Chap 1 – Security Principle

Module 1

- CIA Triad
  - Confidentiality - permitting authorized access to information
    - Personally Identifiable Information (PII) - any data about an individual that could be used to identify them
    - Protected Health Information (PHI) - information regarding one's health status, and classified or sensitive information
  - Integrity - ensures its completeness, accuracy, internal consistency, and usefulness for a stated purpose
    - Baseline – documented, lowest level of security configuration allowed by organization
  - Availability - systems and data are accessible at the time users need them
- Authentication - verifying or proving the user's identification
  - 3 types of authentications
    - Something you know: Passwords or paraphrases
    - Something you have: Tokens, memory cards, smart cards
    - Something you are: Biometrics, measurable characteristics
- Non-repudiation - protection against an individual falsely denying having performed a particular action.
- Privacy - right of an individual to control the distribution of information about themselves
  - GDPR (only for EU or person in EU) - Euro
    - handling the private data of people in a particular legal jurisdiction must abide by its privacy requirements.
  - HIPAA (Health Insurance Portability and Accountability Act) - USA
    - Control how privacy of medical information should be maintained

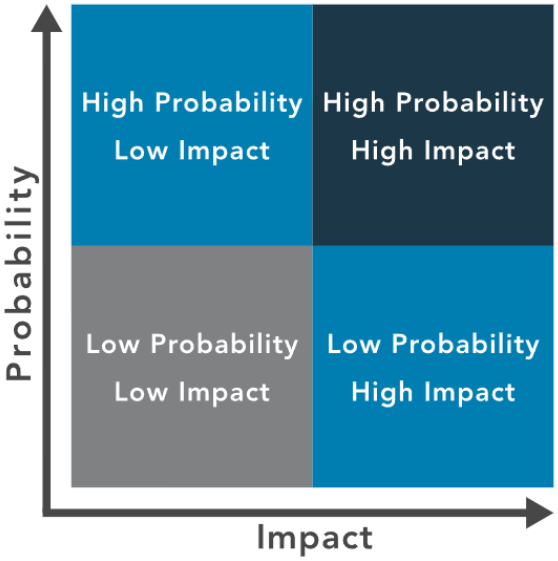
Authorization	*The right or a permission that is granted to a system entity to access a system resource.*
Integrity	*The property that data has not been altered in an unauthorized manner.*
Confidentiality	*The characteristic of data or information when it is not made available or disclosed to unauthorized persons or processes.*
Privacy	*The right of an individual to control the distribution of information about themselves.*
Availability	*Ensuring timely and reliable access to and use of information by authorized users.*
Non-repudiation	*The inability to deny taking an action, such as sending an email message.*
Authentication	*Access control process that compares one or more factors of identification to validate that the identity claimed by a user or entity is known to the system.*

Module 2

- Assets – something that need to protect
- Risk - potential consequences of what's going on in our environment.
- Vulnerability - weakness in an organization's protection of its valuable assets, including information.
- Threat - something or someone that aims to exploit a vulnerability to gain unauthorized access.
    - Threat actors
        - Insider
        - Outsider
        - Formal entity
        - Bots and AI
    - Threat vector (approach & technique taken by threat actor)
- Likelihood - weighted factor based on a subjective analysis of the probability that a given threat or set of threats is capable of exploiting a given vulnerability
- Risk Assessment - process of identifying, estimating and prioritizing risks to an organization's operations, assets, individuals, other organizations and even the nation
- Risk Treatment - making decisions about the best actions to take regarding the identified and prioritized risk
    - Avoidance - decision to attempt to eliminate the risk entirely.
    - Acceptance - taking no action to reduce the likelihood of a risk occurring
    - Mitigation - most common type of risk management and includes taking actions to prevent or reduce the possibility of a risk event or its impact.
    - Transfer - practice of passing the risk to another party (typically an insurance policy)

Mitigation	*Taking action to prevent or reduce the impact of an event.*
Acceptance	*Ignoring the risks and continuing risky activities.*
Avoidance	*Ceasing the risky activity to remove the likelihood that an event will occur.*
Vulnerability	*An inherent weakness or flaw.*
Asset	*Something of value that is owned by an organization, including physical hardware and intellectual property.*
Threat	*A person or entity that deliberately takes action to exploit a target.*
Transference	*Passing risk to a third party.*

- Highlighting future needs of SOC by using template provided by CISO

- Risk Priorities
  - qualitative risk analysis - A method for risk analysis that is based on the assignment of a descriptor such as low, medium or high.
  - Quantitative risk analysis - A method for risk analysis where numerical values are assigned to both impact and likelihood based on statistical probabilities and monetarized valuation of loss or gain.
  - 

Module 3

- Security Controls - physical, technical and administrative mechanisms that act as safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity and availability of the system and its information.
- Physical vs Logical
  - Physical protect against area & assets
  - Logical protect against system & computer

  - **Physical Control** - physical hardware devices, such as badge readers, architectural features of buildings and facilities, and specific security actions to be taken by people
  - **Technical Controls** - computer systems and networks directly implement.
  - **Administrative Controls** - directives, guidelines or advisories aimed at the people within the organization.

