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

RAIMUNDAS KALESNYKAS

Project Expert

Lecturer of Kazimieras Simonavičius University, Lithuania

Kazimieras Simonavicius University

SECURITY RISK MANAGEMENT:

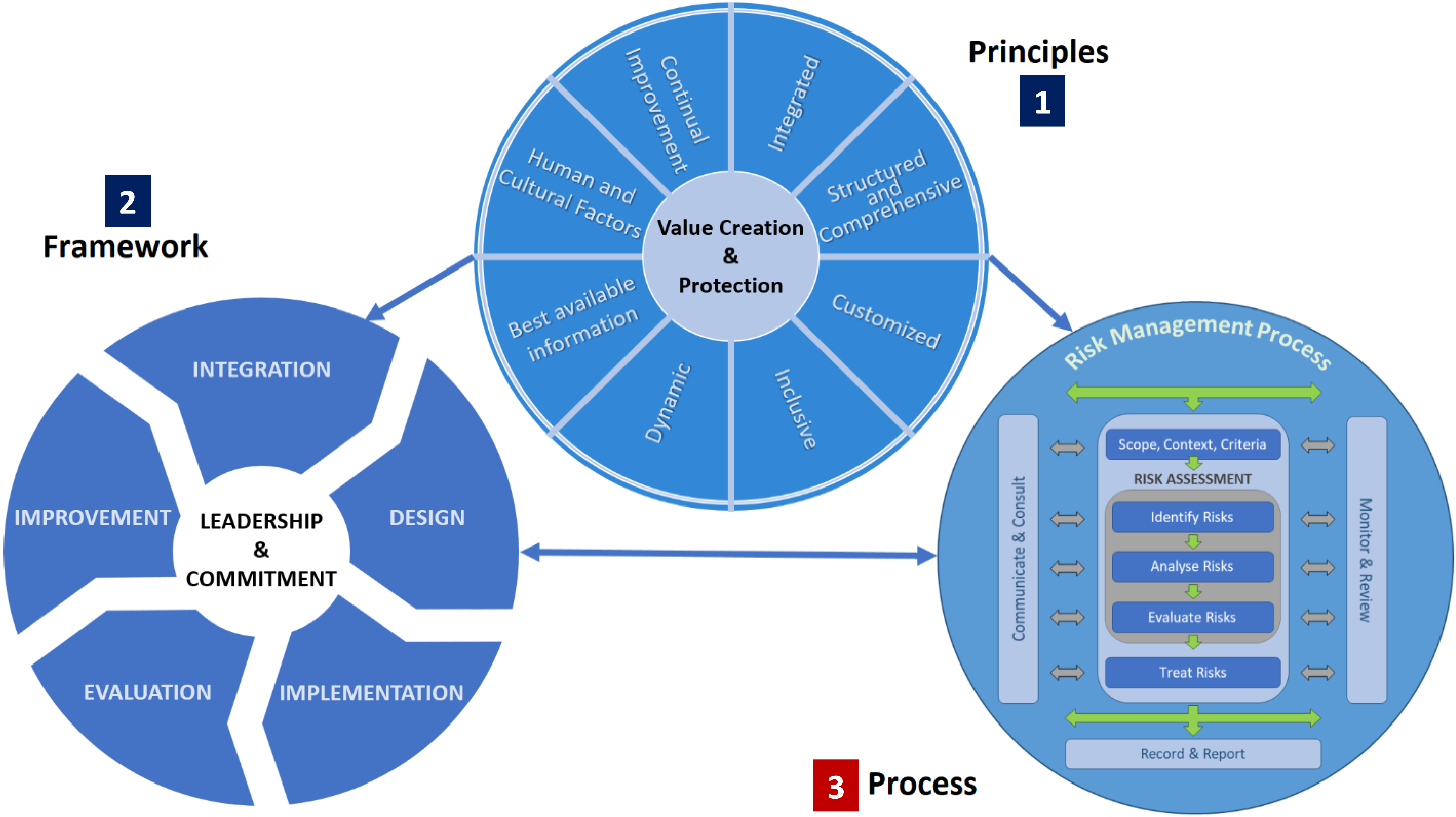
Scope, Context, Risk Criteria

2021-1-LV01-KA220-HED-000023056

Learning Objectives

- Provide knowledge about a systematic approach to the security risk management process
- Understand where to start when assessing the scope of security risk management for an organization in the line of ISO 31000
- Be familiar with the requirements and importance of establishing the context of organization to manage security risk
- Be able to define criteria according to which risks would be determined and assessed in the security management process

