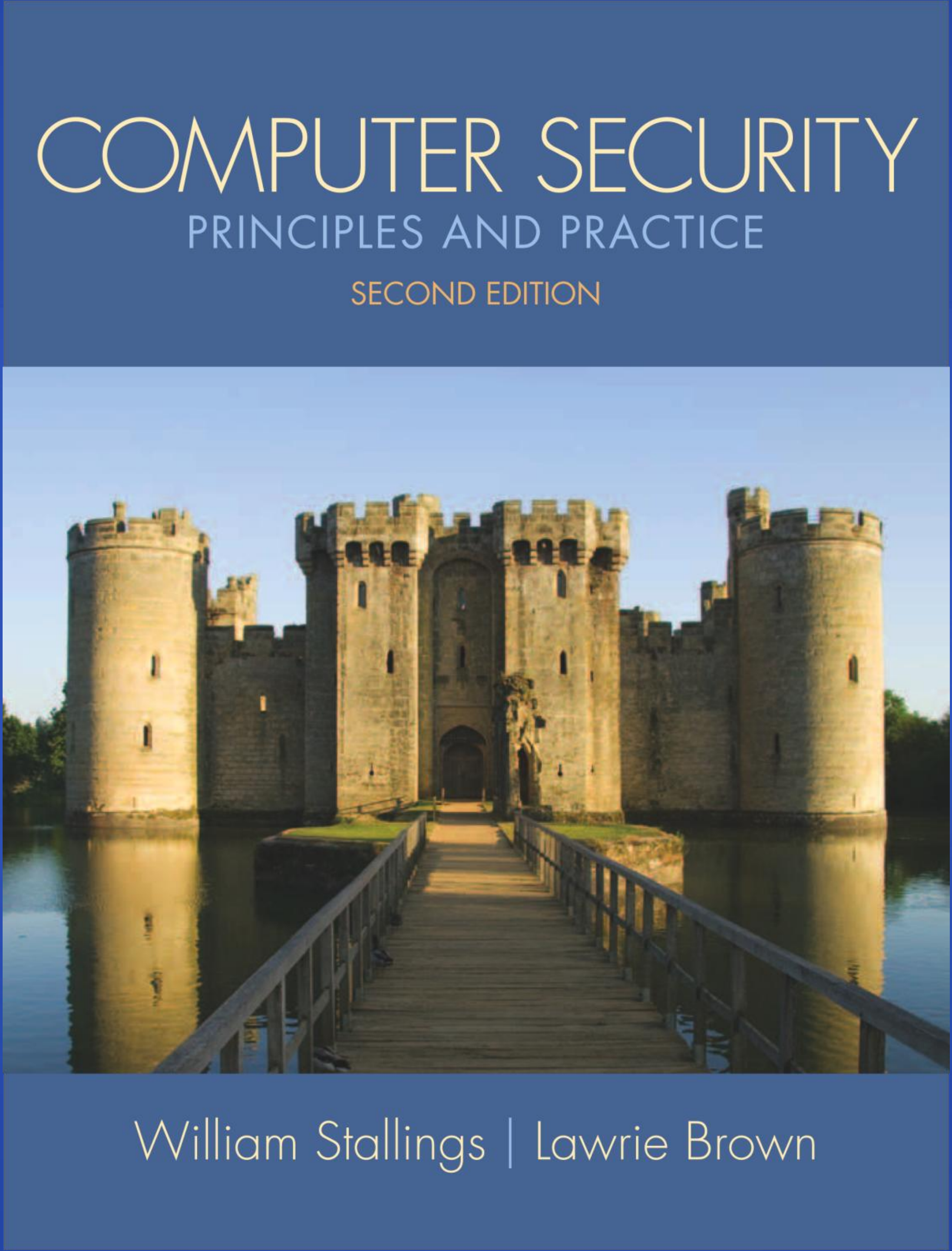


COMPUTER SECURITY

PRINCIPLES AND PRACTICE

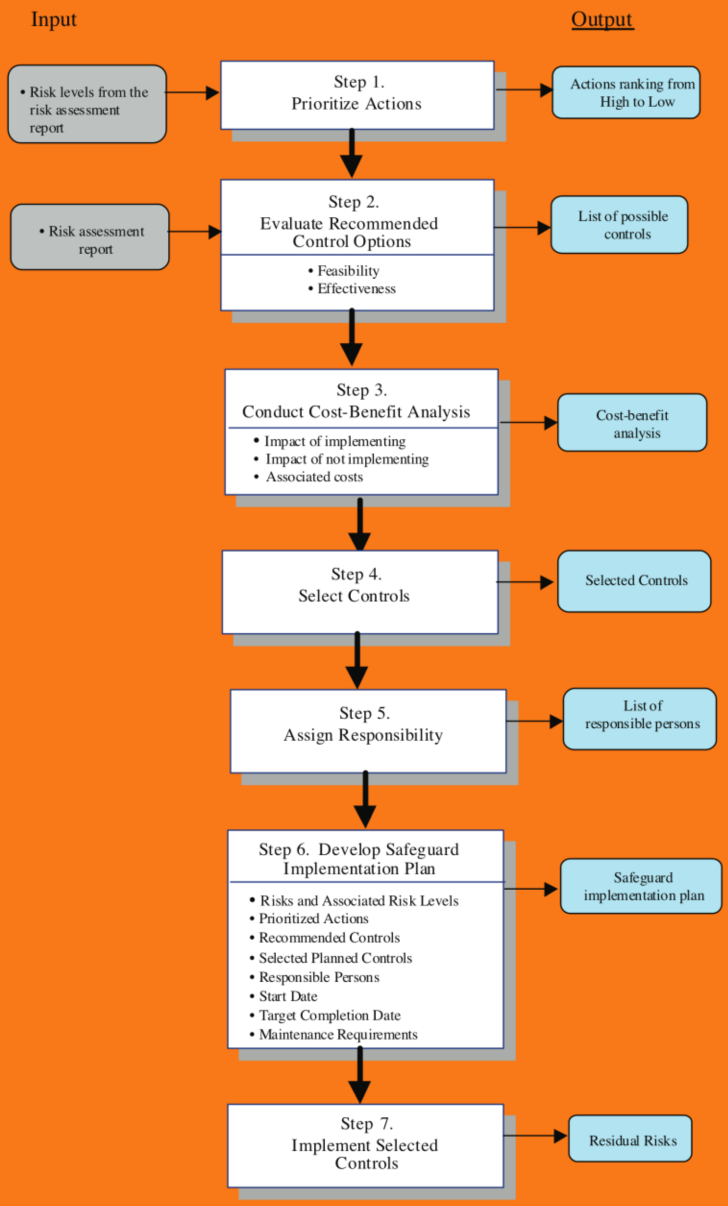
SECOND EDITION

William Stallings | Lawrie Brown

Chapter 15

IT Security Controls, Plans, and Procedures

Implementing IT Security Management



Input

Output

- Risk levels from the risk assessment report

Step 1.
Prioritize Actions

Actions ranking from High to Low

- Risk assessment report

Step 2.
Evaluate Recommended Control Options

- Feasibility
- Effectiveness

List of possible controls

Step 3.
Conduct Cost-Benefit Analysis

- Impact of implementing
- Impact of not implementing
- Associated costs

Cost-benefit analysis

Step 4.
Select Controls

Selected Controls

Step 5.
Assign Responsibility

List of responsible persons

Step 6. Develop Safeguard Implementation Plan

- Risks and Associated Risk Levels
- Prioritized Actions
- Recommended Controls
- Selected Planned Controls
- Responsible Persons
- Start Date
- Target Completion Date
- Maintenance Requirements

Safeguard implementation plan

Step 7.
Implement Selected Controls

Residual Risks

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

- refer to issues that management needs to address
- focuses on reducing the risk of loss and protecting the organization's mission

operational controls

- address correct implementation and use of security policies
- relate to mechanisms and procedures that are primarily implemented by people rather than systems

technical controls

- involve the correct use of hardware and software security capabilities in systems

