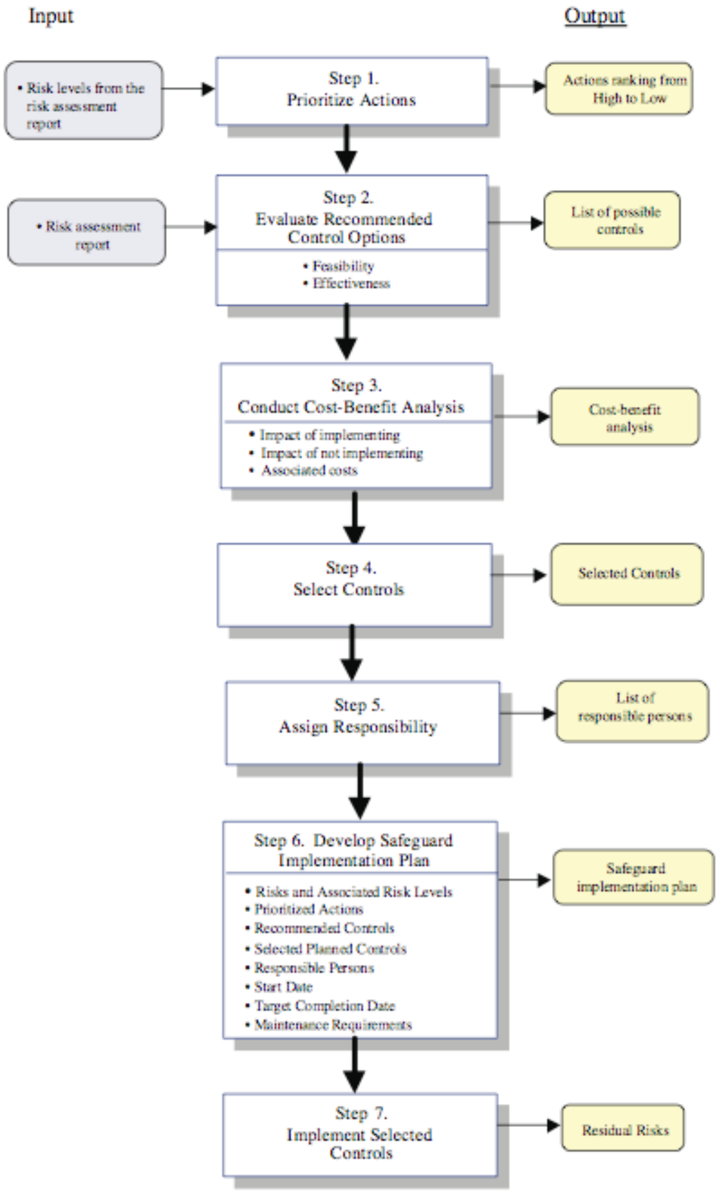
Computer Security: Principles and Practice

