

# Security in Organizations (2IF07)

## Course Notes

Jos Wetzels

a.l.g.m.wetzels@student.utwente.nl

## 1 Introduction

### 1.1 Information Security

- Preservation of confidentiality, integrity and availability of information (ISO)
- The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (NIST).
- The condition in which confidentiality, integrity and availability of information and information technology are protected by appropriate safeguards. (BSI).

A **security incident** is an event where confidentiality, integrity of information was lost.

**Information security** is ensuring that **security incidents from the past cannot occur (again)** in the organisation, **at least not with high impact**.

### 1.2 Security Organization Outline

- Arranging ‘standard’ things, e.g. HR, physical security, user account management.
- Dealing with third parties (procurement department)
- Allocate business responsibilities for security and guidelines on how to fill in these responsibilities
- Day to day assistance and compliancy checking
- Internal audit
- Periodic review of security

- Reporting to management
- ...

Information security is the **concern of the security officer** but **ultimately he/she is not responsible for it!**

### 1.3 Summary

- In essence, getting proper Information Security is a **nontechnical problem** as it **is about getting the right attention (and budget!) from management**.
- **Complicating** factors in implementing Information Security (IS) are its **multidisciplinary nature** and **constraints on budget, effort and getting management attention**
- ISO 27002 is a (long) list of IS controls divided over many chapters originally dating from the nineties
- **Practice shows that ‘just’ implementing ISO 27002 is not the way to secure organizations because not all controls are equally relevant** for all organizations and circumstances
- **To address this ISO 27002 was supplemented with ISO 27001** which describes ‘security management’ that we will discuss next week.

## 2 Security Management (ISO 27001)

**Key message of ISO 27001:** information security is an **improvement process** (and not a product!)

ISO 27001 is based on a (simple!) **Plan-Do-Check-Act** cycle also known as the **Deming cycle**.

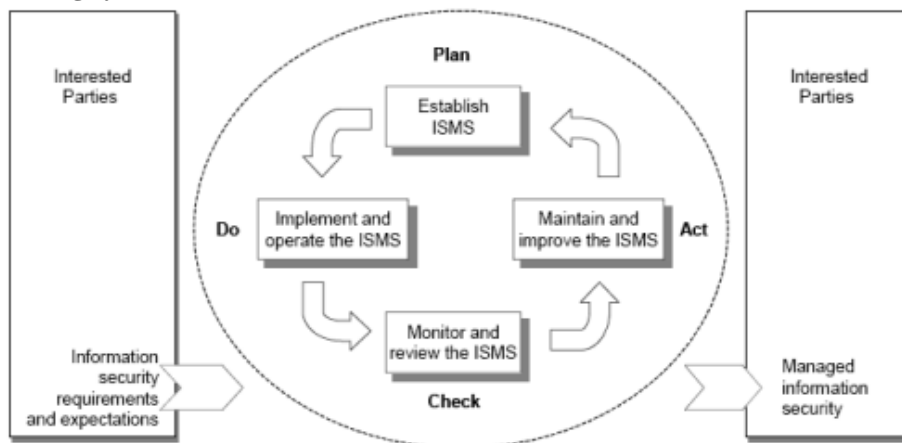


Figure 1 — PDCA model applied to ISMS processes

### 2.1 The ISO 27001 Cycle

- **Plan**
  - Document scope & boundaries
  - Document **Information Security Management System** (ISMS) policy
  - Develop & document risk assessment methodology
  - Determine assets ('everything that has value to the organization')
  - Conduct risk assessment of the assets
  - Select controls for treatment of risk (ISO 27002)
  - Management approval of residual risks
  - Implement and operate ISMS
  - Prepare statement of applicability
- **Do**
  - Formulate risk treatment plan
  - Implement selected controls
  - Document how to measure the effectiveness of selected controls
  - Implement training and awareness programs
  - Implement ISMS
  - Implement response to security incidents

- **Check**
  - Regular reviews / internal audits of ISMS effectiveness
  - Measurement effectiveness of controls
  - Review risk assessments at planned intervals
- **Act**
  - Implement the identified improvements
  - Management shall review the organization's ISMS at planned intervals (at least once a year)
  - Take into account feedback from interested parties, internal audits, effectiveness measurements, security incidents
  - The output from the management review shall include any decisions and actions
  - The organization shall continually improve the effectiveness of the ISMS

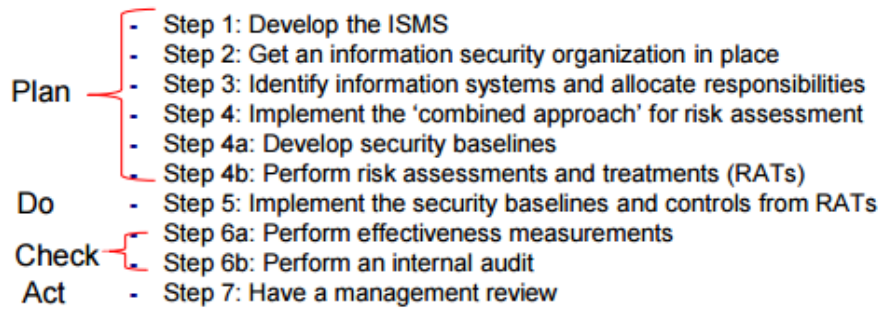
## 2.2 Security Management Based on ISO 27001

**Combined approach:** apply 'evident controls' without much risk-assessment (**baseline**) and implement specific, additional (costly) controls based on a risk assessment.

### Challenges

- Finding the right balance between the (theoretical) standard and pragmatism
- The avoidance of just creating a lot of paperwork
- Actually getting your organization more 'secure' in a practical sense as a result of ISO 27001 implementation.
- Multidisciplinary nature (technical, organizational, human)
- Constraints on budget and effort
- Constraints on attention

## Overview



### 2.2.1 Step 1: Develop the ISMS & Step 2: Get an information security organization in place

A project team is formed, typically chaired by the CSO, in which all stakeholders are involved. The project team then develops the ISMS, a project plan to implement it and approval/budget of management.

