Chapter 1 - Security Governance Through Principles and Policies

Confidentiality, integrity, and availability (CIA) (i.e., the CIA Triad) are typically viewed as the primary goals and objectives of a security infrastructure.

Confidentiality is the concept of the measures used to ensure the protection of the secrecy of data, objects, or resources. The goal of confidentiality protection is to prevent or minimize unauthorized access to data.

Numerous countermeasures can help ensure confidentiality against possible threats. These include encryption, network traffic padding, strict access control, rigorous authentication procedures, data classification, and extensive personnel training.

Integrity is the concept of protecting the reliability and correctness of data. Integrity protection prevents unauthorized alterations of data.

Confidentiality and integrity depend on each other. Without object integrity (in other words, the inability of an object to be modified without permission), confidentiality cannot be maintained.

Numerous countermeasures can ensure integrity against possible threats. These include strict access control, rigorous authentication procedures, intrusion detection systems, object/ data encryption, hash verifications, and extensive personnel training.

Availability means authorized subjects are granted timely and uninterrupted access to objects. Availability depends on both integrity and confidentiality.

Numerous countermeasures can ensure availability against possible threats. These include monitoring performance and network traffic, using firewalls and routers to prevent DoS attacks, implementing redundancy for critical systems, and maintaining and testing backup systems.

One interesting security concept is the opposite of the CIA Triad, which is the DAD Triad. Disclosure, alteration, and destruction make up the DAD Triad. The DAD Triad represents the failures of security protections in the CIA Triad.

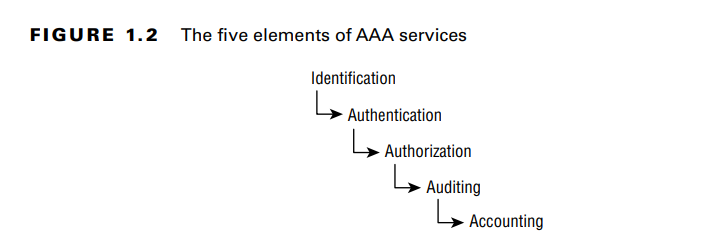
It may also be worthwhile to know that too much security can be its own problem. Overprotecting confidentiality or integrity can result in a restriction of availability.

Authenticity is the security concept that data is authentic or genuine and originates from its alleged source. This is related to integrity, but it’s more closely related to verifying that it is from a claimed origin.

Nonrepudiation ensures that the subject of an activity or who caused an event cannot deny that the event occurred.

**AAA ( IAAA/ IAAAA )** services is a core security mechanism of all security environments (majorly used in authentication context). The three As in this abbreviation refer to authentication, authorization, and accounting (or sometimes auditing).

However, what is not as clear is that although there are three letters in the acronym, it actually refers to five elements: identification, authentication, authorization, auditing, and accounting.



**Identification** - Verifying identity of a subject to keep a track of their activities performed across the system.

**Authentication** - Identity must be verified before use by providing additional information such as passwords or tokens. Identification and authentication are often used together as a single two-step process.

**Authorization** - Validate if the authenticated subject has relevant permissions or rights to perform the activity.

**Auditing** - Record activities of a subject in a log file.

**Accountability** - Capability to review log files to make subjects accountable for their action.

**Protection Mechanisms**

**Defense in depth** is 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. It is also referred to as layering, levels, multi-level, classifications, zones, realms, compartments, silos, segmentations, lattice structure, and protection rings.

**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. Abstraction simplifies security by enabling you to assign security controls to a group of objects collected by type or function.

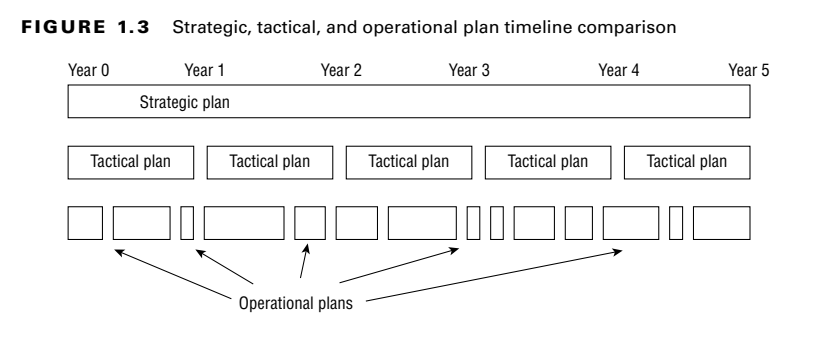
**Data hiding** is exactly what it sounds like: preventing data from being discovered or accessed by a subject by positioning the data in a logical storage compartment that is not accessible or seen by the subject. For eg - keeping database private, restricting subject at lower classification level to access objects at higher level.

