Week 10

IT SECURITY CONTROLS, PLANS, AND PROCEDURES

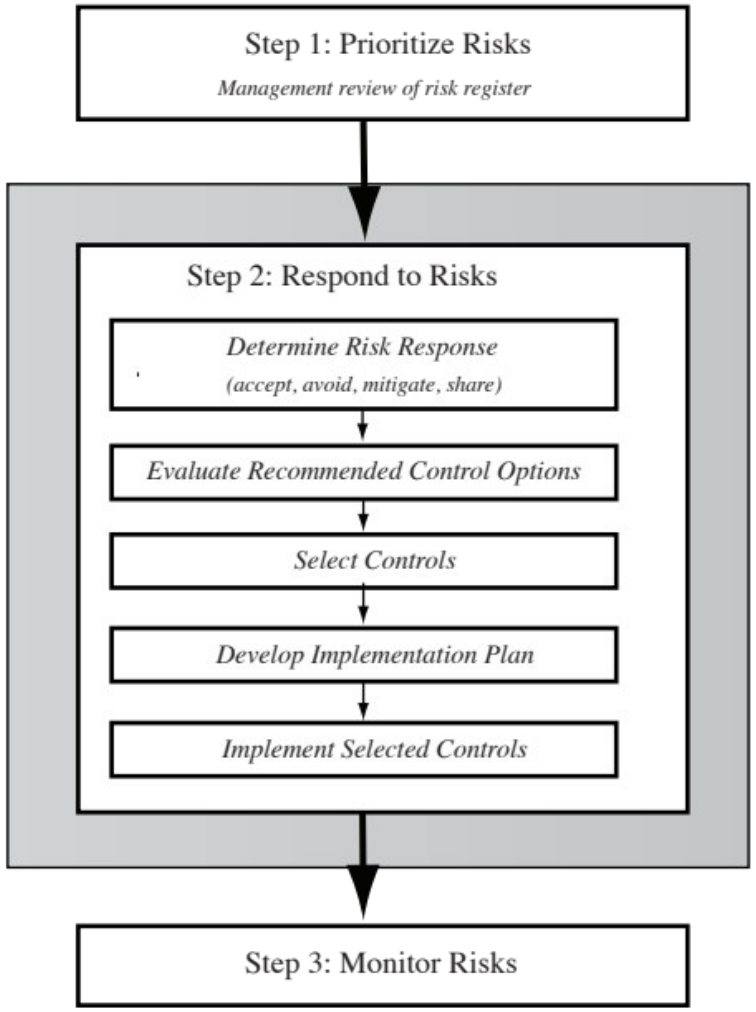


Figure 15.1 IT Security Management Controls and Implementation

IT Security Management Controls

Security Control

Control is defined as:

“An action, device, procedure, or other measure that reduces risk by eliminating or preventing a security violation, by minimizing the harm it can cause, or by discovering and reporting it to enable corrective action.”

