BAIT1093 Introduction to Computer Security

Chapter 8: IT Security Controls, Plans, and Procedures

Topics

8.1 Implementing IT Security Management
8.2 Security Controls
8.3 IT Security Plan
8.4 Implementation Plan
8.5 Implementation Follow-up

8.1 Implementing IT Security Management [1]

Chap 7

Chap 8

IT Security Management Process

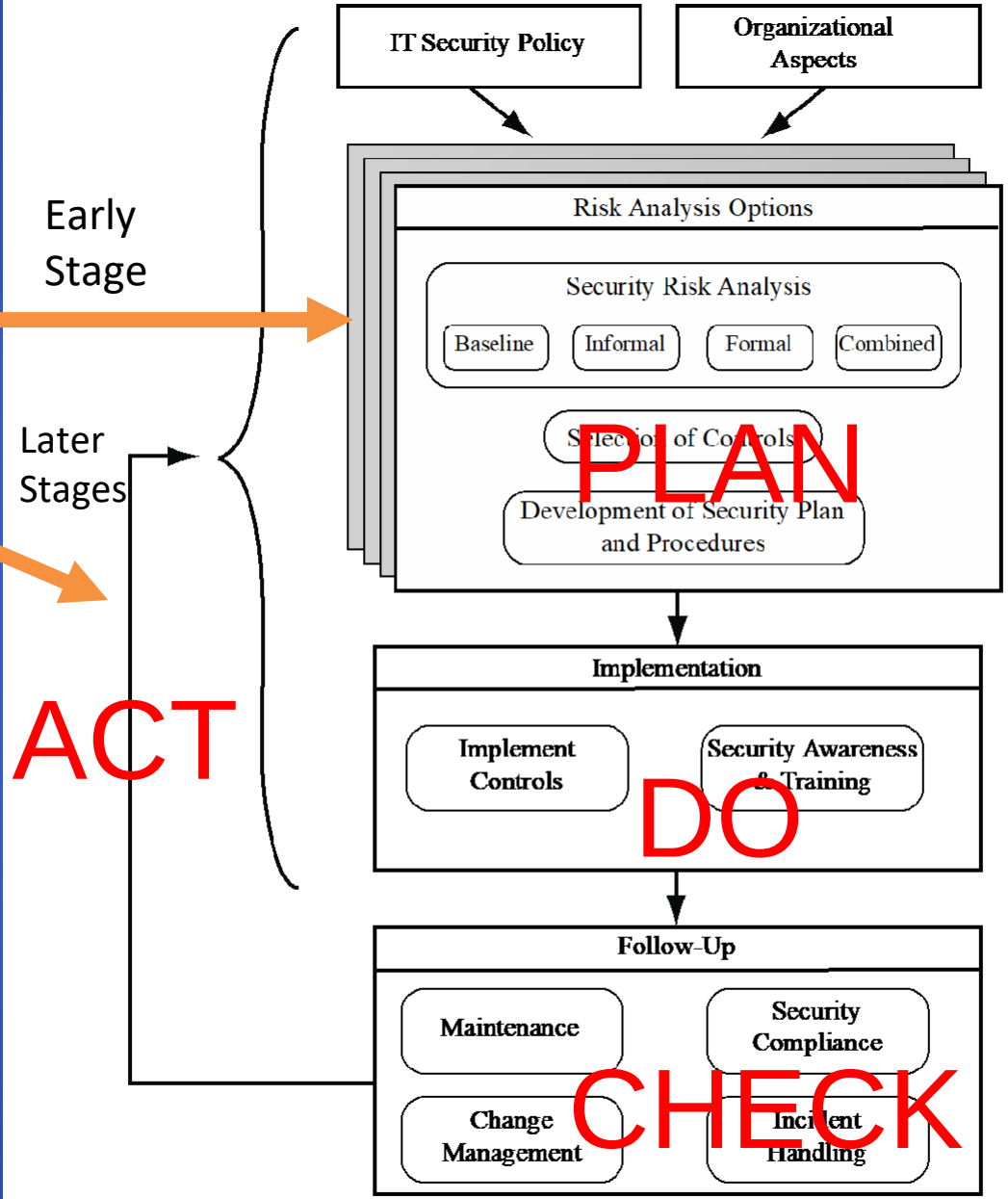


Figure 14.1 Overview of IT Security Management

8.1 Implementing IT Security Management [1]

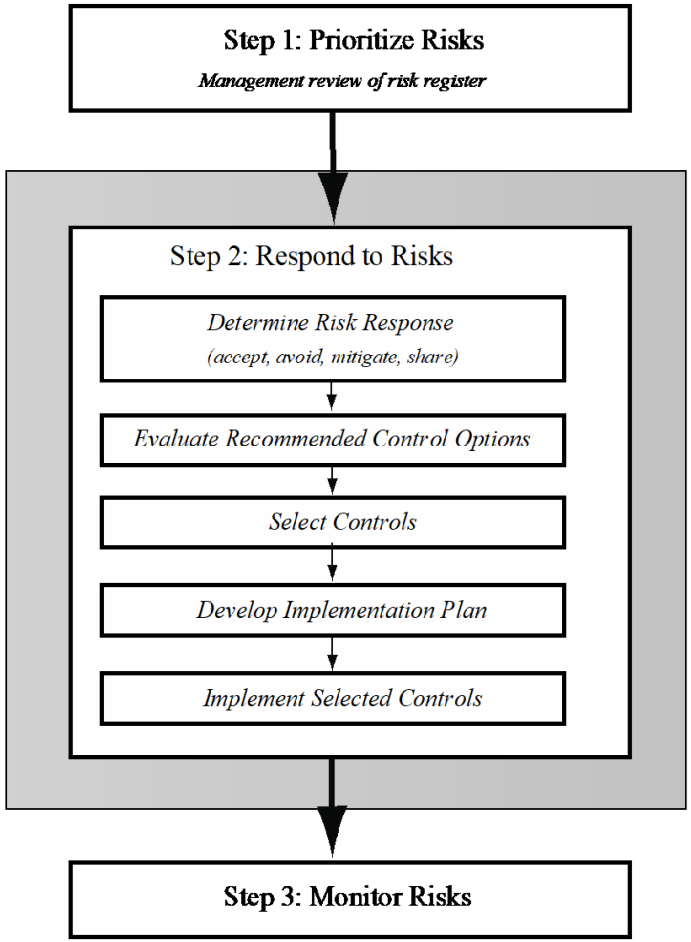


Figure 15.1 IT Security Management Controls and Implementation

8.2 Security Controls [1]

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."

8.2 Security Controls [2]

- A security control is a safeguard or countermeasure employed within an organizational information system to protect the confidentiality, integrity, and availability of the technology system and its data.
- A security control attempts to limit exposure to a danger.

8.2 Security Controls [1]

Control Classes

management controls

- **refer to issues that management needs to address**
- **security policies, planning, guidelines**, and **standards** 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**
- These range from simple to complex measures that work together to **secure critical and sensitive data, information, and IT systems functions**.

8.2 Security Controls [2]

Table 15-6 Categories of controls

Control category	Description	Phishing example
Managerial	Controls that use administrative methods	Acceptable use policy that specifies users should not visit malicious websites.
Operational	Controls implemented and executed by people	Conducting workshops to help train users to identify and delete phishing messages.
Technical	Controls incorporated as part of hardware, software, or firmware	Unified threat management (UTM) device that performs packet filtering, antiphishing, and web filtering.

8.2 Security Controls [2]

Specific types of controls are found within the three broad categories of controls.

- Deterrent controls. A deterrent control attempts to discourage security violations before they occur.
- Preventative controls. A preventative control works to prevent the threat from coming in contact with the vulnerability.
- Physical controls. A physical control implements security in a defined structure and location.
- Detective controls. A detective control is designed to identify any threat that has reached the system.

8.2 Security Controls [2]

Specific types of controls are found within the three broad categories of controls (cont.).

- Compensating controls. A compensating control is a control that provides an alternative to normal controls that for some reason cannot be used.
- Corrective controls. A control that is intended to mitigate or lessen the damage caused by the incident is called a corrective control.

