



EXERCISE FOR SECURITY STUDENTS

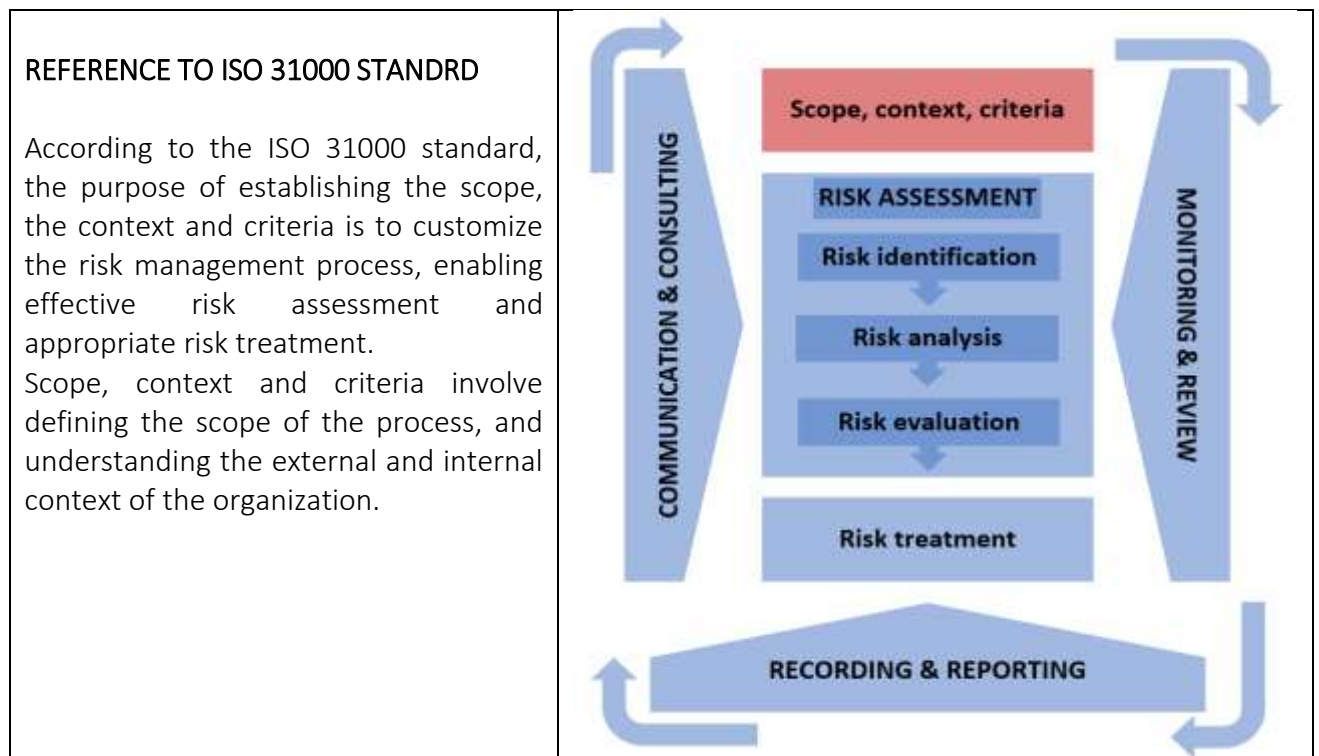
Scope, Context, Criteria in Security Risk Management Process

AUTHOR: Raimundas Kalesnykas, Kazimieras Simonavičius University, Lithuania

BACKGROUND:

The success of security risk management will depend on the effectiveness of the management framework, which assists in managing security risks effectively through the application of the risk management process at varying levels and within specific contexts of the organization.

Before starting the design and implementation of the framework for managing security risk, it is important: (a) to understand both the external and internal context of the organization; (b) define the external and internal parameters for risk management, and (c) set the scope and risk criteria for the security risk management process as described in ISO 31000:2018.



GOAL OF THIS EXERCISE

Students will get theoretical knowledge and enhance practical skills about the procedures and methods of understanding the context of the organization that allows them to establish the scope of security risk management process, and conduct evaluation of environment by using different methods from ISO 31000 in which the organization seeks to achieve its objectives for managing security risk.

