IT Baseline Security

Jaak Tepandi

Tallinn University of Technology

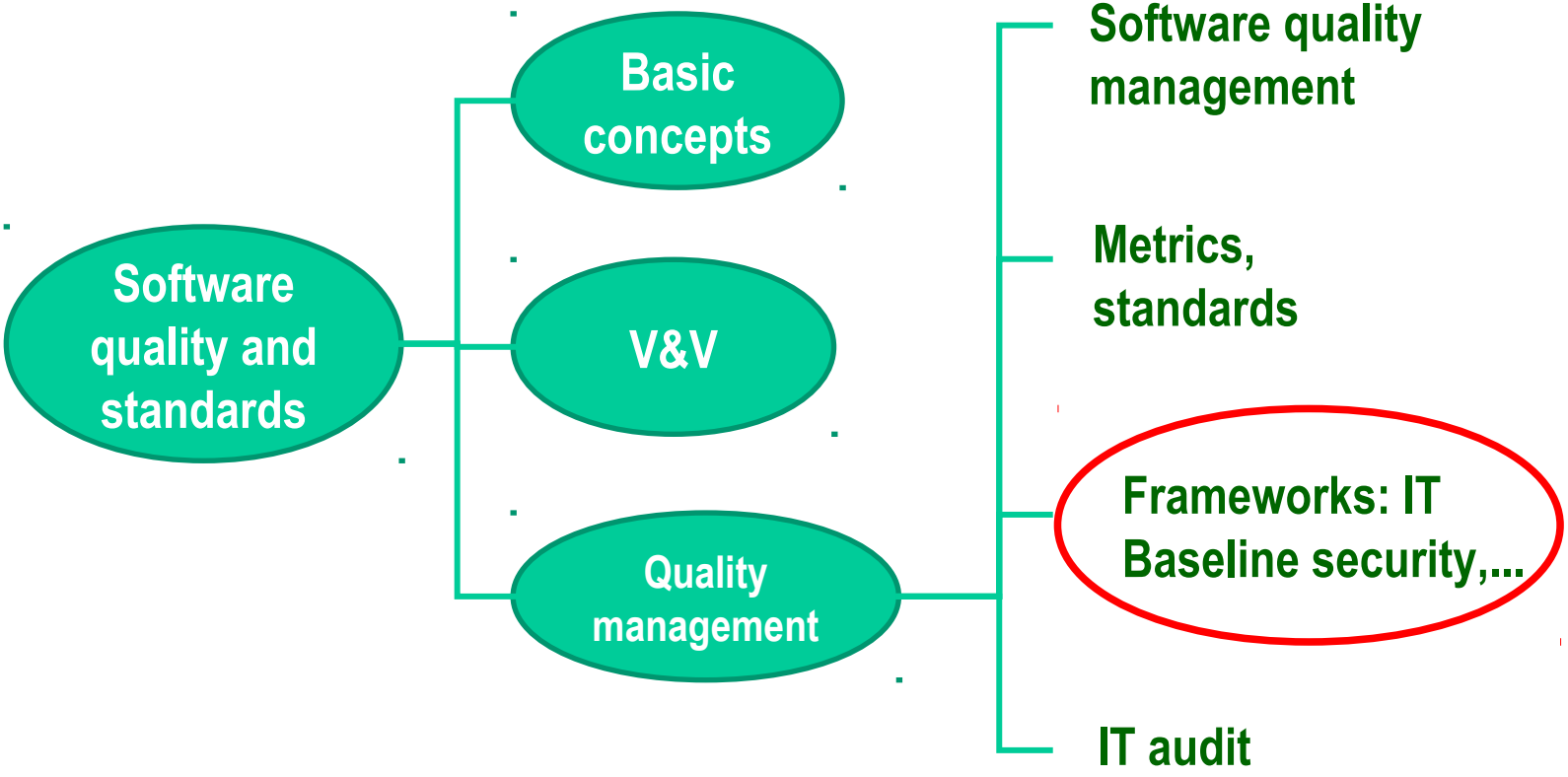
Institute of Informatics

Moodle: „Software Quality (Tarkvara kvaliteet)”

