5. Security Management Models And Practices

Introduction

- To create or maintain a secure environment
  1. Design working security plan
  2. Implement management model to execute and maintain the plan
  - May have steps:
    - begin with creation or validation of **security framework**,
    - followed by an information security blueprint describing existing controls and identifying other necessary security controls

Introduction (Continued)

- Framework:
  - outline of the more thorough blueprint,
  - Blueprint
    - basis for the design, selection, and implementation of all subsequent security controls
- Most organizations draw from established **security models** and practices to develop a blueprint or methodology

Security Management Models

- **A security model** is a generic blueprint offered by a service organization.
- One way to create the blueprint is to look at what other organizations have done (benchmarking).
- One way to select a methodology is to adapt or adopt an existing **security management model** or **set of practices**.

BS 7799

- One of the most widely referenced and often discussed security models
  - Information Technology – Code of Practice for Information Security Management,
  - originally published as British Standard BS 7799
- The purpose of ISO/IEC 17799
  - give recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organization

BS 7799 (Continued)

- Intended to provide
  - a common basis for developing organizational security standards,
  - effective security management practice, and
  - confidence in inter-organizational dealings

- Volume 2
  - provides information on how to implement Volume 1 (17799) and
  - how to set up an Information Security Management Structure (ISMS)

The Ten Sections Of ISO/IEC 17799

1. Organizational Security Policy
2. Organizational Security Infrastructure objectives
3. Asset Classification and Control
4. Personnel Security objectives
5. Physical and Environmental Security objectives
6. Communications and Operations Management objectives
7. System Access Control objectives
8. System Development and Maintenance objectives
9. Business Continuity Planning
10. Compliance objectives