## Tasks and responsibilities in keywords

Who	What
Senior management	Providing resources, management review (Act)
(Chief) Security officer	Steering, guidance, monitoring (day to day) Operating ISMS
Project organization	Steering, drafting ISMS handbook, procedures/baselines (Plan)
Business / process owner	Conducting risk analyses (Plan)
ICT department	Implementing ICT controls (Do)
Facility management	Implementing physical controls (Do)
Human Resource	Implementing HR controls (Do)
Finance department	Imposing security on external parties (Do)
Legal department	Legal compliance (e.g., privacy, contracts)
Internal audit department	Conducting audits (Check)
External auditors	Conducting audits (Check)

### 2.2.2 Step 3: Identify information systems and allocate responsibilities

According to ISO 27001, **responsibility for information security should be placed at business process level**. Finding the right business level is the challenge. **If the level is too high, one will not gain proper insight in the risks**. Making a 'business process owner' responsible for security in his business process is typically **too abstract**. Many organizations struggle with how to organize their business processes. This also means that as a security officer you get involved in all this too. In modern organizations **business processes and 'information systems' are closely aligned**. So **allocating responsibility at an information system level is a workable approach**.

#### Information System:

*"a system of people, data records and activities that process the data and information in an organization, and it includes the organization's manual and automated processes"*

- Organizations often have a good idea of the 'ICT components' they possess (e.g. servers, routers, software licenses).
- They often also have a reasonable understanding of the 'information systems' or 'applications' they possess.
- But often the link between systems and business processes that depend on them is often not sufficiently known. As a result, responsibility for information systems is often not properly allocated to business management, leaving choices to IT.
- So the first step is to make an inventory of the information systems and allocate the responsibility for them. This can be a lot of work.
- To avoid that one gets too many 'information systems' it is a good idea to cluster systems/applications.

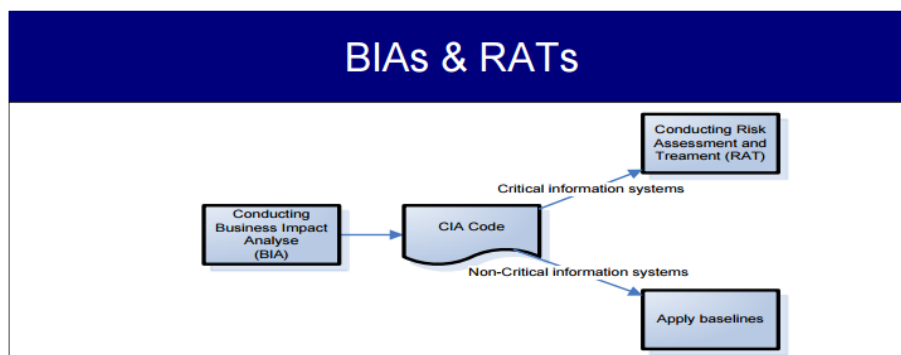
### 2.2.3 Step 4: Implement the 'combined approach' for risk assessment

- The methodology to select a 'simple' set of ISO 27002 controls as a starting point for the risk assessment process is called the 'combined approach' for risk assessment'. It is a middle ground between:
  - the 'old' idea of 'simply' from the 1990's implementing all ISO 27002 controls which is not practical/too expensive
  - the 'new' ISO 27001 idea that all controls selected should be based on a risk assessment while some controls are simply common sense.

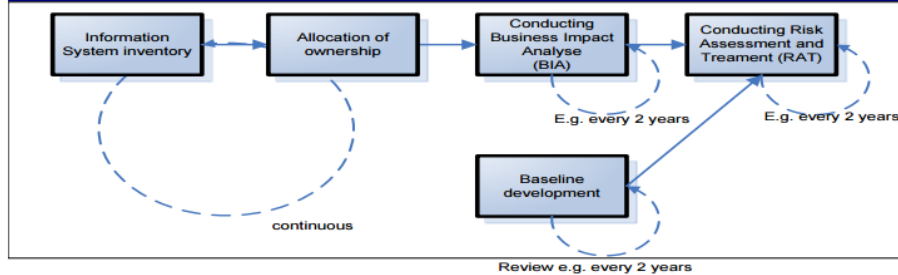
- One should perform a risk assessment on (all) business processes
- It must be avoided to have the same (rigorous) risk assessment process for all information systems
- One needs a separation between ‘critical’ and ‘non-critical’ information systems:
  - for ‘non-critical’ systems the security baselines suffice
  - ‘critical’ systems need an additional risk assessment

#### **Business Impact Analysis (BIAs) & Risk Assessment and Treatment (RAT)**

- By using a high level risk analysis (**Business Impact Analysis or BIA**) decide what the organization’s critical information systems are.
- An **information system is called critical** when one of its **CIA characteristics is ‘High’** otherwise it is non-critical.
- Non-critical information systems solely rely on ‘baselines’ for their information security, i.e. minimal sets of security controls
- Baselines also apply to the critical information systems but in addition a detailed level risk analysis (**Risk Assessment and Treatment or RAT**) is conducted, leading to possible controls additional to the baselines.



