Security Management and Risk Assessment

Security 1 (CM0475, CM0493) 2020-21
Università Ca' Foscari Venezia

Riccardo Focardi
www.unive.it/data/persone/5590470
secgroup.dais.unive.it

Introduction

Security Management

Select and implement **technical** and **administrative** measures to address an organization's **security requirements**

1. **What assets** do we need to protect?
2. How are those assets **threatened**?
3. What can we do to **counter** those threats?

Introduction

Risk Assessment

Determining IT security objectives and general **risk profile**

For each asset, perform an IT security **risk assessment**

Decide what **management**, **operational**, and **technical** controls are needed to reduce the risks to an **acceptable level**

Standards

ISO 27000 series: best practice recommendations on IT security management and techniques

NIST SP 800-18: *Guide for Developing Security Plans for Federal Information Systems*, February 2006

NIST SP 800-30: *Guide for Conducting Risk Assessments*, September 2012

NIST SP 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations*, January 2015

NIST *Framework for Improving Critical Infrastructure Cybersecurity* published in 2014, provides guidance to organizations on systematically managing **cybersecurity risks**

IT security management

Definition: **Formal process** to develop and maintain appropriate levels of computer security for an organization's assets

Steps:

1. determining security **objectives**, **strategies**, and **policies**
2. performing an IT security **risk assessment**
3. selecting cost-effective **remedial controls**
4. writing **plans** and **procedures** to implement selected controls
5. **implementing** controls
6. raise security **awareness** and develop **training** programs
7. monitor and **maintain** effectiveness of controls
8. detect **incidents** and react

Overview

IT Security Management

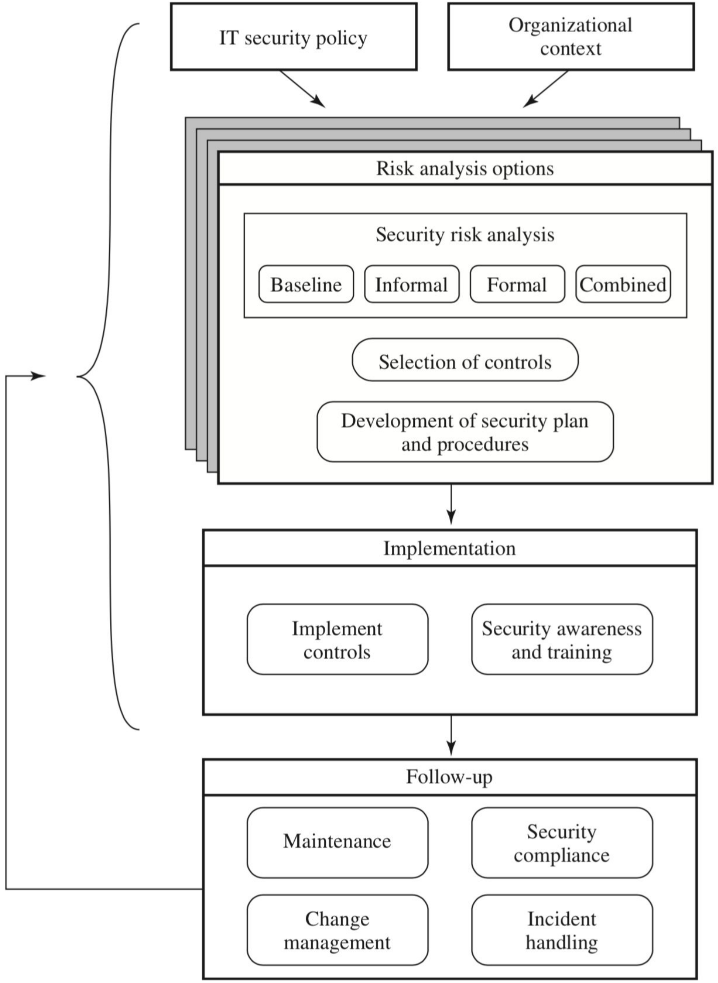


Figure from Lawrie Brown, William Stallings. *Computer Security: Principles and Practice*, 4/E, Pearson.

