Computer Security

Security management

Prof. Jean-Noël Colin
jean-noel.colin@unamur.be
Office #306

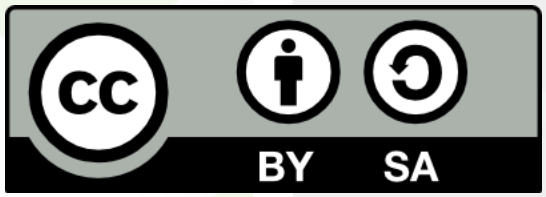
University of Namur
Computer Science Faculty

UNIVERSITÉ DE NAMUR

www.unamur.be

Agenda

- Security management process
  - Introduction
  - Managing security with ISO 27001 & ISO 27003
  - Securing the IS with ISO 27002
  - Managing risks with ISO 27005
  - Attack trees



A risk-based approach

- Motivations
  - understand
  - identify
  - evaluate
  - decide
  - plan
  - prioritize
  - react
  - communicate
  - establish and maintain a knowledge base

A structured approach

- Why a structured approach?
  - to define a common vocabulary
  - to define a clear end structured process
  - to help make the analysis as exhaustive as possible
  - to build and improve a knowledge base
  - to ensure a continuous application
  - to improve the process itself

Overall process

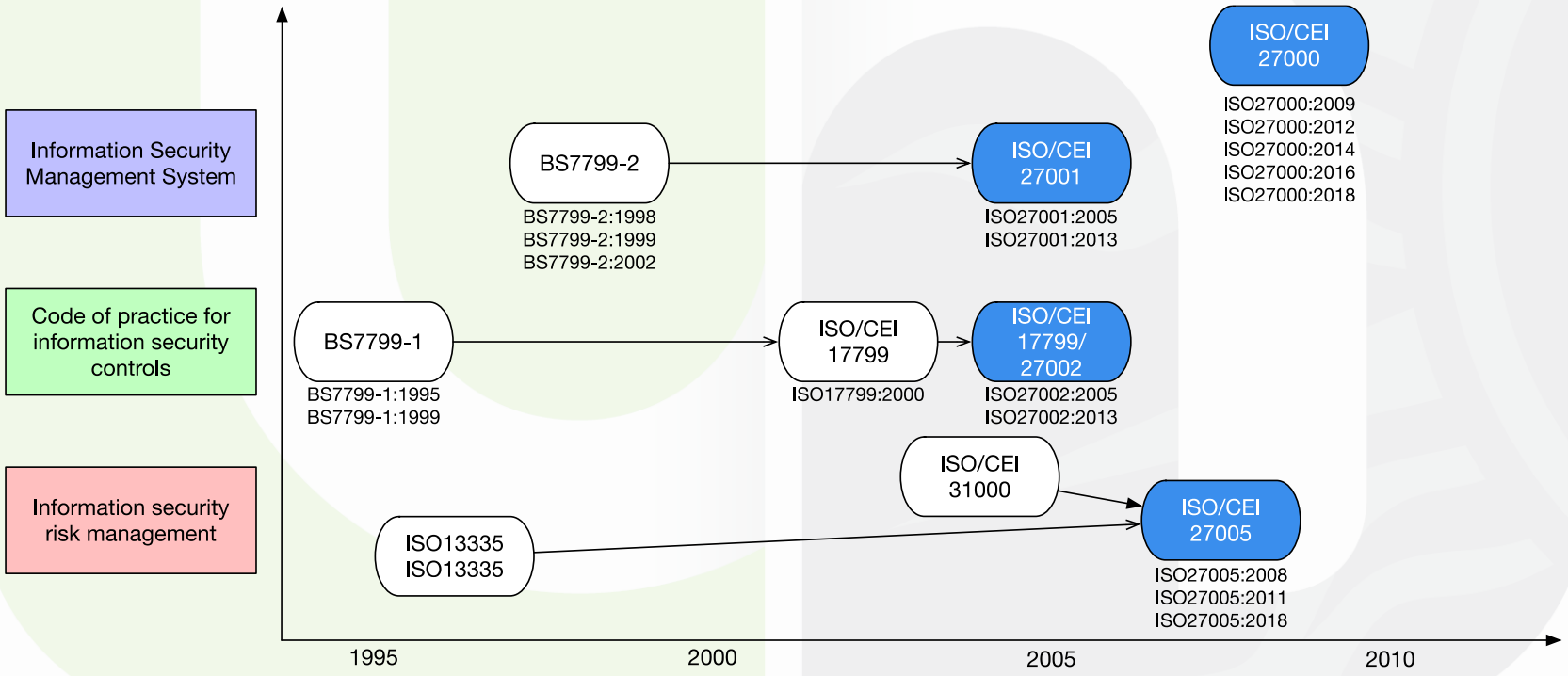
- Risk management is
  - iterative
    - Periodically re-evaluate the system, the environment and past choices
  - recursive
    - From system to component
  - supported by many methods
    - Different levels of complexity and application contexts
    - Octave, CRAMM, EBIOS, Mehari. . .

ISO 27000… an overview

- ISO: International Organization for Standardization
- [Standard] « document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context »
- [Requirement] « expression, in the content of a document, that conveys **objectively verifiable criteria** to be fulfilled and from which no deviation is permitted if conformance with the document is to be claimed »
- [Recommendation] « expression, in the content of a document, that conveys a suggested possible **choice or course of action deemed to be particularly suitable without necessarily mentioning or excluding others »**
- [Statement] « expression, in the content of a document, that conveys information »

Source: ISO/IEC Directives, Part 2 Principles and rules for the structure and drafting of ISO and IEC documents

A long evolution process



ISO 27000 Family

number	type	published	title
27000	**V**	**2018**	**Information security management systems – Overview and vocabulary**
27001	**R**	**2013**	**Information security management systems – Requirements**
27002	**G**	**2013**	**Code of practice for information security controls**
27003	G	2017	Information security management – Guidance
27004	G	2016	Information security management – Monitoring, measurement, analysis and evaluation
27005	**G**	**2018**	**Information security risk management**
27006	R	2015	Requirements for bodies providing audit and certification of information security management systems

V: Vocabulary
G: Guidelines
R: Requirements
SG: Sector-specific Guidelines

ISO 27000 Family

number	type	published	title
27007	G	2017	Guidelines for information security management systems auditing
27008 (TR)	G	2019	Guidelines for the assessment of information security controls
27009	R	2016	Information security, cybersecurity and privacy protection — Sector-specific application of ISO/IEC 27001 — Requirements
27010	SG	2015	Information security management for inter-sector and inter-organizational communications
27011	SG	2016	Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations
27013	G	2015	Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
27014	G	2013	Governance of information security
27016	G	2014	Information security management — Organizational economics

V: Vocabulary
G: Guidelines
R: Requirements
SG: Sector-specific Guidelines

ISO 27000 Family

number	type	published	title
27017	SG	2015	Code of practice for information security controls based on ISO/IEC 27002 for cloud services
27018	SG	2019	Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
27019	SG	2017	Information security controls for the energy utility industry
27021	G	2017	Competence requirements for information security management systems professionals
2703x, 2704x			Guidelines specific to a security control. Ex: 27039: IDPS, 27035: incident management, 27033: network incidents
27701	R/G	2019	Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
numerous other documents in preparation			