## BIAs & RATs



## Example BIA questions & Answers for patient record system

Confidentiality: Organizational impact when information in the system is compromised				
Question	Impact			Explanation
Privacy sensitivity of data	None	Standard registry (e.g., memberships)	Sensitive data (e.g. financial, medical or criminal)	PATIENT DATA!
Financial loss as result of information disclosure	< 2,5k	2,5k -- 50k	> 50k	
Possible fraud as a result of information disclosure	< 2,5k	2,5k -- 50k	> 50k	
Reputation loss as a result of information disclosure	No negative publicity	Local negative publicity	National negative publicity	
Liability issues as a result of information disclosure	None	Limited	High	
To what extent can information disclosure lead to injuries	None	Serious injuries	Loss of life	
<b>Result</b>	<b>Low</b>	<b>Medium</b>	<b>High</b>	
			X	

Integrity: Organizational impact when information is incorrect				
Question	Impact			Explanation
Financial loss as result of unintentional changes in information	< 2,5k	2,5k -- 50k	> 50k	
Financial loss as result of intentional changes in information (fraud)	< 2,5k	2,5k -- 50k	> 50k	?
Reputation loss as a result of incorrect information	No negative publicity	Local negative publicity	National negative publicity	
Liability issues as a result of incorrect information	None	Limited	High	
Possible wrong management decisions as a result of incorrect information	None	Limited	High	
Safety dangers as a result of incorrect information	None	Serious injuries	Loss of life	PATIENT DATA
<b>Result</b>	<b>Low</b>	<b>Medium</b>	<b>High</b>	
			X	



Availability: Organizational impact when the system is unavailable				
Question	Duration			Explanation
Acceptable downtime before substantial financial loss (> 50k) occurs	> 1 day	< 1 day	< 4 hours	
How long is manual processing as an alternative feasible	> 1 day	< 1 day	< 4 hours	PAPER FILES
After what downtime are important management decisions no longer possible	> 1 day	< 1 day	< 4 hours	
After what downtime is the reputation of the organization in danger	> 1 day	< 1 day	< 4 hours	
After what downtime external requirements are no longer met	> 1 day	< 1 day	< 4 hours	
How many employees can not work when the system is unavailable	1%	10%	50%	
To what extent can unavailability lead to injuries	None	Serious injuries	Loss of life	PAPER FILES
<b>Result</b>	<b>Low</b>	<b>Medium</b>	<b>High</b>	Acceptable downtime
		X		1 DAY.

### Baselines

- Selecting 'appropriate' ISO 27002 controls and underlying guidelines based on a 'common sense' risk analysis.
- Clustering them into procedures and handbooks
- ISO 27002 is technology neutral, so adopting technical baselines (e.g., on Windows, Linux, Cisco) is important too from a pragmatic perspective
- Finding the right balance between cost and effectiveness in selecting baselines is challenging.
- The baselines are documented as part of the ISMS.
- The security controls enforced to you by either **law** or **contract** must be part of the baselines

#### 2.2.4 Step 4b: Perform risk assessments and treatments (RATs)

- The risk assessments and treatments are documented as part of the ISMS.
- In our setup the risk assessments and treatment need to be performed on information systems.
- The owner of the information system is responsible for conducting the risk assessment and to implement the additional controls
- In practice the system owner is assisted by the security officer.
- We focus on risk assessments and treatments in the next class

### 2.2.5 Step 5: Implement the security baselines and controls from RATs

### 2.2.6 Step 6a: Perform effectiveness measurements

H	ISO 27002	Measurement example
5	Security Policy	% of people that are aware of it
6	Organization of Information Security	# incidents w.r.t. responsibility allocation
7	Asset Management	% of system components in CMDB % of systems w. allocated responsibility
8	Human resources security	# of staff violations
9	Physical and Environmental Security	% of staff wearing badges # of unattended visitors.
10	Communications and Operations Management	# of unsuccessful backups # lost backup media # successful virus attacks
11	Access Control	% of easily guessed passwords
12	Information Systems Acquisition, Development and Maintenance	# new systems without risk assessment # security incidents with new systems
13	Information Security Incident Management	% of security incidents reported # of repeated security incidents
14	Business Continuity Management	# of downtime incidents not consistent with service level agreements
15	Compliance	# of complaints

### 2.2.7 Step 6b: Perform an internal audit

- As part of the ISMS it is documented how the internal audits need to be conducted.
- Important general topics in audits are
  - Scope of the audits
  - Depth of the audits (only documentation or also detailed inspections)
  - impartiality requirements of auditors
  - providing auditees the opportunity to respond to findings ('hoor en wederhoor')
  - ethics, e.g., 'do not audit your own work'
  - quality, e.g. filing of evidence

### 2.2.8 Step 7: Have a management review

- The management review takes place at least annually.
- It is the place where the management is informed on the state of the ISMS and its opportunity to be in control of information security

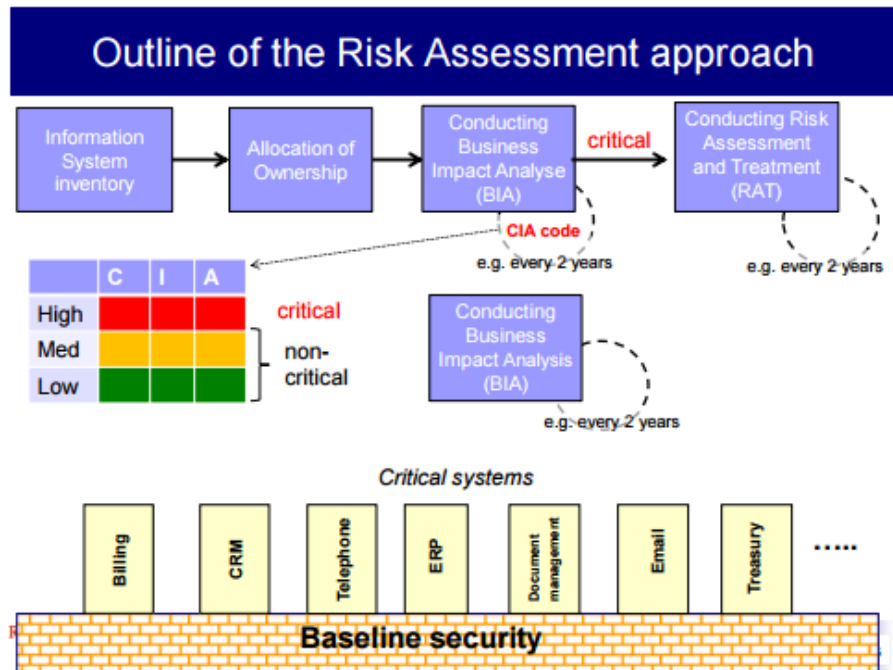
## Topics in a management review (input)

1. Results of control effectiveness measurements
2. Results of external security reviews (e.g., external auditors, accountants)
3. Results of internal security reviews
4. Feedback and complaints of interested parties (e.g., clients)
5. Changes affecting information security (e.g., organization, contractual or legal conditions)
6. Status of corrective actions (results of earlier reviews)
7. Results of information security programs (including status of conducted risk assessments)
8. Reported information security incidents and trends
9. Recommendations done by the authorities
10. Information security trends in general
11. ...