8.2 Security Controls [2]

Table 15-7 Control types

Control type	Description	When it occurs	Example
Deterrent control	Discourage attack	Before attack	Posting signs indicating that the area is under video surveillance
Preventive control	Prevent attack	Before attack	Providing security awareness training for all users
Physical control	Prevent attack	Before attack	Building fences that surround the perimeter
Detective control	Identify attack	During attack	Installing motion detection sensors
Compensating control	Alternative to normal control	During attack	Isolating an infected computer on a different network
Corrective control	Lessen damage from attack	After attack	Cleaning a virus cleaned from an infected server

8.2 Security Controls [2]

- Controls change over time as new hardware and software are added and new procedures are implemented.
- **Inherent risk** is defined as the current risk level given the existing set of controls.
- **Residual risk** is the risk level that remains after additional controls are applied.

8.2 Security Controls [2]

- The goal of security is not to eliminate all risk.
- Instead, the goal in designing and implementing controls is to reach a balance between achieving an acceptable level of risk and expense while minimizing losses.
- Some assets, however, must be protected irrespective of the perceived risk. For example, controls based upon regulatory requirements may be required regardless of risk (regulations that affect risk posture).

8.2 Security Controls [1]

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

8.3 IT Security Plan [1]

- 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

8.4 Implementation Plan [1]

DO

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

IT Security Plan should include details of

- Risks (asset/threat/vulnerability combinations)
- Recommended controls (from the risk assessment)
- Action priority for each risk
- Selected controls (on the basis of the cost-benefit analysis)
- Required resources for implementing the selected controls
- Responsible personnel
- Target start and end dates for implementation
- Maintenance requirements and other comments

8.4 Implementation Plan [1]

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

8.4 Implementation Plan [1]

Security Plan Implementation (cont.)

- The implementation process should be monitored to ensure its correctness.
- This is typically performed by the organizational security officer, who checks that
  - The implementation costs and resources used stay within identified bounds.
  - The controls are correctly implemented as specified in the plan, in order that the identified reduction in risk level is achieved.
  - The controls are operated and administered as needed.

8.4 Implementation Plan [1]

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

8.5 Implementation Follow Up [1]

CHECK

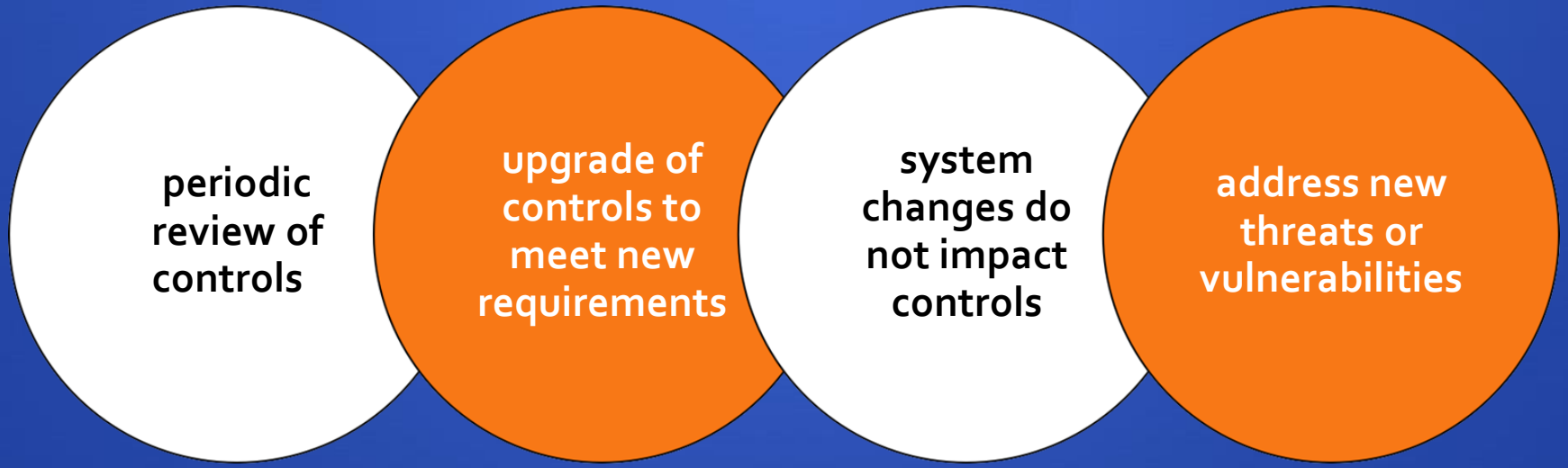
- security management is a cyclic process
  - constantly repeated to respond to changes in the IT systems and the risk environment
- need to monitor implemented controls
- evaluate changes for security implications
  - otherwise increase chance of security breach

includes a number of aspects
• maintenance of security controls • security compliance checking • change and configuration management • incident handling