V: Vocabulary
G: Guidelines

R: Requirements
SG: Sector-specific Guidelines

ISO 27000 Family

- The Belgian Bureau for Normalization gives access to ISO standards for free to UNamur users (staff and students)

https://edu.mynbn.be

- Some documents are made available directly from ISO

https://www.iso.org/obp

- Other interesting resource

https://www.iso27001security.com

ISO27001:2013

- Definitions and vocabulary
  - [Asset] any element of value to the organization
  - [Vulnerability] weakness of an asset or control that can be exploited by one or more threats
  - [Threat] potential cause of an unwanted incident which may result in harm to a system or organization
  - [Consequence] outcome of an event affecting objectives

ISO27001:2013

- Definitions and vocabulary
  - [Risk] effect of uncertainty on objectives
    - Risk = Vulnerability * Threat * Consequence
  - [Risk identification] process of finding, recognizing and describing risks
  - [Risk analysis] process to comprehend the nature of risks and to determine the level of risks
  - [Risk evaluation] process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable
  - [Risk assessment] overall process of risk identification, risk analysis and risk evaluation

Managing security with ISO 27001

ISO27001:2013

- A Management System includes the following key components
  - Policy
  - Persons with defined responsibilities
  - Management processes related to
    - Policy establishment
    - Awareness and competence provision
    - Planning
    - Implementation
    - Operation
    - Performance assessment
    - Management review
    - Improvement
  - Documented information

ISO27001:2013

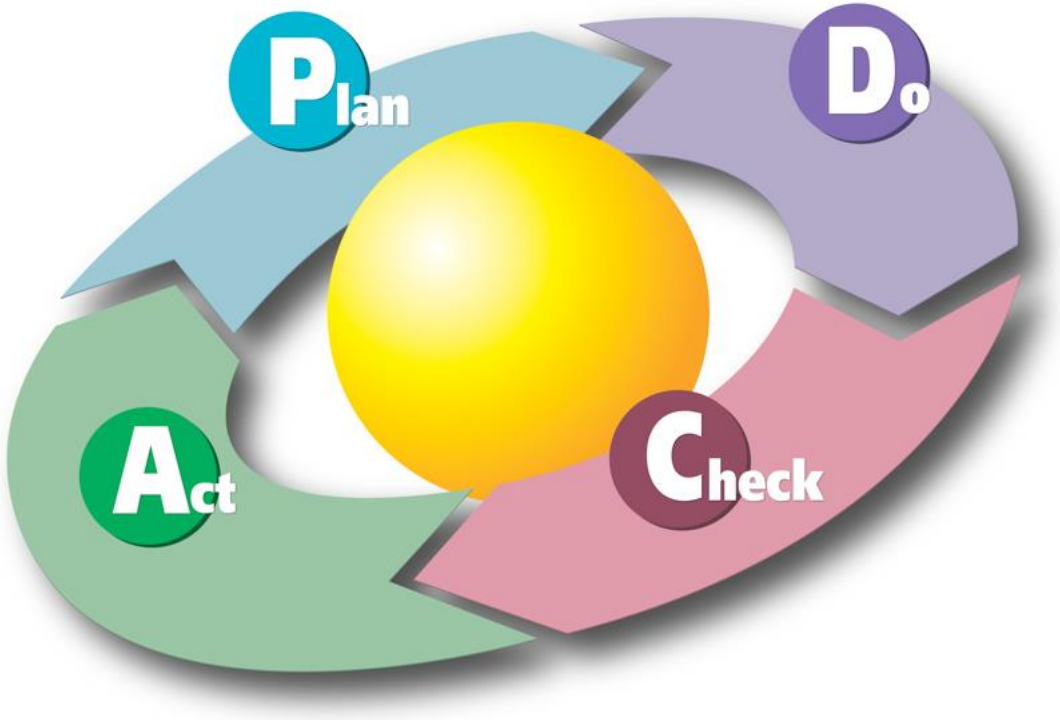
- What is an ISMS?
  - « *The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed* »
  - An ISMS is a Management System that includes information security risk assessment and risk treatment

ISO27001:2013

- Principles of ISO 27001
  - *ISO 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system in the context of the organization*
  - *ISO 27001 also includes the requirements for the assessment and treatment of information security risks tailored to the needs of the organization*
  - *Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this International Standard*

ISO27001:2013

- Deming's wheel: continuous improvement



ISO27001:2013

Clause		Plan	Do	Check	Act
4	Context of the organization	X			
5	Leadership	X			
6	Planning	X			
7	Support	X	X	X	X
8	Operation		X		
9	Performance evaluation			X	
10	Improvement				X

7 Clauses of ISO 27001:2013 and their relationship to Deming's wheel

ISO27001:2013

- Clause 4: Context of the organization
  - Understanding the organization and its context

    "The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its ISMS "
  - Understanding the needs and expectations of interested parties

    "The organization shall determine the interested parties that are relevant to the ISMS and their requirements relevant to information security "
  - Determining the scope of the information security management system

    "The organization shall determine the boundaries and applicability of the ISMS to establish its scope, considering the external and internal issues, the requirements, and the interfaces and dependencies between activities performed by the organization and those that are performed by other organizations "
  - Information security management system

    "The organization shall establish, implement, maintain and continually improve an ISMS, in accordance with the requirements of this International Standard"

ISO27001:2013

- Clause 5: Leadership
  - Leadership and commitment
    - *"top management shall demonstrate leadership and commitment with respect to the ISMS*
      - *defining objectives aligned with organization strategy*
      - *committing appropriate level of resources*
      - *promoting continual improvement*
      - *directing and supporting persons"*

ISO27001:2013

- Clause 5: Leadership
  - Policy
    - *“top management shall establish an information security policy”*
    - *“policy shall be appropriate to the purpose of the organization, including the relevant security objectives, and a commitment to satisfy the requirements and to continual improvement of the ISMS”*
    - *“the policy shall be made available and communicated”*

ISO27001:2013

- Clause 5: Leadership
  - Organizational roles, responsibilities and authorities
    - *“top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated”*
    - *“roles include*
      - *(a) ensuring that the ISMS conforms to the requirements of the standard and*
      - *(b) reporting on the performance of the ISMS to top management”*

ISO27001:2013

- Clause 6: Planning
  - Actions to address risks and opportunities
    - *“the organization shall determine the risks and opportunities that need to be addressed, define and apply a risk assessment process together with a risk treatment process”*
    - *“assessment results should be consistent, valid and comparable”*
    - *“the Statement of Applicability contains the list of necessary controls and justification for inclusions, whether they are implemented or not, and the justification for exclusions”*

ISO27001:2013

- Clause 6: Planning
  - Information security objectives and planning to achieve them
    - *“the organization shall establish information security objectives at relevant functions and levels”*
    - *“objectives result from the risk assessment”*
    - *“planning information must include the action, the resources, timing, responsibility, evaluation process”*

ISO27001:2013

- Clause 7: Support
  - Resources, competences, awareness
    - *“the organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the ISMS”*
    - *“determine, assign, develop, retain competences”*
    - *“ensure awareness”*
  - Communication
    - “the organization shall determine the need for internal and external communication”
    - “what, when, with whom, who?”