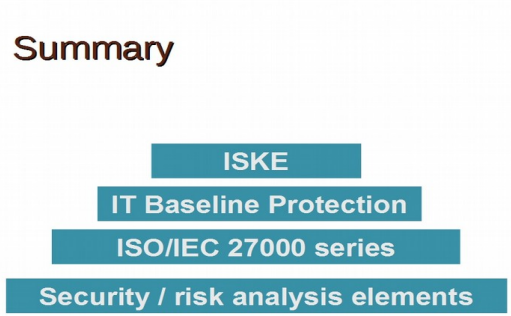
Alternate download: tepandi.ee

Version 7.12.2016

Context and content

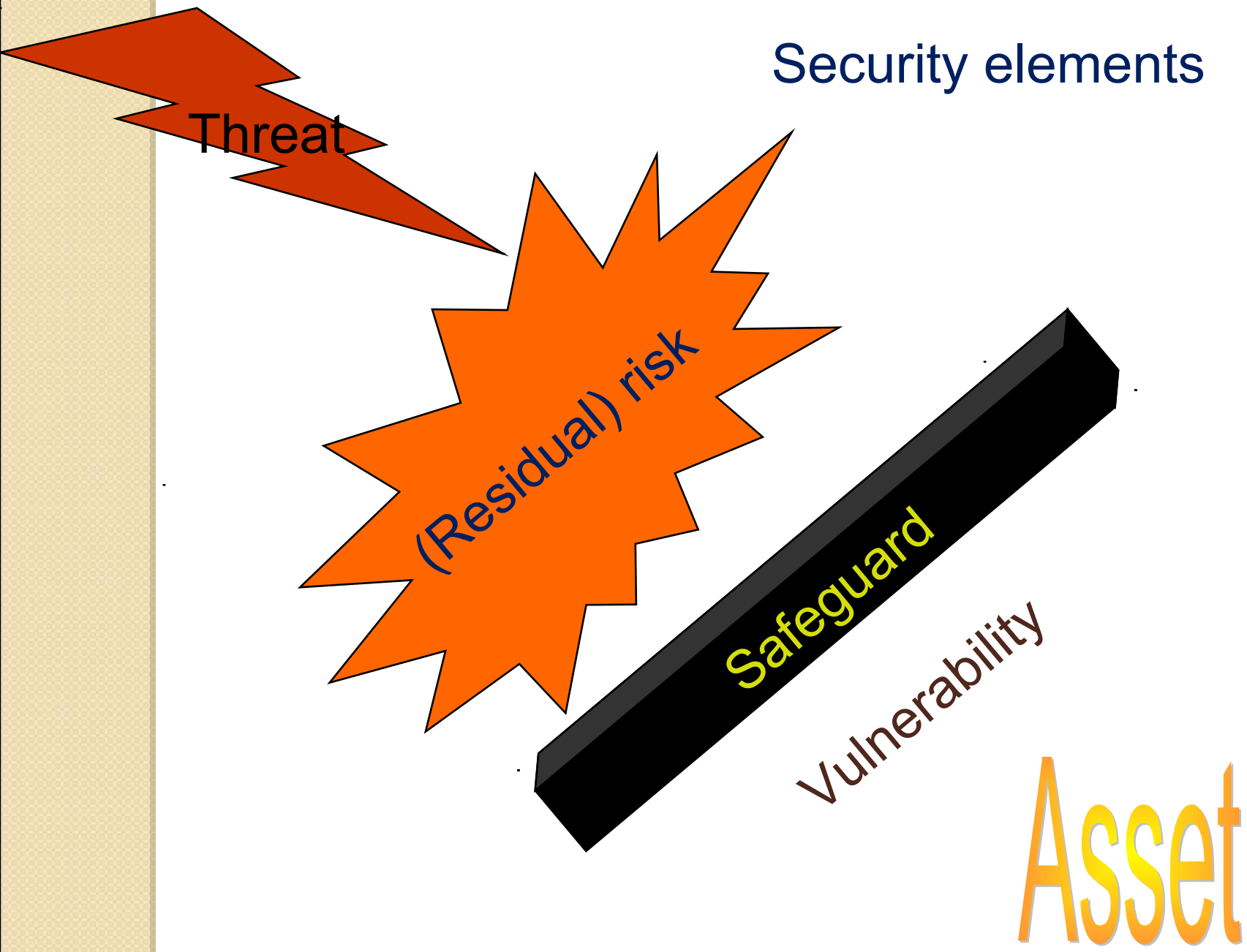


Outline

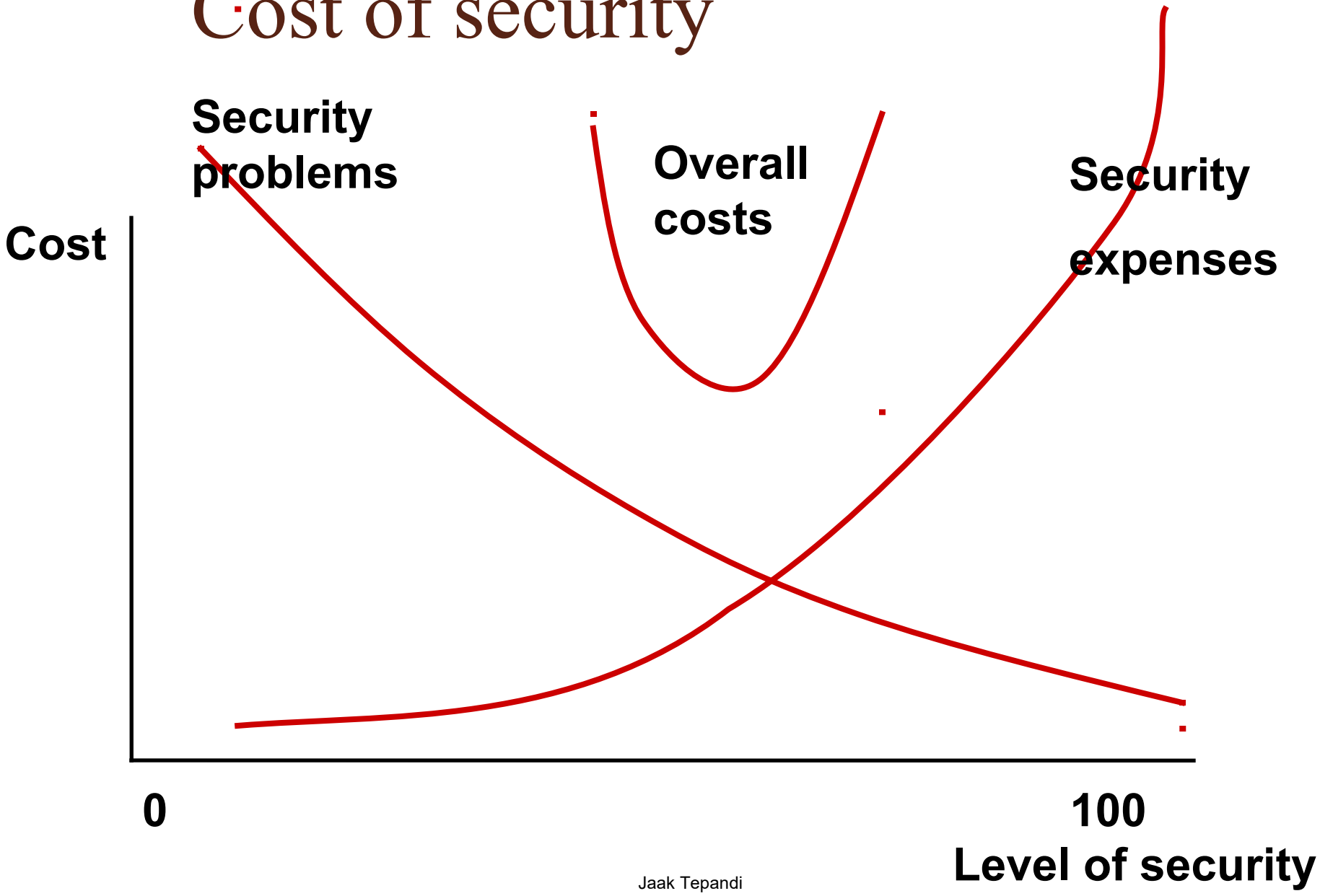


- Security elements and risk analysis options
- ISO/IEC 27000 series
- Three-level IT Baseline Security System (ISKE) & IT Baseline Protection (IT Grundschutz): standards, catalogues

Security elements



Cost of security



Risk management 4Ts

- Treat (control)
- Transfer (share)
- Tolerate (accept)
- Terminate (avoid)

Information Security Management System

- An Information Security Management System (ISMS): policies, procedures, guidelines, resources, activities, managed by an organization to protect its information assets
- Systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving organization’s information security to achieve business objectives
- Based upon risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks

The ISMS family of standards / ISO/IEC 27000 series: selection

Intended to assist organizations to implement and operate an ISMS

- ISO/IEC 27000 — Information security management systems — Overview and vocabulary
- ISO/IEC 27001 — Information security management systems — Requirements
- ISO/IEC 27002 Code of practice for information security controls (previous 17799)
- ISO/IEC 27005 — Information security risk management
- …..

Options for risk analysis strategy

- The same baseline approach for all IT systems
- Informal approach to perform risk analysis and concentration on high risk IT systems
- Detailed risk analysis using a formal approach for all IT systems
- Initial 'high level' risk analysis to identify IT systems exposed to high risks and those which are critical for the business => detailed risk analysis for these systems & baseline security to all other systems

Baseline Approach

[Compare: programming with or without libraries]

Advantages:

- time and effort is reduced
- similar baseline safeguards for many systems => a cost-effective solution

Disadvantages:

- baseline level too high => too expensive or too restrictive security for some systems
- baseline level too low => not enough security for some systems
- difficulties in managing security related changes (eg to assess after upgrade whether the original baseline safeguards are still sufficient)

