Co-funded by
the European Union

isecureu
DIGITAL EDUCATION TOOLS
FOR SECURITY RISK MANAGEMENT

ERASMUS+ cooperation partnership

Digital education tools for SECURITY RISK MANAGEMENT

2021-1-LV01-KA220-HED-000023056

Co-funded by
the European Union

ERASMUS+ cooperation partnership
Digital education tools for
SECURITY RISK MANAGEMENT

isecureu
DIGITAL EDUCATION TOOLS
FOR SECURITY RISK MANAGEMENT

ISO 31000 and Security Management Part II

Bert Bambach
Avans University of Applied Science

2021-1-LV01-KA220-HED-000023056

ISO 31000 and Security Management II

Objectives

- Understanding why to work with the ISO 31000 in the field of Security Management
- Understanding advantages and disadvantages of working with ISO 31000 in the field of Security Management
- Insight in how ISO 31000 can be applied for Security Management
- Insight in best practice working with ISO 31000 and Security Management

ISO 31000 and Security Management II

Why work with ISO 31000 in Security Management?

By working with the ISO 31000, you work in a standardized way this makes it easier to explain how you work - not only internally but also to colleagues outside the organization - even if that differs from how other organizations perform the work. This also makes it easier to explain how you contribute to the security dividend and add value to the organization.

Security dividend

- Business efficiency
- Attractiveness for customers
- Avoiding staff retention
- Demonstrable corporate social responsibility [sustainable development goals]
- Reduction of (legal) claims

[Article Corprate Security: A Cost or Contributor to the Bottom Line? – Security Dividend, Challenger]

Demonstrate added value

- Demonstrating the added value of security using KPI's
- Substantiation for financing security
- Measure the contribution of security activities and focus on them

[Article Corporate Security: A Cost or Contributor to the Bottom Line? - How can corporate security demonstrate its value?, Challenger]

ISO 31000 and Security Management II

Advantages and disadvantages of working with ISO 31000 in Security Management

Advantage

- Roll out and manage measures in a standardized way;
- Unambiguous way of communicating, everyone in the organization speaks the same language as they understand the building blocks of the ISO 31000;
- Easier to determine the desired level of work to be carried out.

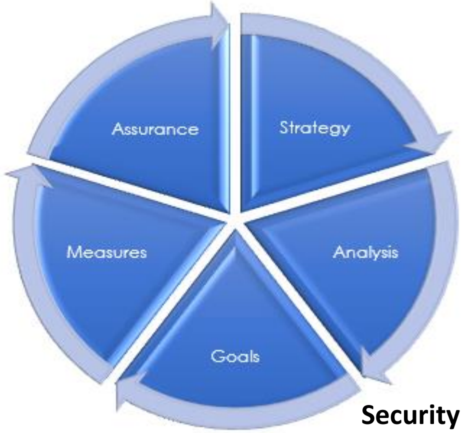
Disadvantage

- The prescribed arrangement of measures based on the ISO 31000 (sometimes) does not reflect the actual design and risks of a location;
- Sometimes it is only checked whether individual components of the ISO 31000 are present, but not whether these in conjunction lead to an effective and efficient security process to support the primary process;
- Due to the scale of the process to initiate the ISO 31000, it is not always clear where to start.

ISO 31000 and Security Management II

How to apply the ISO 31000 to Security Management

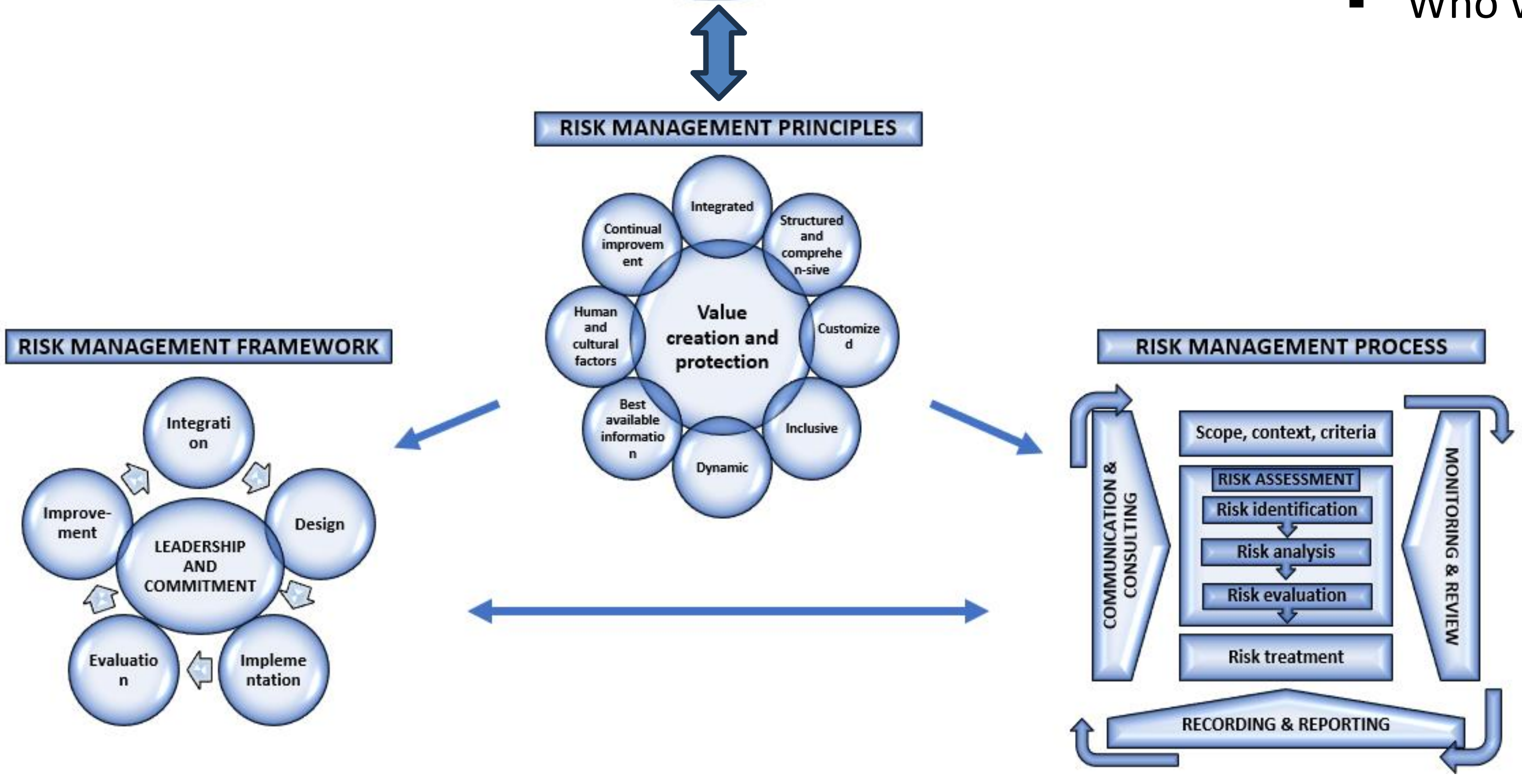
Security Risk Management
Coordinated activities to direct and control an organization regarding Security Risk Management