ISO27001:2013

- Clause 7: Support
  - Documented information
    - *“ISMS shall be documented”*
    - *“using appropriate format, review process, identification and description of document (author, version)”*
    - *“availability”*
    - *“documentation shall be adequately protected”*

ISO27001:2013

- Clause 8: Operation
  - Operational planning and control
    - *“the organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions to meet information security objectives”*
    - *“proper documentation shall be maintained and a review of the planned changes shall be organized”*
  - Information security risk assessment
    - *“the organization shall perform information security risk assessments at planned intervals or when significant changes occur or are proposed”*
  - Information security risk treatment
    - *“the organization shall implement the risk treatment plan”*

ISO27001:2013

- Clause 9: Performance evaluation
  - Monitoring, measurement, analysis and evaluation
    - *"the organization shall evaluate the information security performance and the effectiveness of the ISMS"*
    - *“identify indicators, monitoring methods, results analysis responsibilities”*
  - Internal audit
    - *"the organization shall conduct internal audits at planned intervals to provide information on whether the ISMS conforms to the organization's own requirements and to this standard's requirements”*
    - *“plan the audit program, identify scope, auditors, document and report audit results to management”*

ISO27001:2013

- Clause 9: Performance evaluation
  - Management review
    - *“top management shall review the organization's ISMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness”*
    - *“review status of actions of past reviews, changes in external and internal issues, feedback on information security performance”*

ISO27001:2013

- Clause 10: Improvement
  - Nonconformity and corrective action
    - *"when a nonconformity occurs, the organization shall react and take action to correct it and deal with the consequences"*
  - Continual improvement
    - *"the organization shall continually improve the suitability, adequacy and effectiveness of the ISMS"*

ISO27001:2013

- Annex A
  - contains a list of reference control objectives and controls directly derived from ISO 27002:2013, clauses 5 to 18
  - to be used in the context of clause 6: Planning
  - inclusions and exclusions need to be properly documented
  - can be completed with additional objectives and controls
- ISO 27003
  - provides guidance on implementing ISO 27001
  - somewhat clarifies the steps by presenting examples
  - annex gives some clue about what a information security policy is, and how to define it

Securing the IS with ISO 27002

ISO 27002:2013

- Code of practice for information security controls
- 14 security control clauses
- each clause contains one or more categories
- each category defines a control objective as well as ine or more controls that can be applied to achieve the objective
- each control is presented with implementation guidelines
- in total: 35 categories and 114 controls, covering the IS security dimension as exhaustively as possible

ISO 27002:2013

Clause
Information security policies
Organization of information security
Human resource security
Asset management
Access control
Cryptography
Physical and environmental security
Operations security
Communications security
System acquisition, development and maintenance
Supplier relationships
Information security incident management
Information security aspects of business continuity management
Compliance

ISO 27002:2013

- 5 Information security policies
  - 5.1 Management direction for information security
  - Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations
    - 5.1.1 Policies for information security
    - 5.1.2 Review of the policies for information security

ISO 27002:2013

- 6 Organization of information security
  - 6.1 Internal organization
  - Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.
    - 6.1.1 Information security roles and responsibilities
    - 6.1.2 Segregation of duties
    - 6.1.3 Contact with authorities
    - 6.1.4 Contact with special interest groups
    - 6.1.5 Information security in project management
  - 6.2 Mobile devices and teleworking
  - Objective: To ensure the security of teleworking and use of mobile devices.
    - 6.2.1 Mobile device policy
    - 6.2.2 Teleworking

ISO 27002:2013

- 7 Human resource security
  - 7.1 Prior to employment
  - Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.
    - 7.1.1 Screening
    - 7.1.2 Terms and conditions of employment
  - 7.2 During employment
  - Objective: To ensure that employees and contractors are aware of and fulfil their informations security responsibilities.
    - 7.2.1 Management responsibilities
    - 7.2.2 Information security awareness, education and training
    - 7.2.3 Disciplinary process
  - 7.3 Termination and change of employment
  - Objective: To protect the organization’s interests as part of the process of changing terminating employment.
    - 7.3.1 Termination or change of employment responsibilities

ISO 27002:2013

- 8 Asset management
  - 8.1 Responsibility for assets
  - Objective: To identify organizational assets and define appropriate protection responsibilities.
    - 8.1.1 Inventory of assets
    - 8.1.2 Ownership of assets
    - 8.1.3 Acceptable use of assets
    - 8.1.4 Return of assets
  - 8.2 Information classification
  - Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.
    - 8.2.1 Classification of information
    - 8.2.2 Labelling of information
    - 8.2.3 Handling of assets

ISO 27002:2013

- 8 Asset management (cont'd)
  - 8.3 Media handling
  - Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.
    - 8.3.1 Management of removable media
    - 8.3.2 Disposal of media
    - 8.3.3 Physical media transfer

ISO 27002:2013

- 9 Access control
  - 9.1 Business requirements of access control
  - Objective: To limit access to information and information processing facilities.
    - 9.1.1 Access control policy
    - 9.1.2 Access to networks and network services
  - 9.2 User access management
  - Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.
    - 9.2.1 User registration an de-registration
    - 9.2.2 User access provisioning
    - 9.2.3 Management of privileged access rights
    - 9.2.4 Management of secret authentification information of users
    - 9.2.5 Review of user access rights
    - 9.2.6 Removal or adjustment of access rights

ISO 27002:2013

- 9 Access control (cont'd)
  - 9.3 User responsibilities
  - Objective: To make users accountable for safeguarding their authentication information.
    - 9.3.1 Use of secret authentication information
  - 9.4 System and application access control
  - Objective: To prevent unauthorized access to systems and applications.
    - 9.4.1 Information access restriction
    - 9.4.2 Secure log-on procedures
    - 9.4.3 Password management system
    - 9.4.4 Use of privileged utility programs
    - 9.4.5 Access control to program source code

ISO 27002:2013

- 10 Cryptography
  - 10.1 Cryptographic controls
  - Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.
    - 10.1.1 Policy on the use of cryptographic controls
    - 10.1.2 Key management

ISO 27002:2013

- 11 Physical and environmental security
  - 11.1 Secure areas
  - Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.
    - 11.1.1 Physical security perimeter
    - 11.1.2 Physical entry controls
    - 11.1.3 Securing offices, rooms and facilities
    - 11.1.4 Protecting against external and environmental threats
    - 11.1.5 Working in secure areas
    - 11.1.6 Delivery and loading areas

ISO 27002:2013

- 11 Physical and environmental security (cont'd)
  - 11.2 Equipment
  - Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.
    - 11.2.1 Equipment siting and protection
    - 11.2.2 Supporting utilities
    - 11.2.3 Cabling security
    - 11.2.4 Equipment maintenance
    - 11.2.5 Removal of assets
    - 11.2.6 Security of equipment and assets off-premises
    - 11.2.7 Secure disposal or re-use of equipment
    - 11.2.8 Unattended user equipment
    - 11.2.9 Clear desk and clear screen policy

ISO 27002:2013

- 12 Operation security
  - 12.1 Operational procedures and responsibilities
  - Objective: To ensure correct and secure operations of information processing facilities.
    - 12.1.1 Documented operating procedures
    - 12.1.2 Change management
    - 12.1.3 Capacity management
    - 12.1.4 Separation of development, testing and operational environments
  - 12.2 Protection from malware
  - Objective: To ensure that information and information processing facilities are protected against malware.
    - 12.2.1 Controls against malware
  - 12.3 Backup
  - Objective: To protect against loss of data.
    - 12.3.1 Information backup