1. This can protect information in a file cabinet from being viewed by unauthorized persons (confidentiality) as well as keeping any documents from being modified (integrity).

Door Lock **Door Lock**

---

2. This one is abstract but could be linked to availability, because the sooner it works, the more data remains available.

Fire Extinguisher **Fire Extinguisher**

---

3. This can provide confidentiality by protecting data from unauthorized access and integrity from unauthorized changes. It could even be stretched to provide availability if shared emergency access to information is needed by more than one person.

Password Policy **Password Policy**

---

4. This is usually associated with integrity, to protect files from tampering or to provide non-repudiation. It is also commonly used to protect data in transit from prying eyes, so it could be aiding confidentiality as well.

Encryption **Encryption**

---

5. This protects availability by ensuring continued access to systems during a power outage.

Generator **Generator**

---

6. This would most generally be associated with confidentiality and identity management, but could be argued for all three, the same as a password policy.

Biometrics **Biometrics**

  -

Module 4

- Governance Elements
  - **Procedures** - detailed steps to complete a task that support departmental or organizational policies.

- **Policies** - put in place by organizational governance, such as executive management, to provide guidance in all activities to ensure that the organization supports industry standards and regulations.
- **Standards** - used by governance teams to provide a framework to introduce policies and procedures in support of regulations.
    - ISO, NIST, IETF
- **Regulations** - commonly issued in the form of laws, usually from government (not to be confused with governance) and typically carry financial penalties for noncompliance.
    - GDPR, HIPAA

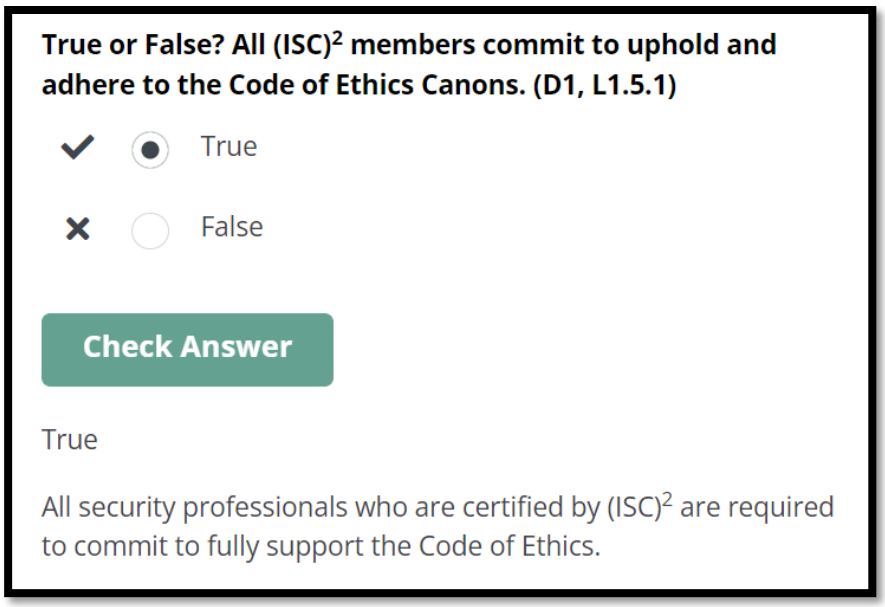
1. policies are the highest-level governance documents in an organization, usually approved and issued by management, usually to support a compliance initiative. (D1, L.1.5)

