

Information Security

Dr./ Ahmed Mohamed Rabie

Chapter 1

Introduction to Information Security

Control Frameworks

Crafting a security stance for an organization often involves a lot more than just writing down a few lofty ideals. In most cases, a significant amount of planning goes into developing a solid security policy. Many Dilbert fans may recognize the seemingly absurd concept of holding a meeting to plan a meeting for a future meeting. But it turns out that planning for security must start with planning to plan, then move into planning for standards and compliance, and finally move into the actual plan development and design.

Skipping any of these “planning to plan” steps can derail an organization’s security solution before it even gets started. One of the first and most important security planning steps is to consider the overall control framework or structure of the security solution desired by the organization. You can choose from several options in regard to security concept infrastructure.

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,

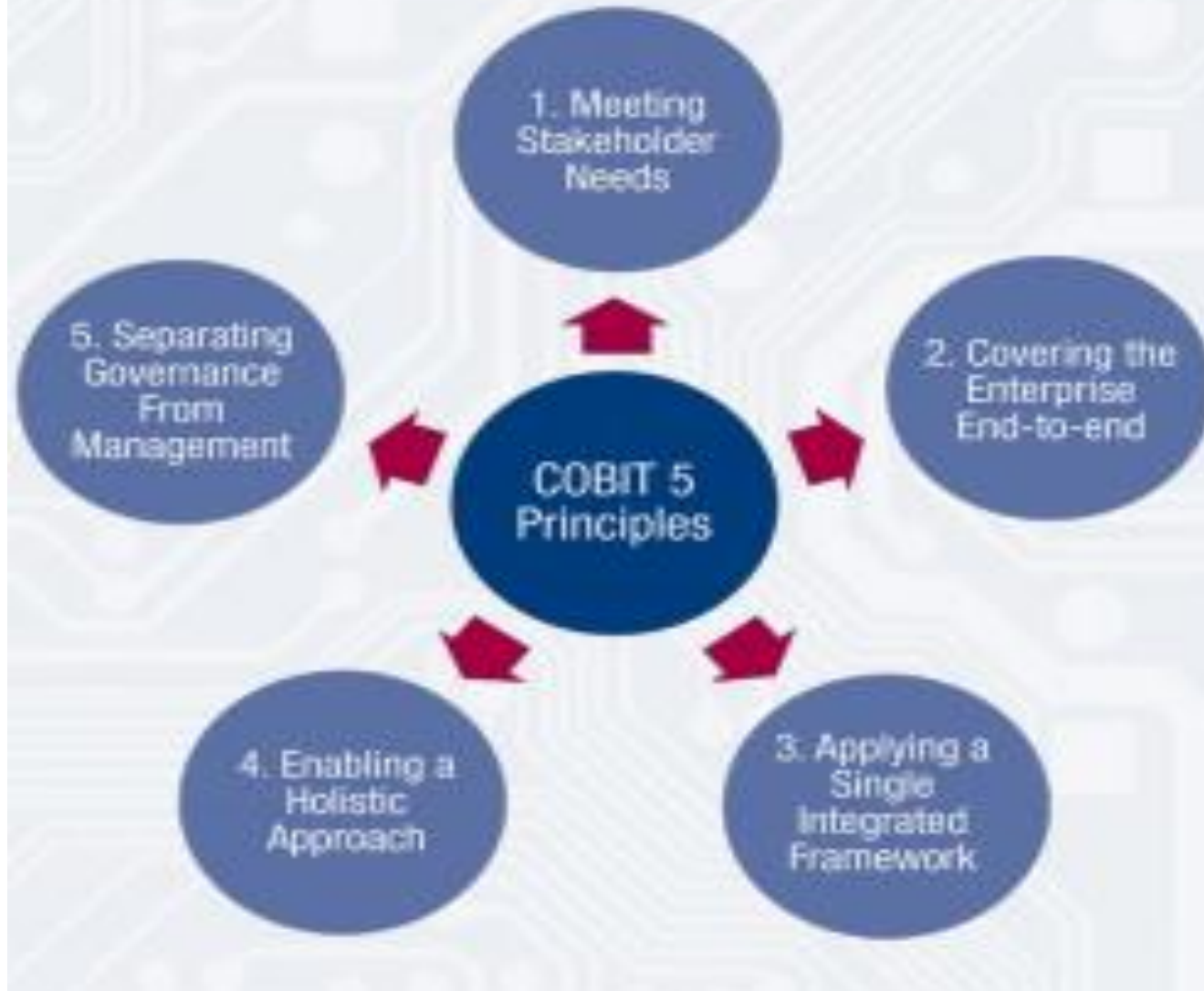
Principle 3: Applying a Single, Integrated Framework,