ISO 27002:2013

- 12 Operation security (cont'd)
  - 12.4 Logging and monitoring
  - Objective: To record events and generate evidence.
    - 12.4.1 Event logging
    - 12.4.2 Protection of log information
    - 12.4.3 Administrator and operator logs
    - 12.4.4 Clock synchronisation
  - 12.5 Control of operational software
  - Objective: To ensure the integrity of operational systems.
    - 12.5.1 Installation of software on operational systems

ISO 27002:2013

- 12 Operations security (cont'd)
  - 12.6 Technical vulnerability management
  - Objective: To prevent exploitation of technical vulnerabilities.
    - 12.6.1 Management of technical vulnerabilities
    - 12.6.2 Restrictions on software installation
  - 12.7 Information systems audit consideration
  - Objective: To minimise the impact of audit activities on operational systems.
    - 12.7.1 Information systems audit controls

ISO 27002:2013

- 13 Communications security
  - 13.1 Network security management
  - Objective: To ensure the protection of information in networks and its supporting information processing facilities.
    - 13.1.1 Network controls
    - 13.1.2 Security of network services
    - 13.1.3 Segregation in networks
  - 13.2 Information transfer
  - Objective: To maintain the security of information transferred within an organization and with any external entity.
    - 13.2.1 Information transfer policies and procedures
    - 13.2.2 Agreements on information transfer
    - 13.2.3 Electronic messaging
    - 13.2.4 Confidentiality or non-disclosure agreements

ISO 27002:2013

- 14 System acquisition, development and maintenance
  - 14.1 Security requirements of information systems
  - Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks
    - 14.1.1 Information security requirements analysis and specification
    - 14.1.2 Securing application services on public networks
    - 14.1.3 Protecting application services transactions

ISO 27002:2013

- 14 System acquisition, development and maintenance (cont'd)
  - 14.2 Security in development and support processes
  - Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.
    - 14.2.1 Secure development policy
    - 14.2.2 System change control procedures
    - 14.2.3 Technical review of applications after operating platform changes
    - 14.2.4 Restrictions on changes to software packages
    - 14.2.5 Secure system engineering principles
    - 14.2.6 Secure development environment
    - 14.2.7 Outsourced development
    - 14.2.8 System security testing
    - 14.2.9 System acceptance testing
  - 14.3 Test data
  - Objective: To ensure the protection of data used for testing.
    - 14.3.1 Protection of test data

ISO 27002:2013

- 15 Supplier relationships
  - 15.1 Information security in supplier relationships
  - Objective: To ensure protection of the organization's assets that is accessible by suppliers.
    - 15.1.1 Information security policy for supplier relationships
    - 15.1.2 Addressing security within supplier agreements
    - 15.1.3 Information and communication technology supply chain
    - 15.2 Supplier service delivery management
  - 15.2 Supplier service delivery management
  - Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.
    - 15.2.1 Monitoring and review of supplier services
    - 15.2.2 Managing changes to supplier services

ISO 27002:2013

- 16 Information security incident management
  - 16.1 Management of information security incidents and improvements
  - Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.
    - 16.1.1 Responsibilities and procedures
    - 16.1.2 Reporting information security events
    - 16.1.3 Reporting information security weaknesses
    - 16.1.4 Assessment of and decision on information security events
    - 16.1.5 Response to information security incidents
    - 16.1.6 Learning from information security incidents
    - 16.1.7 Collection of evidence

ISO 27002:2013

- 17 Information security aspects of business continuity management
  - 17.1 Information security continuity
  - Objective: Information security continuity should be embedded in the organization's business continuity management systems.
    - 17.1.1 Planning information security continuity
    - 17.1.2 Implementing information security continuity
    - 17.1.3 Verify, review and evaluate information security continuity
  - 17.2 Redundancies
  - Objective: To ensure availability of information processing facilities.
    - 17.2.1 Availability of information processing facilities

ISO 27002:2013

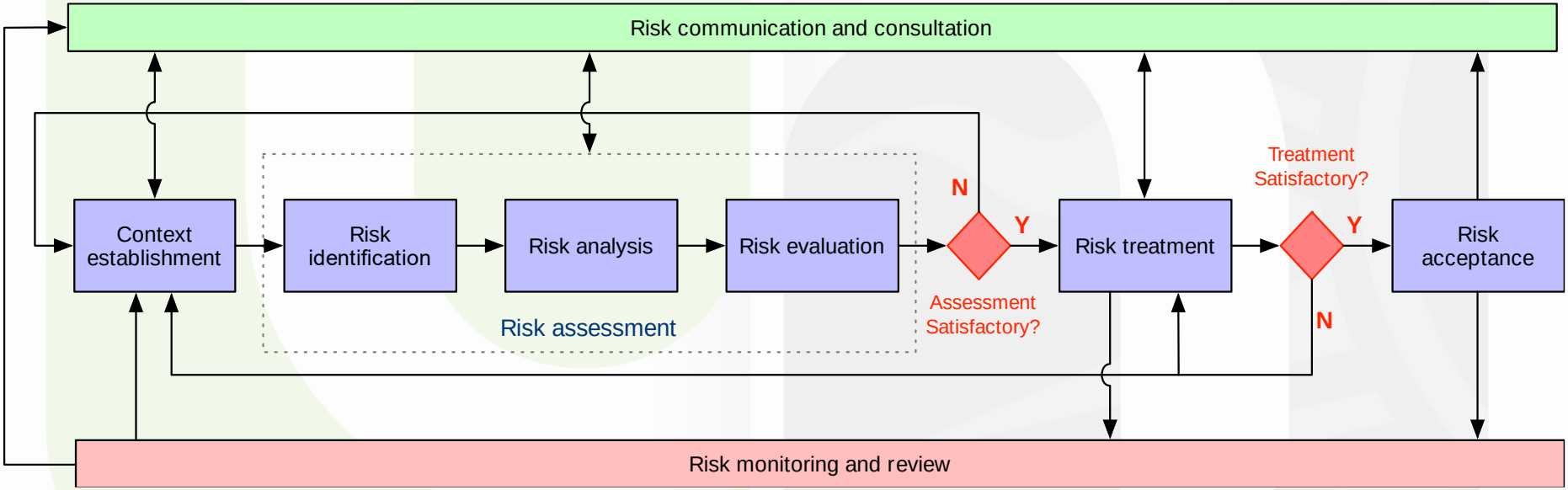
- 18 Compliance
  - 18.1 Compliance with legal and contractual requirements
  - Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.
    - 18.1.1 Identification of applicable legislation and contractual requirements
    - 18.1.2 Intellectual property rights
    - 18.1.3 Protection of records
    - 18.1.4 Privacy and protection of personally identifiable information
    - 18.1.5 Regulation of cryptographic controls
  - 18.2 Information security reviews
  - Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.
    - 18.2.1 Independent review of information security
    - 18.2.2 Compliance with security policies and standards
    - 18.2.3 Technical compliance review

Managing risks with ISO 27005

ISO 27005:2018

- *"Information Security Risk Management"*
- defines guidelines for information security risk management
- **does not** define a specific methodology
- includes recommendations about
  - defining the scope and boundaries of risk management process
  - identifying and valuing assets and impact
- also provides
  - a list of common threats
  - a list of common vulnerabilities and methods for vulnerability