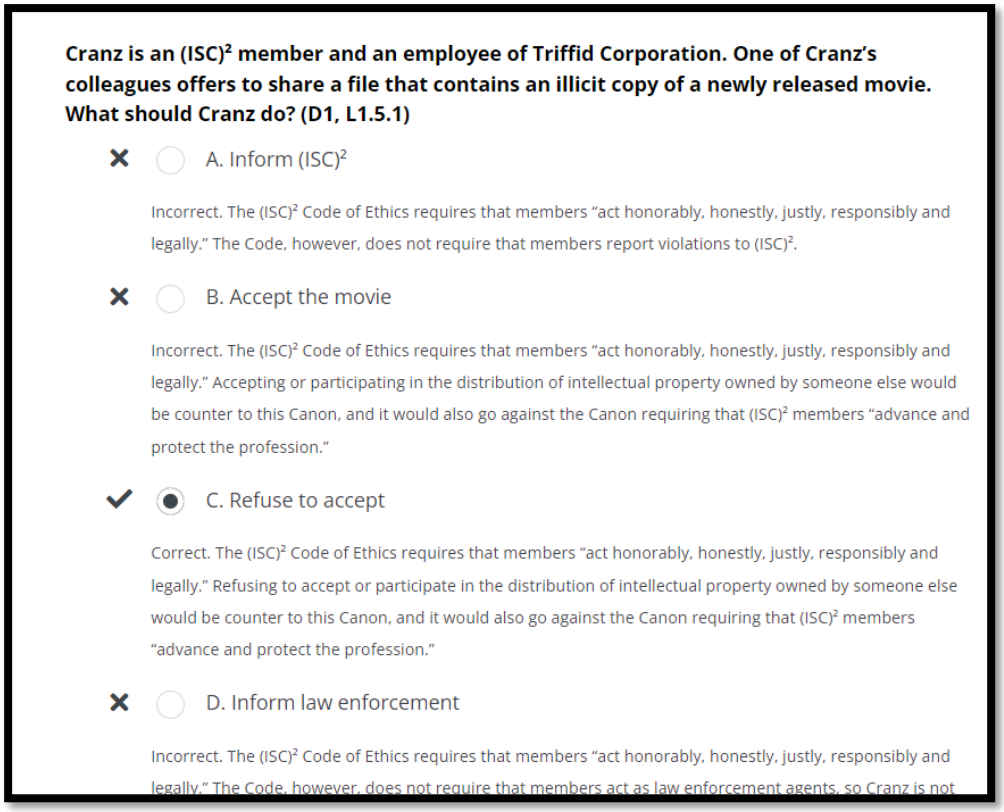
2. A security practitioner who needs step-by-step instructions to complete a provisioning task might use a procedures to ensure they are performing the task in a consistent manner. (D1, L.1.5)

3. Frameworks, or standards are often offered by third-party organizations and cover specific advisory or compliance objectives. (D1, L.1.5)

4. Usually mandated by a government agency, Rules and Regulations are a set of rules that everyone must comply with and usually carry monetary penalties for noncompliance. (D1, L.1.5)

The Healthcare Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal laws in the United States that requires certain actions be taken to protect health information. Many organizations use published frameworks, or standards, to guide the organizational policies that support the compliance effort. Many departments or workgroups within the organization implement procedures that detail how they complete day-to-day tasks while remaining compliant. (D1, L.1.5)

- Code of Ethics
  - 

  - 

A chief information security officer (CISO) at a large organization documented a policy that establishes the acceptable use of cloud environments for all staff. This is an example of a: (D1, L1.3.1)

A) Management/Administrative control

B) Technical control

C) Physical control

D) Cloud control

Is it possible to avoid risk? (D1, L1.2.1)

A) Yes

B) No

C) Sometimes

D) Never

What is meant by non-repudiation? (D1, L1.1.1)

A) If a user does something, they can't later claim that they didn't do it.

B) Controls to protect the organization's reputation from harm due to inappropriate social media accounts and personal time.

C) It is part of the rules set by administrative controls.

D) It is a security feature that prevents session replay attacks.

Which of the following is NOT one of the four typical ways of managing risk? (D1, L1.2.1)

A) Avoid

B) Accept

C) Mitigate

D) Conflate

Siobhan is deciding whether to make a purchase online; the vendor wants Siobhan to create a new user account, and is requesting Siobhan's full name, home address, credit card number, phone number, email address, the ability to send marketing messages to Siobhan, and permission to share this data with other vendors. Siobhan decides that the item for sale is not worth the value of Siobhan's personal information, and decides to not make the purchase. What kind of risk management approach did Siobhan make? (D1, L1.2.2)

A) Avoidance

B) Acceptance

C) Mitigation

D) Transfer

Guillermo is the system administrator for a midsized retail organization. Guillermo has been tasked with writing a document that describes, step-by-step, how to securely install the operating system on a new laptop. This document is an example of a _____. (D1, L1.4.1)

A) Policy

B) Standard

C) Procedure

D) Guideline

Lankesh is the security administrator for a small food-distribution company. A new law is published by the country in which Lankesh's company operates; the law conflicts with the company's policies. Which governance element should Lankesh's company follow? (D1, L1.4.2)