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

Selecting Controls or Safeguards

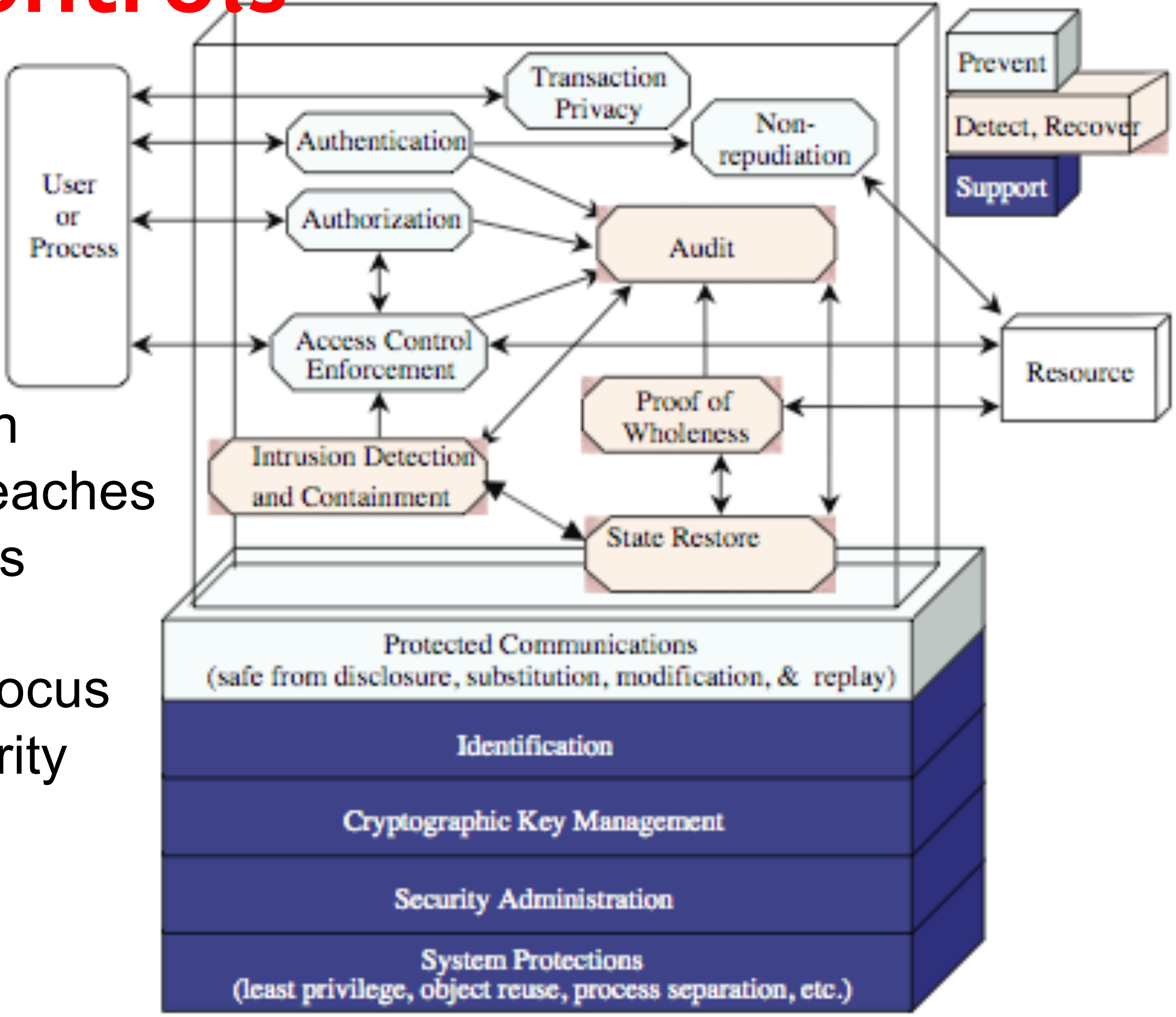
- controls or safeguards are
  - practices, procedures or mechanisms which may protect against a threat, reduce a vulnerability, limit the impact of an unwanted incident, detect unwanted incidents and facilitate recover
- classes of controls:
  - Management: focus on policies, planning
  - Operational: address (correct) implementation
  - Technical: correct uses of SW and hardware