ISO 27005:2018



ISO 27005:2018

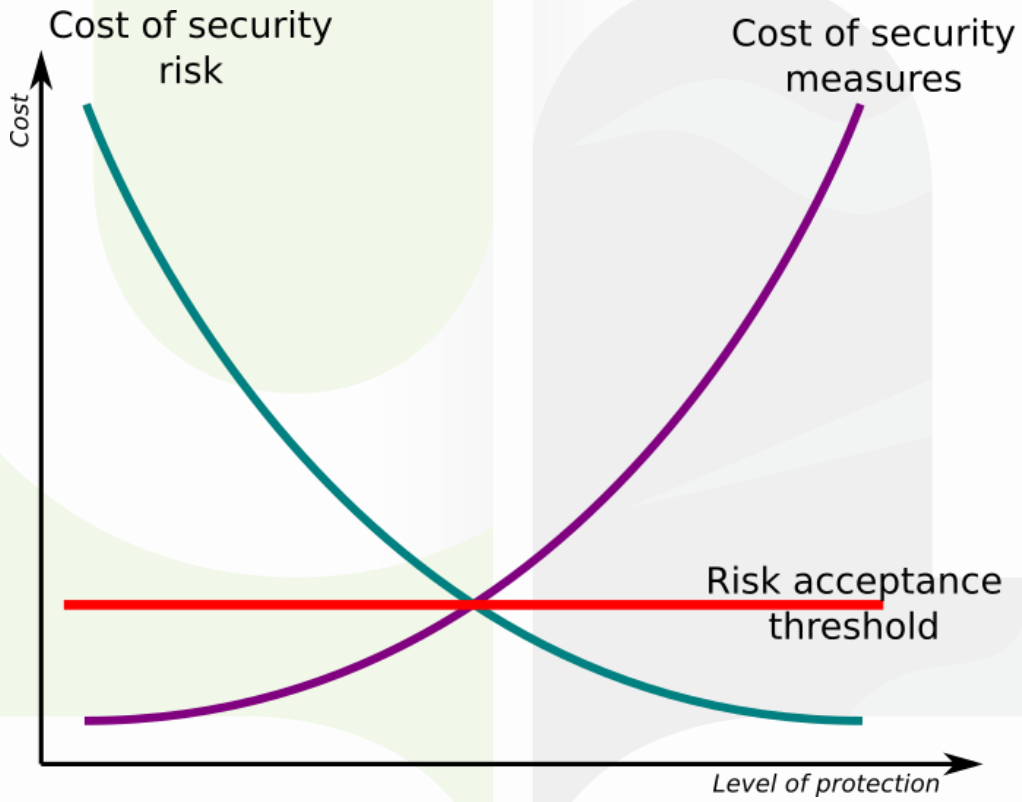
- Context establishment
  - understand the context of the organization: mission, values, goals, strategies
  - identify interested parties
    - person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity
    - interested party is the ISO preferred term, stakeholder is admitted
  - define the purpose of risk management, along with necessary basic criteria, scope and boundaries, as well as appropriate organization
  - purpose can be any of the following (not exhaustive)
    - support the implementation of an ISMS, demonstrate legal compliance, prepare a BCP plan, perform a vulnerability assessment…

ISO 27005:2018

- Context establishment
  - basic criteria
    - risk management approach
    - risk evaluation criteria, based on assets value, legal and regulatory obligations, operational and business importance of availability, integrity, availability
    - impact evaluation criteria, to express and measure the degree of damage or costs to the organization caused by an information security incident. Multiple dimensions like information classification, business continuity, damage to reputation, breach of legal or contractual obligations…
    - risk acceptance criteria, to identify the acceptable level of risks

ISO 27005:2018

- Context establishment



Example of risk acceptance threshold from a quantitative analysis

ISO 27005:2018

- Context establishment
  - scope and boundaries
    - to ensure all relevant elements are taken into account and risks that might arise at boundaries are properly identified
    - relevant elements include stakeholders, business assets, organization, legal and regulatory constraints, cultural environment…
    - scope can cover IT application, IT infrastructure, business process, sub-organization

ISO 27005:2018

- Context establishment
  - organization for information security management
    - setup appropriate roles and responsibilities
      - definition of the RM process, identification of stakeholders, definition of their role, communication lines with stakeholders, escalation procedures

Case study

The Water4All company is in charge of managing the water distribution infrastructure of a large city. The infrastructure is monitored through a network of sensors to detect leaks or obstructions that could require interventions. Valves can be controlled remotely to block or redirect the traffic if needed. Consumer's are equipped with smart meters that collect and send data to the company.

All communications for the monitoring (collecting sensor data and controlling devices) take place via a hybrid network (wireless and wired). Smart meters report their data via 4G network. All data are collected and stored centrally at the company's office, in its datacenter located in the basement of its main building.

Customer management involves registration, invoicing and complaint handling.

The monitoring activity is critical, since it allows to detect and repair as quickly as possible any issue with the distribution. A sophisticated ticketing system is used to alert the on-duty team in real-time and direct them as precisely as possible to the location of the incident.

Case study

The admin team takes care of the customer relationship. The financial team is responsible for invoicing customers, paying suppliers, establishing mandatory reporting (VAT, taxes…) and establishing the annual budget.

The engineering department is in charge of maintaining the pipe network and develop it further, following the city expansion. Engineers mainly use CAD and mapping tools, and store their data on a central server, also stored in the company's datacenter.

An internal IT department manages the servers and workstations. Applications are developed by an external company located in Slovakia. An internal collaboration platform is setup on the local infrastructure and offers mail, calendar and document sharing services.

All teams have a manager who, together with the company director, form the management team.

Case study

- Time to practice
  - identify relevant security criteria
  - define appropriate scales
    - likelihood, severity, risk level
  - define risk acceptance criteria

ISO 27005:2018

- Risk identification
  - goal: understand what could cause a potential loss, and where and why the loss could happen
  - identification of assets
    - primary assets: process, information, knowledge
    - secondary assets: infrastructure, software, building, personnel
    - asset owner
    - asset value; can be defined based on different criteria: replacement cost, creation cost, cost in case of security breach…
    - an asset may receive different values that need to be combined (sum, max…) to reach a common basis
    - output: list of assets to be risk-managed with owner and value
    - check ISO 27005:2018 Annex B for examples of assets and valorization criteria

Case study

- Time to practice
  - identify primary and secondary assets with their value

Asset #: _____	
Asset name	
Asset type	
Asset owner	
Asset value	

ISO 27005:2018

- Risk identification
  - identification of threats
    - threats have the potential to harm organization's assets
    - can be identified from existing lists, incident reports, expert advices…
    - can have a natural (environmental) or human origin, be deliberate or accidental, internal or external
    - output: list of threats with type and source
    - check ISO 27005:2018 Annex C for a list of typical threats

ISO 27005:2018

- Risk identification
  - identification of existing controls
    - identify controls already in place to avoid re-implementing them
    - check that they are implemented and effective
    - document any gap
  - identification of vulnerabilities
    - from the list of assets, threats and existing controls, identify the means through which a threat could harm the assets
    - different kinds of vulnerabilities: environment, personnel, procedures, infrastructure, software, dependence on third-party…
    - output: list of vulnerabilities in relation to assets, threats and controls
    - check ISO 27005:2018 Annex D for list of vulnerabilities and how to detect them

