Navigating ISO/IEC 27001: Risk Management

Presenter:
Dejan Kosutic

in Follow

PERRY JOHNSON REGISTRARS, INC.

Hosted by Perry Johnson Registrars, Inc.

Advisera

What are the basic steps in ISO 27001 risk management?

If you're planning to start the risk assessment and treatment…

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

Advisera

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

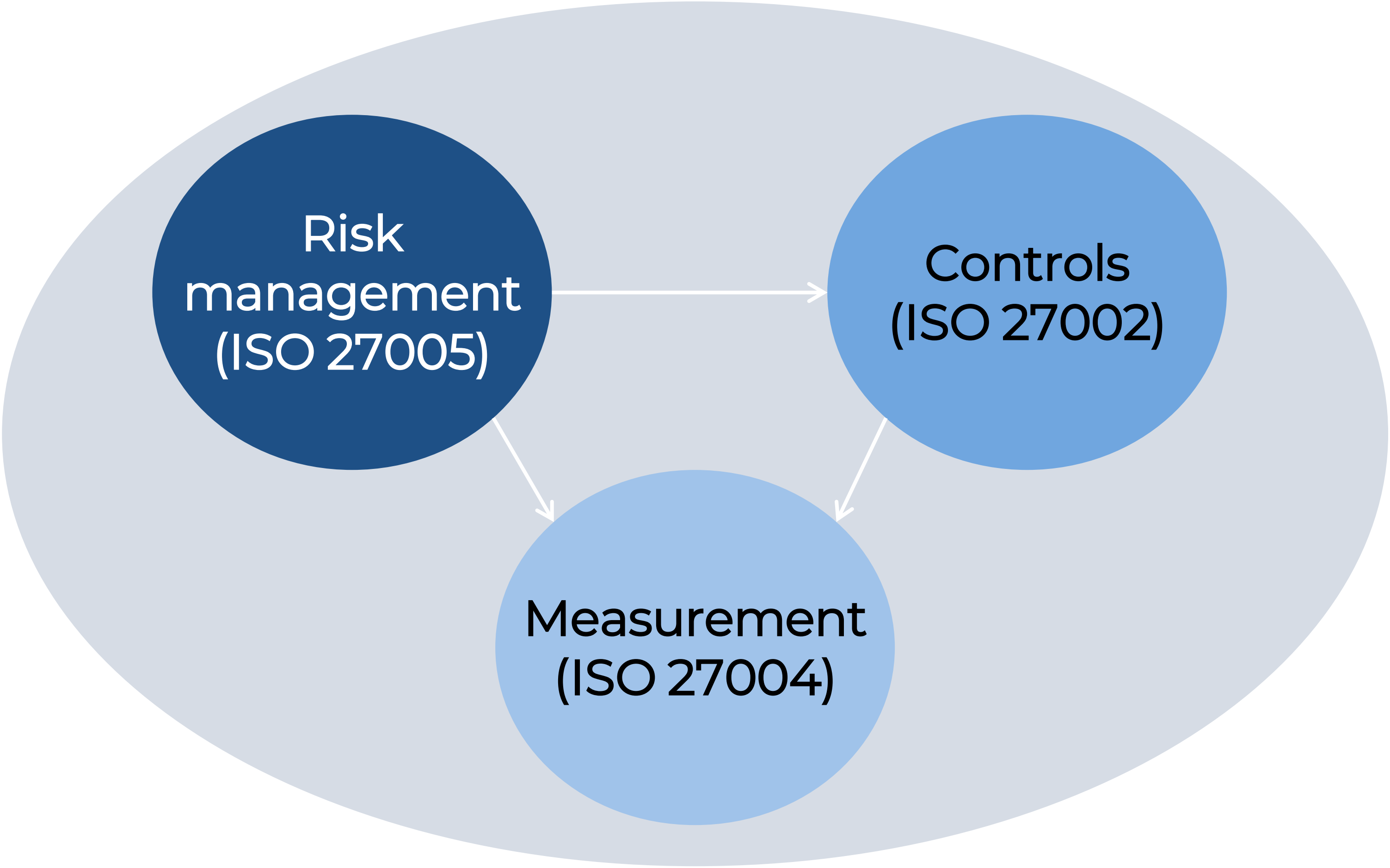
Advisera

Agenda

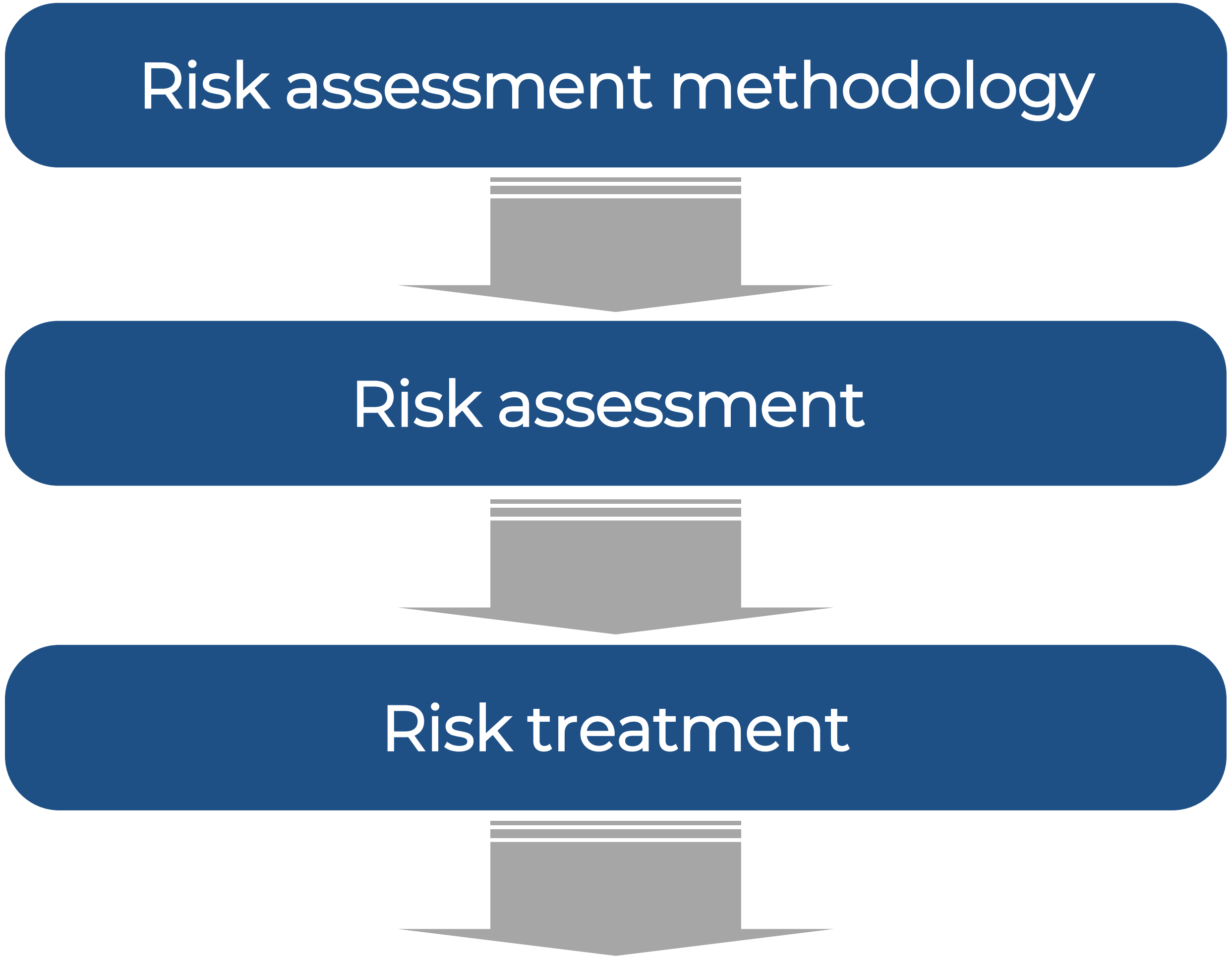
- Why risk management?
- The process of risk management
- Elements of risk assessment
- Identification of assets
- Threats and vulnerabilities
- Impact and likelihood
- 4 options for risk treatment

Why risk management?

Information security management (ISO 27001)