Technical Controls

Supportive: generic, underlying technical IT capabilities

Preventative: focus on preventing security breaches by warning of violations

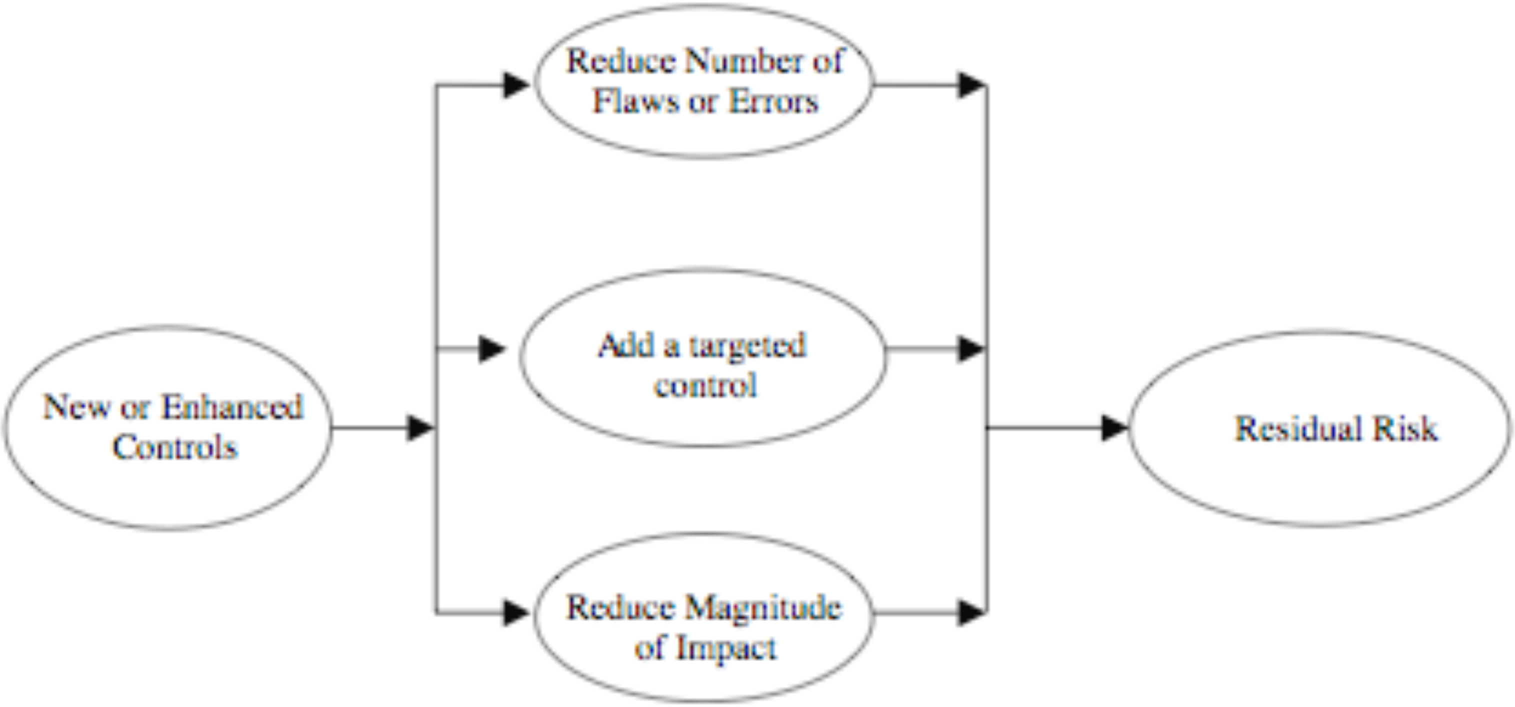
Detection/recovery: focus on response to a security breach



Lists of Controls (NIST, ISO; choose a combination)

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

Residual Risk



After implementing a new control: reduction in threat

Cost-Benefit Analysis Is cost of implementing a control justifiable by the reduction in level of risk to an asset?

- Fundamentally a business decision
- Conduct to determine appropriate controls
  - greatest benefit given resources available
- Reduces risk more than needed? Choose a less expensive control
- Costs more than the risk reduction provided? Choose an alternative
- Does not risk sufficiently? More control is needed
- Provides sufficient reduction and is cost effective? Use it

IT Security Plan

- provides details of
  - what will be done
  - what resources are needed
  - who is responsible
- should include
  - risks, recommended controls, action priority
  - selected controls, resources needed
  - responsible personnel, implementation dates

Implementation Plan

Risk (Asset/Threat)	Level of Risk	Recommended Controls	Prio rity	Selected Controls	Required Resources	Responsible Persons	Start - End Date	Other Comments
Hacker attack on Internet Router	High	1. disable external telnet access 2. use detailed auditing of privileged command use 3. set policy for strong admin passwords 4. set backup strategy for router config file 5. set change control policy for the router configuration	1	1. 2. 3. 4. 5.	1. 3 days IT net admin time to change & verify router config, write policies; 2. 1 day of training for net admin staff	John Doe, Lead Network Sys Admin, Corporate IT Support Team	1-Feb-2006 to 4-Feb-2006	1. need periodic test & review of config & policy use