Summary

ISKE

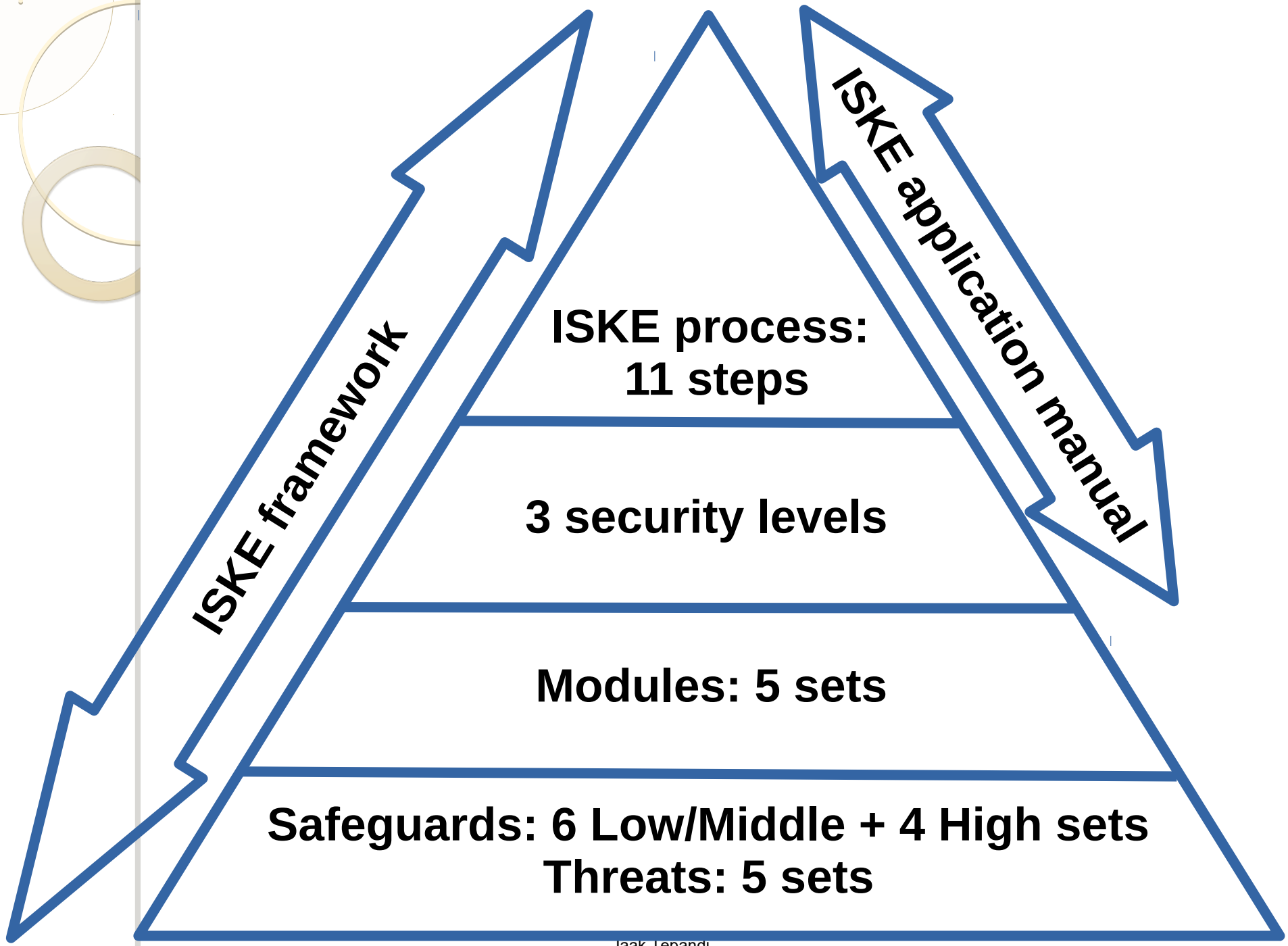
IT Baseline Protection

ISO/IEC 27000 series

Security / risk analysis elements

ISKE in brief

- Organizational, staff, infrastructural and technical security measures
- Three protection levels – Low (L), Medium (M) and High (H)
- Based on the IT-Grundschutz Standards and Catalogues (IT-Grundschutz Handbuch) issued by Germany's BSI (Bundesamt für Sicherheit in der Informationstechnik or Federal Office for Information Security)


ISKE framework
ISKE application manual
ISKE process:
11 steps
3 security levels
Modules: 5 sets
Safeguards: 6 Low/Middle + 4 High sets
Threats: 5 sets