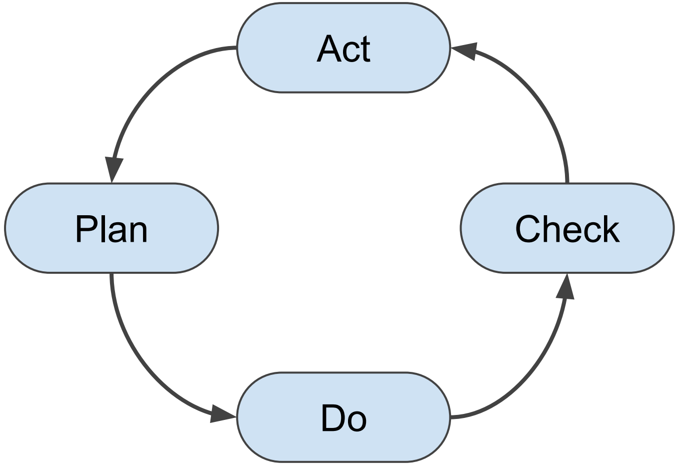
IT management is an *iterative process*

Plan: Security **policy**, **objectives**, procedures; **risk** assessment; develop risk treatment **plan**

Do: **Implement** risk treatment plan

Check: Monitor and **maintain** the risk treatment plan

Act: Maintain and **improve** the risk management process in response to incidents, review, identified changes



IT security objectives

Examination of the organization’s **IT security objectives** in the **context** of the organization’s general risk profile

Role and importance of IT systems

- what key aspects require IT in order to be **efficient**?
- what tasks can **only** be performed with IT support?
- which essential decisions depend on **accuracy**, **currency**, **integrity**, **availability** of data managed by IT systems?
- what data managed by IT systems need **protection**?
- what are the **consequences** of a security failure in IT systems?

Outcome: list of **key security objectives**

IT security policy

Describes the **IT security objectives** and strategies to achieve them

It addresses:

- **scope** and purpose of the policy
- relationship between security objectives, **legal** obligations and **business** objectives
- IT security requirements in terms of expected security **properties**
- **responsibilities** (security officer)
- **risk** management approach
- security **awareness** and training
- legal **sanctions** on staff
- **integration** of security in systems
- information **classification** scheme
- business **continuity** plan
- **incident** detection and handling
- changes and **reviews** to policy

IT security officer

Standards recommend to have a single **IT security officer** responsible for the organization’s IT security

Large organizations will also have **IT project security officers** responsible of specific projects or systems

Responsibilities of IT security officer

- **supervise** the IT security management process
- **cooperate** with other managers on IT security issues
- **maintain** the organization’s IT security objectives and policies
- coordinate security **incident** handling and response
- manage IT security **awareness** and **training** programs
- **interact** with IT project security officers

Risk assessment

Fundamental component of IT security management that guides in deploying **cost-effective controls**

Ideally: *every asset* is evaluated and *every possible risk* is considered

⇒ if risk too high then **remedial controls** are deployed

⇒ too long and expensive in practice! (a **compromise** is needed)

Ideally: we would like to **remove** the risk completely

In practice: we just **reduce** it!

What is an *acceptable level or risk*?

Idea: **cost** of resources to reduce risk are proportional to the **cost** to the organization if the risk occurs

⇒ **likelihood** also matters!

Risk Assessment

standard approaches

Baseline approach

Informal approach

Detailed risk analysis

Combined approach

Baseline approach

Idea: implement **basic security controls** using baseline documents and industry best practices

Goal: protection against most **common threats**

🙂 few additional resources
🙂 same controls over many systems

☹️ independent of the effective risk
☹️ might be excessive or inadequate

Example: hardening measures for OS security (previous class)

Baseline recommendations from

- **standards**
- security-related **organizations** such as CERT, NSA, ENISA
- **industry** sector councils

OK for small organizations with no budget for other approaches

Informal approach

Idea: **informal** risk analysis for the organization's IT systems

Goal: more **accurate** and **targeted** controls than baseline approach

🙂 internal experts (quick and cheap)
🙂 targets specific vulnerabilities

☹️ not very accurate
☹️ might be biased
☹️ inconsistent if repeated

It might provide **insufficient justification** for suggested controls

Recommended for small to medium-sized organizations where

- the IT systems are **not** necessarily essential to meeting the organization's business objectives
- additional **expenditure** on risk analysis cannot be justified

Detailed risk analysis

Idea: risk analysis for the organization's IT systems through a **formal**, structured process

Goal: accurate and repeatable

1. identification of **assets**
2. identification of **threats** and **vulnerabilities** for assets
3. **likelihood** of the risk
4. **consequences** to organization