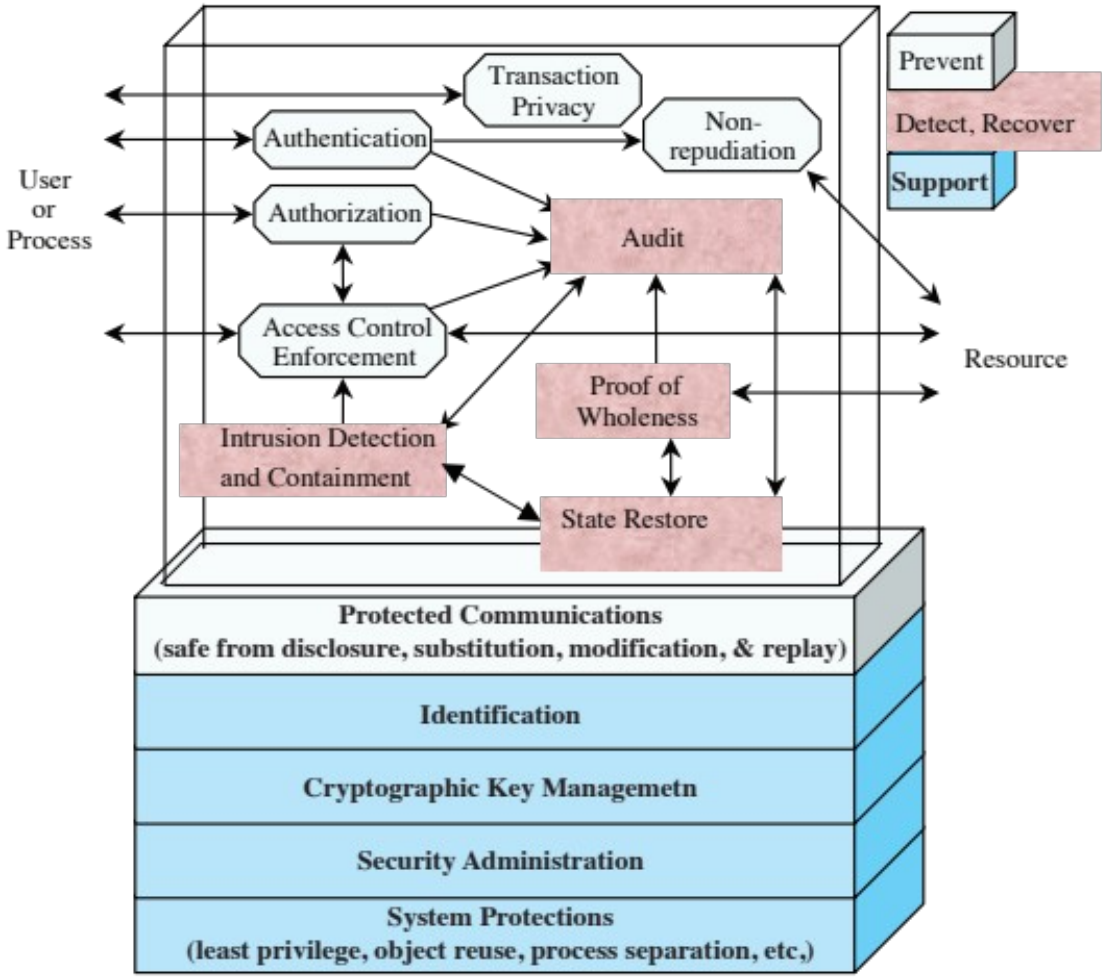


Figure 15.2 Technical Security Controls

Technical Security Controls

Control Classifications

Management controls

- Focus on security policies, planning, guidelines, and standards that influence the selection of operational and technical controls to reduce the risk of loss and to protect the organization's mission
- These controls refer to issues that management needs to address

Operational controls

- Address the correct implementation and use of security policies and standards, ensuring consistency in security operations and correcting identified operational deficiencies
- These controls relate to mechanisms and procedures that are primarily implemented by people rather than systems
- They are used to improve the security of a system or group of systems

Technical controls

- Involve the correct use of hardware and software security capabilities in systems
- These range from simple to complex measures that work together to secure critical and sensitive data, information, and IT systems functions

Table 15.1 – NIST SP800-53 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 15.2 – ISO/IEC 27002 Security Controls

Security Policies Ensure that information security policies support business requirements and comply with relevant laws and regulations.

Organization of Information Security Provide a management framework for controlling the implementation of security policies, and ensuring security of mobile devices.

Human Resource Security Ensure that employees and contractors understand and comply with security policies. Protect the organization's interests during the process of terminating or changing employment.

Asset Management Identify assets to be protected and define appropriate responsibilities for managing assets. prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

Access Control Define access privileges for access to information and information processing facilities. Ensure authorized user access and prevent unauthorized user access. Hold users accountable for safeguarding their authentication information.

Cryptography Ensure proper and effective use of cryptographic software and hardware so as to provide confidentiality, integrity, and authenticity services.

Physical and Environmental Security Define and implement policies to secure information processing facilities and to manage physical access to secure locations and secured facilities. Prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

Operations Security Ensure that the operation of information processing facilities conforms to security policies. Measures include ensuring that information and information processing facilities are protected against malware; protecting against loss of data; recording events and generate evidence; ensuring the integrity of operational systems to prevent exploitation of technical vulnerabilities.

Communications Security Implement security policies to protect network equipment and facilities, and to protect information transferred within an organization and with an external entity.

System acquisition, development and maintenance Ensure that security policies and procedures apply throughout a system's lifetime.

Supplier relationships Ensure that agreements with suppliers meet security policy requirements. Monitor and assess compliance with security agreements.

Information security incident management Implement an incident management capability that enables management of information security incidents, including reporting and documenting incidents and responses.