ISO 27005:2018

- Risk identification
  - identification of consequences (impact)
    - identify the consequences that **a loss of confidentiality, integrity or availability** may have on the identified assets
    - impact can be direct (broken asset, activity stopped) or indirect (missed opportunity, failure to comply with regulatory constraints…)
    - information leak, degraded activity, information corruption, broken hardware, information theft…
    - financial, reputation, repair time, time lost…
    - output: list of *incident scenarios* and their consequences, related to assets

ISO 27005:2018

- Risk identification
  - conduct interviews
  - poll using questionnaires
  - review available documents
  - use scanning tools
  - …

Case study

- Time to practice
  - using the list of assets identified previously,
  - identify min. 3 threats
  - identify min. 5 incident scenarios combining assets, vulnerabilities, threats and consequences

Incident scenario #: _____	
Primary asset	
Secondary asset(s)	
Security criteria	
Vulnerability	
Threat	
Consequence	

ISO 27005:2018

- Risk analysis
  - Select an appropriate approach; different methods exist
    - qualitative
      - use a scale of qualitative attributes to describe the severity of consequences and likelihood of incident
      - ex: low, medium, high
      - easy to understand but subjective
    - quantitative
      - use a scale of numerical values to measure the severity of consequences and likelihood of incidents
      - can derived from models or history
      - hard to obtain accurate data

ISO 27005:2018

- Risk analysis
  - Assessment of consequences
    - goal: establish a measure of the severity of incident scenarios, based on the cost of the asset (acquisition, replacement, repair), consequence on the activity, reputation, compliance or any relevant valorization criteria…
    - output: list of assessed consequences of an incident scenario, with respect to assets and impact criteria

ISO 27005:2018

- Risk analysis
  - Assessment of incident likelihood
    - goal: establish a measure of the likelihood of a security incident, based on threat motivation and resources, ease of vulnerability exploitation…
    - past incident statistics may provide useful information
    - output: list of incident scenarios with their likelihood (qualitative of quantitative)

ISO 27005:2018

- Risk analysis
  - Determination of risk level
    - goal: determine the level of risk for each incident scenario
    - output: list of risks with associated level (quantitative or qualitative)
    - various methods, from high level to detailed
    - check ISO 27005:2018 Annex E for methods to estimate the level of risks

ISO 27005:2018

- Risk analysis – qualitative risk analysis

High
Medium
Low

High-level approach

likelihood \ *severity*	1	2	3	4	5
1	0	1	2	3	4
2	1	2	3	3	4
3	2	3	4	5	6
4	3	4	5	6	7

Detailed approach

ISO 27005:2018

- Risk analysis – qualitative risk analysis

consequence severity / *threat likelihood* / *vulnerability level*	*Low*			*Medium*			*High*		
	L	*M*	*H*	*L*	*M*	*H*	*L*	*M*	*H*
1	0	1	3	1	2	3	2	3	4
2	1	2	3	2	3	4	3	4	5
3	2	3	4	3	4	5	4	5	6
4	3	4	5	4	5	6	5	6	7

Detailed approach

ISO 27005:2018

- Risk analysis – quantitative risk analysis with ROSI
  - Return On Security Investment
  - Used to compute the annual loss expectancy (ALE) for incident scenario
  - ALE defines the maximum amount to spend on a yearly basis to protect the asset against the identified risk

ISO 27005:2018

- Risk analysis – quantitative risk analysis with ROSI
  - [Asset value (AV)] value of the asset to be considered
  - [Exposure factor (EF)] portion of the asset exposed to the incident scenario (percentage)
  - [Single Loss Expectancy (SLE)] Loss associated with one occurrence of the incident scenario
    - SLE=AV x EF
  - [Annualized rate of occurrence (ARO)] frequency of occurrence of the incident scenario on a yearly basis
  - [Annualized Loss Expectancy (ALE)] Loss associated with all the occurrences of the incident scenario over one year
    - ALE=SLE x ARO

ISO 27005:2018

- Risk analysis – quantitative risk analysis with ROSI
  - The value of a security measure can be computed as
  - $Value = ALE_{before} - ALE_{after} - annual\ cost$

ISO 27005:2018

- Risk analysis – ROSI example
  - Assuming that in case of fire, up to 20% of the datacenter which is worth 5M€, would be affected; SLE is thus 1M€
  - If the frequency of the fire scenario is 0.1 (once in 10 years), ALE would be 100K€
  - 100K€ is the maximum amount to spend on a yearly basis to protect against fire

Case study

- Time to practice
  - data worth 20K€ are stored on a server; it is assumed that in case of malware infection, 80% of data would be lost. Such incident is expected to happen once every 8 years. What are the SLE and ALE?
  - a security measure is cost-effective as long as its value is >0. Assuming that an access control system costs 50K€ and that ALE after implementing it is estimated at 250K€, what should be the minimal value of the asset to make the measure worthwhile, knowing that EF and ARO = 0.1

Case study

- Time to practice
  - from the list of incident scenarios, determine risk level using one of the approaches above (not the high-level one)