ISO 31000:2018 for Security Risk Management



Principles

1

Continual Improvement

Integrated

Structured and Comprehensive

Customized

Inclusive

Dynamic

Best available information

Human and Cultural Factors

Value Creation & Protection

2

Framework

INTEGRATION

DESIGN

IMPLEMENTATION

EVALUATION

IMPROVEMENT

LEADERSHIP & COMMITMENT

Risk Management Process

Communicate & Consult

Scope, Context, Criteria

RISK ASSESSMENT

Identify Risks

Analyse Risks

Evaluate Risks

Treat Risks

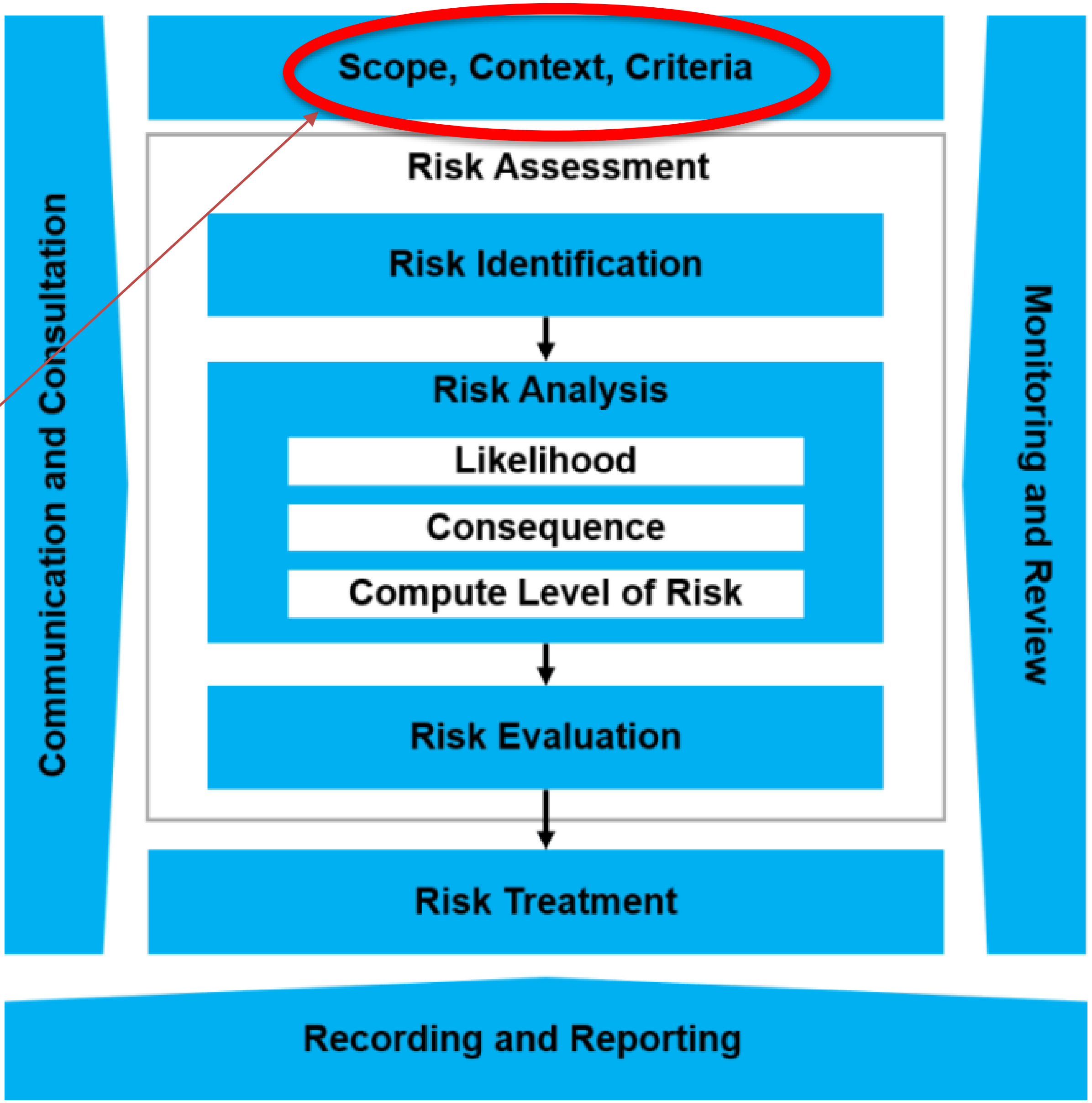
Monitor & Review

Record & Report

3 Process

