The primary goals and objectives of security are contained within the CIA Triad. Confidentiality Integrity & Availability.

**Confidentiality**

The first principle of the CIA Triad is confidentiality. If a security mechanism offers confidentiality, it offers a high level of assurance that data, objects, or resources are restricted from unauthorized subjects. If a threat exists against confidentiality, unauthorized disclosure could take place.

**Sensitivity** refers to the quality of information, which could cause harm or damage if disclosed. Maintaining confidentiality of sensitive information helps to prevent harm or damage.

**Discretion** is an act of decision where an operator can influence or control disclosure in order to minimize harm or damage.

**Criticality** The level to which information is mission critical is its measure of criticality. The higher the level of criticality, the more likely the need to maintain the confidentiality of the information. High levels of criticality are essential to the operation or function of an organization.

**Concealment** is the act of hiding or preventing disclosure. Often concealment is viewed as a means of cover, obfuscation, or distraction.

**Secrecy** is the act of keeping something a secret or preventing the disclosure of information.

**Privacy** refers to keeping information confidential that is personally identifiable or that might cause harm, embarrassment, or disgrace to someone if revealed.

**Seclusion** involves storing something in an out-of-the-way location. This location can also provide strict access controls. Seclusion can help enforcement confidentiality protections.

**Isolation** is the act of keeping something separated from others. Isolation can be used to prevent commingling of information or disclosure of information.

**Integrity**

The second principle of the CIA Triad is integrity. For integrity to be maintained, objects must retain their veracity and be intentionally modified by only authorized subjects. If a security mechanism offers integrity, it offers a high level of assurance that the data, objects, and resources are unaltered from their original protected state. Alterations should not occur while the object is in storage, in transit, or in process. Thus, maintaining integrity means the object itself is not altered and the operating system and programming entities that manage and manipulate the object are not compromised.

Integrity can be examined from three perspectives:

■ Preventing unauthorized subjects from making modifications

■ Preventing authorized subjects from making unauthorized modifications, such as mistakes

■ Maintaining the internal and external consistency of objects so that their data is a correct and true reflection of the real world and any relationship with any child, peer, or parent object is valid, consistent, and verifiable.

Numerous attacks focus on the violation of integrity. These include viruses, logic bombs, unauthorized access, errors in coding and applications, malicious modification, intentional replacement, and system back doors.

**Integrity is dependent on confidentiality. Without confidentiality, integrity cannot be maintained. Other concepts, conditions, and aspects of integrity include accuracy, truthfulness, authenticity, validity, nonrepudiation, accountability, responsibility, completeness, and comprehensiveness**

**Availability**

The third principle of the CIA Triad is availability, which means authorized subjects are granted timely and uninterrupted access to objects. If a security mechanism offers availability, it offers a high level of assurance that the data, objects, and resources are accessible to authorized subjects.

For availability to be maintained on a system, controls must be in place to ensure authorized access and an acceptable level of performance, to quickly handle interruptions, to provide for redundancy, to maintain reliable backups, and to prevent data loss or destruction.

**Availability depends on both integrity and confidentiality. Without integrity and confidentiality, availability cannot be maintained. Other concepts, conditions, and aspects of availability include usability, accessibility, and timeliness.**

**Identification**

Identification is the process by which a subject professes an identity and accountability is initiated. A subject must provide an identity to a system to start the process of authentication, authorization, and accountability (AAA).

**Authentication**

The process of verifying or testing that the claimed identity is valid is authentication.

**Authorization**

Once a subject is authenticated, access must be authorized. The process of authorization ensures that the requested activity or access to an object is possible given the rights and privileges assigned to the authenticated identity. Authorization is usually defined using one of the concepts of access control, such as discretionary access control (DAC), mandatory access control (MAC), or role-based access control (RBAC)

**Auditing** **recording a log of the events and** activities related to the system and subjects. Auditing, or monitoring, is the programmatic means by which a subject’s actions are tracked and recorded for the purpose of holding the subject accountable for their actions while authenticated on a system

**Accounting** (aka accountability) reviewing log files **to check for compliance and violations in order to hold subjects accountable for their actions.** An organization’s security policy can be properly enforced only if accountability is maintained.

**Nonrepudiation**

Nonrepudiation ensures that the subject of an activity or event cannot deny that the event occurred. Nonrepudiation prevents a subject from claiming not to have sent a message. Nonrepudiation can be established using digital certificates, session identifiers, transaction logs, and numerous other transactional and access control mechanism.