## Possible management review actions (output)

1. Revision of information security policies
2. Revision of the information security framework (including risk assessment and -treatment methodology)
3. Revision of budget and / or responsibilities
4. Initiation of new information security programs
5. ...

### 3 Information Security Risk Assessments (ISO 27005)



#### 3.1 Risk assessment and treatment (RAT) process

- The purpose is to identify serious potential security incidents before they actually (can) occur.
- Identifying security incidents that have never occurred before at your or other organizations are usually difficult to identify
- v But, security incidents that have occurred elsewhere and that have been published can typically be identified. And as an organization it will be difficult to explain why you haven't learned from when they do occur.

**Information Security:** Preservation of confidentiality, integrity and availability of information (ISO).

**Alternative definition:** Adequately protecting the confidentiality, integrity and availability of information against possible security incidents.

**Security Incident:** Based on a manifestation of **Threat** (= who or what) and **Vulnerability** (= how).

**Difference between a threat and a vulnerability is that a vulnerability can be treated (mitigated) while a threat cannot.**

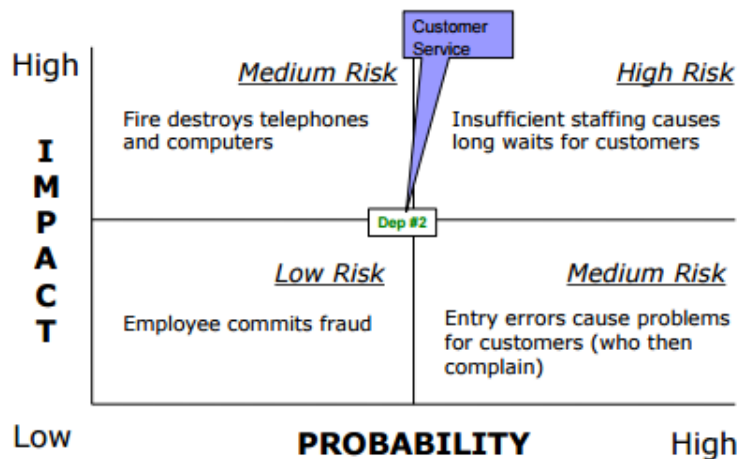
### **3.2 ISO27001 requirements on RAT process**

- **Define** the risk assessment approach of the organization.
  - Identify a risk assessment methodology that is suited to the ISMS, and the identified business information security, legal and regulatory requirements.
  - Develop criteria for accepting risks and identify the acceptable levels of risk. (Note: aka 'risk appetite')
  - **There should be a documented methodology, risk appetite should be determined.**
- **Identify** the risks.
  - Identify the **assets** within the scope of the ISMS, and the owners of these assets.
  - Identify the **threats** to those assets
  - Identify the **vulnerabilities** that might be exploited by the threats.
  - Identify the **impacts** that losses of confidentiality, integrity and availability may have on the assets.
  - **The methodology should involve assets, threats, vulnerabilities and impacts.**
- **Analyze** and **evaluate** the risks.
  - Assess the business **impacts** upon the organization that might result from security failures,
  - Assess the realistic **likelihood** of security failures occurring in the light of prevailing threats and vulnerabilities, and impacts associated with these assets, and the controls currently implemented.
  - **Estimate** the **levels** of risks.
  - Determine whether the risks are **acceptable** or require treatment using the criteria for accepting risks
  - **Prioritize risks and determine which need treatment:**
    - **RISK = IMPACT X LIKELIHOOD**
- **Identify** and **evaluate** options for the treatment of risks
  - Applying controls, accepting risks, avoiding risks, transferring risks to other parties
- **Select control objectives** and controls for the treatment of risks
- **Obtain management approval** of the proposed residual risks

- Either accept, avoid, transfer risks or select controls.

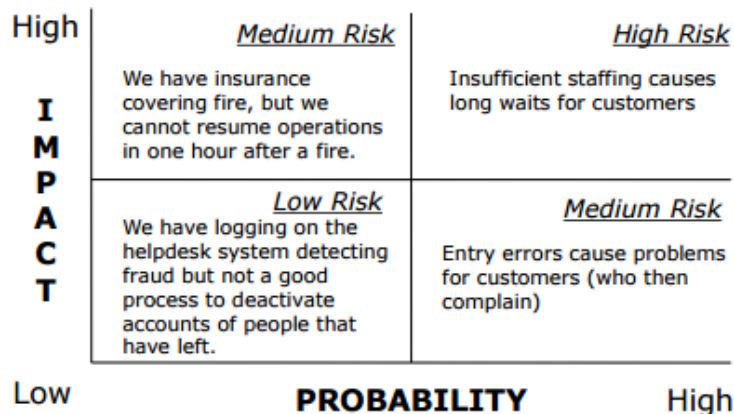
## Example: Risk Assessment

### ■ Without baselines






## Example: Risk Assessment

### ■ With baselines



## Example: Risk Response

		<u>Medium Risk</u>	<u>High Risk</u>
<b>I M P A C T</b>	High	Have a contract with an external helpdesk to take over in one hour when there is a fire. <b>Transfer</b>	Customer has a long wait -hire enough people -freebees for long waits <b>Control</b>
	Low	Fraud ignore <b>Accept</b>	Entry errors input validation <b>Control</b>
		<u>Low Risk</u>	<u>Medium Risk</u>
		Low	High
		<b>PROBABILITY</b>	

### 3.3 ISO27005 RAT process

1. Context establishment
  - a. Determine legal requirements
  - b. Determine scope and boundaries (eg. Business process lifecycle, Information system lifecycle)
  - c. Determine dependencies with other 'systems'.
2. Risk assessment
  - a. Identify assets (= familiarize with system)
  - b. Identify threats
  - c. Relate actual security incidents
  - d. Identify vulnerabilities
  - e. Relate existing controls (baselines in our setting)
  - f. Determine consequences (potential incidents)
3. Risk estimation/evaluation
  - a. Prioritize risks (potential incidents)
  - b. Determine the 'real' risks

- c. Estimation could be qualitative or quantitative (e.g. based on historic data). In practice one uses qualitative estimations.