Starting point in the process of Security Risk Management

Kazimieras Simonavicius University

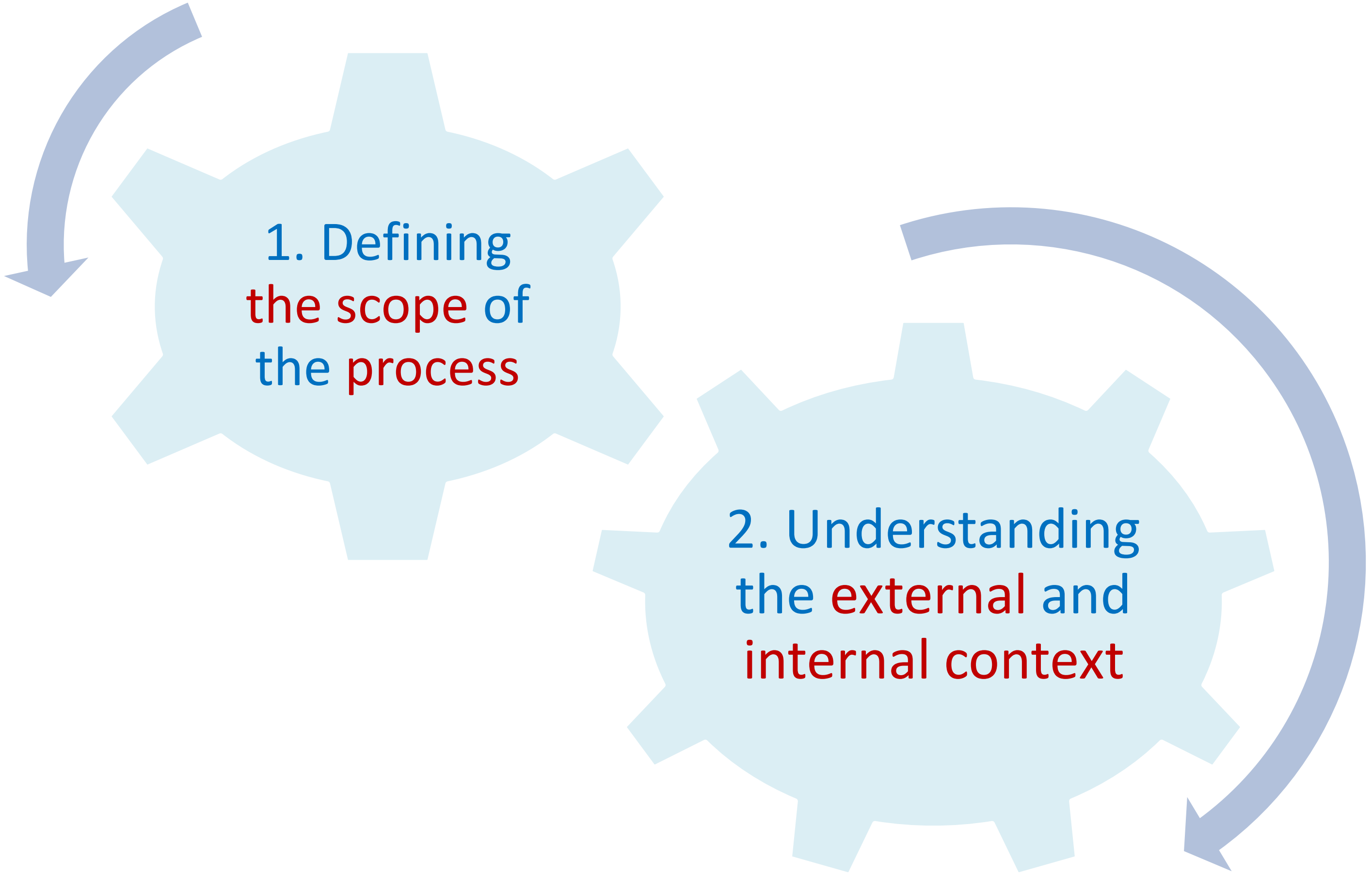


3: PROCESS

secureu
DIGITAL EDUCATION TOOLS
FOR SECURITY RISK MANAGEMENT

THE PURPOSE
of establishing the scope, the context and risk criteria

To customize the security risk management process, enabling effective risk assessment and appropriate risk treatment!



1. Defining the scope of the process

2. Understanding the external and internal context

DIGITAL EDUCATION TOOLS
FOR SECURITY RISK MANAGEMENT

DEFINING THE SCOPE

of security risk management activities

