IS Policies and Procedures

Harshul Joshi, CISA, CISM, CISSP

hjoshi@cbiz.com

Agenda

- Overview
- Policies vs. Procedures vs. Standards
- Creating Policies
- Mapping Policies with Procedures
- Managing and Communicating
- Complying with Compliances
- Mistakes

Overview

- Policy –
  - Big picture statement
  - The formal guidance needed to coordinate and execute activity throughout the institution. When effectively deployed, policy statements help focus attention and resources on high priority issues - aligning and merging efforts to achieve the institutional vision.

Overview

- Policies are high-level strategic governance with executive sponsorship.
- Policies should be short and to the point, since those who sign off on them don't need to know the technical details. An example might be: "We will monitor all database activity based on the sensitivity of the data, as well as relevant legal and contractual requirements." Keep in mind that since policies should be signed off on by senior management, you want to keep them generic enough that you don't have to go back to the CEO/CIO/CFO/COO every time you want to change a firewall configuration or AV product.

Overview

- The next layer down is high-level tactical documentations – plans and standards.
- The security plan is how you intend to satisfy the policy, but it's still not at the level of specific steps. Keeping with our policy above, the plan would specify the contractual requirements, basic data classification, which activity will be monitored, and so on.
- While plans define how *security* will do things, standards define how *everyone else* has to do things.