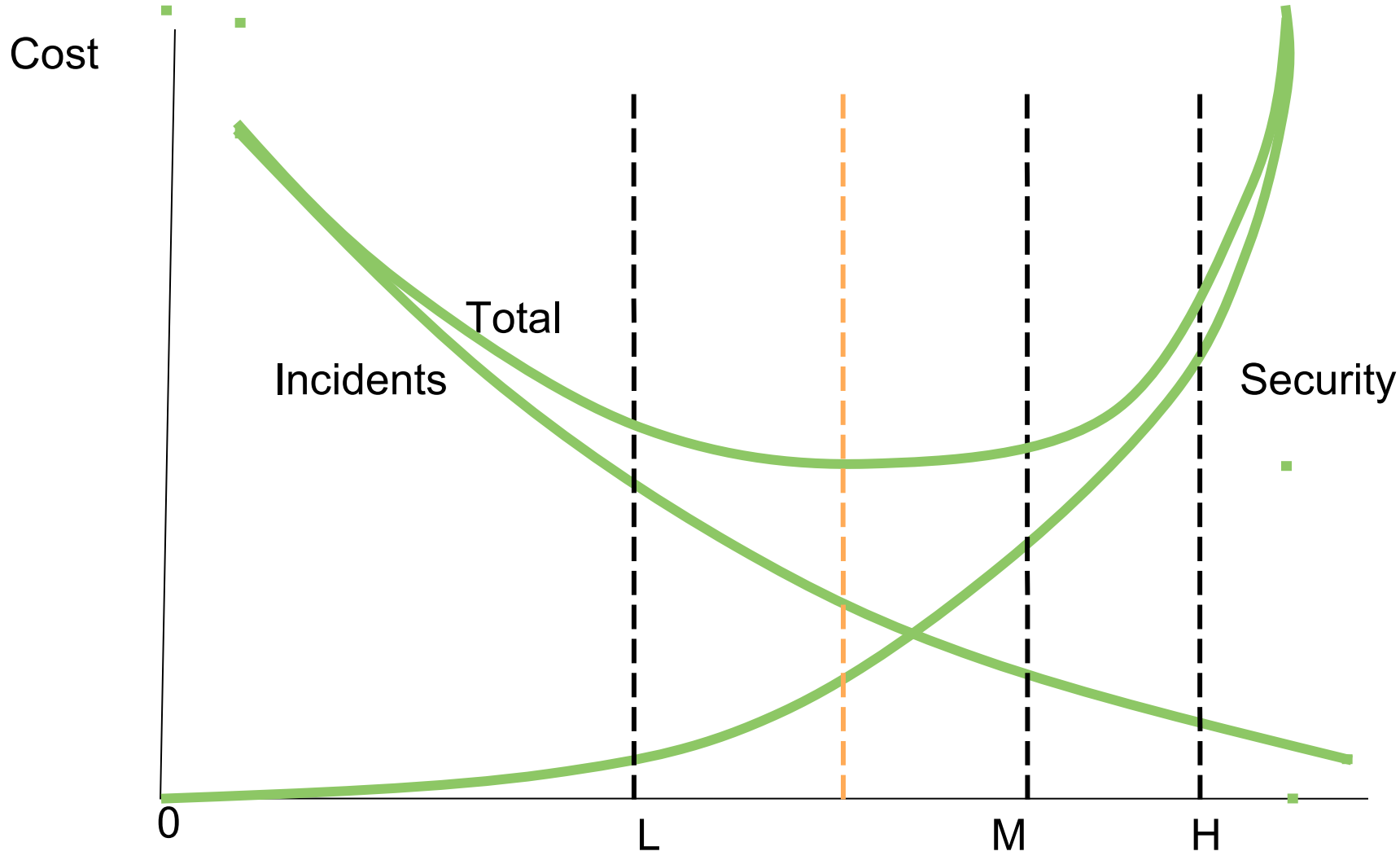
ISKE basics

- The Government of the Republic of Estonia has approved the System of Security Measures for Information Systems
- Follows from the Estonian Public Information Act - ISKE is compulsory for administrators of state and local administration databases
- To ensure the security level sufficient for the data processed in IT systems
- ISKE first version - October 2003, 7. version - 2015
- Updated continuously

ISKE: main ideas

- Information security is based on risk analysis...
- ... which in its detailed form is very expensive...
- ... and in the one-level baseline form is too general
- => Three-level IT Baseline Security System
  - In which level should the data be protected?
  - How much should we invest into IT Security?
  - Which safeguards to apply?
- Catalogues of threats, modules, safeguards

Three-level baseline security



Basic properties (incl the CIA triad)

- Confidentiality - property that information is not made available or disclosed to unauthorized individuals, entities, or processes
- Integrity - property of protecting the accuracy and completeness of assets
- Availability - property of being accessible and usable upon demand by an authorized entity
- + Authenticity - property that an entity is what it claims to be
- + Reliability - property of consistent intended behaviour and results
- + Non-repudiation - ability to prove the occurrence of a claimed event or action