TASK DESCRIPTION FOR STUDENTS:

- 1.** Form students' groups as instructed by a lecturer. Keep the diversity in forming groups (field of study, program, level and year of study, work experience – if any, etc.)
- 2.** Each students' group familiarizes itself with the *Case Scenario*, and with the specific task assigned to a separate student group on a *Case Scenario*. Case will be analysed in an organization (public, private) specifying the sector in which organization operates (state border protection agency, business company for developing critical infrastructure)
- 3.** Each students' group is given one method applicable to understanding and establishing the context for security risk management process following the requirements of ISO 37001.
- 4.** Familiarize yourself with the method given to you, and complete the task using brainstorming according to the lecturer's instruction. Time limit for the implementation of tasks to each group of students – 15 min.
- 5.** Prepare a short presentation of method given to you for your fellow students. Presentation is given optionally from the following ways: orally, post-it notes (flipchart), on the whiteboard, PowerPoint, etc.
- 6.** Each students' group will nominate the speaker to present the group outcomes/conclusions of the provided task for your fellow students. Time limit for the presentation is up to 5 min.
- 7.** Listen the presentations of the fellow students. After each presentation discuss 2 minutes with your group if their method would have been applicable for your target. Share your thoughts with the class in your turn.
- 8.** After all presentations and by leading the lecturer discuss in your group which of the presented parameters (internal and external) would be taken into account for the further process of managing security risk. Share your thoughts with the class. Time limit for the discussion is up to 10 min.

TASK DESCRIPTION FOR TEACHER / TRAINER:

- 1.** Create students' groups (not less than 3 and more than 5 people in one group is recommended). Decide on the method by which students will be assigned to groups.
- 2.** Provide a brief overview of *Case Scenario* related to security risk management process. Present the main provisions of establishing the context in the security risk management according to the ISO 31000.
- 3.** Explain the task assigned to the each group of students. References to the requirements for establishing the context of security risk management process are provided based on the ISO 31000.
- 4.** Assign each group of students with one of the provision from ISO 31000, i.e. understanding the organization and its context (public and/or private), establish external factors (context), establish internal factors (context), define risk criteria, and establish the scope of security risk management process. Depending on the number of groups of students, the content of the tasks can be narrowed or expanded.
- 5.** Develop and provide a template (paper document) for assignment to each group of students. Each group of students are asked to work on that template. Explain what outcomes/results are expected according to the given task.


6. Set time limit for the implementation of tasks to each group of students (15 min.)
7. Facilitate students' work and assist if they have questions on the provided tasks.
8. Instruct each group of students to prepare a short presentation of outcomes/conclusions under provided tasks. Presentation can be done orally, post-it notes (flipchart), on the whiteboard, PowerPoint, etc. Time limit for the presentation is up to 5 min.
9. After all presentations, lead all students in a discussion of which of the presented parameters (internal and external) would be taken into account for managing security risk. Time limit for the discussion is up to 10 min.
10. Summarize the overall results of the inputs to assignment of all groups of students.

ADDITIONAL SKILLS THAT THE STUDENT ACQUIRES THROUGH THIS ASSIGNMENT:

- Working in a group
- Working under time pressure
- Giving presentation and arguing their case
- Multi-disciplinary skills and critical thinking

SUPPORT MATERIALS

ISO 31000: Understanding the organisation and its context

| | |
|--|--|
|  <p style="text-align: center;">PESTLE</p> | <p>Common factors to consider when understanding the context of the organisation in relation to external factors can be assessed using the PESTLE acronym:</p> <ul style="list-style-type: none"> ◆ Political ◆ Economic ◆ Social ◆ Technological ◆ Legal ◆ Environmental <p>More: https://pestleanalysis.com/pest-analysis-template/</p> |
|--|--|

Defining the Scope

*different levels of the organization activities
(e.g. strategic, operational, programme, project, or other)*

- ◆ objectives and decisions that need to be made
- ◆ outcomes expected from the steps to be taken in the 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 Context

environment in which the organization seeks to achieve its objectives

EXTERNAL

- the social, cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environmental factors, whether 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

- 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. capital, time, people, intellectual property, processes, systems and technologies)
- data, information systems and information flows, decision making processes (both formal and informal)
- relationships with internal stakeholders, taking into account their perceptions and values
- contractual relationships and commitments
- interdependencies and interconnections