4. Risk treatment

- a. Risks can be treated with controls
- b. Risks can be accepted
- c. Risks can be avoided
- d. Risks can be transferred

Typically combinations are used in practice, e.g., first accept a risk but gradually implement controls mitigating it.

5. Risk acceptance

- a. After risk treatment a risk revaluation should be performed.
- b. Risk acceptance criteria should be formalized.
- c. Risk treatment (residual risks) must be accepted by management.

6. Documentation/communication

7. Risk monitoring



		Likelihood of risk path				
		Very unlikely (1)	Unlikely (2)	Possible (3)	Likely (4)	Frequent (5)
Impact	Very Low (1)	1	2	3	4	5
	Low (2)	2	4	6	8	10
	Medium (3)	3	6	9	12	15
	High (4)	4	8	12	16	20
	Very High (5)	5	10	15	20	25

Orange = risk appetite border

## NEN 7512 Risk assessment

	Low Risk	Medium Risk	High Risk	Very high Risk
Person registration	Self proclaimed	Register verification	face2face	face2face
System registration	Self proclaimed	Register verification	Register verification	Register verification
Authentication	Password	Password+ Token Biometrics	Token+ Biometrics+	Token+ Biometrics+
Signature	Electronic	Advanced	Advanced	Qualified (using 'smartcard')
Encryption	none	SSL / TLS	Secure messaging	Secure messaging

## 4 Information Security Policies

### Guidance

- Definition of information security
- Management intent and support
- Framework for implementing IS

- General principles to follow (e.g., legal, awareness, BCP, security incidents)
- Roles and responsibilities • References to documentation

#### Guidance on input

- Feedback from interested parties
- Results from (independent) reviews
- Status of preventive and corrective actions
- Results of previous management reviews
- Changes that could affect the organization's IS approach
- Trends related to threats and vulnerabilities
- Reported information security incidents
- Recommendations provided by relevant authorities

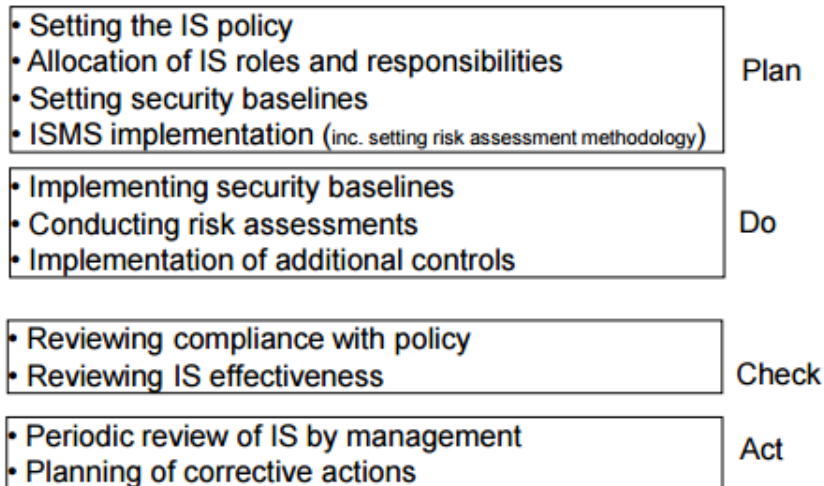
#### Guiden on output

- Improvement of the organization's approach to managing information security and its processes
- Improvement of control objectives and controls
- Improvement in the allocation of resources and responsibilities.

#### An information security policy document includes:

- Strategic principles and conditions on IS
- Description of the IS organization including responsibilities
- IS baselines
- Frequency of IS policy review
- Descriptions on how security awareness is increased

## The IS process/framework in helicopter view



### 4.1 Distinguished IS roles within an organization

- Senior Management
- Security officers
- Supporting internal / external services
- Line management (system owners)
- Internal / external auditors
- IS projects
- Employees of the organization

### 4.2 Senior Management

- What:
  - Giving commitment on information security
  - Approval of IS policy
  - Bootstrapping the ISMS (appointing security officer)
  - Providing resources and budget
  - Management of serious security incidents

- Periodic review of IS ('Act'), including adjusting the IS policy
  - Sponsoring of IS projects
- Reports to:
  - Stakeholders
  - Supervisory board ('Raad van commissarissen')
  - Regulators (Examples ?)

#### 4.3 Security Officers

- What:
  - IS center point; sits between senior management and the organization
  - Drafting / revising information security policy/plans including security baselines (but not the approval!)
  - Providing specific guidelines on information security
  - Daily supervision on information security
  - Security incident handling
  - Progress control on IS including IS projects
  - Initiation of IS projects
  - Arranging the periodic management review
  - **Not responsible for Information Security!**
- Reports to:
  - Senior management

#### 4.4 Supporting internal / external services

- What:
  - IT department (!), facility department, HR, legal department etc.
  - employment agencies, contractors, couriers, security guards
  - Compare the ISO 27002 chapters
  - Implementing security baselines
  - Implementing specific additional security controls arising from risk assessments
- Reports to:
  - Security office on progress
  - 'Clients' (=line management)

#### 4.5 Line management (system owners)

- What:
  - Conducting risk assessments on their systems
  - Implementing security (baselines, additional controls)

- Agreements with internal / external parties on security, e.g. as arising from risk assessments
  - Supervision on information security, e.g. talking to noncompliant employees, addressing security in job evaluation conversations.
  - **And of course: giving the right example!**
- Reports to:
    - Security Office on progress