Technical Controls

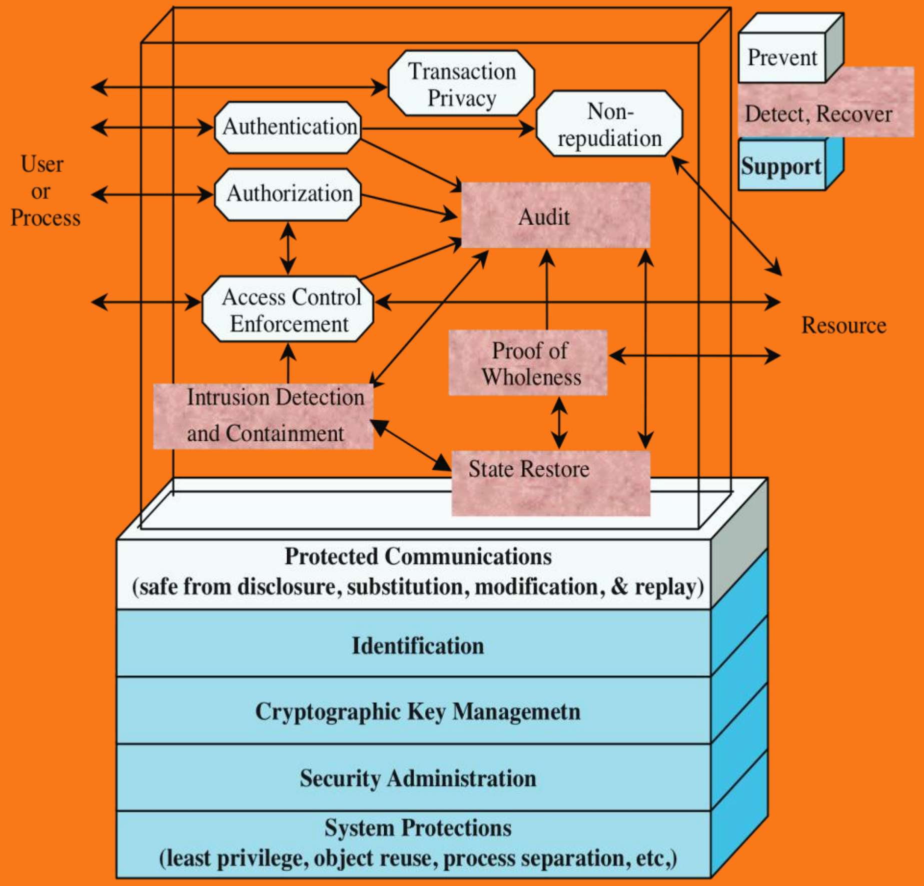