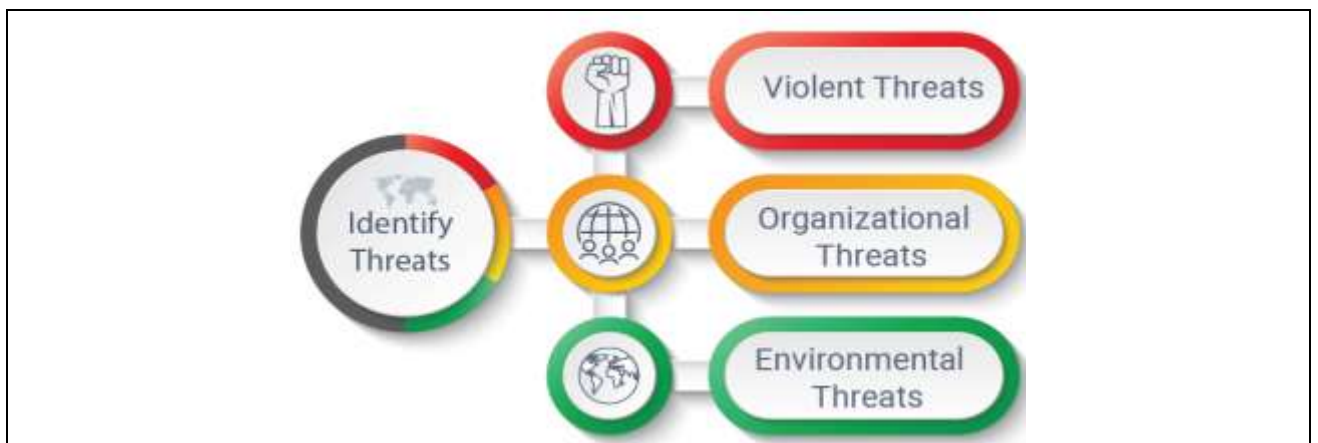
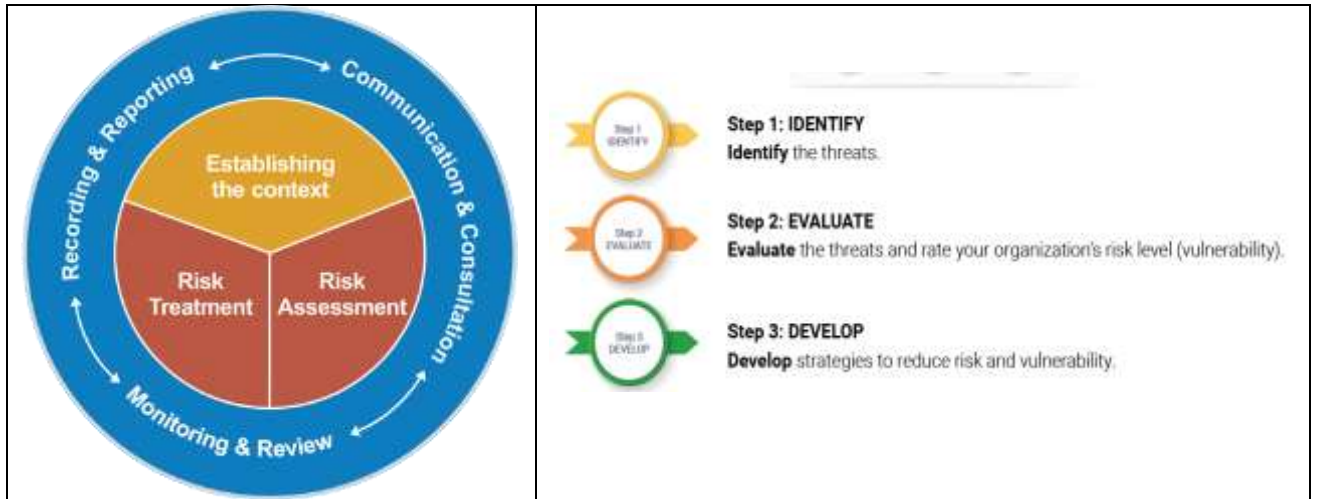
Defining Risk Criteria

- ◆ 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 of the likelihood and/or consequence(s)
- ◆ consistency in the use of measurements
- ◆ how the level of risk is to be determined, becomes acceptable or tolerable
- ◆ how combinations and sequences of multiple risks will be taken into account and, if so, how and which combinations should be considered
- ◆ the organization's capacity

SAMPLE

SECURITY RISK MANAGEMENT is the process of *identifying, evaluating, and treating risks* around the organization’s activities

CONTEXT ANALYSIS – IDENTIFY THREATS



| Violent Threats | Organizational Threats | Environmental Threats |
|--|--|---|
| <ul style="list-style-type: none"> • Targeted armed attack • Non-targeted armed conflict • Kidnapping • Terrorism • Carjacking • Sexual violence • Civil unrest • Religious violence • Crime • Other types of violence | <ul style="list-style-type: none"> • Reputation risk • Financial risk (banking system, currency exchange, theft, misappropriation) • Corruption • Legal risk (work permits, compliance with domestic legislation, resistance to advocacy) • Political risk • Workplace violence or discrimination • Cultural challenges | <ul style="list-style-type: none"> • Natural hazards (weather, earthquakes, flooding) • Medical risks (access to suitable medical treatment for staff) • Health-related issues (food, water, disease, stress) • Traffic and roadside accidents • Other accidents • Fire |

More: <https://frontex.europa.eu/what-we-do/monitoring-and-risk-analysis/ciram/>