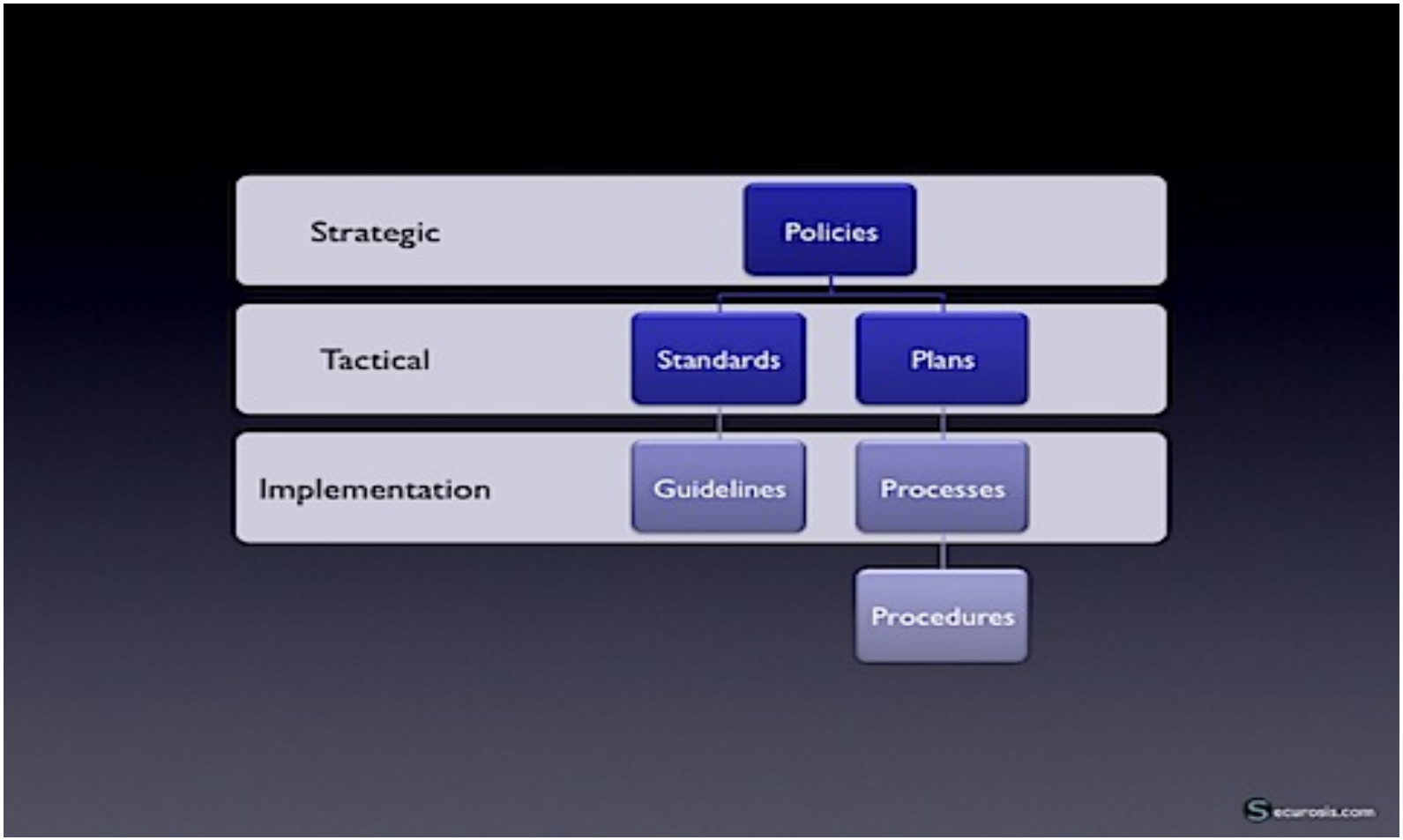
Overview

- Procedures
  - The operational processes required to implement institutional policy. Operating practices can be formal or informal, specific to a department or applicable across the entire institution. If a policy is "what" the institution does operationally, then it’s procedures are "how" it intends to carry out those operating policy expressions.

Overview

- Below that are specific implementation documentations – processes, guidelines, and procedures.
- Here's where we get into the nitty-gritty of actual implementation and step by step guides.
- A process is a repeatable series of steps to achieve an objective, while procedures are the specific things you do at each of those steps.
- Keeping with our example above, the process would define how monitoring occurs (*e.g.,* third party DAM tool), and the procedure is which bits to flip within the tool.

In a nutshell



http://securosis.com/2008/10/07/policies-vs-plans-vs-procedures-vs-standards/

Creating one

- Top down vs. Bottom up
  - Depends on the current environment
  - Starting from scratch vs. reinventing the wheel
  - Management buy-in
  - Maps with business goals and objectives

Key ingredients – Security Policy

- Who
- What
- When
- Where
- Why
  - IT Security policy writers craft effective policies by asking themselves five questions: *who*, *what*, *where*, *when*, and *why*. These questions provide a consistent framework for all technical writing. They especially apply to policy writing. By excluding this specific information, policy writers diminish the readability, effectiveness, and usefulness of their work.

Business Writing

- *The technology resources that make up the enterprise's IT assets constitute a sizable monetary investment that must be protected.*

- *The enterprise IT resources constitute a sizable monetary investment that must be protected.*

Business Writing

- Active vs. Passive
  - The purpose of this policy is to establish …
  - The policy establishes ……..

Policies and Procedures

- Real Life – Procedures may already exist in an informal fashion
- Try and leverage existing procedures to create policies
- Same goes for informal standards
  - Operating system configuration
  - Perimeter devices

Key IS Policies

- Security
- Change Management
- Development
- Operations

Security

- Acceptable Use
- Access Control
- Segregation of duties
- Logging and Monitoring
- Servers
- Perimeter
- Remote Access

Managing and Communicating

- Process of internal communication
- Hard policies vs. Soft policies
- Use of various medium
  - Intranet
  - Lunch sessions
  - Department meetings
  - Memo

Policies – Just for compliance ☺

- SOX
- GLBA
- HIPAA
- PCI
- Red Flag Rules

Let's take an example

- Policies required for Compliance mandates - PCI / GLBA / SOX
  - Information Security Policy
  - Daily Operational Security Procedures
  - Usage policy
  - Vendor management policy
  - Incident Response Plan
  - Security Awareness Program
  - Privacy
  - Data Classification
  - Data Retention
  - Disaster Recovery

Mistakes

- Creating a policy just for show
- No procedures in place to comply with the policy
- Different policies for different locations / business function etc.
- Exceptions without justification

What to Audit

- Fit with overall business and IT goals
- Procedures and Controls in place to support the policies
- Centralized as far as possible

Questions

Harshul Joshi, CISA, CISM, CISSP

Director, IT Services

CBIZ MHM, LLC

hjoshi@cbiz.com

408-794-3597