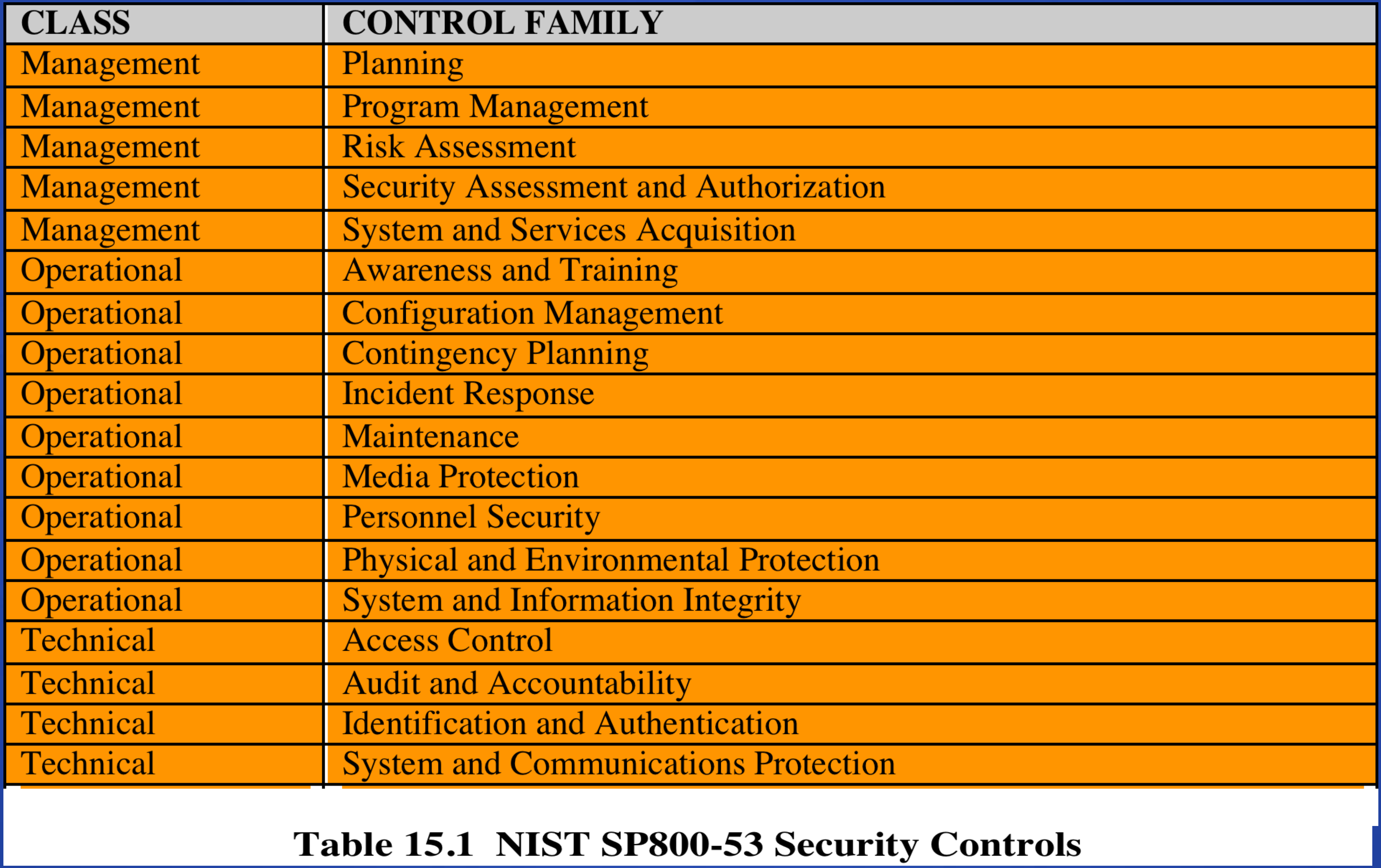
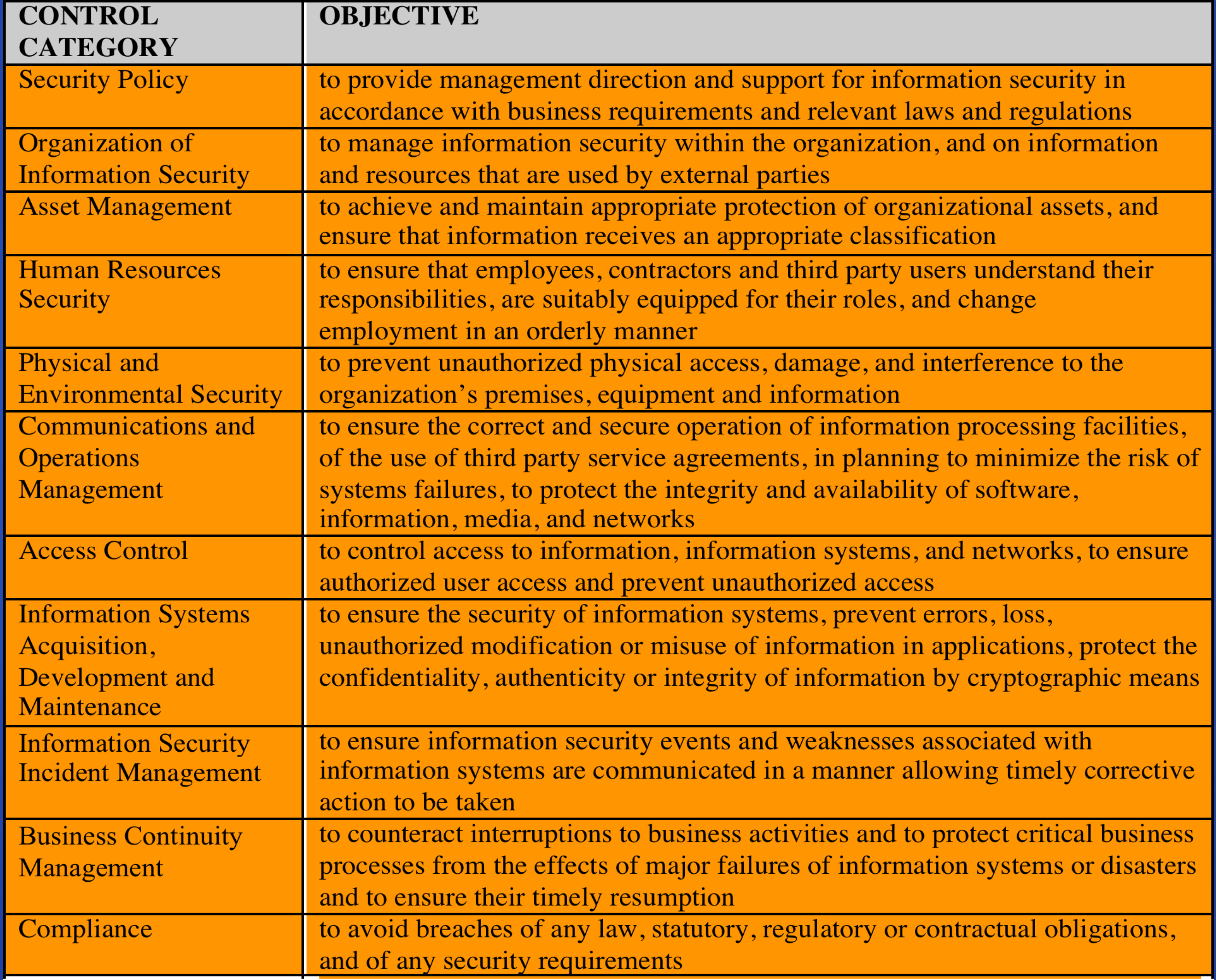