The process of risk management …



Risk assessment methodology

Risk assessment

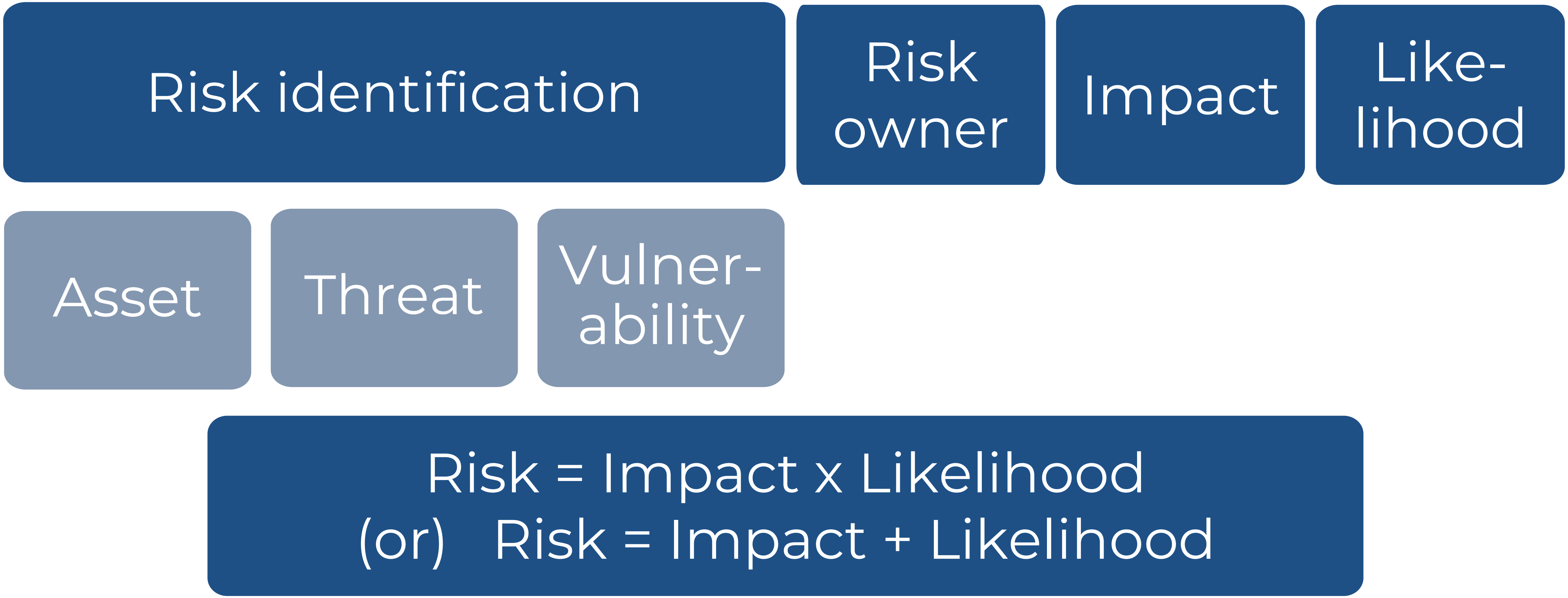
Risk treatment

… The process of risk management

Statement of Applicability

Risk treatment plan

Elements of risk assessment



Risk identification

Risk owner

Impact

Likelihood

Asset

Threat

Vulnerability

Risk = Impact x Likelihood

(or) Risk = Impact + Likelihood

Assets – What do we protect?

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

Vulnerabilities – Why the assets are not protected?

Examples:

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

Threats – What can happen to assets?

Examples:

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

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	Administrator	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

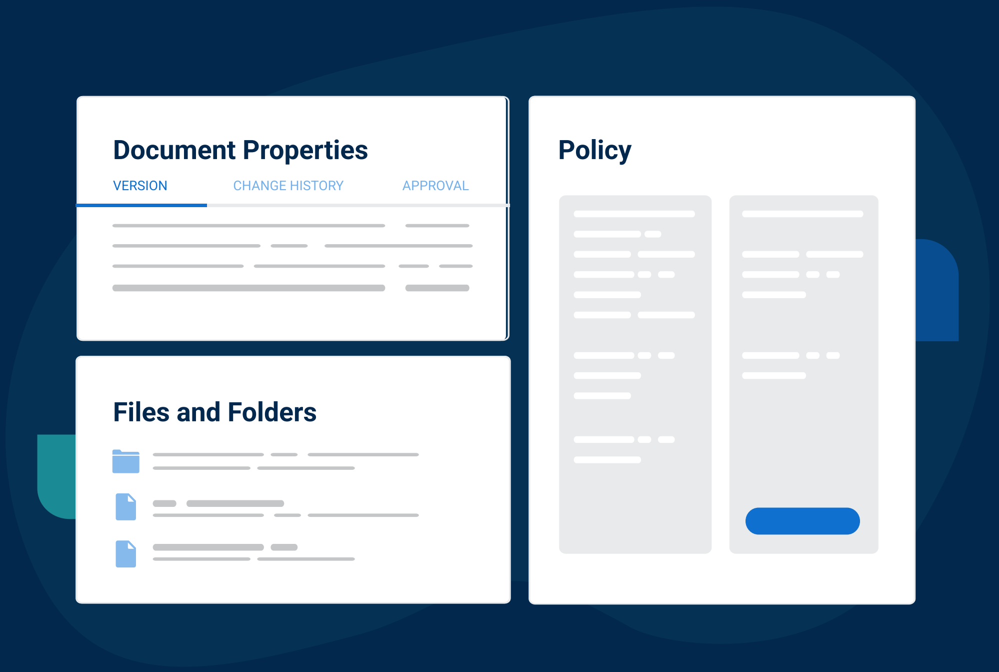
Transfer risks

Conclusion

Doing risk assessment properly does not mean you have to spend too much time on it

Conformio
ISO 27001 software

https://advisera.co/ConformioSoftware



Q&A

Dejan
Kosutic

in Follow

Advisera

Thank You

https://advisera.co/ConformioSoftware

Advisera