**Nonrepudiation is an essential part of accountability. A suspect cannot be held accountable if they can repudiate the claim against them.**

**Protection Mechanisms**

**Layering**

Layering, also known as defense in depth, is simply the use of multiple controls in a series. No one control can protect against all possible threats. Using a multilayered solution allows for numerous, different controls to guard against whatever threats come to pass. When security solutions are designed in layers, most threats are eliminated, mitigated, or thwarted. Using layers in a series rather than in parallel is important. Performing security restrictions in a series means to perform one after the other in a linear fashion

**Abstraction**

Abstraction is used for efficiency. Similar elements are put into groups, classes, or roles that are assigned security controls, restrictions, or permissions as a collective. Thus, the concept of abstraction is used when classifying objects or assigning roles to subjects. **Abstraction is used to define what types of data an object can contain, what types of functions can be** performed on or by that object, and what capabilities that object has. Abstraction simplifies security by enabling you to assign security controls to a group of objects collected by type or function.

**Data Hiding**

Data hiding is exactly what it sounds like: preventing data from being discovered or accessed by a subject by positioning the data in a logical storage compartment that is not accessible or seen by the subject. Forms of data hiding include keeping a database from being accessed by unauthorized visitors and restricting a subject at a lower classification level from accessing data at a higher classification level. Preventing an application from accessing hardware directly is also a form of data hiding. Data hiding is often a key element in security controls as well as in programming.

**Encryption**

Encryption is the art and science of hiding the meaning or intent of a communication from unintended recipients. Encryption can take many forms and be applied to every type of electronic communication.

Apply Security Governance Principles

Security governance is the collection of practices related to supporting, defining, and directing the security efforts of an organization.

**Alignment of Security Function to Strategy, Goals, Mission, and Objectives**

One of the most effective ways to tackle security management planning is to use a top down approach. **Upper, or senior, management is responsible for initiating and defining policies for the organization. Security policies provide direction for all levels of the organization’s hierarchy**. It is the responsibility of **middle management to flesh out the security policy into standards, baselines**, **guidelines, and procedures**. The **operational managers or security professionals must then implement the configurations prescribed in the security management documentation. Finally, the end users must comply with all the security policies of the organization.**

**A strategic plan should include a risk assessment.**

**Some examples of tactical plans are project plans, acquisition plans, hiring plans, budget plans, maintenance plans, support plans, and system development plans.**

**Operational plan include resource allotments, budgetary requirements, staffing assignments, scheduling, and step-by-step or implementation procedures. Operational plans include details on how the implementation processes are in compliance with the organization’s security policy. Examples of operational plans are training plans, system deployment plans, and product design plans**.

**Organizational Processes**

Security governance needs to address every aspect of an organization. This includes the organizational processes of acquisitions, divestitures, and governance committees. Acquisitions and mergers place an organization at an increased level of risk. Such risks include inappropriate information disclosure, data loss, downtime, or failure to achieve sufficient return on investment (ROI). In addition to all the typical business and financial aspects of mergers and acquisitions, a healthy dose of security oversight and increased scrutiny is often essential to reduce the likelihood of losses during such a period of transformation.

**Often, security governance is managed by a governance committee or at least a board of directors. This is the group of influential knowledge experts whose primary task is to oversee and guide the actions of security and operations for an organization. Security** is a complex task. Organizations are often large and difficult to understand from a single viewpoint. Having a group of experts work together toward the goal of reliable security governance is a solid strategy. **Two additional examples of organizational processes that are essential to strong security governance are change control/change management and data classification.**

**Change Control/Management**

The goal of change management is to ensure that any change does not lead to reduced or compromised security. Change management is also responsible for making it possible to roll back any change to a previous secured state. Change management can be implemented on any system despite the level of security. It is a requirement for systems complying with the Information Technology Security Evaluation and Criteria (ITSEC) classifications of B2, B3, and A1. Ultimately, change management improves the security of an environment by protecting implemented security from unintentional, tangential, or affected diminishments. Although an important goal of change management is to prevent unwanted reductions in security, its primary purpose is to make all changes subject to detailed documentation and auditing and thus able to be reviewed and scrutinized by management.

The change control process of configuration or change management has several goals or requirements:

■ Implement changes in a monitored and orderly manner. Changes are always controlled.

■ A formalized testing process is included to verify that a change produces expected results.