A) The law

B) The policy

C) Any procedures the company has created for the particular activities affected by the law

D) Lankesh should be allowed to use personal and professional judgment to make the determination o

Kristal is the security administrator for a large online service provider. Kristal learns that the company is harvesting personal data of its customers and sharing the data with local governments where the company operates, without the knowledge of the users, to allow the governments to persecute users on the basis of their political and philosophical beliefs. The published user agreement states that the company will not share personal user data with any entities without the users' explicit permission. According to the (ISC)² Code of Ethics, to whom does Kristal ultimately owe a duty in this situation? (D1, L1.5.1)

A) The governments of the countries where the company operates

B) The company Kristal works for

C) The users

D) (ISC)²

While taking the certification exam for this certification, you notice another candidate for the certification cheating. What should you do? (D1, L1.5.1)

A) Nothing—each person is responsible for their own actions.

B) Yell at the other candidate for violating test security.

C) Report the candidate to (ISC)².

D) Call local law enforcement.

The concept of "secrecy" is most related to which foundational aspect of security? (D1, L1.1.1)

A) Confidentiality

B) Integrity

C) Availability

D) Plausibility

Chap 2 – Incident Response, Business Continuity, Disaster Recovery

Module 1

- **Incident Terms**
  - **Breach** - The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence
  - **Event** - Any observable occurrence in a network or system.
  - **Exploit** - A particular attack. It is named this way because these attacks exploit system vulnerabilities
  - **Incident** - An event that actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits.
  - **Intrusion** - A security event, or combination of events, that constitutes a deliberate security incident in which an intruder gains, or attempts to gain, access to a system or system resource without authorization
  - **Threat** - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image or reputation), organizational assets, individuals, other organizations or the nation through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service.
  - **Vulnerability** - Weakness in an information system, system security procedures, internal controls or implementation that could be exploited by a threat source.
  - **Zero Day** - A previously unknown system vulnerability with the potential of exploitation without risk of detection or prevention because it does not, in general, fit recognized patterns, signatures or methods.
- **Components of Incident Response Plan**
  - Preparation -> Detection and Analysis -> Containment -> Post-Incident Activity

Breach	*The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for other than an authorized purpose.*
Incident	*An event that actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits.*
Exploit	*A particular attack. It is named this way because these attacks exploit system vulnerabilities.*
Intrusion	*A security event, or combination of events, that constitutes a deliberate security incident in which an intruder gains, or attempts to gain, access to a system or system resource without authorization.*
Vulnerability	*Weakness in an information system, system security procedures, internal controls or implementation that could be exploited or triggered by a threat source.*
Threat	*Any circumstance/event with the potential to adversely impact organizational operations (including mission, functions, image or reputation), organizational assets, individuals, other organizations or the nation through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service.*
Event	*Any observable occurrence in a network or system.*

You are working in your organization's security office. You receive a call from a user who has tried to log in to the network several times with the correct credentials, with no success. This is an example of a(n)_____. (D2, L2.1.1)

A) Emergency

B) Event

C) Policy

D) Disaster

You are working in your organization's security office. You receive a call from a user who has tried to log in to the network several times with the correct credentials, with no success. After a brief investigation, you determine that the user's account has been compromised. This is an example of a(n)_____. (D2, L2.1.1)

A) Risk management

B) Incident detection

C) Malware

D) Disaster

An external entity has tried to gain access to your organization's IT environment without proper authorization. This is an example of a(n) _____. (D2, L2.1.1)

A) Exploit

B) Intrusion

C) Event

D) Malware

When responding to a security incident, your team determines that the vulnerability that was exploited was not widely known to the security community, and that there are no currently known definitions/listings in common vulnerability databases or collections. This vulnerability and exploit might be called _____. (D2, L 2.1.1)

- A) Malware
- B) Critical
- C) Fractal
- D) Zero-day

True or False? The IT department is responsible for creating the organization's business continuity plan. (D2, L2.2.1)

- True
- False

The Business Continuity effort for an organization is a way to ensure critical _____ functions are maintained during a disaster, emergency, or interruption to the production environment. (D2, L 2.2.1)

- A) Business
- B) Technical
- C) IT
- D) Financial

Which of the following is very likely to be used in a disaster recovery (DR) effort? (D2, L 2.3.1)

- A) Guard dogs
- B) Data backups
- C) Contract personnel

D) Anti-malware solutions

Which of the following is often associated with DR planning? (D2, L 2.3.1)