Principle 4: Enabling a Holistic Approach,

and Principle 5: Separating Governance From Management.

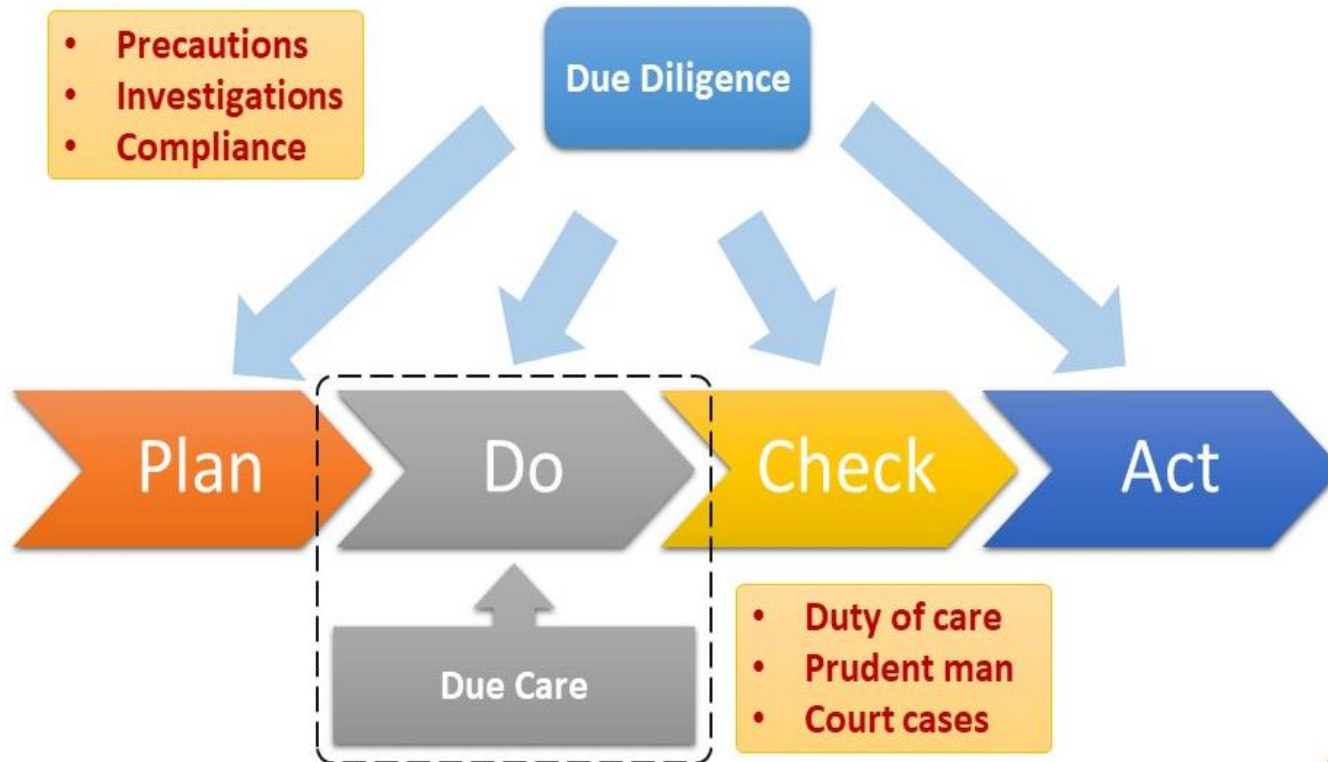
COBIT is used not only to plan the IT security of an organization but also as a guideline for auditors.