#### 4.6 Internal / external auditors

- What:
  - Conducting audits on compliance with IS policies
  - Can be done by separate department, external parties or can take the form of 'peer review'.
  - Conducting audits on ISMS:
    - are all parties doing the things they should do?
    - is the ISMS effective?
  - Conducting specific audits, e.g., compliance with baselines
  - Independence is important
- Reports to:
  - Senior Management

#### 4.7 IS Projects

- What:
  - Implementation of specific security (e.g. PKI, IDS, IAM)
- Reports to:
  - Project / Program leaders
  - Security office

#### 4.8 Employees of the organization

- What:
  - Adhering to security baselines and specific controls arising from risk assessments
  - Reporting security incidents
- Reports to:
  - Security office
  - Line management

## 5 Incident Response

### 5.1 Prevention

- Secure your infrastructure
  - Network
    - Keep components up-to-date
    - Know the traffic patterns
    - Use network-detection
    - Keep logs
    - Find your weak spots (pentests/redteams/hacking)
  - Systems
    - Keep operating systems up-to-date
    - Keep logs
  - Applications
    - Keep applications up-to-date
    - Use access-control
- Secure your people
  - Be clear on what can be done and what not
    - On systems
    - On the Internet
    - On social media
  - Make them aware of:
    - Phishing mails and sites
    - Social engineering
    - Computer-use and software policy

### 5.2 Preparation

- Know your organization
  - Have critical services defined
  - Know the service-owners
  - Have critical systems defined
  - Know the system-owners
  - What is important for these systems
    - Confidentiality/Integrity/Availability
  - Have up-to-date phone-lists available
    - Anyone and everyone you might need
  - Become good friends with your legal department
- Know your infrastructure

- Network
  - Know the topology (and keep drawings up-to-date)
  - Know the traffic-patterns
  - Know where to get the information you need
  - Detect anomalies (Unexpected traffic, networkscans)
- Systems
  - Know which systems connect to which systems
  - Know what should run on which systems
- Applications
  - Know what each of your applications does
  - Know who has which permissions on which applications
  - Detect anomalies
- Build a security team/fire department to deal with incidents
  - Form your team
  - Train your team
  - Learn from others
  - Establish a workflow
  - Enable secure communications
- Get to know the people you might need
  - Establish relationship with 3rd parties
    - Software-vendors
    - Serviceproviders
    - ISP/Telco and/or other suppliers
    - Security guards

### 5.3 Detection

- You will get hacked
  - In many cases, criminals (or others) will already be in your network
  - The level of damage that has been done varies
    - It could be a simple backing trojan
    - But it might also be state sponsored espionage
- The trick is to detect anomalies that might indicate a 'hack' as early as possible
  - To be able to minimize the damage caused
  - To keep your business running
- Many advanced attackers go undetected for months
  - Lack of detection capabilities
- Implement intrusion detection systems on your network

- Deploy malware detection (AV)
- Detect anomalies
  - Failed logon attempts
  - Increase in traffic or scans
  - Deploy honeypots
- Train your staff in detecting anomalies
  - Not only IT and security staff: the whole organization
- Follow the news to identify new threats
- Detection: Enrichment and sharing (STIX)
  - Standardised and structured way of specifying threat information
  - Allows documenting and sharing of this information
  - Types of information
    - Indicators (of Compromise)
    - Targets (vulnerabilities, systems)
    - Tactics and techniques
    - Actors
    - Course of action (response)

#### **5.4 Triage, Isolation**

#### **5.5 Eradication**

##### **Incident response vs Evidence collection**

Main goal of incident response: keeping your business running

- Getting rid of the badness
- While minimizing damage
- And minimizing downtime

Evidence collection might conflict with this goal

- Case-by-case decision if you want to delay incident response

These days incident response is hard without live forensics

- 8TB hard drives
- Malware sometimes only in memory
- Many systems on different locations
- Encrypted hard drives

Making images of hard drives just takes too long, but:

- Leave the 'crimescene' as intact as possible
- Coordinate with the authorities
- Document your actions



## 5.6 Recovery, Evaluation

# 6 Business Continuity Management

- Business Continuity Management (BCM) provides a framework for building organizational resilience
- BCM increases the capability of an organization to respond to disruptions / crisis events in an effective way, to safeguard the interests of its key stakeholders, reputation and value-creating activities.
- BCM is all about planning ahead, when there is time to consider rationally

### Why BCM

- Surviving / Maintain reputation (awareness of not being prepared)
- Societal responsibility (critical infrastructure)
- Good governance / compliance
- Increased probability of disasters / disruptions (cybercrime / global changes in climate and stability / higher dependencies on IT and energy)
- Increased impact of disruption (complex dependencies and interrelations: IT / suppliers / energy / just in time delivery)
- Accountants / regulators / supervisors / government / insurers
- Clients (contractual obligations / snowball effect)
- Marketing / competitive advantage (certified in BCM)

## 6.1 How to implement BCM according to ISO22301

- **Plan:** Establish business continuity policy, objectives, targets, controls, processes and procedures relevant to improving business continuity
  - Context of the organization
    - Understanding of the organization and its context
    - Understanding the needs and expectations of interested parties
    - Determining the scope of the BCMS
  - Leadership
    - Management commitment (not only words but also actions)
    - Organizational roles, responsibilities and authorities
  - Planning
    - Actions to address risks and opportunities
    - Business continuity policy & objectives and plans to achieve them
  - Support
    - Resources, competences, awareness
- **Do:** Implement and operate the business continuity policy, controls, processes and procedures

