BIA or a risk analysis. The risk analysis must be done first before the appropriate decisions can be made on how to mitigate risk. There are four ways to mitigate risk: Risk avoidance, Risk transference, Risk reduction, and Risk acceptance. Testing the BCP or the Disaster Recovery Plan (DRP) occurs after the alternatives have been accessed, chosen, and built. Part of the BIA is to analyze the financial impact of a disaster, but that is just a piece of calculating the risk. So, this is almost the best answer here. But the answer marked correct is a more complete answer by adding in 'identify critical functions' and making the calculation of risk more generic so that it includes the financial calculation.

96.

Because cookies can track a user's movements on the internet, what do they risk violating?

Privacy laws

The need-to-know principle

An organization's acceptable use policy

The principle of least privilege

Correct answer: Privacy laws

Because cookies can track behaviors that a user believes to be private and personal, they can potentially run afoul of privacy laws. By way of example, cookies are strictly regulated in the European Union (EU) under the General Data Protection Regulation (GDPR). Under these regulations, websites must notify users and obtain consent for cookie use while allowing users to "opt-out".

The need-to-know principle is the idea that if a user does not require data for their job, they do not need to know it. If they do require the data then they have a need to know. An Acceptable Use Policy (AUP) tells the employees what they are allowed to do with company resources such as their computer, phone, and internet access. The principle of least privilege states that users should be given just enough access to be able to do their job. If that is read access only then the user should only receive read access.