Security classes and levels

- Three levels of security – „L“ – low, „M“ – medium, „H“ – high
- „Z“ - measures that may be needed
- A layered structure - medium security level is achieved by adding certain measures to the measures of the low security level etc
- Parameters: availability (K), integrity (T) and confidentiality (S), scale from 0 to 3
- Example of security subclass: K1
- Example of security class: K1T2S3

Sources of requirements

- Legislation, contracts (eg public data - S2)
- Business
- Consequences

Availability scale

- K0 – availability < 80%
- K1 - availability 80%...99%
- K2 - availability 99%...99,9%
- K3 - availability >99,9%
- + additional requirements + SLAs

Integrity scale

- T0 – protecting the accuracy and completeness of information is not important
- T1 – integrity is required; integrity checks as needed
- T2 – integrity is required; periodical integrity checks
- T3 – information has proof value; real-time integrity checks

Confidentiality scale

- S0 – public info
- S1 –for internal use; allowed in case of legitimate interest
- S2 – secret; allowed for given groups in case of legitimate interest
- S3 – top secret; allowed for given users in case of legitimate interest

Consequences

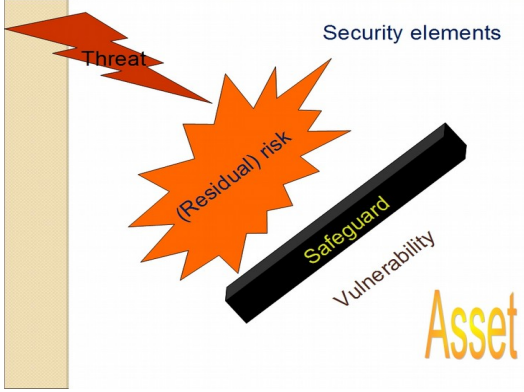
- R0 - no significant harm
- R1 - minor damage, significant barriers to agency function, or significant financial loss
- R2 - significant losses, significant barrier to agency's performance, risk to human health or the environment
- R3 - mission critical damage, agency function failure, significant disruption of public order, the threat to human life or environmental pollution

Security level

- Rules?

		K0	K1	K2	K3
T0	S0	L	L	M	H
	S1	L	L	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T1	S0	L	L	M	H
	S1	L	L	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T2	S0	M	M	M	H
	S1	M	M	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T3	S0	H	H	H	H
	S1	H	H	H	H
	S2	H	H	H	H
	S3	H	H	H	H

ISKE procedure



1. Inventory of ICT assets
2. Assignment of security classes to databases
3. Assignment of security classes to other ICT assets
4. Definition of security levels
5. Design of zones
6. Selection of modules
7. Selection of security measures for B 1.0
8. Planning for B 1.0 and others
9. Realization of the plan
10. Checking the results
11. Configuration and change management

Security classes - examples

- Accounting system?
- Study information system?
- Personnel system?
- Mobile bank?
- Warehouse management?

Modules

5 sets:

- **Generic aspects of IT**
- **Security of the infrastructure**
- **Security of the IT systems**
- **Security in the network**
- **Security of applications**

Safeguards

6 sets for low/middle level

- **Infrastructure**
- **Organisation**
- **Personnel**
- **Hardware and software**
- **Communication**
- **Contingency planning**

4 sets for high level

- **General**
- **Availability**
- **Integrity**
- **Confidentiality**

Threats

5 sets:

- **Force majeure**
- **Organisational shortcomings**
- **Human failure**
- **Technical failure**
- **Deliberate acts**

Priorities

	Possible	Difficult
Important	+++	++
Less important	+	

ISKE audits

- «H» - by March 1, 2010 => every 2 years
- «M» - by December 1, 2010 => every 3 years
- «L» - by March 1, 2011 => every 4 years

Summary

ISKE

IT Baseline Protection

ISO/IEC 27000 series

Security / risk analysis elements

Additional reading (examples)

ISO 27000 family of standards, http://www.iso.org/iso/iso27001

IT Grundschutz,
https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html

ISKE, https://www.ria.ee/en/iske-en.html