Security Plan Implementation

- plan documents what is required
- identified personnel perform needed tasks
  - to implement new or enhanced controls
  - may need upgrades or new system installation
  - or development of new/extended procedures
  - need support from management
- monitored to ensure process correct
- when completed management approves

Security Training / Awareness

- responsible personnel need training
  - on details of design and implementation
- need general awareness workshop for all
  - spanning all levels in organization
  - essential to meet security objectives
  - lack of training leads to poor practices reducing security

Security Awareness Issues to address

- organization’s security objectives, strategies, policies
- need for security, general risks to organization
- understanding why security controls are used
- roles and responsibilities for various personnel
- the need to act in accordance with policy and procedures, consequences of unauthorized actions
- the need to report any security breaches observed and to assist with their investigation

Maintenance of Implemented Controls

- need continued maintenance and monitoring
  - to ensure continued correct functioning and appropriateness
- tasks include:
  - periodic review of controls
  - upgrade of controls to meet new requirements
  - check system changes do not impact controls
  - address new threats or vulnerabilities
- goal to ensure controls perform as intended

Security Compliance (Audit/Verify)

- audit process to review security processes
- to verify compliance with security plan
- using internal or external personnel
- usually based on checklists to check
  - 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
  - evaluate security and wider impact of changes
  - part of general systems administration process
  - cf. management of bug patch testing and install
  - may be informal or formal
- configuration management is keeping track of configuration and changes to each system
  - to help restoring systems following a failure
  - to know what patches or upgrades might be relevant
  - also part of general systems administration process

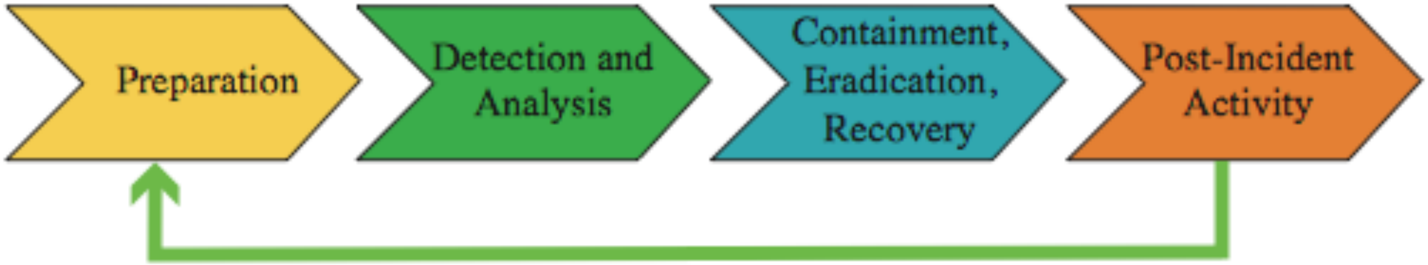
Incident Handling: Essential Control

- need procedures specifying how to respond to a security incident
  - given it will most likely occur sometime
- 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?
    - responsible individual should make a decision (the policy should indicate how to contact the individual)

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 user’s access
  - denying access to another user
- unauthorized modification of info on a system
  - corrupting information
  - changing information without authorization
  - unauthorized processing of information

Managing Security Incidents



Detecting Incidents

- reports from users or admin staff
  - train and 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
- admins must monitor vulnerability reports

Responding to Incidents

- need documented response procedures
- 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

Documenting Incidents

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

Sample Implementation Plan for Silver Star Mines

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 & response system	2	1.
Integrity of stored file and database information	Extreme	1. audit of critical documents 2. document creation & storage policy 3. user security education and training	3	1. 2. 3.
Availability & integrity of Financial, Procurement, & Maintenance/ Production Systems	High	-	-	(general controls)
Availability, integrity and confidentiality of email	High	1. contingency planning – backup email service	4	1.

Summary

- security controls or safeguards
  - management, operational, technical
  - supportive, preventative, detection / recovery
- IT security plan
- implementation of controls
  - implement plan, training and awareness
- implementation followup
  - maintenance, compliance, change / config management, incident handling