■ All changes can be reversed (also known as backout or rollback plans/procedures). Users are informed of changes before they occur to prevent loss of productivity.

■ The effects of changes are systematically analyzed.

■ The negative impact of changes on capabilities, functionality, and performance is minimized.

■ Changes are reviewed and approved by a CAB (change approval board).

**One example of a change management process is a parallel run, which is a type of new system deployment testing where the new system and the old system are run in parallel**.

**Data Classification**

The primary objective of data classification schemes is to formalize and stratify the process of securing data based on assigned labels of importance and sensitivity. Data classification is used to provide security mechanisms for storing, processing, and transferring data. It also addresses how data is removed from a system and destroyed.

The following are benefits of using a data classification scheme:

■ It demonstrates an organization’s commitment to protecting valuable resources and assets.

■ It assists in identifying those assets that are most critical or valuable to the organization.

■ It lends credence to the selection of protection mechanisms.

■ It is often required for regulatory compliance or legal restrictions.

■ It helps to define access levels, types of authorized uses, and parameters for declassification and/or destruction of resources that are no longer valuable.

■ It helps with data life-cycle management which in part is the storage length (retention), usage, and destruction of the data.

The criteria by which data is classified vary based on the organization performing the classification. However, you can glean numerous generalities from common or standardized classification systems:

■ Usefulness of the data ■ Timeliness of the data , Value or cost of the data ■ Maturity or age of the data ■ Lifetime of the data (or when it expires) ■ Association with personnel , Data disclosure damage assessment, Data modification damage assessment , National security implications of the data , Authorized access to the data , Restriction from the data , Maintenance and monitoring of the data , Storage of the data

To implement a classification scheme, you must perform seven major steps, or phases:

1. Identify the custodian and define their responsibilities.

2. Specify the evaluation criteria of how the information will be classified and labeled.

3. Classify and label each resource. (The owner conducts this step, but a supervisor should review it.)

4. Document any exceptions to the classification policy that are discovered and integrate them into the evaluation criteria.

5. Select the security controls that will be applied to each classification level to provide the necessary level of protection.

6. Specify the procedures for declassifying resources and the procedures for transferring custody of a resource to an external entity.

7. Create an enterprise-wide awareness program to instruct all personnel about the classification system.

**The two common classification schemes are government/military classification and commercial business/private sector classification.**

**Items labeled as confidential, secret, and top secret are collectively known as classified. Often, revealing the actual classification of data to unauthorized individuals is a violation of that data. Thus, the term classified is generally used to refer to any data that is ranked above the unclassified level.**

**All classified data is exempt from the Freedom of Information Act as well as many other laws and regulations.**

**Security Roles and Responsibilities**

**Senior Manager** The organizational owner (senior manager) role is assigned to the person who is ultimately responsible for the security maintained by an organization and who should be most concerned about the protection of its assets. The senior manager must sign off on all policy issues. In fact, all activities must be approved by and signed off on by the senior manager before they can be carried out. is responsible for exercising due care and due diligence in establishing security for an organization.

**Security Professional** The security professional, information security (InfoSec) officer, or computer incident response team (CIRT) role is assigned to a trained and experienced network, systems, and security engineer who is responsible for following the directives mandated by senior management. Security professionals

are not decision makers; they are implementers. All decisions must be left to the senior manager.

**Data Owner** The data owner role is assigned to the person who is responsible for classifying information for placement and protection within the security solution. The data owner is typically a high-level manager who is ultimately responsible for data protection. However, the data owner usually delegates the responsibility of the actual data management tasks to a data custodian.

**Data Custodian** The data custodian role is assigned to the user who is responsible for the tasks of implementing the prescribed protection defined by the security policy and senior management. The data custodian performs all activities necessary to provide adequate protection for the CIA Triad (confidentiality, integrity, and availability) of data and to fulfill the requirements and responsibilities delegated from upper management. These activities can include performing and testing backups, validating data integrity, deploying security solutions, and managing data storage based on classification

**User** The user (end user or operator) role is assigned to any person who has access to the secured system. A user’s access is tied to their work tasks and is limited so they have only enough access to perform the tasks necessary for their job position (the principle of least privilege). Users are responsible for understanding and upholding the security policy of an organization by following prescribed operational procedures and operating within defined security parameters.

**Auditor** An auditor is responsible for reviewing and verifying that the security policy is properly implemented and the derived security solutions are adequate. The auditor role may be assigned to a security professional or a trained user. The auditor produces compliance and effectiveness reports that are reviewed by the senior manager.