Figure 15.2 Technical Security Controls



CLASS	CONTROL FAMILY
Management	Planning
Management	Program Management
Management	Risk Assessment
Management	Security Assessment and Authorization
Management	System and Services Acquisition
Operational	Awareness and Training
Operational	Configuration Management
Operational	Contingency Planning
Operational	Incident Response
Operational	Maintenance
Operational	Media Protection
Operational	Personnel Security
Operational	Physical and Environmental Protection
Operational	System and Information Integrity
Technical	Access Control
Technical	Audit and Accountability
Technical	Identification and Authentication
Technical	System and Communications Protection

Table 15.1 NIST SP800-53 Security Controls



CONTROL CATEGORY	OBJECTIVE
Security Policy	to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations
Organization of Information Security	to manage information security within the organization, and on information and resources that are used by external parties
Asset Management	to achieve and maintain appropriate protection of organizational assets, and ensure that information receives an appropriate classification
Human Resources Security	to ensure that employees, contractors and third party users understand their responsibilities, are suitably equipped for their roles, and change employment in an orderly manner
Physical and Environmental Security	to prevent unauthorized physical access, damage, and interference to the organization's premises, equipment and information
Communications and Operations Management	to ensure the correct and secure operation of information processing facilities, of the use of third party service agreements, in planning to minimize the risk of systems failures, to protect the integrity and availability of software, information, media, and networks
Access Control	to control access to information, information systems, and networks, to ensure authorized user access and prevent unauthorized access
Information Systems Acquisition, Development and Maintenance	to ensure the security of information systems, prevent errors, loss, unauthorized modification or misuse of information in applications, protect the confidentiality, authenticity or integrity of information by cryptographic means
Information Security Incident Management	to ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken
Business Continuity Management	to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption
Compliance	to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements

Table 15.2 ISO/IEC 27002 Security Controls

Residual Risk

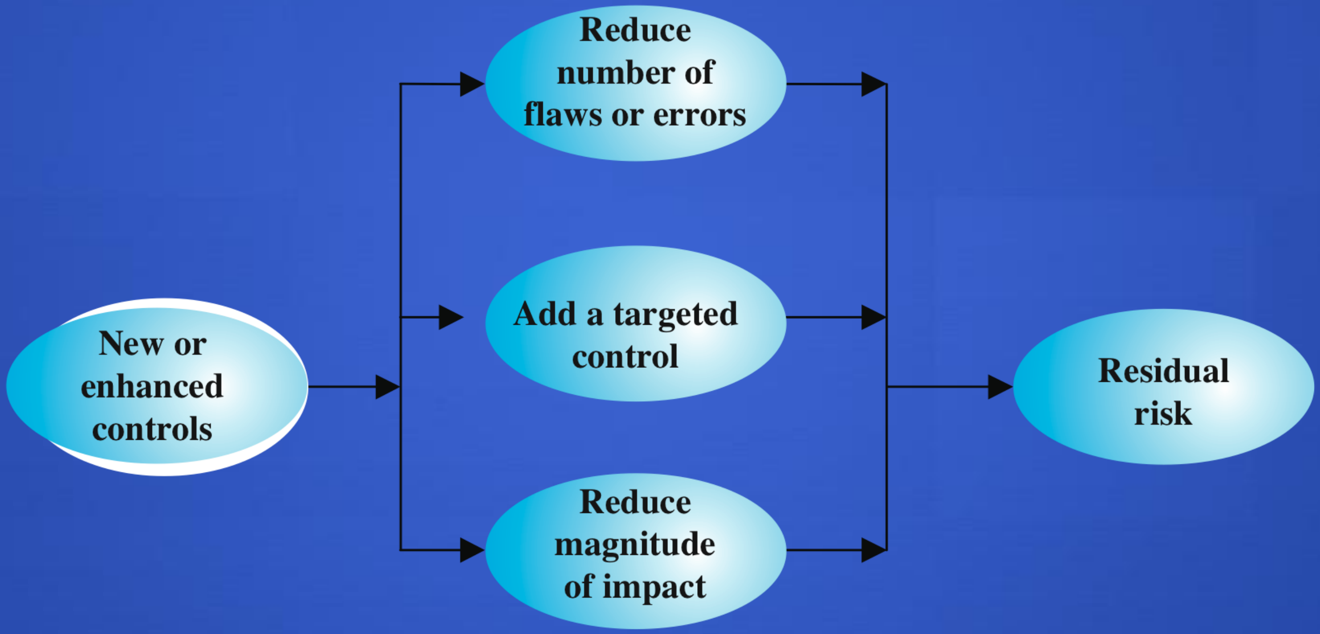


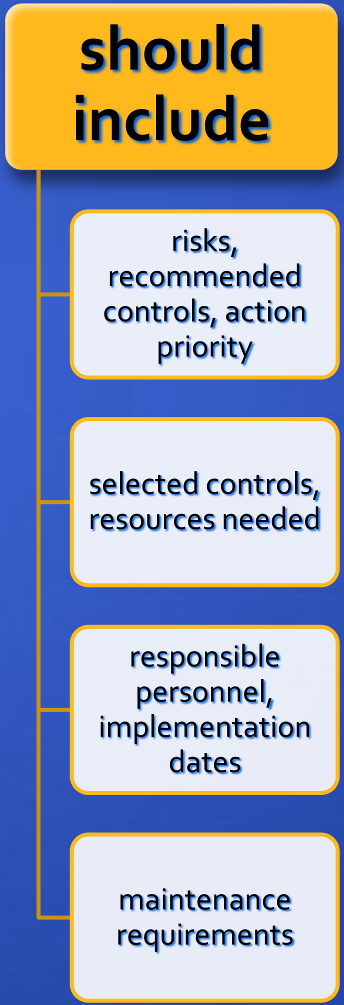
Figure 15.3 Residual Risk

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