**Encryption** is the science of hiding the meaning or intent of a communication from unintended recipients.

A security boundary exists between a high-security area and a low-security one, such as between a LAN and the internet. Security boundaries must be identified for the environment and security controls must be deployed to control the flow of information across the boundary.

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. 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 security management planning team should develop three types of plans, as shown in Figure:



Security governance should address every aspect of an organization, including the organizational processes of acquisitions, divestitures, and governance committees.

**Security Control Frameworks**

Control Objectives for Information and Related Technology (COBIT) is a set of best IT security practices crafted by ISACA. COBIT is based on six key principles:

■ Provide Stakeholder Value

■ Holistic Approach

■ Dynamic Governance System

■ Governance Distinct from Management

■ Tailored to Enterprise Needs

■ End-to-End Governance System

NIST SP 800-53 is a U.S. government–sourced general recommendations for organizational security.

Center for Internet Security (CIS) provides OS, application, and hardware security configuration guides.

ISO/ IEC 27000 family is an international standard that can be the basis of implementing organizational security and related management practices.

Information Technology Infrastructure Library (ITIL) was initially crafted by the British government for domestic use but is now an international standard for security best practices.

**Due diligence** is knowing what should be done and planning for it; **due care** is doing the right action at the right time.

The security policy is an overview or generalization of an organization’s security needs. It defines the strategic security objectives, vision, and goals and outlines the security framework of an organization.

Standards define compulsory requirements for the homogenous use of hardware, software, technology, and security controls. They provide a course of action by which technology and procedures are uniformly implemented throughout an organization.

A baseline defines a minimum level of security that every system throughout the organization must meet.

A guideline offers recommendations on implementation of standards and baselines. Guidelines are flexible, include suggested actions, and are not compulsory.

A procedure or standard operating procedure (SOP) is a detailed, step-by-step how-to document that describes the exact actions necessary to implement a specific security mechanism, control, or solution.

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.

Not all threats can be predicted during the design phase, so a reactive approach to threat management is needed to address unforeseen issues. This concept is often called threat hunting or may be referred to as an adversarial approach. This technique of threat hunting is the core concept behind ethical hacking, penetration testing, source code review, and fuzz testing.

Process for Attack Simulation and Threat Analysis (PASTA) is a risk-centric seven-stage threat modeling methodology.

There’s an almost infinite possibility of threats, so it’s important to use a structured approach to accurately **identify** relevant threats. For example, some organizations use one or more of the following three approaches:

1. Focused on Assets
2. Focused on Attackers
3. Focused on Software

When attempting to inventory and **categorize** threats, it is often helpful to use a guide or reference. Microsoft developed a threat categorization scheme known as the **STRIDE** threat model. STRIDE is an acronym for Spoofing, Tampering, Repudiation, Information disclosure, Denial of service (DoS), Elevation of privilege.

Threat **Prioritization** can be performed using a wide range of techniques, such as Probability × Damage Potential ranking, high/ medium/low rating, or the DREAD system.

DREAD - Disaster, Reproducibility, Exploitability, Affected Users, and Discoverability

In many situations, especially related to government or military agencies or contractors, if the vendor fails to meet minimum security requirements of third-party governance, it can result in a loss of or a voiding of authorization to operate (ATO).

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, its internal components, as well as its interactions with external elements.

Key concepts of reduction analysis are:

* **Trust Boundaries** - Any location where the level of trust or security changes
* **Dataflow Paths** - The movement of data between locations
* **Input Points** - Locations where external input is received
* **Privileged Operation**s - 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