27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

The basics of risk assessment and treatment according to ISO 27001

Presenter: Dejan Kosutic

Which are the basic steps in ISO 27001 risk assessment and treatment?

If you're planning to start the risk assessment…

… to succeed, you need to understand the significance of risk management, and learn what is acceptable according to the standard

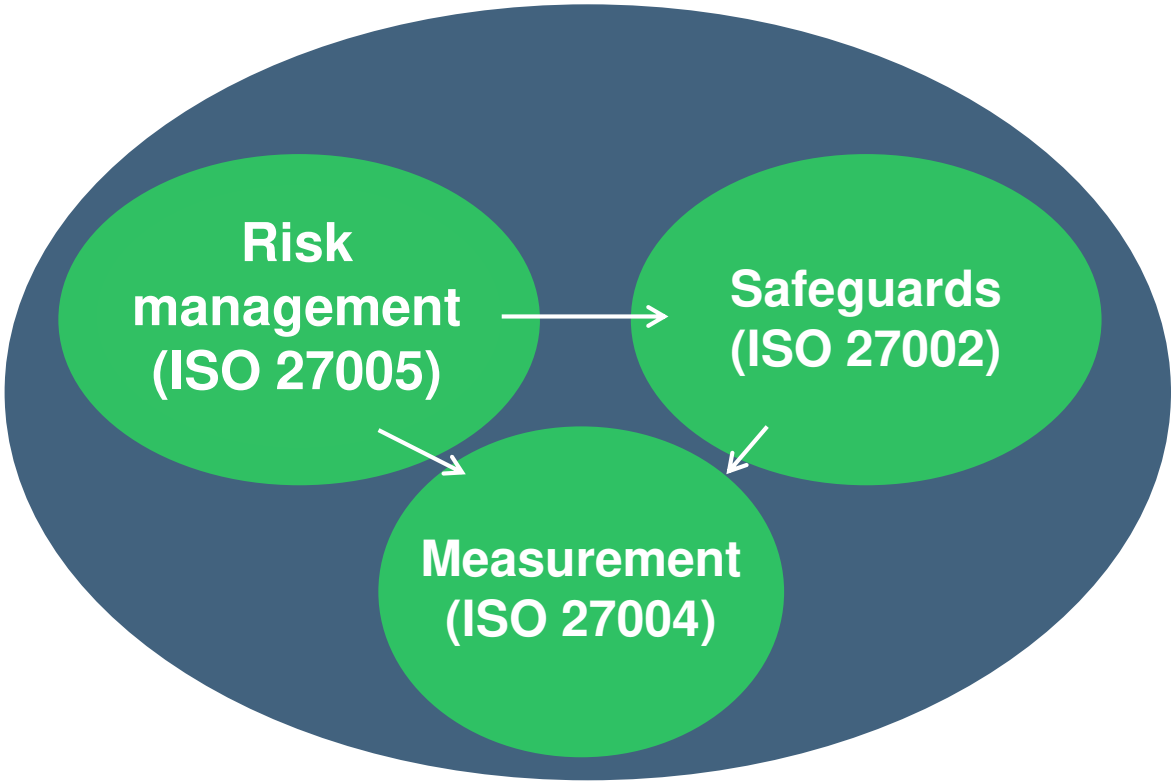
Risk management is the critical first step in ISO 27001 implementation – it determines everything that happens afterward.

Agenda

- Why risk management?
- The process of risk management
- Elements of risk assessment
- Identification of assets
- Threats and vulnerabilities
- Impact and likelihood
- 4 options for risk treatment
- Biggest challenges with risk management

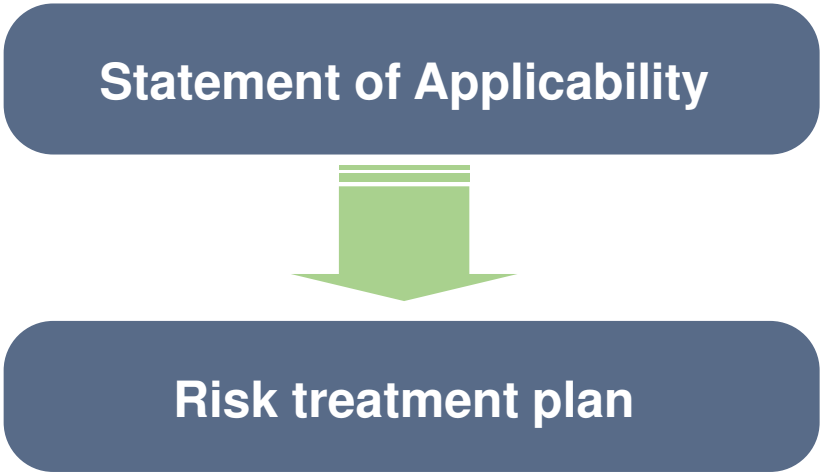
Why risk management?