Security Management Cycle

Always be able to explain:

- Where do you start?
- Why you start there?
- What your approach is?
- Who will be your allies?



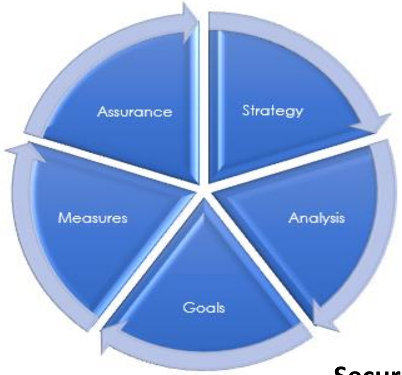
ISO 31000 Risk Management

ISO 31000 and Security Management II

Best practice:

Implementing Security Risk Management for an organization operating as an electricity grid manager in the critical infrastructure

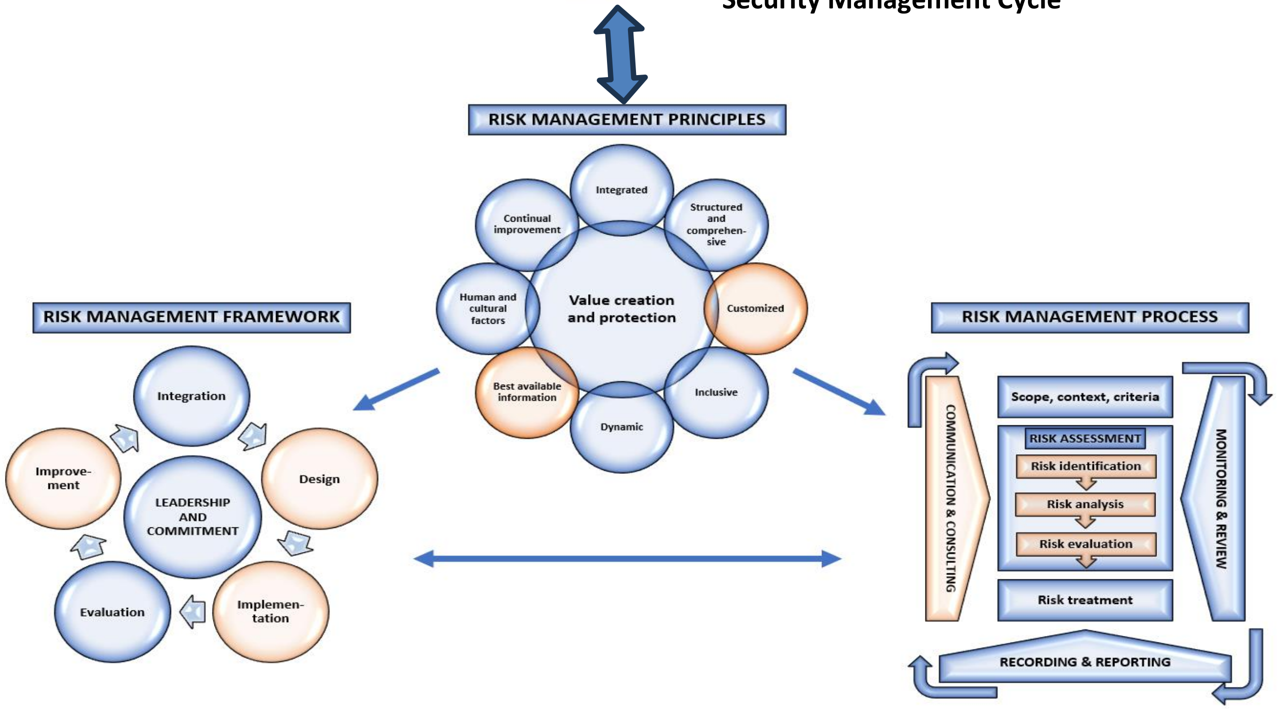
Security Risk Management
Coordinated activities to direct and control an organization regarding Security Risk Management



Security Management Cycle

Always be able to explain:

- Where do you start?
- Why you start there?
- What your approach is?
- Who will be your allies?



ISO 31000 Risk Management

Co-funded by the Erasmus+ Programme of the European Union

secureu
DIGITAL EDUCATION TOOLS FOR SECURITY RISK MANAGEMENT

Thank you for watching