🙂 **detailed** examination
🙂 strong **justification** for controls
🙂 information for **managing** changes

☹️ **expensive** and **slow**
☹️ requires **specialized** skills

Often a **legal requirement** (e.g., government and key infrastructures)

Also, large organizations with critical IT systems and enough **budget**

Combined approach

Idea: **combine** baseline, informal, and detailed risk analysis approaches

Goal: reasonable level of protection as **quick** as possible and **secure key systems** over time

1. **baseline** security
2. identify **high risk** systems
3. **immediate** informal risk analysis
4. possible **detailed** analysis if considered necessary

🙂 **basic security** quickly
🙂 high risk analysis **fast** and **cheaper**
🙂 use resources where most **needed**

☹️ if high risk analysis is wrong, critical systems might remain **vulnerable** (should be fixed by further reviews)

ISO 13335 recommends this approach as the **most cost-effective**

Detailed Risk Analysis

Context

Not all organizations are **equally at risk**. **Examples**:

Education is typically less at risk than **banking**, **finance** and **health care**

Critical infrastructures such as electric, water, oil, gas are at high risk

Transports and **health-critical** industry, e.g. mining, are at high risk

Legal and regulatory constraints should be identified

Risk appetite is the level of risk that an organization is prepared to accept

- Banks have **little** appetite
- Leading-edge manufacturers have much **bigger** appetite

Boundaries: which IT systems will be analyzed (e.g. when part of a group)

Assets

Our first initial question: **what assets** do we need to protect?

- computers
- infrastructure
- software
- people

Ideally: consider all possible assets

In practice: key assets contributing to the organization’s objectives

It is necessary to draw on the expertise of the people in the **relevant areas** of the organization

A key element of this process step is **identifying** and **interviewing** such personnel

Outcome: list of **assets**, with brief descriptions of their **use** by, and **value** to, the organization

Threats and vulnerabilities

Our second initial question: How are key assets **threatened**?

Threat agent: **who** or **what** could cause harm

- **natural**: fire, flood, storm, …
- **human deliberate**: insider, hacker
- **human accident**: incorrect configuration, accidental leakage

Statistics about natural threats: typical from insurances

Annual **computer crime reports** about most common threats: should be tailored to the organization profile

Vulnerabilities: identifying flaws that could be **exploited** by threat agents

Outcome: threats and vulnerabilities and how/why they might occur.

Risk analysis

Ideally: for each threat determine

- consequences, in terms of cost **c**, if the threat occur
- probability **p** that the threat occurs

Risk = **c** x **p**

Note: It can be directly compared with the value of the threatened asset for the organization

In practice: difficulty in computing **c** and **p** makes it necessary to adopt a **qualitative** approach

Consequences and probability are **classified** using suitable tables that provide a “definition” for each class

Classes are sorted so that it is possible to **order** risks based on the relative **urgency**

Risk likelihood: qualitative approach

Rating	Description	Detailed definition
1	**Rare**	May occur only in **exceptional circumstances**
2	**Unlikely**	Could occur at some time but not expected given current **controls**, **circumstances**, and recent **events**
3	**Possible**	Might occur at some time. It may be difficult to control its occurrence due to **external influences**
4	**Likely**	Will **probably occur** in some circumstances
5	**Almost certain**	**Expected to occur** in most circumstances

Based on **environment**, existing **controls**, **threat/vulnerability** details from previous steps, the risk analyst decides the appropriate rating

Risk consequences: qualitative (1)

Based upon the judgment of the **asset's owners**, and the **organization's management**

Rating	Description	Detailed definition
1	**Insignificant**	**minor** security breach; less than few **days** and minor expenditure to rectify; **no tangible** detriment to the organization
2	**Minor**	security breach in **1 or 2 areas**; less than one **week** and intervention of **project team** to rectify; **no tangible** detriment, maybe efficiency issues
3	**Moderate**	limited **systemic** security breaches; less than **two weeks** with **management intervention** and some compliance **costs**; **customers** might notice the event

Risk consequences: qualitative (2)

Rating	Description	Detailed definition
4	**Major**	ongoing **systemic** security breaches; **4-8 weeks** with significant **management intervention** and substantial compliance **costs**; **customers** will be aware of the event; loss of business possible
5	**Catastrophic**	**Major** systemic security breaches; >**3 months** with senior **management intervention** and very substantial compliance **costs**; substantial public or political **debate**; loss of business **expected**; possible **legal actions** on personnel involved
6	**Doomsday**	**Multiple major** systemic security breaches; hard to estimate time and intervention necessary (**major restructuring**); compliance costs as **annual losses**; substantial public or political **debate**; loss of business **unavoidable**; **legal actions** on personnel involved