COBIT 5 Principles

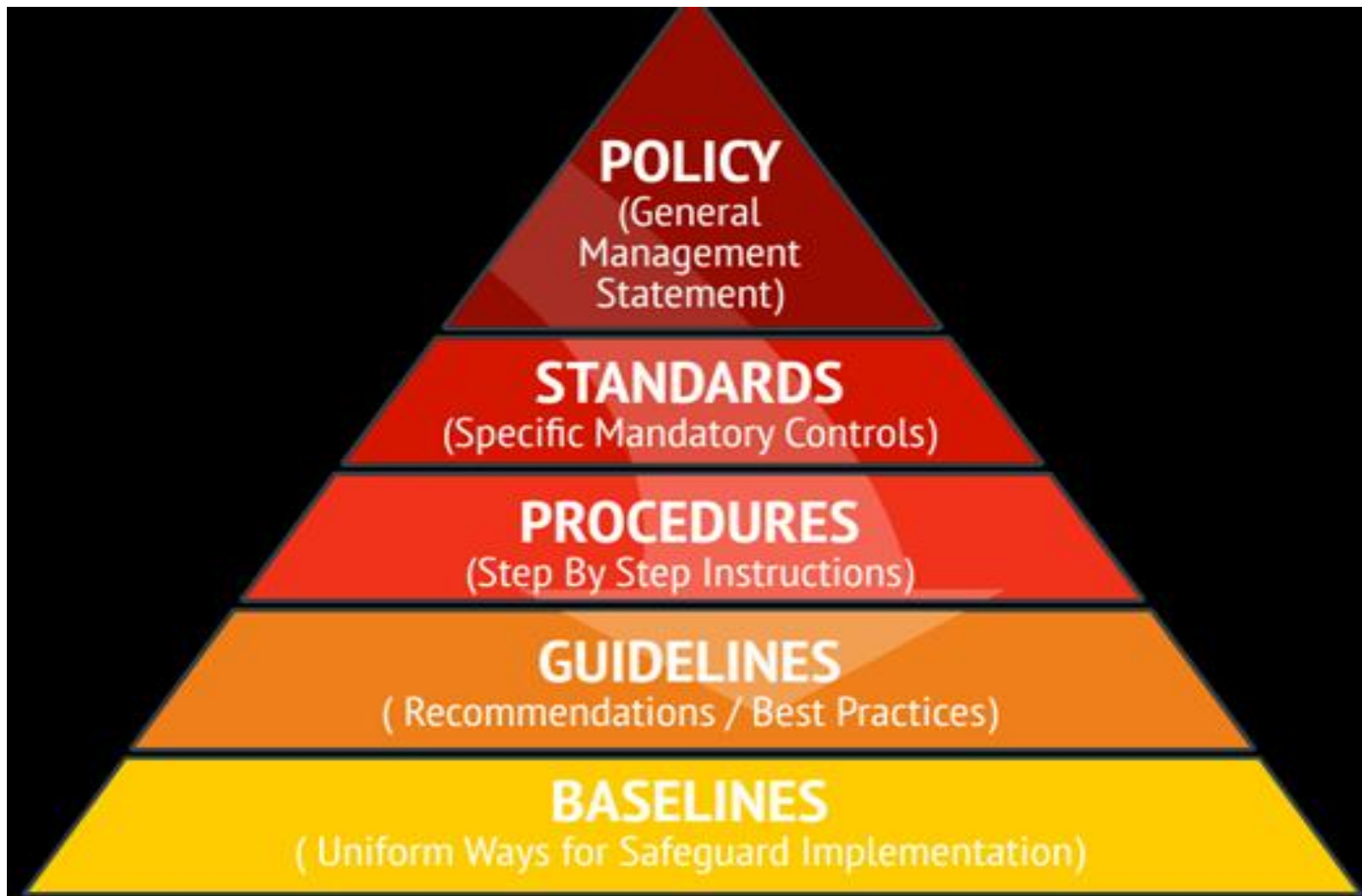


Why is planning to plan security so important? One reason is the requirement for due care and due diligence. **Due care** is using reasonable care to protect the interests of an organization. **Due diligence** is practicing the activities that maintain the due care effort. For example, due care is developing 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.