Security risk management process may be applied at different levels of organizations' activities:

- STRATEGIC
- OPERATIONAL
- PROGRAMME
- PROJECT
- TECHNICAL
- TACTICAL
- OTHERS

Considerations

- ❑ objectives and decisions that need to be made
- ❑ outcomes expected from the steps to be taken in the SRM process
- ❑ time, location, specific inclusions and exclusions
- ❑ appropriate risk assessment tools and techniques
- ❑ resources required
- ❑ responsibilities and records to be kept
- ❑ relationships with other projects, processes and activities

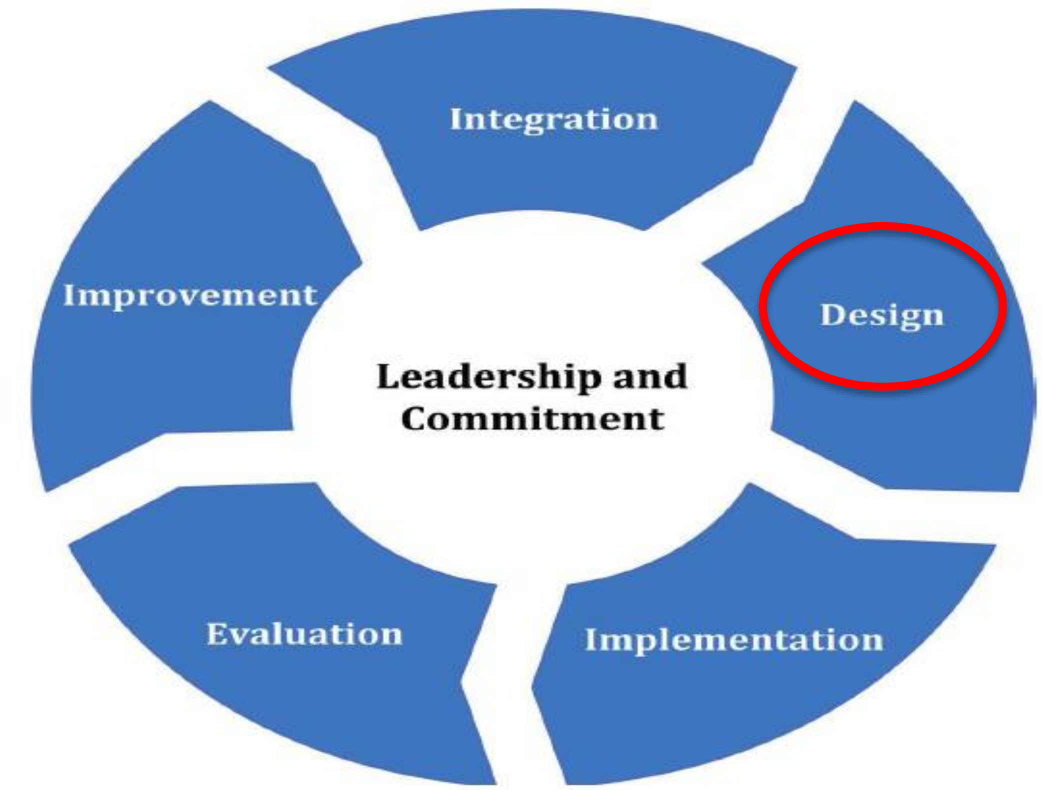
ESTABLISHING THE EXTERNAL AND INTERNAL CONTEXT