**Control Frameworks**

COBIT is a documented set of best IT security practices crafted by the Information Systems Audit and Control Association (ISACA). It prescribes goals and requirements for security controls and encourages the mapping of IT security ideals to business objectives. **COBIT 5 is based on five key principles for governance and management of enterprise IT: Principle 1: Meeting Stakeholder Needs, Principle 2: Covering the Enterprise End-to-End, Principle 3: Applying a Single, Integrated Framework, Principle 4: Enabling a Holistic Approach, and Principle 5: Separating Governance From Management. COBIT is used not only to plan the IT security of an organization but also as a guideline for auditors**

**Due Care and Due Diligence**

**Due care is using reasonable care to protect the interests of an organization. Due diligence is practicing the activities that maintain the due care effort. For example, due care is developing a formalized security structure containing a security policy, standards, baselines, guidelines, and procedures. Due diligence is the continued application of this security structure onto the IT infrastructure of an organization**.

**Security Policies**

The security policy is an overview or generalization of an organization’s security needs. It defines the main security objectives and outlines the security framework of an organization. It also identifies the major functional areas of data processing and clarifies and defines all relevant terminology. It should clearly define why security is important and what assets are valuable. It is a strategic plan for implementing security. It should broadly outline the security goals and practices that should be employed to protect the organization’s vital interests.

The security policy is used to assign responsibilities, define roles, specify audit requirements, outline enforcement processes, indicate compliance requirements, and define acceptable risk levels. This document is often used as the proof that senior management has exercised due care in protecting itself against intrusion, attack, and disaster. Security policies are compulsory

**An issue-specific security policy focuses on a specific network service, department**, function, or other aspect that is distinct from the organization as a whole. **A system-specific security policy focuses on individual systems or types of systems and prescribes approved hardware and software**, outlines methods for locking down a system, and even mandates firewall or other specific security controls.

In addition to these focused types of security policies, there are three overall categories of security policies: regulatory, advisory, and informative. A regulatory policy is required whenever industry or legal standards are applicable to your organization. This policy discusses the regulations that must be followed and outlines the procedures that should be used to elicit compliance. An advisory policy discusses behaviors and activities that are acceptable and defines consequences of violations. It explains senior management’s desires for security and compliance within an organization. Most policies are advisory. An informative policy is designed to provide information or knowledge about a specific subject, such as company goals, mission statements, or how the organization interacts with partners and customers. An informative policy provides support, research, or background information relevant to the specific elements of the overall policy. **Standards are the next level below security policies.**

**Standards are tactical documents that define steps or methods to accomplish the goals and overall direction defined by security policies**

At the next level are baselines. **A baseline defines a minimum level of security that every system throughout the organization must meet. All systems not complying with the baseline should be taken out of production until they can be brought up to the baseline**. The baseline establishes a common foundational secure state on which all additional and more stringent security measures can be built. Baselines are usually system specific and often refer to an industry or government standard, like the Trusted Computer System Evaluation Criteria (TCSEC) or Information Technology Security Evaluation and Criteria (ITSEC) or NIST (National Institute of Standards and Technology) standards.

**A guideline offers recommendations on how standards and baselines are implemented** and serves as an operational guide for both security professionals and users. Guidelines are flexible so they can be customized for each unique system or condition and can be used in the creation of new procedures. They state which security mechanisms should be deployed instead of prescribing a specific product or control and detailing configuration settings. They outline methodologies, include suggested actions, and are not compulsory.

**Security Procedures**

Procedures are the final element of the formalized security policy structure. A procedure is a detailed, step-by-step how-to document that describes the exact actions necessary to implement a specific security mechanism, control, or solution

**Not all users need to know the security standards, baselines, guidelines, and procedures for all security classification levels.**

**■ When changes occur, it is easier to update and redistribute only the affected material rather than updating a monolithic policy and redistributing it throughout the organization**

Understand and Apply Threat Modeling

Threat modeling is the security process where potential threats are identified, categorized, and analyzed. Threat modeling can be performed as a proactive measure during design and development or as a reactive measure once a product has been deployed. In either case, the process identifies the potential harm, the probability of occurrence, the priority of concern, and the means to eradicate or reduce the threat.

