Security Policy and Standards

Part I

- 1. Introduction
- 2. Policy
- 3. Why Policy should be developed.
- 4. www policies

Introduction

- Focuses on information security policy:
  - What it is
  - How to write it
  - How to implement it
  - How to maintain it

Policy

- Policy is an essential foundation of effective infosec program
- The success of an information resources protection program depends on the policy generated, & on the attitude of management toward securing information on automated systems.

- You, the policy maker, set the tone & the emphasis on how important a role infosec will have within your agency.

- Your primary responsibility is to set the information resource security policy for the organization with the objectives of reduced risk, compliance with laws & regulations, & assurance of operational continuity, information integrity, & confidentiality."

- A quality infosec program begins & ends with policy
- Policies are least expensive means of control & often the most difficult to implement
- Basic rules to follow when shaping policy:
  - Never conflict with law
  - Stand up in court
  - Properly supported and administered
  - Contribute to the success of the organization
  - Involve end users of information systems

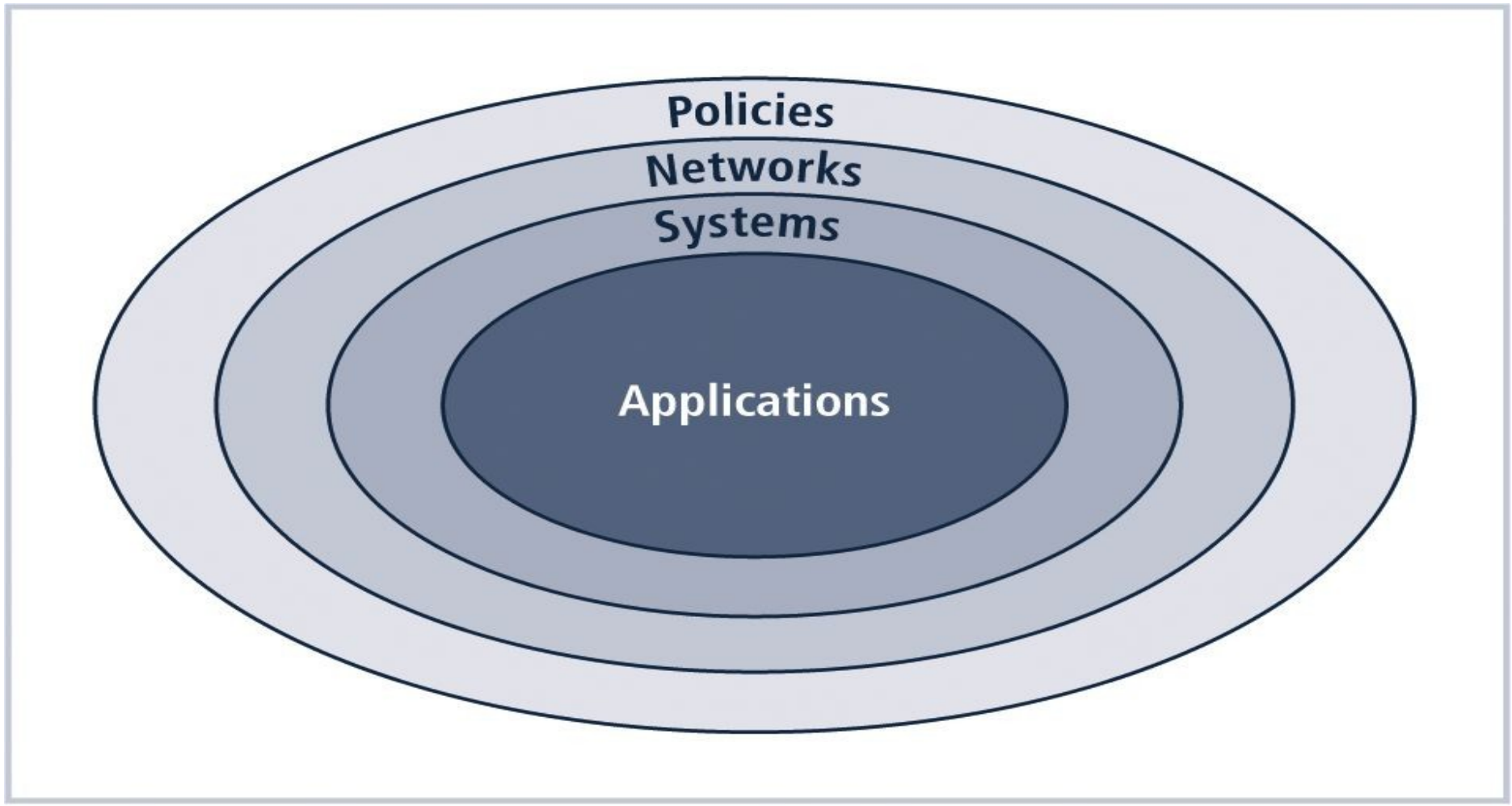

FIGURE 4-1 The Bull's-Eye Model

Bulls-eye model layers

1. Policies: first layer of defense
2. Networks: threats first meet organization's network
3. Systems: computers & manufacturing systems
4. Applications: all applications systems

- Policies are important reference documents for internal audits & for resolution of legal disputes about management's due diligence
- Policy documents can act as a clear statement of management's intent