A) Checklists

B) Firewalls

C) Motion detectors

D) Non-repudiation

Which of these activities is often associated with DR efforts? (D2, L2.3.1)

A) Employees returning to the primary production location

B) Running anti-malware solutions

C) Scanning the IT environment for vulnerabilities

D) Zero-day exploits

Which of these components is very likely to be instrumental to any disaster recovery (DR) effort? (D2, L2.3.1)

A) Routers

B) Laptops

C) Firewalls

D) Backups

Chap 3 – Access Control

Module 1

- **Security Control Overview**
  - Subject - entity that requests access to our assets.
  - Object - anything that a subject attempts to access
  - Rule - instruction developed to allow or deny access to an object by comparing the validated identity of the subject to an access control list.
- **Defense in Depth**
  - Physical Control (largest)
    - Policies, procedures
  - Technical Control
    - programming
  - Administrative Control
  - Assets (Smallest)

user provisioning - process of creating & managing user identity on the system

- **Principle of Least Privilege**
  - standard of permitting only minimum access necessary for users or programs to fulfill their function
- **Segregation of Duties**
  - For example, an employee may submit an invoice for payment to a vendor (or for reimbursement to themselves), but it must be approved by a manager prior to payment;
  - Two-Person Integrity

Compare and Contrast a Regular User Account Permissions to a Privileged User Account Permissions.

Which role would get Regular Account permissions? (Select all that would apply.)

- [x] Part-time Employee
- [x] Remote Employee
- [ ] This option is incorrect. Chief Information Security Officer
- [ ] This option is incorrect. Network Admin
- [ ] This option is incorrect. System Admin
- [x] Full-time Employee
- [x] Temporary Employee
- [x] Manager/Team Lead

Compare and Contrast a Regular User Account to a Privileged User Account.

A Privileged User Account: (Select all that would apply.)

- ✔ ■ Has access to interact directly with servers and other infrastructure devices.
- ☐ This option is incorrect. Has access to log on only to authorized workstations.
- ☐ This option is incorrect. Is most likely to have read-only access to a database.
- ☐ This option is incorrect. Has access levels that are typically needed for daily business operations.
- ☐ This option is incorrect. Has the lowest level of logging associated with actions.
- ✔ ■ Should require the use of MFA.
- ✔ ■ Uses the most stringent access control.
- ✔ ■ Has the highest level of logging associated with actions.
- ✔ ■ Often has the ability to create users and assign permissions.

○

○ **Physical Access Controls**

- can physically touch.
- physical mechanisms deployed to prevent, monitor, or detect direct contact with systems or areas within a facility.
- Turnstile (mcm kt office), mantraps (kne lalu 2 pintu)
- Crime Prevention through Environmental Design (CPTED) - creating safer workspaces through passive design elements
- Biometrics have 2 authentication processes – enrollment (register the biometric) and verification (compare whether biometric data is same as stored one)

When using physical access control tokens, how are the user's credentials read so they can be transmitted to a logical access control system? (D3 L3.2.1)

- ✘ ○ A. Swiped (magnetic stripe)
- ✘ ○ B. Inserted (smart card or proximity)
- ✘ ○ C. Placed on or near a reader (proximity)
- ✔ ◉ D. All of the above

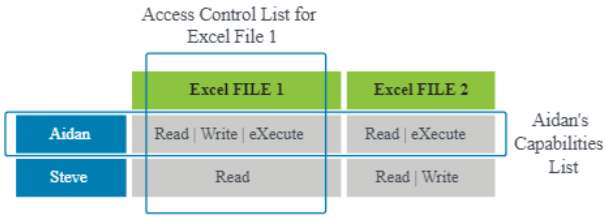
Check Answer

Correct answer: D.

Swiped, inserted and placed on or near a reader are all ways the user's credentials are read so they can be transmitted to a logical access control system.

- ■

- **Logical Access Controls**
  - Meaning
    - are electronic methods that limit someone from getting access to systems, and sometimes even to tangible assets or areas. Types of logical access controls include:
    - Passwords, Biometrics (implemented on a system, such as a smartphone or laptop), Badge/token readers connected to a system
  - **Discretionary access control (DAC)**
    - access control policy that is enforced over all subjects and objects in an information system.
    - allow users to establish or change these permissions on files they create or otherwise have ownership of



    - This methodology relies on the discretion of the owner of the access control object to determine the access control subject's specific rights.
  - **Mandatory Access Control (MAC)**
    - one that is uniformly enforced across all subjects and objects within the boundary of an information system.
    - Mandatory Access Control, it is mandatory for security administrators to assign access rights or permissions
  - **Role-Based Access Control (RBAC)**
    - sets up user permissions based on roles. Each role represents users with similar or identical permissions.