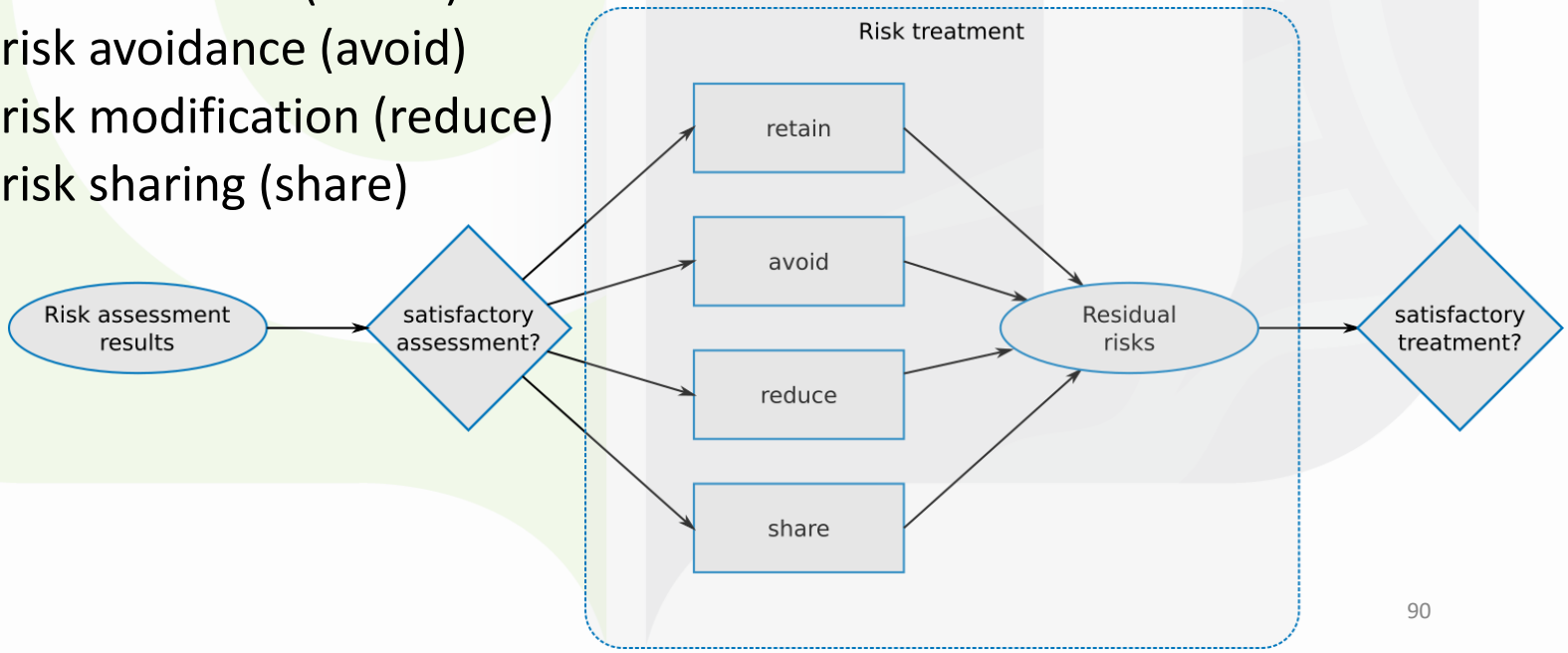
Incident scenario #: _____	
Risk level	

27005:2018

- Risk evaluation
  - goal: from the risk acceptation criteria and list of risks established at previous step, identify risks to be mitigated and prioritize their treatment
  - output: a list of risks prioritized according to the risk evaluation criteria

27005:2018

- Risk treatment
  - goal: select controls to mitigate the risk and establish a risk treatment plan
  - different risk treatment options
    - risk retention (retain)
    - risk avoidance (avoid)
    - risk modification (reduce)
    - risk sharing (share)



Case study

- Time to practice
  - for the two most important risks you have identified
    - select a risk treatment option
    - propose 3 security control to reduce the risk level

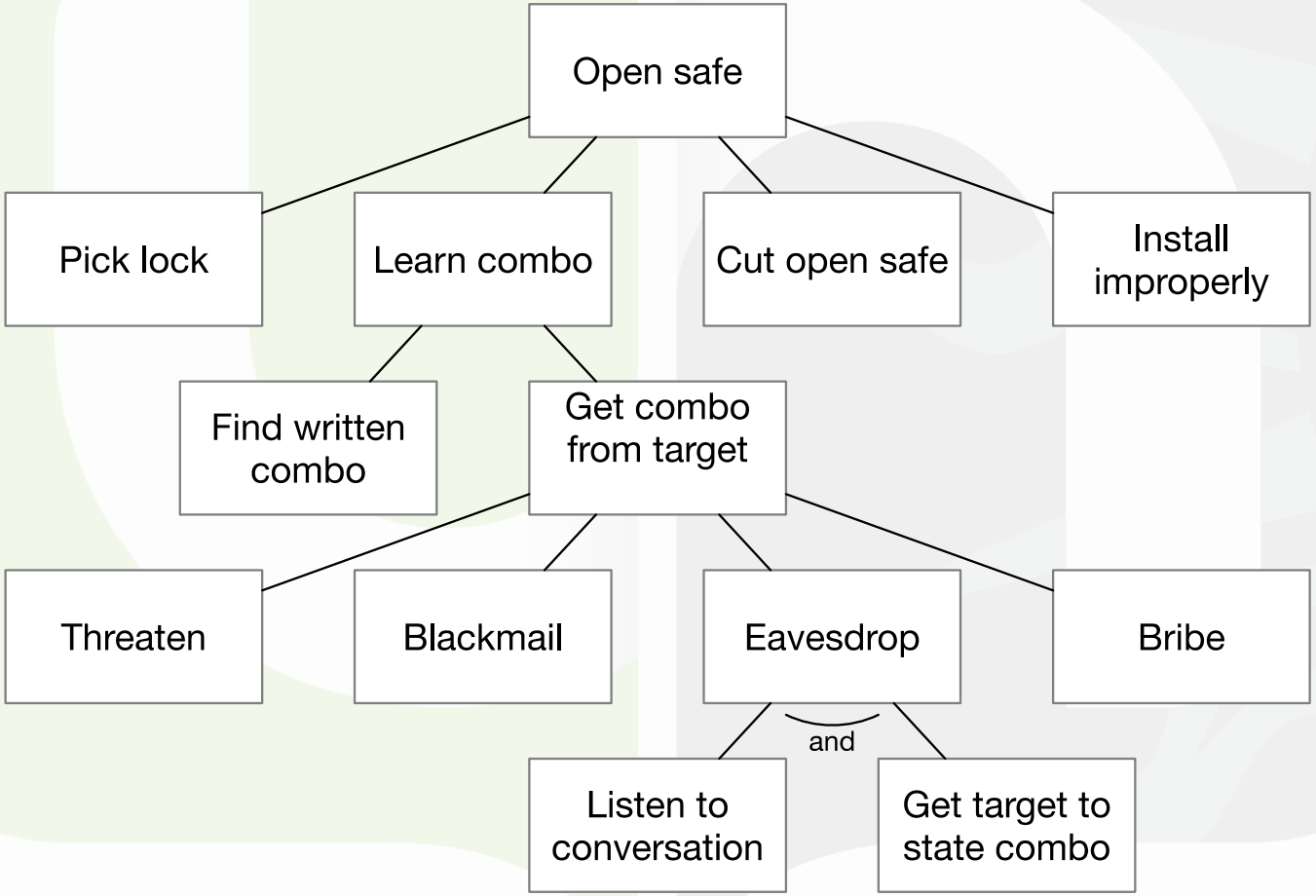
27005:2018

- Risk acceptance
  - formal approval by the management of the action plan and residual risks
  - output: list of accepted risks with justification in case they do not meet the normal risk acceptance criteria
- Risk communication
  - exchange information about risk between decision makers and all stakeholder, incl. existence, nature, importance, treatment…
- Monitoring and review
  - review risks and their factors to identify changes in the organization context and provide timely response