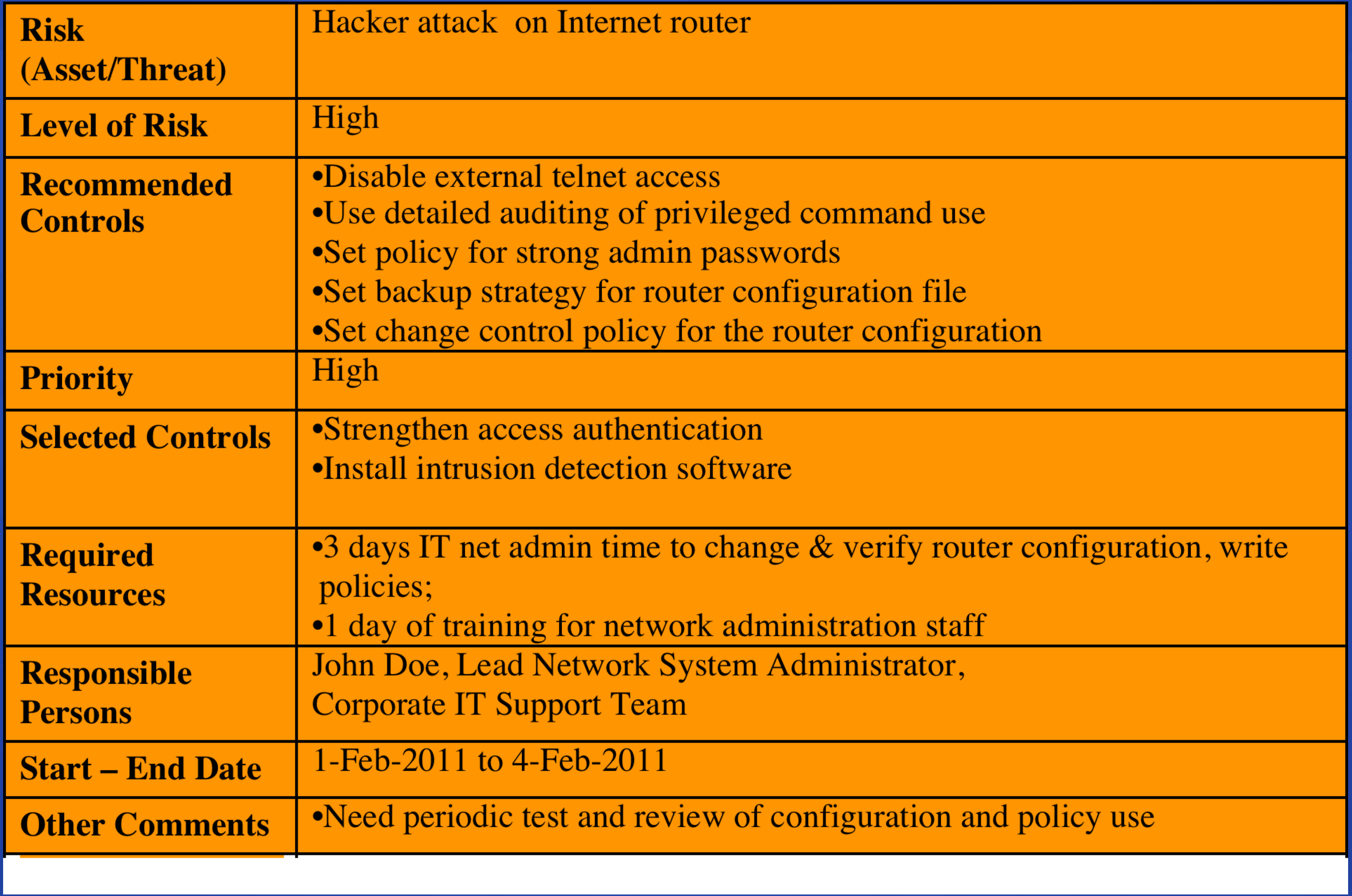
- provides details of:
  - what will be done
  - what resources are needed
  - who is responsible
- goal is to detail the actions needed to improve the identified deficiencies in the risk profile