Question 1 1 / 1 point

Which of the following is a subject? (D 3, L3.1.1)

A) A file

B) A fence

C) A filename

D) A user

1 / 1 point

Question 2

Lia works in the security office. During research, Lia learns that a configuration change could better protect the organization's IT environment. Lia makes a proposal for this change, but the change cannot be implemented until it is approved, tested, and then cleared for deployment by the Change Control Board. This is an example of _____. (D3, L3.1.1)

A) Defense in depth

B) Holistic security

C) Threat intelligence

D) Segregation of duties

1 / 1 point

Question 3

Duncan and Mira both work in the data center at Triffid, Inc. There is a policy in place that requires both of them to be present in the data center at the same time; if one of them has to leave for any reason, the other has to step out, too, until they can both re-enter. This is called _____. (D 3, L3.1.1)

A) Blockade

B) Multifactor authentication

C) Two-person integrity

D) Defense in depth

1 / 1 point

Question 4

Clyde is the security analyst tasked with finding an appropriate physical control to reduce the possibility that unbadged people will follow badged employees through the entrance of the organization's facility. Which of the following can address this risk? (D3, L3.2.1)

A) Fences

B) Dogs

C) Bollards

D) Turnstiles

1 / 1 point

Question 5

Sinka is considering a physical deterrent control to dissuade unauthorized people from entering the organization's property. Which of the following would serve this purpose? (D3, L3.2.1)

- A) A wall
- B) Razor tape
- C) A sign
- D) A hidden camera

1 / 1 point

Question 6

Which of these combinations of physical security controls share a single point of failure? (D3, L3.2.1)

- A) Guards and fences
- B) Badge readers and walls
- C) Dogs and bollards
- D) High-illumination lighting and cameras

1 / 1 point

Question 7

Lakshmi presents a userid and a password to a system in order to log on. Which of the following characteristics must the ***userid*** have? (D3, L3.3.1)

- A) Confidential
- B) Complex
- C) Unique
- D) Long

1 / 1 point

Question 8

Lakshmi presents a userid and a password to a system in order to log on. Which of the following characteristics must the ***password*** have? (D3, L3.3.1)

- A) Confidential
- B) Unique
- C) Mathematical
- D) Shared

Question 9 1 / 1 point

Derrick logs on to a system in order to read a file. In this example, Derrick is the _____. (D3, L3.3.1)

- A) Subject
- B) Object
- C) Process
- D) Predicate

Question 10 1 / 1 point

Which is a physical control that prevents "piggybacking" or "tailgating"; that is, an unauthorized person following an authorized person into a controlled area? (D3, L3.2.1)

- A) Bollard
- B) Turnstile
- C) Fence
- D) Wall

Chap 5 – Security Operations

Data handling

- Life cycle model
  - Create - Creating the knowledge (tacit knowledge)
  - Store (store or record, make it explicit)
  - Use (using the knowledge, maybe being modified)
  - Share (copy or moving from 1 location to another)
  - Archive (archiving data when temporarily not needed)
  - Destroy (delete data when not needed)
- OSHA (protect wellbeing of worker)
- HIPAA – Healthcare insurance …. (medical record need to be kept for 10 years)
- OSHA – medical record of employee kept for 30 years
- Degaussing – process of eliminate unwanted magnetic field (data) stored on disk

Data handling Practices

- **Classification** (1st step) - process of recognizing the organizational impacts if the information suffers any security compromises related to its characteristics of confidentiality, integrity and availability. Derived from laws, regulation, standard
- **Labeling** - implementing controls to protect classified information.
  - Highly restricted -> could possibly put the organization's future existence at risk.
  - Moderately restricted -> could lead to loss of temporary competitive advantage, loss of revenue or disruption of planned
  - Low sensitivity (internal use only) -> could cause minor disruptions, delays or impacts
  - Unrestricted public data -> data is already published, no harm can come from further dissemination or disclosure.
- **Retention** - data should be kept only for as long as it is beneficial, no more and no less.
  - Data destruction performed when assets reached retention limit
  - Records retention – policy indicate how long organization required to maintain information & assets
  - Mistake -> applying the longest retention period to all types of information in an organization.
- **Destruction** – data left on media after delete know as remanence.
  - Clearing the device or system (writing multiple patterns of random values throughout storage media)
  - Purging the device or system (greatly reduce but may still be recovered). Some magnetic disk have ghosts of data on surface when data overwritten multiple time. Degaussing is **not sufficient**
- **Physical destruction** – disk mechanically chopped, burned, shredded

