# COMPUTER SECURITY

## PRINCIPLES AND PRACTICE

SECOND EDITION

William Stallings | Lawrie Brown

# Chapter 15

## IT Security Controls, Plans, and Procedures

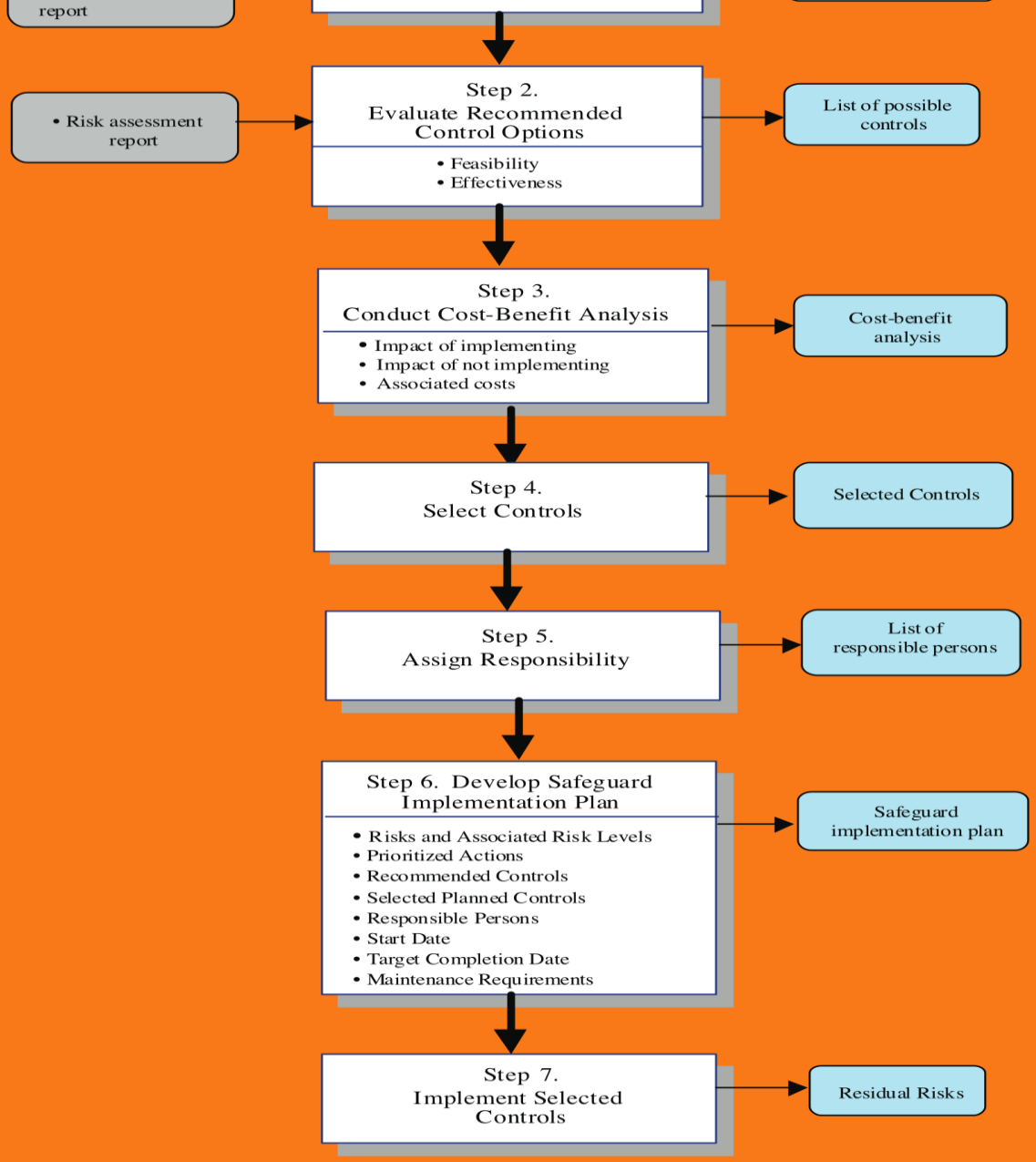



**Figure 15.1 IT Security Management Controls and Implementation**

# Security Control

Control is defined as:

"a means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of administrative, technical, management, or legal nature"

# Control Classes

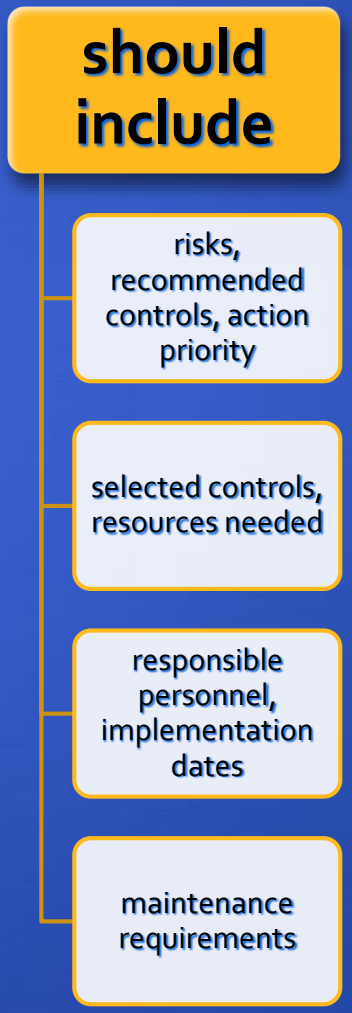
| management controls | operational controls | technical controls |
| --- | --- | --- |
| • refer to issues that management needs to address<br>• focuses on reducing the risk of loss and protecting the organization's mission | • address correct implementation and use of security policies<br>• relate to mechanisms and procedures that are primarily implemented by people rather than systems | • involve the correct use of hardware and software security capabilities in systems |