- Operational planning and control
  - Implement business continuity controls and document effectiveness
- Risk Assessment
- Business Impact Analysis (BIA)
  - Activities necessary for products/services
  - Identification of dependencies and necessary resources
  - Impact of disruption during X hours / days
  - Maximum tolerable outage
  - Recovery priorities
- Criticality assessment, resource requirements, impacts and trends
- Business Continuity Strategy
  - Determine and select
  - Establish resource requirements
  - Protection and mitigation
- Establish and implement business continuity measures and procedures
  - Incident response structure
  - Warning and communication
  - Business continuity plans
  - Recovery
- Exercising and testing
- **Check:** Monitor and review performance of business continuity arrangement
  - Monitoring and evaluation / internal audit
    - Evaluation of continuity procedures
    - Determine compliance with ISO and own BCM requirements
    - Determine effectiveness of management system
    - Recording of evidence
  - Management review
    - Status of improvement actions from previous reviews, audits
    - Changes in internal/external environment that are relevant for the BCMS
    - Trends in business continuity performance
    - Opportunities for continuous improvement
- **Act:** Maintain and improve the Business Continuity Management System (BCMS) by taking corrective action and reappraising the scope of the BCMS and business continuity policy and objectives
  - Nonconformity and corrective action
    - Identify nonconformities and causes
    - Determine and implement improvements
    - Review effectiveness of corrective reaction
  - Continual improvement
    - BCM is not a project with an end delivery date, but a continuous process
    - BCM must be integrated in normal day-to-day business operations.

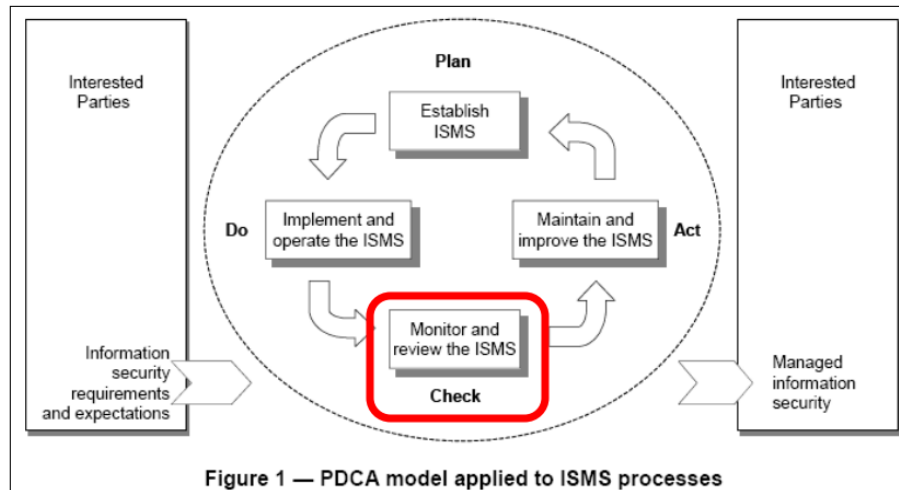
- Continually improve the suitability, adequacy and effectiveness of the business continuity management system.

## **6.2 Crisis Response Procedure**

- Alert phase
  - Monitoring firewalls, intrusion detection systems, antivirus software, etc.
  - Report (potential) incidents to Security Officer / Crisis Manager
- Triage phase
  - Gather information about malicious activity (what systems are targeted? is incident inside trusted network?)
  - Determine priority level (Is response urgent? Will response alert the attacker and to we care?)
- Response phase
  - Take control of situation & contain incident (prevent further intrusion, isolate infected systems, change settings, block ports / connections, scale up resources, activate continuity arrangements)
  - Notify appropriate stakeholders (staff, agencies, public)
- Recovery phase
  - Preserve evidence against intruder (back-up logs)
  - Restore and validate system (determine which systems first)
  - Monitor to verify normal operations without further system or data compromise
- Follow-up phase
  - Evaluate incident and assess damage (what was discovered)
  - Identify lessons learned and determine improvement actions
  - Take corrective actions (updating security settings, change response procedures, additional awareness trainings, etc.)
  - Inform appropriate stakeholders

## **7 Information Security Audits & Certification**

### **Audit Context**



### Terminology

- An audit is the process in which an competent, **impartial** judgment ('opinion') is formed on one or more aspects of an object ('criteria').
- The result of an audit is typically a **document** in which the auditor expresses his opinion, the supporting findings and the limitations that apply
- The opinion provides **assurance** to the auditee itself or to a third party
- The assurance type can be either positive or negative:
  - **Positive assurance** - An affirmative statement or opinion given by the auditor, generally based on a high level of work performed. 'Our opinion is that the organization is compliant with ...'
  - **Negative assurance** - A statement indicating that nothing came to the auditor's attention indicating that the subject matter in question did not meet a specified criteria. 'We have seen no indications that the organization is not compliant with ...'
- The audit process should be **reproducible** and should not depend on the (qualified) auditor
- An opinion can also take the form of a 'certificate'.
- Audits are historically associated with (financial) accounting: a financial audit of the financial accounts ('jaarrekening audit') performed by (registered) accountants. In this situation the criteria are based on the laws on accounting (e.g., 'Wet op de jaarrekening'). In the context of accounting the term 'audit' is a very sensitive term.
- The audit is performed for a client, that also sponsors the audit
- The aspects that form the basis of the audit are formulated as a set of criteria (audit criteria), determined prior to the actual audit and agreed upon with the client. In Dutch these criteria are sometimes called 'de gehanteerde (audit) norm'

- The set of criteria could be an open standard, a tailored version of it, or even some assertions made by the client management. In the latter case, the opinion can be a statement of the auditor that the assertions are correct
- The object type can vary, examples are: a person, a product, a process, a system or an organization
  - Is there a potential issue with criteria formulated by the client itself?
  - Often the sponsor is also the organization being audited. Is there a potential issue with that?