**Threat modeling isn’t meant to be a single event. Instead it’s common for an organization to begin threat modeling early in the design process of a system and continue throughout its life cycle. For example, Microsoft uses a Security Development Lifecycle (SDL) process to consider and implement security at each stage of a product’s development. This supports the motto of “Secure by Design, Secure by Default, Secure in Deployment and Communication” (also known as SD3+C). It has two goals in mind with this process:**

**■ To reduce the number of security-related design and coding defects**

**■ To reduce the severity of any remaining defects**

**A proactive approach to threat modeling takes place during early stages of systems development, specifically during initial design and specifications establishment. This type of threat modeling is also known as a defensive approach. This method is based on predicting threats and designing in specific defenses during the coding and crafting process, rather than relying on post deployment updates and patches. In most cases, integrated security solutions are more cost effective and more successful than those shoehorned in later. Unfortunately, not all threats can be predicted during the design phase, so reactive approach threat modeling is still needed to address unforeseen issues.**

**A reactive approach to threat modeling takes place after a product has been created and deployed. This deployment could be in a test or laboratory environment or to the general marketplace. This type of threat modeling is also known as the adversarial approach. This technique of threat modeling is the core concept behind ethical hacking, penetration testing, source code review, and fuzz testing.**

**Fuzz testing is a specialized dynamic testing technique that provides many different types of input to software to stress its limits and find previously undetected flaws. Fuzz testing software supplies invalid input to the software, either randomly generated or specially crafted to trigger known software vulnerabilities. The fuzz tester then monitors the performance of the application, watching for software crashes, buffer overflows, or other undesirable and/or unpredictable outcomes**

**Identifying Threats**

**Focused on Assets** This method uses asset valuation results and attempts to identify threats to the valuable assets.

**Focused on Attackers** Some organizations are able to identify potential attackers and can identify the threats they represent based on the attacker’s goals.

**Focused on Software** If an organization develops software, it can consider potential threats against the software.

**Microsoft developed a threat categorization scheme known as STRIDE. STRIDE is often used in relation to assessing threats against applications or operating systems.**

**Spoofing**

**Tampering -**Tampering is used to falsify communications or alter static information. Such attacks are a violation of integrity as well as availability.

**Repudiation**

**Information disclosure**

**Denial of service**

**Elevation of privilege**

**Although STRIDE is typically used to focus on application threats, it is applicable to other situations, such as network threats and host threats**. Other attacks may be more specific to network and host concerns, such as sniffing and hijacking for networks and malware and arbitrary code execution for hosts, but the six threat concepts of STRIDE are fairly broadly applicable.

**Performing Reduction Analysis**

The next step in threat modeling is to perform reduction analysis. Reduction analysis is also known as decomposing the application, system, or environment. The purpose of this task is to gain a greater understanding of the logic of the product as well as its interactions with external elements. Whether an application, a system, or an entire environment, **it needs to be divided into smaller containers or compartments.**

In the decomposition process, you must identify five key concepts:

**Trust Boundaries** Any location where the level of trust or security changes

**Data Flow Paths** The movement of data between locations

**Input Points** Locations where external input is received

**Privileged Operations** Any activity that requires greater privileges than of a standard user account or process, typically required to make system changes or alter security

**Details about Security Stance** and Approach The declaration of the security policy, security foundations, and security assumptions

**Prioritization and Response**

As threats are identified through the threat modeling procedure, additional activities are prescribed to round out the process. Next is to fully document the threats. **After documentation, rank or rate the threats. This can be accomplished using a wide range of techniques, such as Probability × Damage Potential ranking, high/medium/low rating, or the DREAD system.**

The ranking technique of Probability × Damage Potential produces a risk severity number on a scale of 1 to 100, with 100 the most severe risk possible. Each of the two initial values can be assigned numbers between 1 and 10, with 1 being lowest and 10 being highest.

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:

■ Damage potential—How severe is the damage likely to be if the threat is realized?

■ Reproducibility—How complicated is it for attackers to reproduce the exploit?

■ Exploitability—How hard is it to perform the attack

Affected users—How many users are likely to be affected by the attack (as a percentage)?

■ Discoverability—How hard is it for an attacker to discover the weakness?

When evaluating a third party for your security integration, consider the following processes

**On-Site Assessment** Visit the site of the organization to interview personnel and observe their operating habits.

**Document Exchange and Review** Investigate the means by which datasets and documentation are exchanged as well as the formal processes by which they perform assessments and reviews.

**Process/Policy Review** Request copies of their security policies, processes/procedures, and documentation of incidents and responses for review..

..