# Cost-Benefit Analysis

- should be conducted by management to identify controls that provide the greatest benefit to the organization given the available resources
- may be qualitative or quantitative
- must show cost justified by reduction in risk
- should contrast the impact of implementing a control or not, and an estimation of cost
- management chooses selection of controls
- considers if it reduces risk too much or not enough, is too costly or appropriate
- fundamentally a business decision

# IT Security Plan

- provides details of:
  - what will be done
  - what resources are needed
  - who is responsible
- goal is to detail the actions needed to improve the identified deficiencies in the risk profile



# Security Plan Implementation

**IT security plan documents:**

- what needs to be done for each selected control
- personnel responsible
- resources and time frame

**identified personnel:**

- implement new or enhanced controls
- may need system configuration changes, upgrades or new system installation
- may also involve development of new or extended procedures
- need to be encouraged and monitored by management

**when implementation is completed management authorizes the system for operational use**

# Security Training and Awareness

- responsible personnel need training
  - on details of design and implementation
  - awareness of operational procedures
- also need general awareness for all
  - spanning all levels in organization
  - essential to meet security objectives
  - lack leads to poor practices reducing security
  - aim to convince personnel that risks exist and breaches may have significant consequences

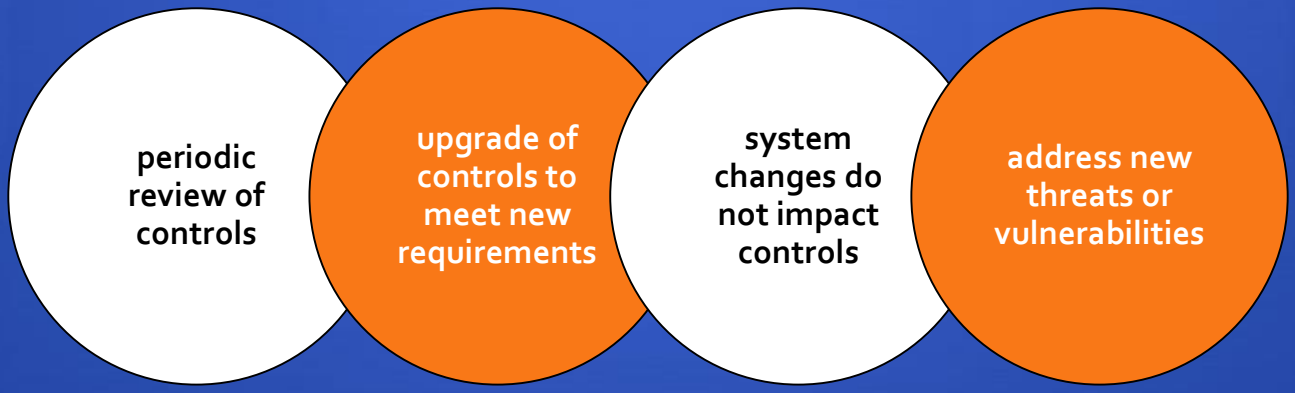
# Implementation Follow-Up

- security management is a cyclic process
  - constantly repeated to respond to changes in the IT systems and the risk environment
- need to monitor implemented controls
- evaluate changes for security implications
  - otherwise increase chance of security breach

| includes a number of aspects |
| --- |
| • maintenance of security controls<br>• security compliance checking<br>• change and configuration management<br>• incident handling |

# Maintenance

- need continued maintenance and monitoring of implemented controls to ensure continued correct functioning and appropriateness
- goal is to ensure controls perform as intended




Tasks

# Security Compliance

- audit process to review security processes
- goal is to verify compliance with security plan
- use internal or external personnel
- usually based on use of checklists which verify:
  - suitable policies and plans were created
  - suitable selection of controls were chosen
  - that they are maintained and used correctly
- often as part of wider general audit

# Change and Configuration Management

change management is the process to review proposed changes to systems

configuration management is specifically concerned with keeping track of the configuration of each system in use and the changes made to them

# Case Study: Silver Star Mines

- given risk assessment, the next stage is to identify possible controls
- based on assessment it is clear many categories are not in use
- general issue of systems not being patched or upgraded
- need contingency plans
- SCADA: add intrusion detection system
- info integrity: better centralize storage
- email: provide backup system

# Silver Star Mines: Implementation Plan

| Risk (Asset/Threat) | Level of Risk | Recommended Controls | Priority | Selected Controls |
|---|---|---|---|---|
| All risks (generally applicable) | | 1. Configuration and periodic maintenance policy for servers<br>2. Malicious code (SPAM, spyware) prevention<br>3. Audit monitoring, analysis, reduction, and reporting on servers<br>4. Contingency planning and incident response policies and procedures<br>5. System backup and recovery procedures | 1 | 1.<br>2.<br>3.<br>4.<br>5. |
| Reliability and integrity of SCADA nodes and network | High | 1. Intrusion detection and response system | 2 | 1. |
| Integrity of stored file and database information | Extreme | 1. Audit of critical documents<br>2. Document creation and storage policy<br>3. User security education and training | 3 | 1.<br>2.<br>3. |
| Availability and integrity of Financial, Procurement, and Maintenance/ Production Systems | High | - | - | (general controls) |
| Availability, integrity and confidentiality of e-mail | High | 1. Contingency planning – backup e-mail service | 4 | 1. |