PLANNING FOR SECURITY

Learning Objectives:

Upon completion of this chapter you should be able to:

- Understand management‘s responsibilities and role in the development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines
- Understand the differences between the organization‘s general information security policy and the requirements and objectives of the various issue-specific and system-specific policies.
- Know what an information security blueprint is and what its major components are.
- Understand how an organization institutionalizes its policies, standards, and practices using education, training, and awareness programs.
- Become familiar with what viable information security architecture is, what it includes, and how it is used.
- Explain what contingency planning is and how incident response planning, disaster recovery planning, and business continuity plans are related to contingency planning.

1.1 Introduction

— The creation of an information security program begins with the creation and/or review of the organization‘s information security policies, standards, and practices.

— Then, the selection or creation of information security architecture and the development and use of a detailed information security blueprint will create the plan for future success.

— This blueprint for the organization‘s information security efforts can be realized only if it operates in conjunction with the organization‘s information security policy.

— Without policy, blueprints, and planning, the organization will be unable to meet the information security needs of the various communities of interest.

— The organizations should undertake at least some planning: strategic planning to manage the allocation of resources, and contingency planning to prepare for the uncertainties of the business environment.

1.2 Information Security Policy, Standards, and Practices

- Management from all communities of interest must consider policies as the basis for all information security efforts like planning, design and deployment.
- Policies direct how issues should be addressed and technologies used
- Policies do not specify the proper operation of equipments or software-this information should be placed in the standards, procedures and practices of user's manuals and systems documentation.
- Security policies are the least expensive control to execute, but the most difficult to implement properly.
- Shaping policy is difficult because:
  - Never conflict with laws
  - Stand up in court, if challenged
  - Be properly administered through dissemination and documented acceptance.

Definitions

- A policy is a plan or course of action, as of a government, political party, or business, intended to influence and determine decisions, actions, and other matters
  A policy is a plan or course of action used by an organization to convey instructions from its senior-most management to those who make decisions, take actions, and perform other duties on behalf of the organization.
- Policies are organizational laws. Policies must define what is right, what is wrong, what the penalties for violating policy, and what the appeal process is..
- Standards, on the other hand, are more detailed statements of what must be done to comply with policy.
- Standards may be published, scrutinized, and ratified by a group, as in formal or de jury standards.
- Practices, procedures, and guidelines effectively explain how to comply with policy.
- For a policy to be effective it must be properly disseminated, read, understood and agreed to by all members of the organization
- Finally, practices, procedures, and guidelines effectively explain how to comply with policy.

— Fig 6-1 shows policies as the force that drives standards, which in turn drive practices, procedures, and guidelines.

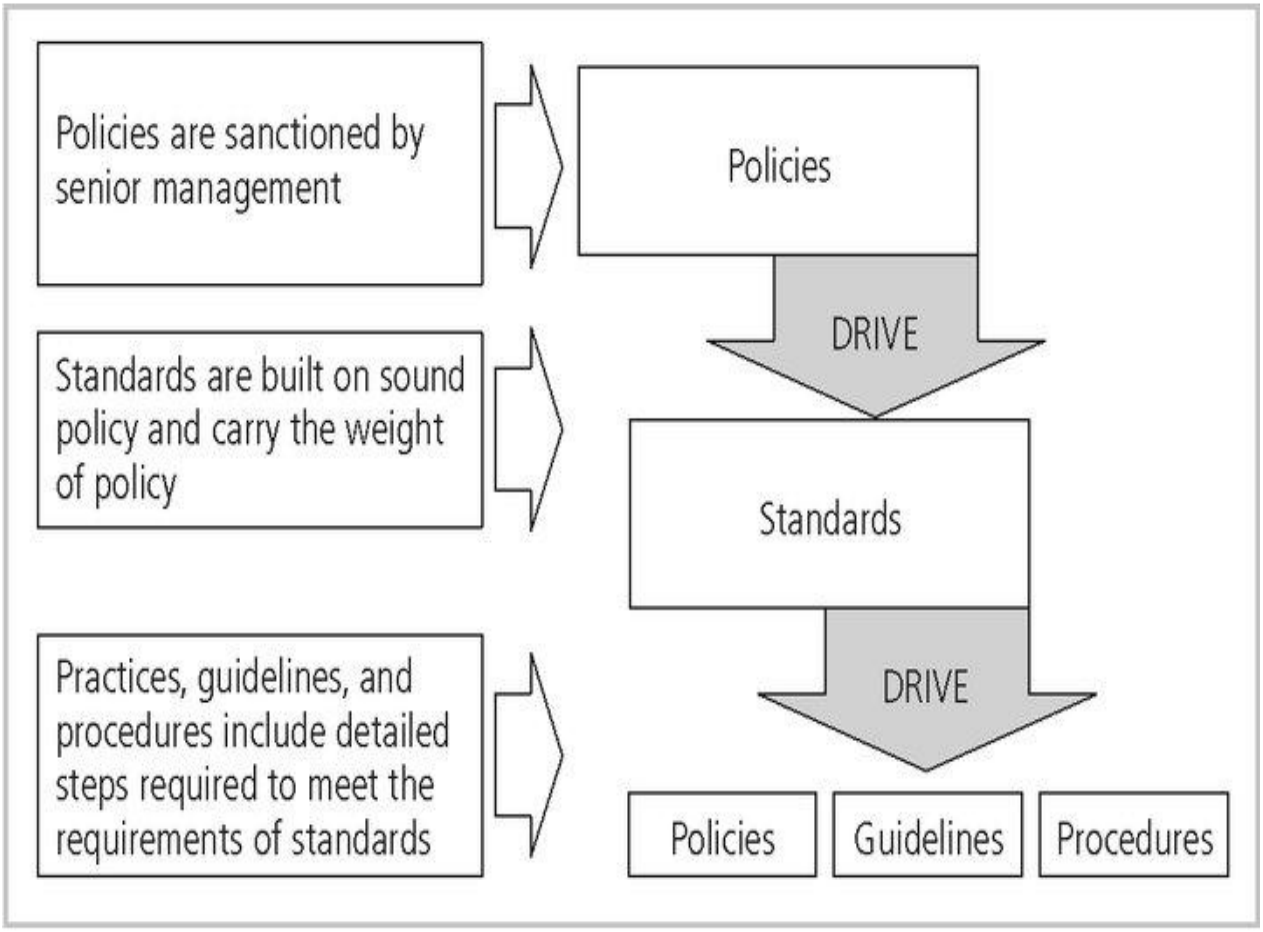

FIGURE 6-1 Policies, Standards, and Practices

— Policies are written to support the mission, vision and strategic planning of an organization.

— The MISSION of an organization is a written statement of an organization‘s purpose.

— The VISION of an organization is a written statement about the organization‘s goals-where will the organization be in five years? In ten?

— Strategic planning is the process of moving the organization towards its vision.

— A policy must be disseminated by all means possible, including printed personal manuals, organization intranets, and periodic supplements.

- All members of the organization must read, understand, and agree to the policies.
- Policies should be considered as the living documents.
- Government agencies discuss policy in terms of national security and national policies to deal with foreign states.
- A security policy can also represent a credit card agency‘s policy for processing credit card numbers.
- In general, a security policy is a set of rules that protect an organization‘s assets.
- An information security policy provides rules for the protection of the information assets of the organization.
- The task of information security professionals is to protect the confidentiality, integrity and availability of information and information systems whether in the state of transmission, storage, or processing.
- This is accomplished by applying policy, education and training programs, and technology.

Source : http://elearningatria.files.wordpress.com/2013/10/ise-viii-information-and-network-security-06is835-notes.pdf