should include

- risks, recommended controls, action priority
- selected controls, resources needed
- responsible personnel, implementation dates
- maintenance requirements

Implementation Plan



Risk (Asset/Threat)	Hacker attack on Internet router
Level of Risk	High
Recommended Controls	•Disable external telnet access •Use detailed auditing of privileged command use •Set policy for strong admin passwords •Set backup strategy for router configuration file •Set change control policy for the router configuration
Priority	High
Selected Controls	•Strengthen access authentication •Install intrusion detection software
Required Resources	•3 days IT net admin time to change & verify router configuration, write policies; •1 day of training for network administration staff
Responsible Persons	John Doe, Lead Network System Administrator, Corporate IT Support Team
Start – End Date	1-Feb-2011 to 4-Feb-2011
Other Comments	•Need periodic test and review of configuration and policy use

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

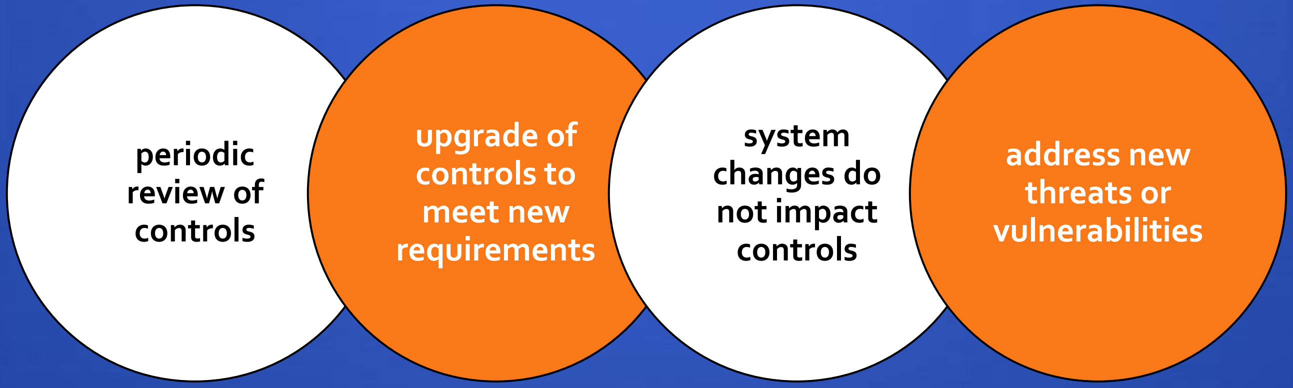
- security management is a cyclic process
  - constantly repeated to respond to changes in the IT systems and the risk environment
- need to monitor implemented controls
- evaluate changes for security implications
  - otherwise increase chance of security breach

includes a number of aspects

- maintenance of security controls
- security compliance checking
- change and configuration management
- 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