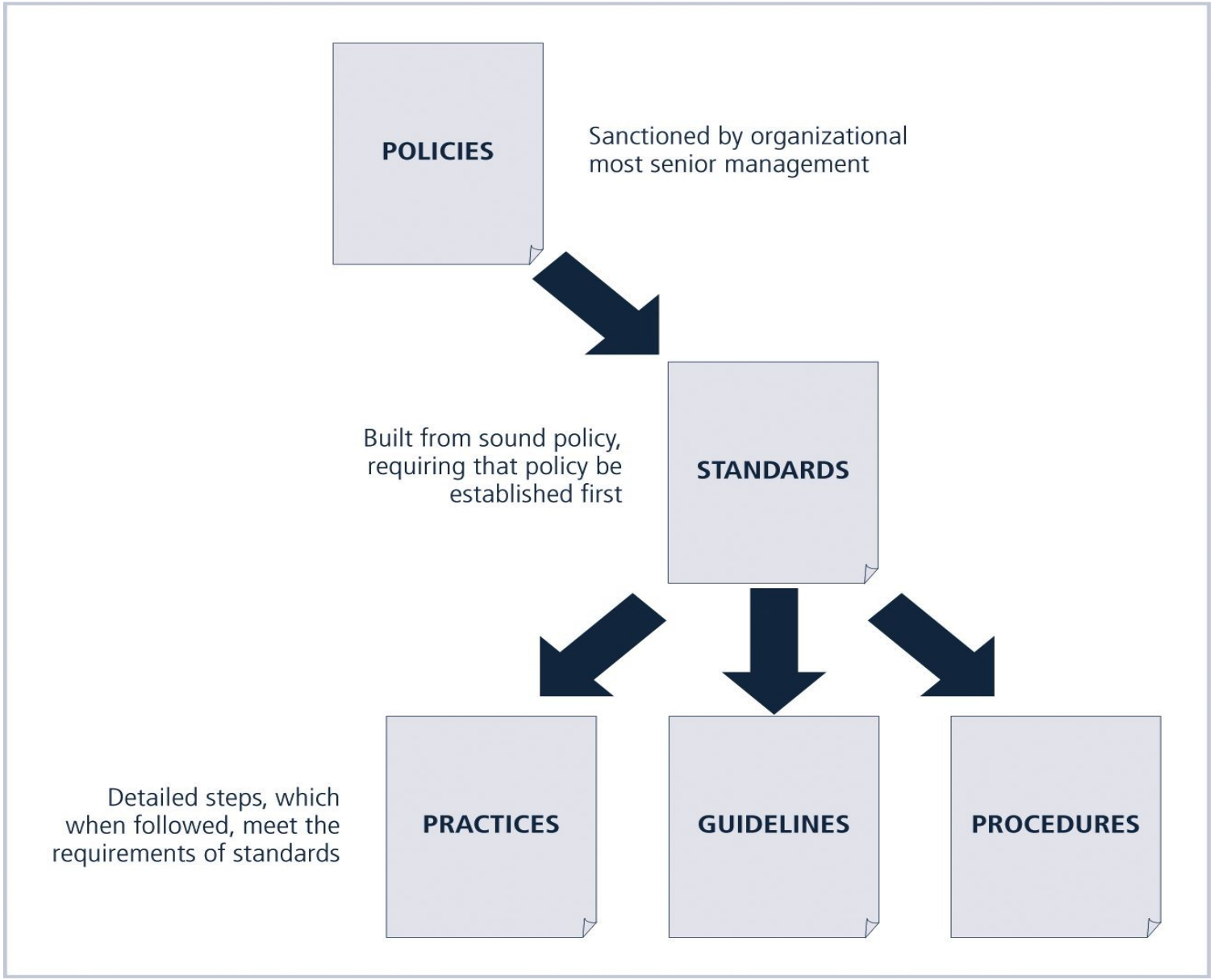

FIGURE 4-2 Policies, Standards, and Practices

- Policy: plan or course of action that influences & determines decisions
- Standards: more detailed statement of what must be done to comply with policy
- Practices, procedures & guidelines:explain how employees will comply with policy

- For policies to be effective, they must be:
  - Properly disseminated
  - Read
  - Understood
  - Agreed-to

- Policies require constant modification & maintenance
- In order to produce a complete infosec policy, management must define 3 types of infosec policy:
  - Enterprise infosec program policy
  - Issue-specific infosec policies
  - Systems-specific infosec policies

Part I

- 1. Introduction
- 2. Policy
- 3. **Why Policy should be developed.**
- 4. www policies

Why Policy should be developed

- Identifies assets the company considers valuable.
- Provides to the security team and its activities.
- Provides a reference to review when conflicts pertaining to security arise.
- States the company's goal and objectives pertaining to security
- Outlines personal responsibility.
- Helps to prevent unaccounted –for events(surprises)
- .

Why Policy should be developed

- Defines the scope and functions of the security team
- Outlines incident response responsibilties
- Outline the company's response to legal,regulatory and standards of due care.

Note: Standards refer to mandatory activities, actions or rules.Standards can give support to policy and reinforcement in direction.

- Introduction
- 2. Policy
- 3. Why Policy should be developed.
- 4. **www policies**

www.Policies

- Web based malware and attacks are proliferating rapidly on the Internet. There are new web security indicators ,techniques and policy communication mechanism sprinkled throughout the various layers of the web and HTTP.
- Some of the points to be consider

a) SSL : Use Public key encryption.server authentication ,use HTTPS protocol.

b) Session : use session instead of Cookies as it stores in browsers and easy for attackers to reveal your passwords.