the *environment* in which the organization seeks to define and achieve its objectives

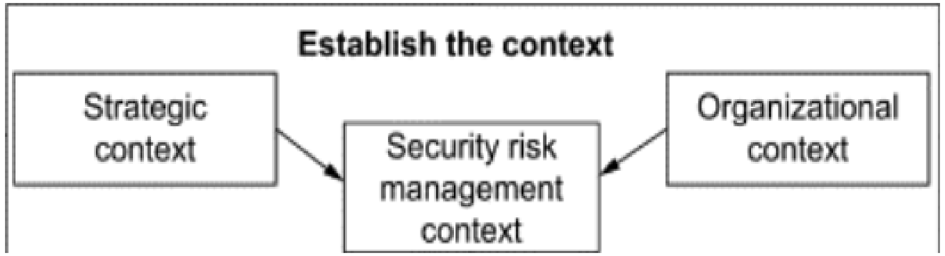
UNDERSTANDING THE ENVIRONMENT

1. … in which the organization operates

2. … reflect the specific environment of the activity to which the security risk management process is to be applied



Organization should ensure that *security risk management is integrated into all organizational activities*…. and *design* *the framework for managing security risk*


Establish the context

Strategic context

Security risk management context

Organizational context

FACTORS OF EXAMINING THE ORGANIZATION’S CONTEXT

EXTERNAL CONTEXT

- social, cultural, political, legal, regulatory, financial, technological, economic and environmental factors
- international, national, regional or local
- key drivers and trends affecting the objectives of the organization
- external stakeholders’ relationships, perceptions, values, needs and expectations
- contractual relationships and commitments
- the complexity of networks and dependencies

INTERNAL CONTEXT

- vision, mission and values
- governance, organizational structure, roles and accountabilities
- strategy, objectives and policies
- the organization’s culture
- standards, guidelines and models adopted by the organization
- capabilities, understood in terms of resources and knowledge (e.g. time, people, processes, systems and technologies)
- data, information systems and information flows
- relationships with internal stakeholders, taking into account their perceptions and values
- interdependencies and interconnections

THE IMPORTANCE of understanding the context

- ❑ Security risk management takes place in the context of *the objectives* and *activities of the organization*
- ❑ *Organizational factors* (external, internal) can be *a source of risk*
- ❑ The purpose and scope of the security risk management process may be *interrelated with the objectives of the organization as a whole*