8.5 Implementation Follow Up [1]

Maintenance

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



8.5 Implementation Follow Up [1]

Security Compliance

- audit process to review security processes. The goal is to verify compliance with security plan using 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

8.5 Implementation Follow Up [1]

Change and Configuration Management

8.5 Implementation Follow Up [1]

Incident Handling

- need procedures specifying how to respond to a security incident
  - given will most likely occur sometime
- reflect range of consequences on organization
- codify action to avoid panic
- e.g. mass email worm
  - exploiting vulnerabilities in common apps
  - propagating via email in high volumes
  - should disconnect from Internet or not?

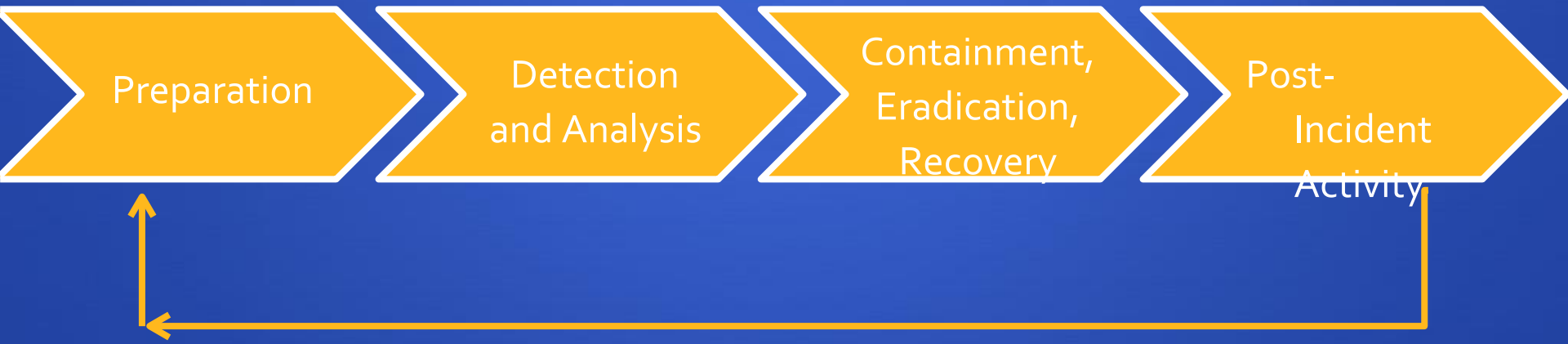
8.5 Implementation Follow Up [1]

Types of Security Incidents

- any action threatening classic security services
- unauthorized access to a system
  - unauthorized viewing by self / other of information
  - bypassing access controls
  - using another users access
  - denying access to another user
- unauthorized modification of info on a system
  - corrupting information
  - changing information without authorization
  - unauthorized processing of information

8.5 Implementation Follow Up [1]

Managing Security Incidents



8.5 Implementation Follow Up [1]

Detecting Incidents

- reports from users or admin staff
  - encourage such reporting
- detected by automated tools
  - e.g. system integrity verification tools, log analysis
  - tools, network and host intrusion detection systems,
  - intrusion prevention systems
  - updated to reflect new attacks or vulnerabilities
  - costly so deployed if risk assess justifies
- admins must monitor vulnerability reports

8.5 Implementation Follow Up [1]

Responding to Incidents

- need documented response procedures
  - how to identify cause of the security incident
  - describe action taken to recover from it
- procedures should
  - identify typical categories of incidents and
  - approach taken to respond
  - identify management personnel responsible for
  - making critical decisions and their contacts
  - whether to report incident to police / CERT etc

8.5 Implementation Follow Up [1]

Documenting Incidents

- need to identify vulnerability used
- and how to prevent it occurring in future
- recorded details for future reference
- consider impact on organization and risk profile
  - may simply be unlucky
  - more likely risk profile has changed
  - hence risk assessment needs reviewing
  - followed by reviewing controls in use

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.

Main References

[1] William Stallings and Lawrie Brown. 2018. Computer Security: Principles and Practice. Pearson.
[2] Mark Ciampa. 2022. CompTIA Security+ Guide To Network Security Fundamentals. Cengage Learning.