Information security continuity Ensure that security policies address requirements for incorporation into the organization's business continuity management systems.

Compliance Ensure that legal, statutory, regulatory or contractual obligations related to information security are met. Ensure that systems and personnel comply with the organization's security policies.

Control Classes

Each of the control classes may include the following:

Supportive controls

- Pervasive, generic, underlying technical IT security capabilities that are interrelated with, and used by, many other controls

Preventative controls

- Focus on preventing security breaches from occurring, by inhibiting attempts to violate security policies or exploit a vulnerability

Detection and recovery controls

- Focus on the response to a security breach, by warning of violations or attempted violations of security policies or the identified exploit of a vulnerability and by providing means to restore the resulting lost computing resources

Planning
Security Planning Policy and Procedures, System Security Plan, Rules of Behavior, Privacy Impact Assessment, Security-Related Activity Planning

Personnel Security
Personnel Security Policy and Procedures, Position Categorization, Personnel Screening, Personnel Termination, Personnel Transfer, Access Agreements, Third-Party Personnel Security, Personnel Sanctions

Risk Assessment
Risk Assessment Policy and Procedures, Security Categorization, Risk Assessment, Vulnerability Scanning

System and Services Acquisition
System and Services Acquisition Policy and Procedures, Allocation of Resources, Life Cycle Support, Acquisitions, Information System Documentation, Software Usage Restrictions, User Installed Software, Security Engineering Principles, External Information System Services, Developer Configuration Management, Developer Security Testing, Supply Chain Protection, Trustworthiness, Critical Information System Components

System and Communications Protection
System and Communications Protection Policy and Procedures, Application Partitioning, Security Function Isolation, Information in Shared Resources, Denial of Service Protection, Resource Priority, Boundary Protection, Transmission Integrity, Transmission Confidentiality, Network Disconnect, Trusted Path, Cryptographic Key Establishment and Management, Use of Cryptography, Public Access Protections, Collaborative Computing Devices, Transmission of Security Attributes, Public Key Infrastructure Certificates, Mobile Code, Voice Over Internet Protocol, Secure Name /Address Resolution Service (Recursive or Caching Resolver), Architecture and Provisioning for Name/Address Resolution Service, Session Authenticity, Fail in Known State, Thin Nodes, Honeypots, Operating System-Independent Applications, Protection of Information at Rest, Heterogeneity, Virtualization Techniques, Covert Channel Analysis, Information System Partitioning, Transmission Preparation Integrity, Non-Modifiable Executable Programs

System and Information Integrity
System and Information Integrity Policy and Procedures, Flaw Remediation, Malicious Code Protection, Information System Monitoring, Security Alerts Advisories and Directives, Security Functionality Verification, Software and Information Integrity, Spam Protection, Information Input Restrictions, Information Input Validation, Error Handling, Information Output Handling and Retention, Predictable Failure Prevention

Program Management
Information Security Program Plan, Senior Information Security Officer, Information Security Resources, Plan of Action and Milestones Process, Information System Inventory, Information Security Measures of Performance, Enterprise Architecture, Critical Infrastructure Plan, Risk Management Strategy, Security Authorization Process, Mission/Business Process Definition