Due Diligence and Due Care



Operational security is the ongoing maintenance of continued due care and due diligence by all responsible parties within an organization. In today's business environment, prudence is mandatory. Showing due care and due diligence is the only way to disprove negligence in an occurrence of loss. Senior management must show due care and due diligence to reduce their culpability and liability when a loss occurs.



Security Policies

For most organizations, **maintaining security is an essential part of ongoing business.** If their security were seriously compromised, many organizations would fail. To reduce the likelihood of a security failure, the process of implementing security has been somewhat formalized with a hierarchical organization of documentation. Each level focuses on a specific type or category of information and issues.

Developing and implementing documented security policy, standards, procedures, and guidelines produces a solid and reliable security infrastructure. This formalization has greatly reduced the chaos and complexity of designing and implementing security solutions for IT infrastructures.

Security Policies The top tier of the formalization is known as a security policy. A security policy is a document that defines the scope of security needed by the organization and discusses the assets that require protection and the extent to which security solutions should go to provide the necessary protection. 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 document discusses the importance of security to every aspect of daily business operation and the importance of the support of the senior staff for the implementation of security. 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.**

Many organizations employ several types of security policies to define or outline their overall security strategy. An organizational security policy focuses on issues relevant to every aspect of an organization. **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.

From the security policies flow many other documents or sub elements necessary for a complete security solution. Policies are broad overviews, whereas standards, baselines, guidelines, and procedures include more specific, detailed information on the actual security solution. Standards are the next level below security policies.

Security Standards

Security Standards, Baselines, and Guidelines

Once the main security policies are set, then the remaining security documentation can be crafted under the guidance of those policies. **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.

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

Security Procedures

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. A procedure could discuss the entire system deployment operation or focus on a single product or aspect, such as deploying a firewall or updating virus definitions.

In most cases, **procedures are system and software specific**. They must be updated as the hardware and software of a system evolve. The purpose of a procedure is to **ensure the integrity of business processes**. If everything is accomplished by following a detailed procedure, then all activities should be in compliance with policies, standards, and guidelines. Procedures help ensure standardization of security

 across all systems.

Security Guidelines

Guidelines are the next element of the formalized security policy structure. 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 Baselines

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.

All too often, policies, standards, baselines, guidelines, and procedures are developed only as an afterthought at the urging of a consultant or auditor. If these documents are not used and updated, the administration of a secured environment will be unable to use them as guides. And without the planning, design, structure, and oversight provided by these documents, no environment will remain secure or represent proper diligent due care.

It is also common practice to develop a single document containing aspects of all these elements.

This should be avoided. Each of these structures must exist as a separate entity because each performs a different specialized function. At the top of the formalization security policy documentation structure there are fewer documents because they contain general broad discussions of overview and goals.

There are more documents further down the formalization structure (in other words, guidelines and procedures) because they contain details specific to a limited number of systems, networks, divisions, and areas.

Keeping these documents as separate entities provides several benefits:

- 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.

Crafting the totality of **security policy** and all supporting documentation can be **a daunting task**.

Many organizations struggle just to define the foundational parameters of their security, much less detail every single aspect of their day-to-day activities. However, in theory, **a detailed and complete security policy supports real-world security in a directed, efficient, and specific manner.**

Once the security policy documentation is reasonably complete, it can be used to guide decisions, train new users, respond to problems, and predict trends for future expansion. A security policy should not be an afterthought but a key part of establishing an organization.

There are a few additional perspectives to understand about the documentation that comprises a complete security policy. The dependencies of these components: policies, standards, guidelines, and procedures. The security policies are the foundation of the overall structure of organized security documentation. Then, standards are based on those policies as well as mandated by regulations and contracts.

From these the guidelines are derived. Finally, procedures are based on the three underlying layers of the structure. The inverted pyramid is used to convey the volume or size of each of these documents. There are typically significantly more procedures than any other element in a complete security policy. Comparatively, there are fewer guidelines than policies, fewer still standards, and usually even fewer still of overarching or organization-wide security policies.