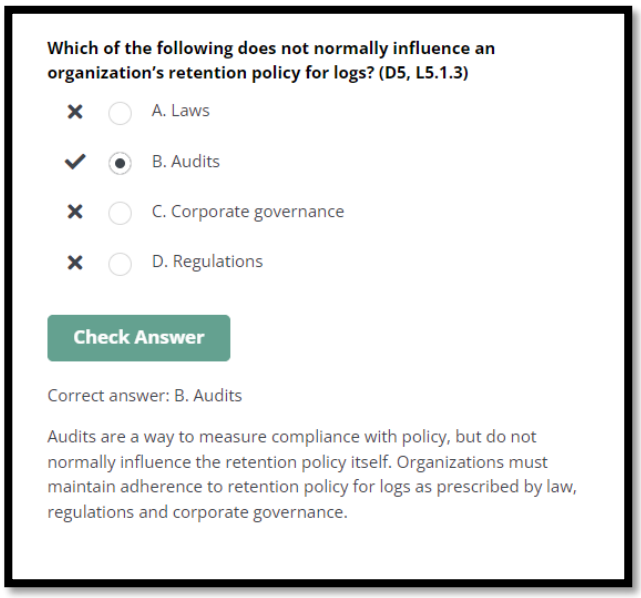
- Security consideration accept that clearing is sufficient, but when system need to be removed/replaced purging or destroy may required

Logging and Monitoring Security Events

- Logging – instrumentation that attempts to capture signal generated by events
- Events – any actions within the system that can be observed

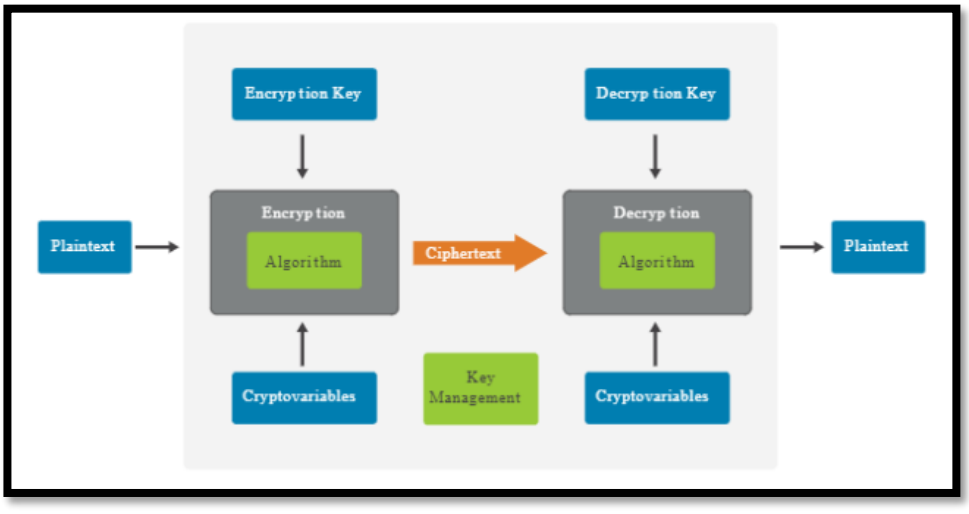
Event Logging Best Practices

- Ingress monitoring – surveillance and assessment of all inbound communication traffic.
    - Include: firewall, ids/ips, siem, anti-malware
- Egress monitoring – regulate data leaving the organization or other term called **DLP**
    - Include: email, ftp, website, api



Encryption Overview

- involved cryptography. Transform plaintext to ciphertext
-



Configuration Management Overview

- process used to ensure that the only changes made to a system are those that have been authorized and validated.
- **Identification** - Baseline identification of a system and all its components, interfaces and documentation.
- **Baseline** - minimum level of protection that can be used as a reference point
- **Change Control** - update process for requesting changes to a baseline, by means of making changes to one or more components in that baseline. (update and patches)
- **Verification and Audit** - validation process, which may involve testing and analysis, to verify that nothing in the system was broken

Common Security Policies

- **Data Handling Policy** - defines whether data is for use within the company, is restricted for use by only certain roles or can be made public to anyone outside the organization.
- **Password Policy** - defines expectations of systems and users.
- **Acceptable Use Policy (AUP)** - defines acceptable use of the organization's network and computer systems and can help protect the organization from legal action.
    - Policy aspects included in AUP:
        - Data access, system access, data disclosure, password, data retention, internet usage
- **BYOD Policy** - organization may allow workers to acquire equipment of their choosing and use personally owned equipment for business (and personal) use.
- **Privacy Policy** - organization documents that the personnel understand and acknowledge the organization's policies and procedures for handling of that type of information and are made aware of the legal repercussions of handling such sensitive data.
- **Change Management Policy** - It consists of three major activities: deciding to change, making the change, and confirming that the change has been correctly accomplished. Change management which will not affect business operations.