### Audit Schemes

- Closely linked with the audit criteria is the audit scheme used. These are rules describing how the audits shall be conducted and what requirements should be met by the auditor organization itself
- An audit scheme provides a ‘manual’ for conducting audits and typically answers questions like:
  - What steps shall an audit have?
  - When is a criterion met (‘audit depth’ see further on)?
  - What qualifications should an auditor have?
  - When can the auditor ‘built’ on prior work done by other auditors?
  - When can an opinion be provided and what can be part of it?
- Important general topics in audit schemes are:
  - impartiality requirements of auditors and the organizations they work for,
  - confidentiality
  - providing auditees the opportunity to respond to findings (‘hoor en wederhoor’)
  - ethics, e.g., ‘do not audit your own work’,
  - quality, e.g. filing of evidence

## 7.1 IT Security Audits in General

- IT security audits (aka IT security reviews) concentrate on information security aspects, i.e.:
  - Confidentiality
  - Integrity
  - Availability
- Sometimes IT security audits are called IT security reviews to prevent confusion with financial audits.
- IT security audits can be:
  - **technically** oriented; then the objects are IT systems, e.g., a whole IT infrastructure, a network, a Windows environment, a specific application

- **process** oriented; then the objects are IT processes, e.g., a security management process, a change management process.

#### **The three audit assurance levels**

- **Design** ('Opzet' in Dutch) The auditor has reviewed the relevant design based on documentation and interviews but not on actual inspections. In effect, the auditor can not provide assurance the design is actually implemented.
- **Existence** ('Bestaan' in Dutch) The auditor has additionally performed inspections of system settings, paper archives and other things providing him with assurance that the design is at least implemented during the audit.
- **Operational Effectiveness** (OE; 'Werking' in Dutch) The auditor has additionally looked for evidence that the implemented controls were effective over a certain amount of time.

#### **The Opinion**

It is vital that the opinion minimally states:

- For who the audit was conducted (client) by whom (auditor/auditor organization)
- The objective of the audit
- The object and its boundaries
- The period in which the audit was performed
- The followed procedures, e.g., documentation review, interviews, inspections etc.
- The audit criteria used and the related audit scheme
- The assurance level of the audit ('design', 'existence' or 'operational effectiveness')
- The opinion itself and any reservations or limitations regarding the opinion (e.g. its use).
- Optionally one can supplement the opinion with recommendations however some schemes preclude that on grounds of impartiality

### **7.2 Management System Certification Audits**

- A management system is framework of policies, procedures guidelines and associated resources to achieve the objectives of the organization. (source: ISO 27000)
- An Information Security Management System (ISMS) is that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. (source: ISO 27001)
- Certification of a management system, such as a quality or environmental management system of an organization, is one means of providing assurance

that the organization has implemented a system for the management of the relevant aspects of its activities, in line with its policy. (source: ISO 17021).

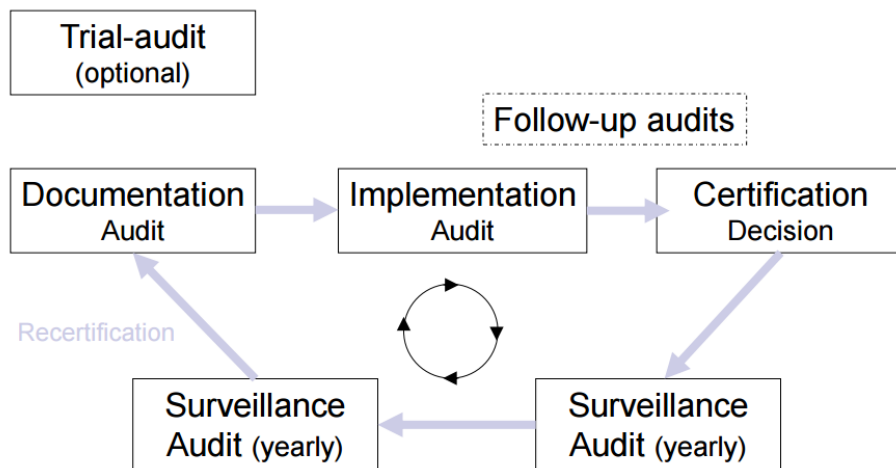
### Limitation

We limit our selves to these two IT security (management) systems:

- ISO 27001 'Information security management systems' which we have focused on in the first three lectures
- TTP.NL which relates to the European guideline on electronic signatures

### Accreditation

Management system auditors are called Certification Bodies and they need to implement a (quality) management system too. A certificate is valid for three years.



### Audit Plan

- For each type of audit, the audit organisation makes an audit plan prior to conducting it
- The audit plan describes:
  - the timing of the audit, including opening and closing meeting
  - the topics of the audit (preferably in reference with the criteria)
  - the staff (internal/external) that needs to be interviewed (when/where)
  - any visits or inspections (in implementation and surveillance audits)
- The audit plan is interactively compiled with the client, typically through email / telephone

### 7.3 IT security product certification audits ('common criteria')

- According to some TCSEC is too hard and ITSEC is too soft
- The CC are published as ISO standards (ISO/IEC 15408):
  - Part 1: Introduction and general model

- Part 2: Security functional requirements
- Part 3: Security assurance requirements
- The guidelines for the CC evaluators (Methodology for IT security evaluation) is also published as an ISO standard (ISO 18045)

### **Protection Profile**

Typically a 'user community' compiles a Protection Profile (PP) for a TOE (Target of Evaluation) type, e.g., a firewall or a smartcard application (e.g., an SSCD).

A PP defines an implementation-independent set of IT security requirements for a category of TOEs which are intended to meet common consumer needs for IT security.

A PP contains:

- The TOE description
- The TOE environment (including threats)
- Security Functional Requirements (SFRs) as specified in CC-part2
- Security Assurance Requirements (SARs) as specified in CC-part3
- Security Requirements for the IT Environment
- Security Requirements for the non-IT Environment
- A rationale

Additional SFRs and SARs can be formulated.

### **Security Targets**

In some cases the Protection Profiles contains more SARs than necessary for a certain EAL level. In that case one uses the term 'augmented'. So EAL 4 augmented (or EAL4+) means all SARs required in EAL 4 plus some additional ones.

When creating a product in compliance with a PP, the manufacturer creates a Security Target for its product. The manufacturer refers to the PP.

In the evaluation process the product (TOE) is evaluated against the SFRs by the evaluator ('laboratory') in accordance with the SARs.

The evaluator uses ISO 18045.