periodic review of controls

upgrade of controls to meet new requirements

system changes do not impact controls

address new threats or vulnerabilities

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

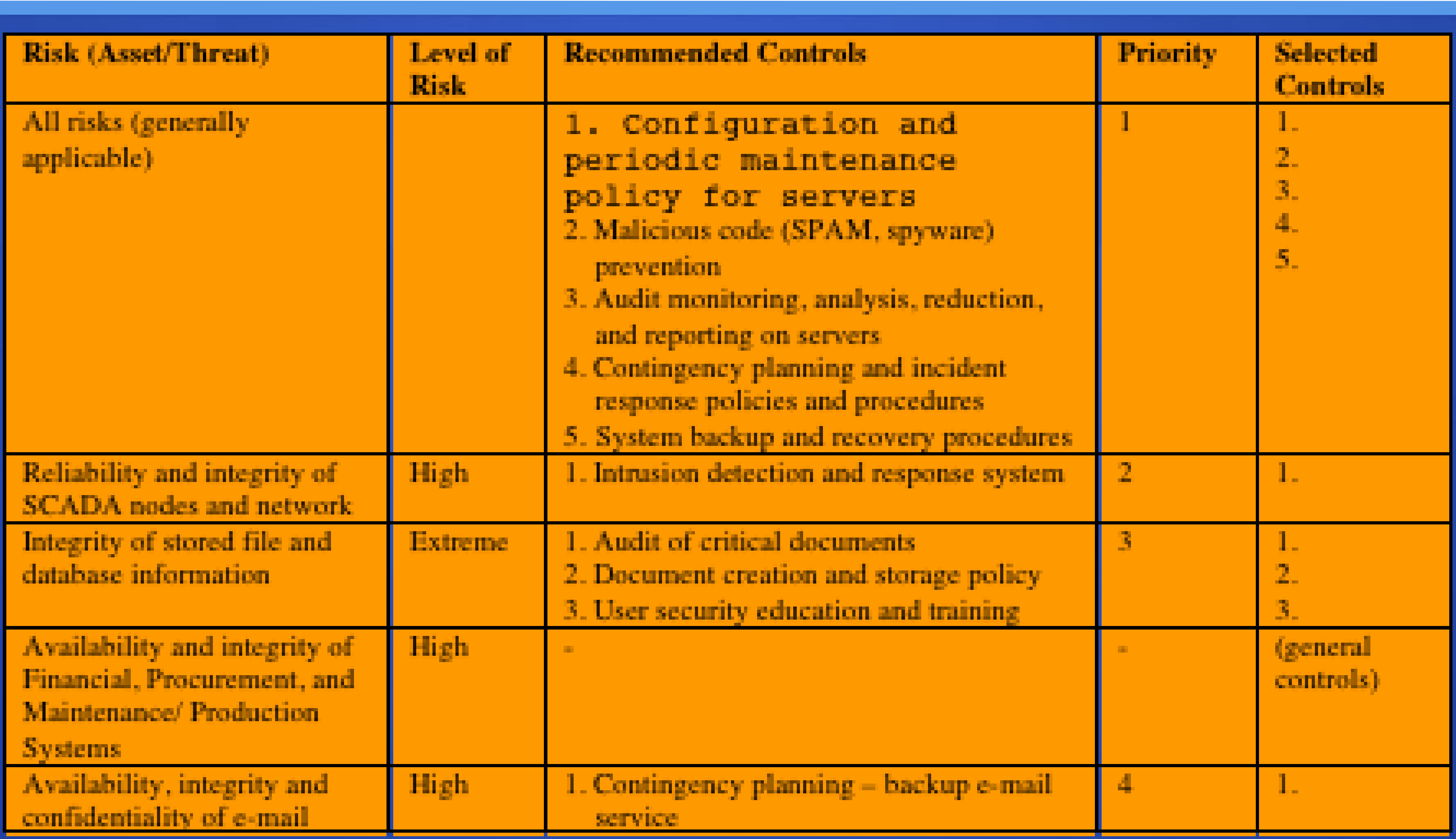
- may be informal or formal
- test patches to make sure they do not adversely affect other applications
- important component of general systems administration process
- evaluate the impact

- also part of general systems administration process
- know what patches or upgrades might be relevant
- keep lists of hardware and software versions installed on each system to help restore them following a failure

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 2. Malicious code (SPAM, spyware) prevention 3. Audit monitoring, analysis, reduction, and reporting on servers 4. Contingency planning and incident response policies and procedures 5. System backup and recovery procedures	1	1. 2. 3. 4. 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 2. Document creation and storage policy 3. User security education and training	3	1. 2. 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.

Summary

- IT security management implementation
- security controls or safeguards
  - management, operational, technical
  - supportive, preventative, detection, recovery
- IT security plan
- implementation of controls
  - implement plan, training and awareness
- implementation follow-up
  - maintenance, compliance, change and configuration management, incident handling
- Case study: Silver Star Mines