Table 15.3 – Detailed NIST Sp800-53 Security Controls

Residual Risk

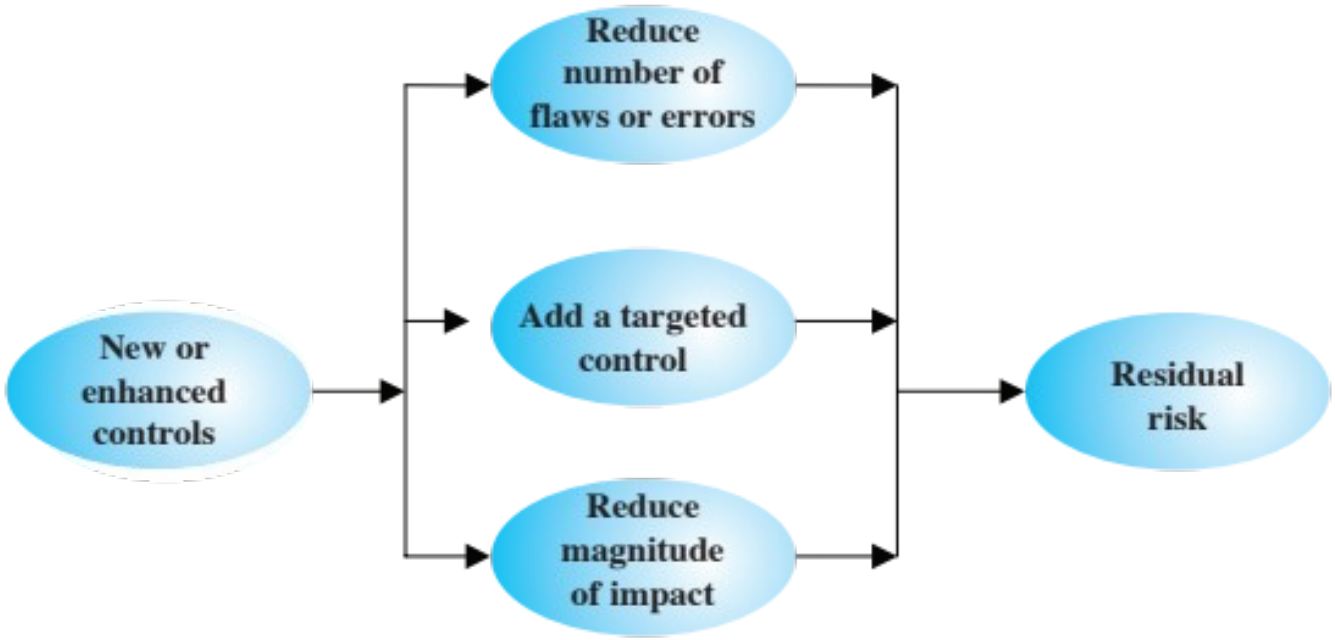


Figure 15.3 Residual Risk

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

Cost Benefit Analysis

Implementation Plan (example)

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	•Implement all recommended controls •Update related procedures with training for affected staff
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	February 6, 2017 to February 9, 2017
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

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

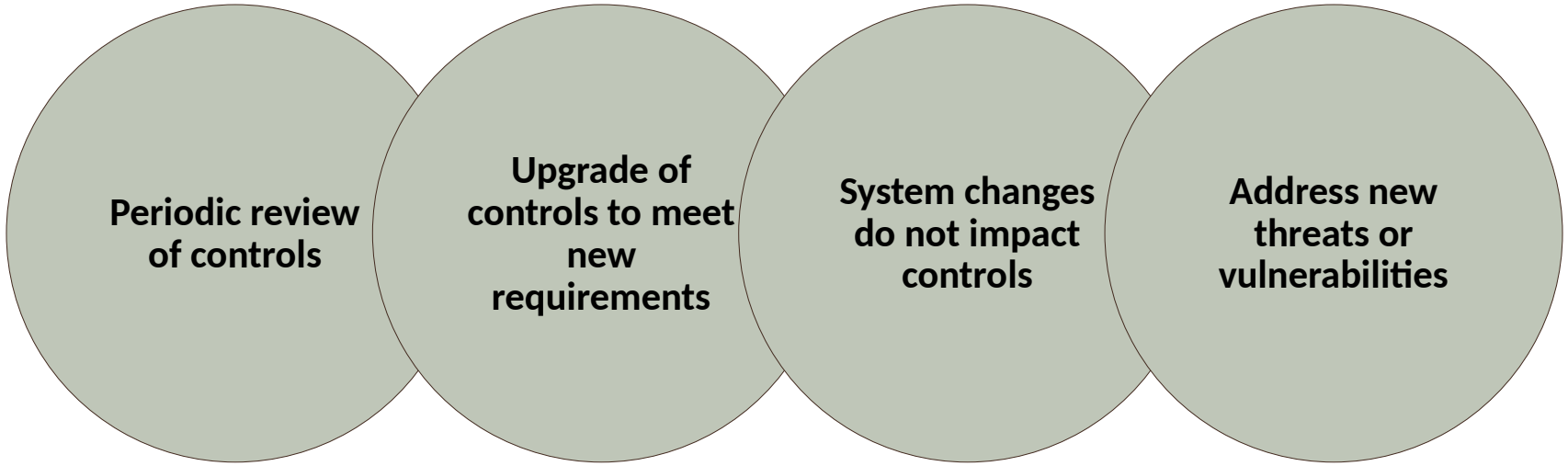
Includes a number of aspects

- 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



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

- 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

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

- 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