Change Management Components (Continuously going)

- Request change – know as RFC (request for change)
- Approval – evaluate RFC, review
- Rollback - immediate or scheduled as a subsequent change if monitoring of the change suggests inadequate performance.

True or False? A privacy policy protects PII/ePHI from disclosure? (D5, L5.3.1)

✔ ◉ True

✘ ○ False

Check Answer

Correct answer: True

It's true. A privacy policy documents how the organization's personnel will handle personally identifiable information (PII), which is also referred to as electronic protected health information [ePHI] in the health industry, to ensure that it complies with any relevant national and international laws, such as the GDPR in the EU and Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada; laws for specific industries in certain countries such as HIPAA and Gramm–Leach–Bliley Act (GLBA) in the U.S.; or local laws in which the organization operates.

-

Change Management Policy

For what purpose is a process required with a change management policy? (D5, L5.3.1)

✘ ○ A. To define the standards for using the organization's network and computer systems.

Incorrect. An acceptable use policy (AUP) defines acceptable use of the organization's network, not a change management policy.

✘ ○ B. To help protect the organization in the event it faces legal action.

Incorrect. The acceptable use, privacy, BOYD and data handling policies help to protect the organization from legal action.

✘ ○ C. To establish the appropriate use of the organization's data.

Incorrect. The data handling policy defines whether data is for use within the company, is restricted for use by only certain roles or can be made public to anyone outside the organization.

✔ ◉ D. To ensure that systems changes are done without adversely affecting business operations.

Correct. Change management requires a process to implement necessary changes so they do not adversely affect business operations.

-

What is Security Awareness Training?

- **Education**: help learners improve their understanding of these ideas and their ability to relate them to their own experiences and apply that learning in useful ways.
- **Training**: Focuses on building proficiency in a specific set of skills or actions, sharpening the perception, focus on low-level skills, an entire task or complex workflows consisting of many tasks.
- **Awareness**: These are activities that attract and engage the learner's attention by acquainting them with aspects of an issue, concern, problem or need.
- **Whaling attacks**: phishing attack targeted top people in organization

Password Advice

- 10 numbers (5 seconds)
- 8 multiple char (35 days)
- 16 char (152,000 years)

Quiz

Which of the following can be used to map data flows through an organization and the relevant security controls used at each point along the way? (D5.1, L5.1.1)

- A) Encryption
- B) Hashing
- C) Hard copy
- D) Data life cycle

Why is an asset inventory so important? (D5.2, L5.2.1)

- A) It tells you what to encrypt
- B) You can't protect what you don't know you have
- C) The law requires it
- D) It contains a price list

Who is responsible for publishing and signing the organization's policies? (D5.3, L5.3.1)

- A) The security office
- B) Human Resources

C) Senior management

D) The legal department

Which of the following is always true about logging? (D5.1, L5.1.3)

A) Logs should be very detailed

B) Logs should be in English

C) Logs should be concise

D) Logs should be stored separately from the systems they're logging

A mode of encryption for ensuring confidentiality efficiently, with a minimum amount of processing overhead (D5.1, L5.1.3)

A) Asymmetric

B) Symmetric

C) Hashing

D) Covert

A ready visual cue to let anyone in contact with the data know what the classification is. (D5.1, L5.1.1)

A) Encryption

B) Label

C) Graphics

D) Photos

A set of security controls or system settings used to ensure uniformity of configuration throughout the IT environment. (D5.2, L5.2.1)

A) Patches

B) Inventory

C) Baseline

D) Policy

What is the most important aspect of security awareness/training? (D5.4, L5.4.1)

A) Protecting assets

B) Maximizing business capabilities

C) Ensuring the confidentiality of data

D) Protecting health and human safety

Which entity is most likely to be tasked with monitoring and enforcing security policy? (D5.3, L5.3.1)

A) The Human Resources office

B) The legal department

C) Regulators

D) The security office

Which organizational policy is most likely to indicate which types of smartphones can be used to connect to the internal IT environment? (D5.3, L5.3.1)

A) The CM policy (change management)

B) The password policy

C) The AUP (acceptable use policy)

D) The BYOD policy (bring your own device)