Domain 2

Risk Management and Security Governance

Security Governance Concepts, Principles, and Policies

- Understand and align security function to goals, mission, and objectives of the organization

- Understand and apply security governance

- Understand and apply concepts of confidentiality, integrity and availability

- Develop and implement security policy

- Manage the information life cycle (classification, categorization and ownership)

Security Management Planning

ensures proper creation, implementation, and

enforcement of a security policy.

Upper/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

Approaches to Information Security Implementation Contd...

14
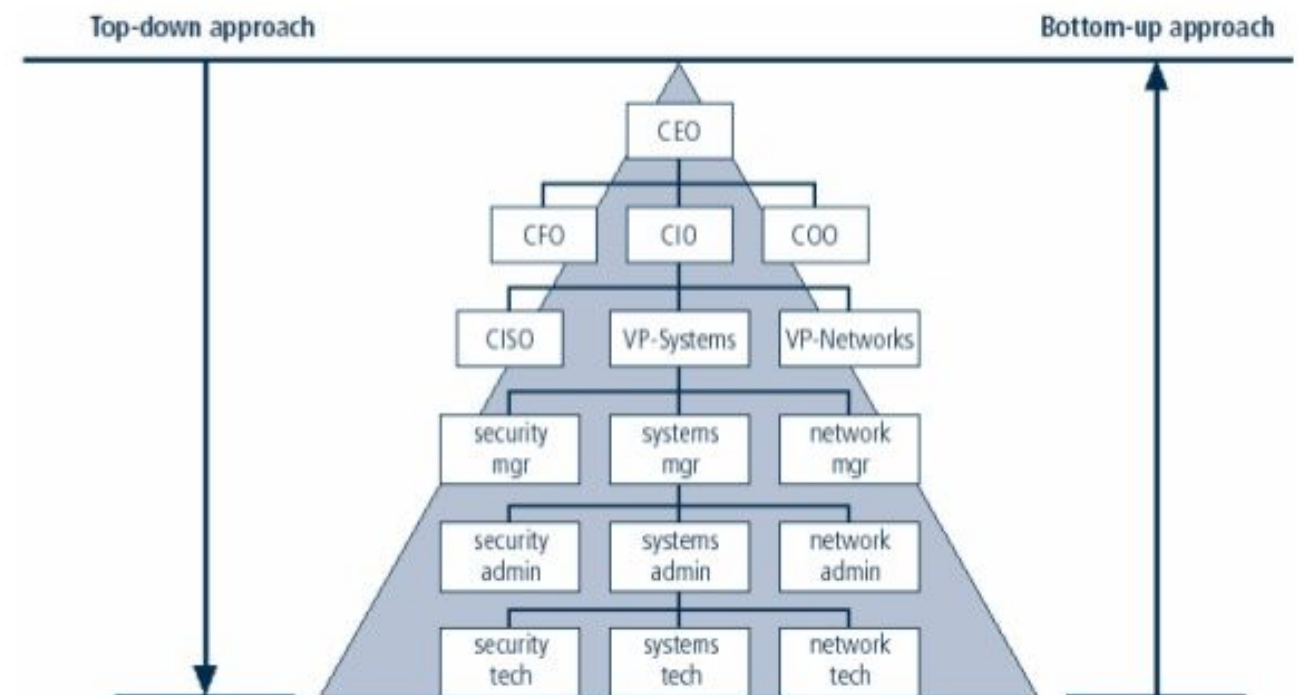
Security Management Planning

- defining security roles;

Elements: how security will be managed,

- who will be responsible for security,

- and how security will be tested for effectiveness;

- developing security policies;

- performing risk analysis;

- and requiring security education for employees.

"The best security plan is useless without one key factor: approval by senior management."

A security management planning team should develop three types of plans:

- Strategic plan

Long-term plan. It defines the organization's security purpose and helps to understand security function and align it to goals, mission, and objectives of the organization. It's useful for about five years. A strategic plan should include a risk assessment.

- Tactical plan

Midterm plan developed to provide more details on accomplishing the goals set forth in the strategic plan. It is typically useful for about a year. Some examples of tactical plans include project plans, acquisition plans, hiring plans, budget plans, maintenance plans, support plans, and system development plans.

- Operational plan

Short-term plan. Highly detailed plan based on the strategic and tactical plans. Operational plans must be updated often (such as monthly or quarterly) to retain compliance with tactical plans. Operational plans include details on how the implementation processes are in compliance with the organization's security policy. Examples of operational plans include training plans, system deployment plans, and product design plans.

Security Governance

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

Security governance must be assessed and verified from time to time.

Security is an organizational process, not just something the IT geeks do behind the scenes. Using the term *security governance* is an attempt to emphasize this point by indicating that security needs to be managed and governed throughout the organization, not just in the IT department.

Security Roles and Responsibilities

- Senior manager

- Security professional, Information Security officer, computer incident response team

- Data owner

- Data custodian

- User

- Auditor

threats come to pass.

Protection Mechanisms

- *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 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.

- *Data hiding* is 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 access- ing data at a higher classification level.

Security Management Concepts and Principles

SELF-READING
CHAPTER 5

A security policy is a document that defines the scope of security needed by the

Develop and Implement Security Policy

organization and discusses the assets that need protection and the extent to which security

solutions should go to provide the necessary protection.

Incudes:

Security objectives

Valuable assets

Terminology

Security goals and practices

Used to:

assign responsibilities,

define roles,

specify audit requirements,

outline enforcement processes,

indicate compliance requirements,

and define acceptable risk levels;

Security Standards, Baselines, and Guidelines

What are the four components of a complete organizational security policy and their basic purpose?

- Policies are broad security statements.

- Standards are definitions of hardware and software security compliance. Standards are tactical documents that define steps or methods to accomplish the goals and overall direction defined by security policies.

- Guidelines are used when there is not an appropriate procedure. Guidelines are flexible so they can be customized for each unique system or condition. 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.

- Procedures are detailed step-by-step instructions for performing work tasks in a secure manner.

Change Control/Management

Data Classification

SELF-READING
CHAPTER 5