Attack trees

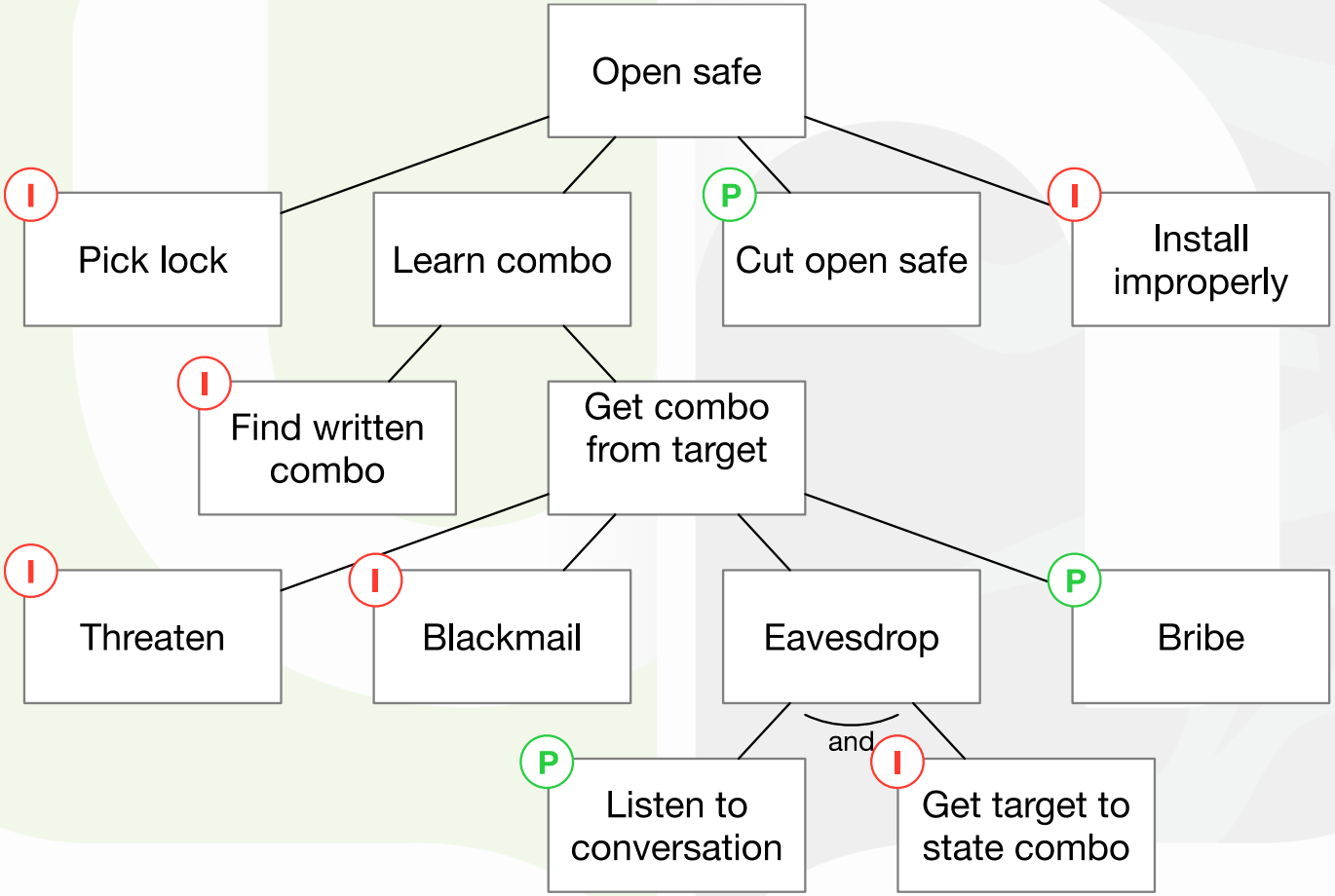
- Sometimes, simple tools are enough…
- Technique proposed by Bruce Schneier in Dr. Dobb's Journal (Dec 1999)
  - model attacks and occurrence conditions
  - decompose attack goal into sub-goals or conditions
  - recursively
  - child nodes can be AND'ed or OR'ed

Example



Source: https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Example

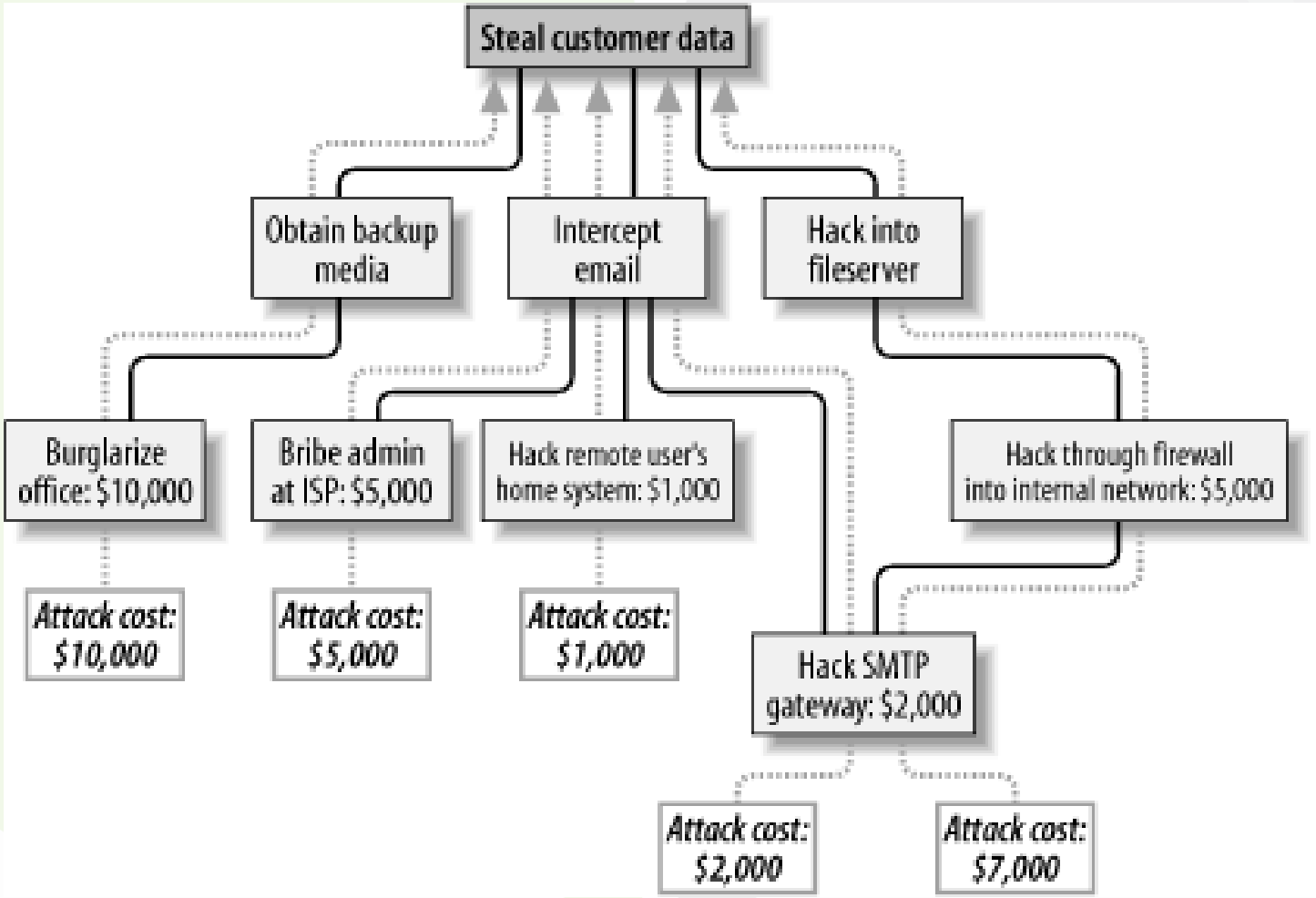


Source: https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Attack trees

- Enrich the tree
  - assign a value to node
    - number, boolean
    - possible/impossible: a OR node is possible if at least one of its children is possible; a AND node is possible of all its children are possible
    - cost: the cost of a OR node is the min cost of its children; the cost of a AND node is the sum of the cost of its children
    - difficulty
- allows to reason on the attack paths
  - what is the cost of an attack?
  - what is the most likely path?
  - what should I protect first?

Example



Source: http://etutorials.org/Linux+systems/secure+linux-based+servers/

Conclusion

- Risk management is the basis for managing the security of a system, by helping to
  - define a strategic approach
  - define a commonly shared perception of risk
  - prioritize actions
  - build and improve a knowledge base
- Non trivial approach
  - time- and resource- consuming
  - not an exact science
- Quick wins can easily be obtained using simple tools