Plan-Do-Check-Act of BS7799:2

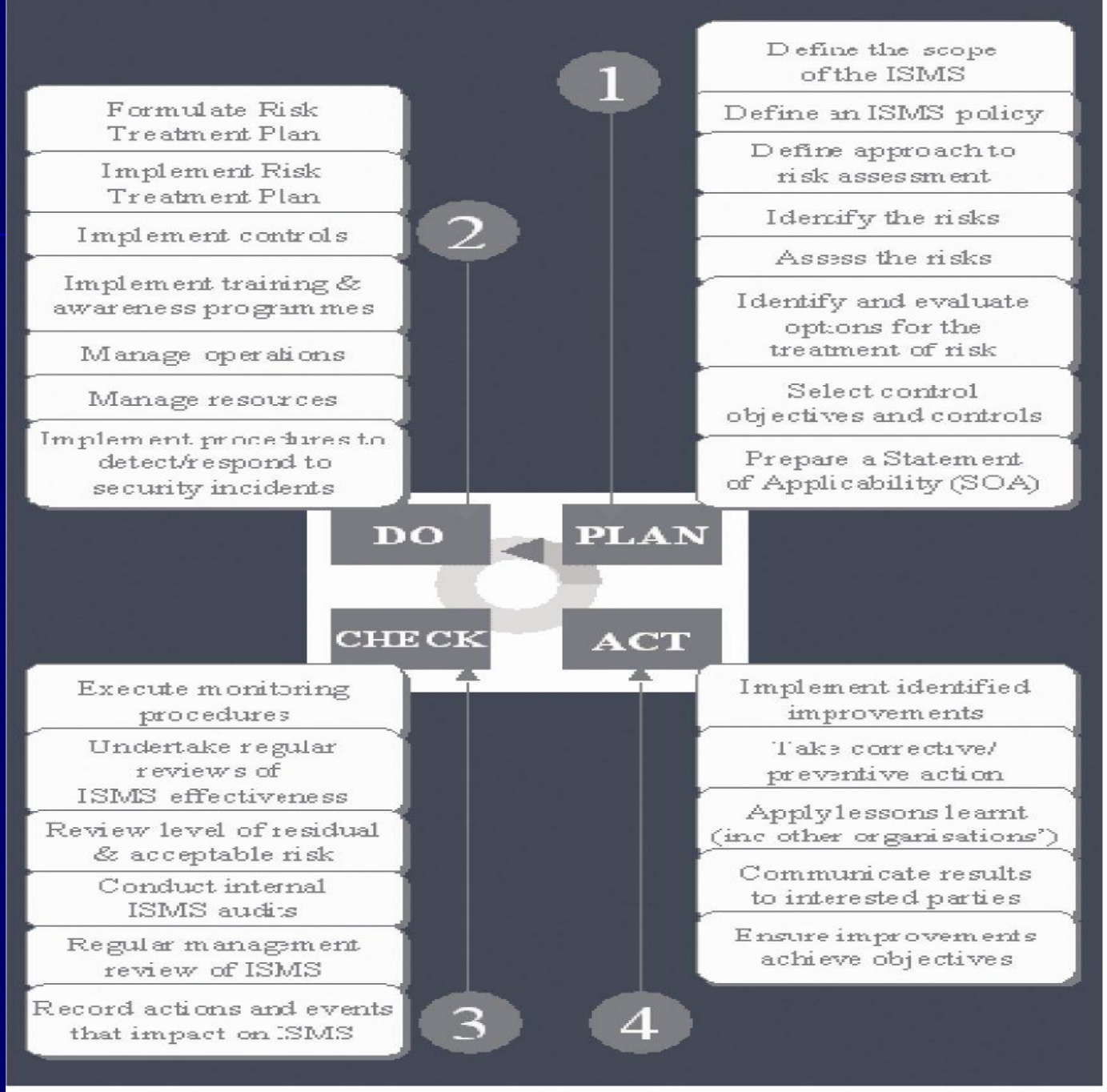

FIGURE 6-2 Plan-Do-Check-Act Cycle from BS 7799:2

NIST Security Models

- NIST documents have two notable advantages:
  - Publicly available at no charge
  - Have been broadly reviewed by government and industry professionals
    - SP 800-12, Computer Security Handbook
    - SP 800-14, Generally Accepted Security Principles & Practices
    - SP 800-18, Guide for Developing Security Plans
    - SP 800-26, Security Self-Assessment Guide-IT Systems
    - SP 800-30, Risk Management for Information Technology Systems

Security Management Practices

- In information security, two categories of benchmarks are used
  - Standards of due care/due diligence
  - Best practices
- Best practices include a sub-category of practices—
  1. called the gold standard
  2. that are generally regarded as "the best of the best"

Standards of Due Care/ Diligence

- When organizations adopt minimum levels of security for a legal defense, they may need to show that they have done what any prudent organization would do in similar circumstances
  - Known as a standard of **due care**
- Implementing controls at this minimum standard, and maintaining them, demonstrates that an organization has performed due diligence

Best Security Practices

- Security efforts that seek to provide a superior level of performance in the protection of information are referred to as
  - Best business practices or simply best practices
  - Some organizations call them recommended practices

- Security efforts that are among the best in the industry are referred to as **best security practices**

Best Security Practices (Continued)

- These practices balance the need for information access with the need for adequate protection
  - Best practices seek to provide as much security as possible for information and information systems while demonstrating fiscal responsibility and ensuring information access
- Companies with best practices may not be the best in every area
  - They may only have established an extremely high quality or successful security effort in one area

Selecting Best Practices

- Choosing which recommended practices to implement can pose a challenge for some organizations
  - In industries that are regulated by governmental agencies, government guidelines are often requirements
  - For other organizations, government guidelines are excellent sources of information and can inform their selection of best practices

Selecting Best Practices (Continued)

- When considering best practices for your organization, consider the following:
  - Does your organization resemble the identified target organization of the best practice?
  - Are you in a similar industry as the target?
  - Do you face similar challenges as the target?
  - Is your organizational structure similar to the target?
  - Are the resources you can expend similar to those called for by the best practice?
  - Are you in a similar threat environment as the one assumed by the best practice?

Best Practices

- Microsoft has published a set of best practices in security at its Web site:
  - Use antivirus software
  - Use strong passwords
  - Verify your software security settings
  - Update product security
  - Build personal firewalls
  - Back up early and often
  - Protect against power surges and loss