Information security management (ISO 27001)

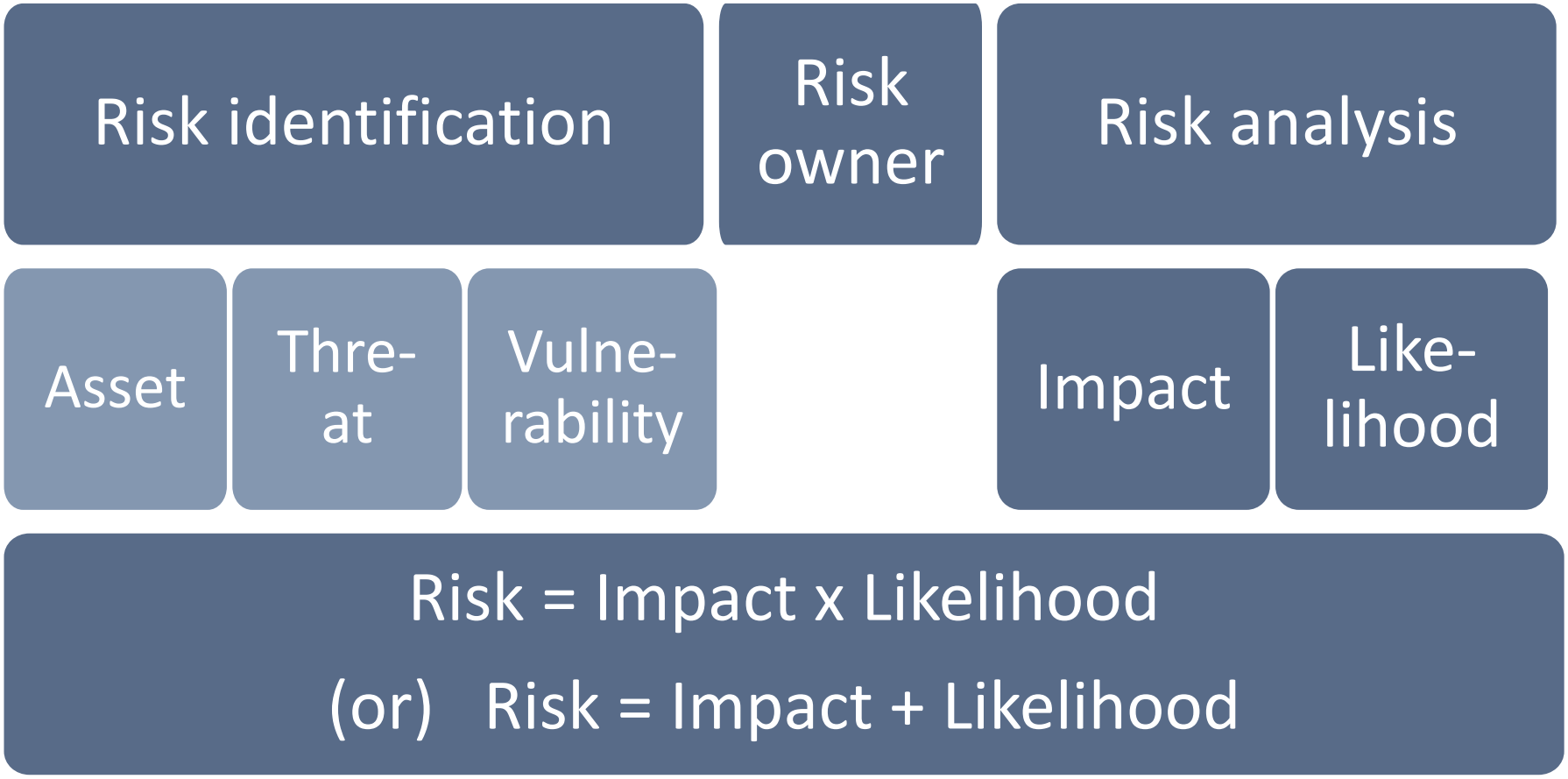


The process of risk management…

…The process of risk management



Elements of risk assessment



Assets – What do we protect?

- Examples:
  - Hardware
  - Software
  - Information (electronic, paper etc.)
  - Infrastructure
  - People!
  - etc.
- Identification of asset owners

Threats – What can happen?

Examples:

- Fire
- Earthquake
- Computer viruses
- Bomb threat
- Equipment malfunction
- Key people leaving the company

Vulnerabilities – Why can that happen?

Examples:

- Lack of fire-extinguishing system
- Lack of business continuity plans
- Lack of anti-virus software
- Lack of incident response procedures
- Obsolete equipment
- Lack of replacement

Impact and likelihood

- Example of assessment scale:
  - High
  - Medium
  - Low
- Or:
  - 1 to 5
  - 1 to 10

Example of Risk assessment table

Asset	Owner	Threat	Vulnerability	Impact (1-5)	Likelihood (1-5)	Risk (=I+L)
Server	Admin.	Electricity outage	No UPS	4	2	6
		Fire	No fire extinguisher	5	3	8
Contract	Managing director	Access by unauthorized persons	The contract is left on a table	4	4	8
		Fire	No fire protection	4	3	7
System administrator	Department head	Accident	No-one else knows the passwords	5	3	8

4 options for risk treatment

Apply appropriate controls

Accept risks

Avoid risks

Transfer risks

Biggest challenges with risk management

- How to document risk management and implemented controls in a way that is easy to understand
- How to get the organisations actors to be committed to the risk assessment process and formulation
- Establishing a risk methodology that is tied to reality and consistently applying that methodology across the company
- Either over-doing or under-doing the risk assessment and treatment
- Reconciling security needs of the company, existing budget, deadlines and regulatory requirements

Conclusion

Don’t skip the risk assessment and treatment – without this kind of analysis your information security will be full of holes!

27001 Academy

ISO 27001 and ISO 22301 Online Consultation Center

Q & A

Dejan Kosutic

27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

Thank you!

www.advisera.com/27001academy/webinars/