DEFINING RISK CRITERIA

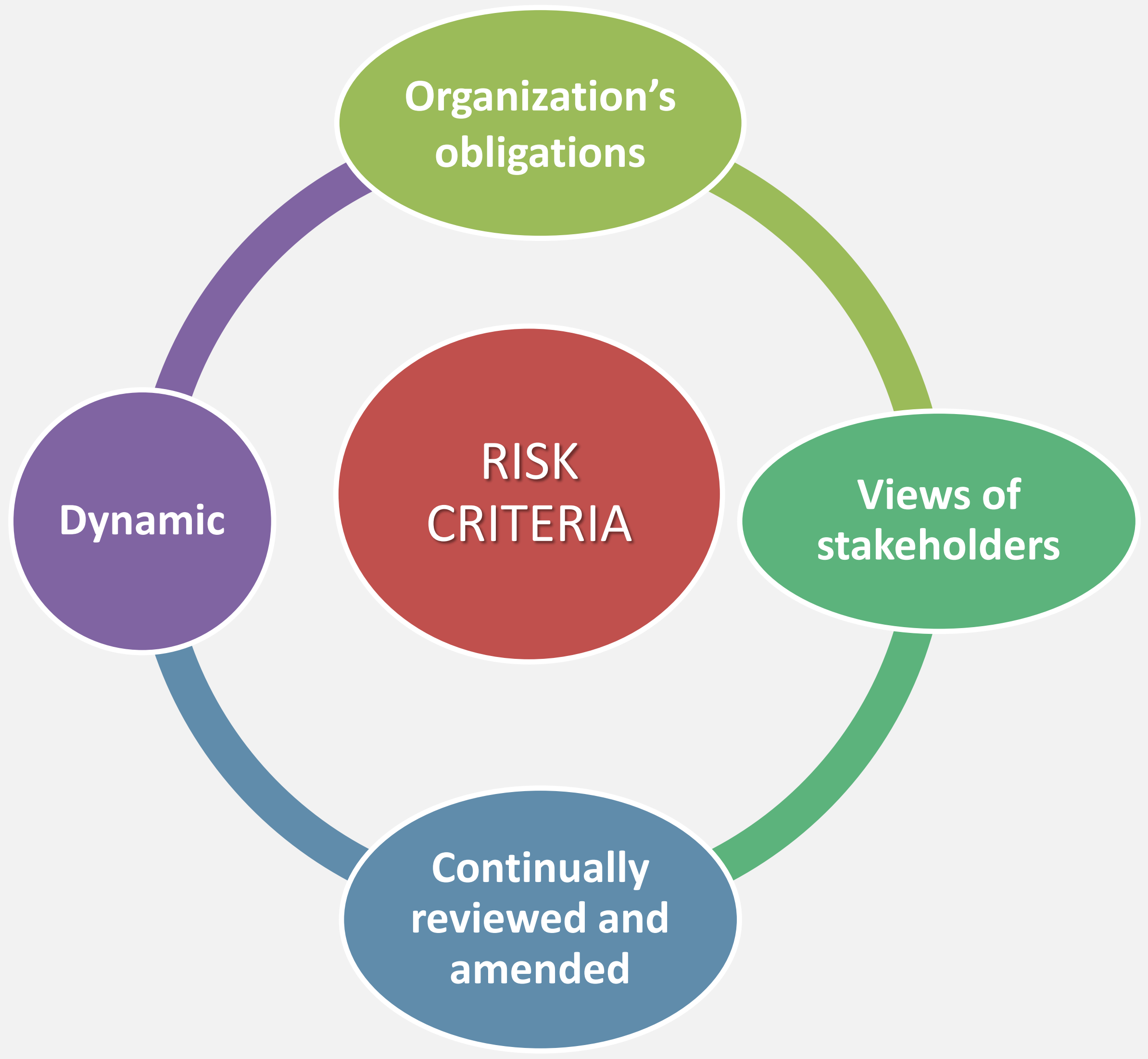
Before security risk assessment process, the organization should:

- specify the amount and type of security risk
- define criteria
  - (a) to evaluate the significance of risk, and
  - (b) to support decision making processes

RISK CRITERIA SHOULD

- be aligned with the risk management framework
- be customized to the specific purpose and scope of the activity under consideration
- reflect the organization’s values, objectives and resources
- be consistent with policies and statements about security risk management

REQUIREMENTS FOR DEFINING RISK CRITERIA



Considerations

- ❑ the nature and type of uncertainties that can affect outcomes and objectives (both tangible and intangible)
- ❑ how consequences (both positive and negative) and likelihood will be defined and measured
- ❑ time-related factors
- ❑ consistency in the use of measurements
- ❑ how the level of risk is to be determined
- ❑ how combinations and sequences of multiple risks will be taken into account
- ❑ the organization's capacity

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

THANK YOU!

https://security.turiba.lv

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

isecureu
DIGITAL EDUCATION TOOLS
FOR SECURITY RISK MANAGEMENT

This video is crated in frame of ERASMUS+ Cooperation partnership project «Digital education tools for security risk management»

Project number: 2021-1-LV01-KA220-HED-000023056

https://security.turiba.lv