Resulting level of risk

	Doomsday	Catastrophic	Major	Moderate	Minor	Insignificant
Almost Certain	E	E	E	E	H	H
Likely	E	E	E	H	H	M
Possible	E	E	E	H	M	L
Unlikely	E	E	H	M	L	L
Rare	E	H	H	M	L	L

Resulting level of risk (meaning)

Risk level	**Description**
E (extreme)	**detailed management** planning at an executive/director level; regular **reviews**; substantial adjustment of **controls** to manage the risk is expected, with **costs** possibly exceeding original forecasts
H (high)	**management** and planning can be left to senior project or team leaders; regular **reviews** are likely, though adjustment of controls is likely to be met from within **existing resources**
M (medium)	managed by **existing** specific monitoring and response procedures, with **appropriate monitoring** and **reviews**
L (low)	Can be managed through **routine procedures**

Outcome

Risk register: A **summary** of risk analysis; risk are sorted in **decreasing order** and **details** about evaluation are provided in separate documents

Aim: provide senior manager with information needed to **make decisions** and keep track of the **formal risk assessment** process

Asset	Threat / vulnerability	Existing controls	Likelihood	Consequence	Level of risk	Risk priority
Internet router	Outside hacker attack	Admin password only	Possible	Moderate	H	1
Data center	Accidental fire or flood	None	Unlikely	Major	H	2

Risk treatment

Evaluation: risks above acceptable level (context dependent) need to be treated; **easy** ones are treated first

Example: tightening router configuration is much simpler than developing a full disaster recovery

Risk acceptance: accept a risk greater than normal for business reasons (too expensive)

Risk avoidance: not proceeding with the activity that creates the risk

Risk transfer: insurance, partnership or contract with other organizations

Reduce consequences: controls to quickly recover, e.g., backups, disaster recovery plans

Reduce likelihood: improve security, e.g, firewalls, password policies, ...

Judgment about risk treatment

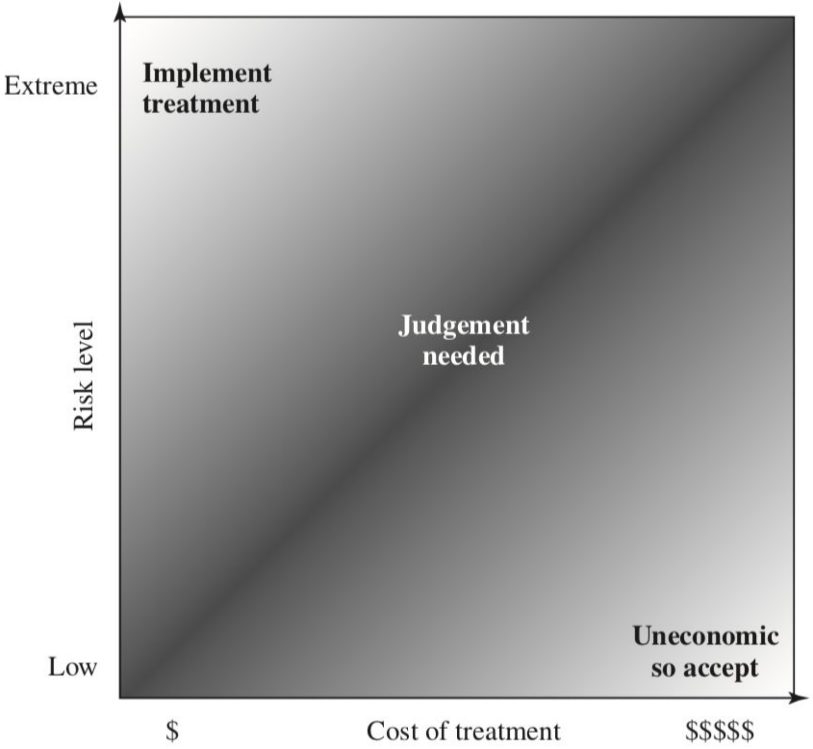


Figure from Lawrie Brown, William Stallings. *Computer Security: Principles and Practice*, 4/E, Pearson.