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

secureu DIGITAL EDUCATION TOOLS FOR SECURITY RISK MANAGEMENT

ERASMUS+ Strategic partnership "Digital education tools for security risk management"
Project number: 2021-1-LV01-KA220-HED-000023056

EXERCISE FOR SECURITY STUDENTS

Risk analysis and new technologies

AUTHORS: Javier Dorado, School of Prevention and Integral Safety and Security, Spain

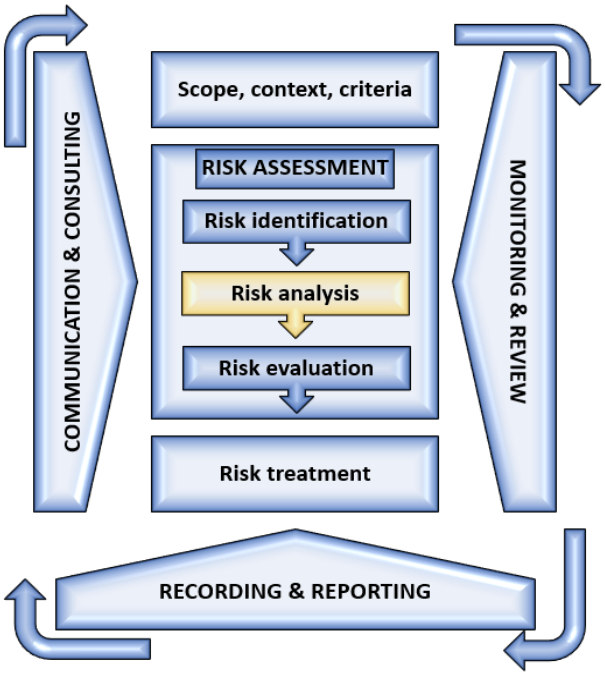
BACKGROUND:

In accordance with ISO 31000, risk analysis consists of understanding the nature of the risk and its characteristics including, if necessary, the level of risk.

REFERENCE TO ISO 31000 STANDARD

Risk analysis includes a thorough and detailed consideration of uncertainties, risk sources, consequences, probabilities, events, scenarios, controls and their effectiveness, such as:

- The likelihood of events and their consequences;
- The nature and magnitude of these consequences;
- Complexity and interconnectedness of the scenario;
- Time-related factors and volatility;
- The effectiveness of existing controls;
- Levels of sensitivity and confidence.



GOAL OF THIS EXERCISE:

Through this exercise, students will be able to conduct a risk analysis in a scenario involving new technologies for security purposes. This can include drones, AI driven technologies, or any other technologies that may affect the security procedures in every company or administration.

TASK DESCRIPTION FOR STUDENTS:

1. Choose a specific scenario in your assigned groups. First, decide if the case will be analysed in a private corporation or public administration / authorities. Once decided, specify in which sector this organization operates (for example, for corporations, a company which organizes events, or for public authorities, local police).
2. Once your group has decided on the scenario, think about one security procedure that this institution might have to address (for example, for the company above, a process to control the access to an event).
3. Once both the general scenario and the specific context have been decided upon, think about a risk that this situation might present. In order to do so, as ISO 31000 states, consider: a) the likelihood of this risk and its consequences; b) the nature and magnitude of those consequences; c) the complexity and interconnectedness of the scenario laid out; and d) the time-related factors.
4. Now think about a new technology that could be useful to tackle the risk. For example, in the scenario set as an example, AI driven technology to biometrically identify persons, or a drone with a camera incorporated to control access. When doing so, take into account that ISO 31000 includes the analysis of the effectiveness of these controls.
5. Lastly, draw up a list of potential risk associated with the use of such technologies. To do so, you can start by asking questions within your group: Are these technologies effective? What unexpected risk may be associated with their use? Normative risk? Risk for the physical integrity of the persons? Risk for the procedure that your department must guarantee (in this example, access control)?

TASK DESCRIPTION FOR TEACHER / TRAINER:

The teacher's tasks are as follows:

1. Make groups of students based on the total number of participants. Ideally, each group should consist of at least three students and up to five students, to make the discussion more flexible and participative.
2. As this exercise centres around risk analysis within the ISO 31000 standard, briefly explain the concept and steps as previously referred in the background and reference to ISO box.
3. Apart from providing information about the risk analysis concept, explain that before reflecting and implementing it, it is necessary to set a specific scenario (which kind of organizations, private, public?), which activity / public duties are associated with that organization, and which main risk they may face in their daily operation. In journalistic terms, they should think about the W's (where, what, who…).

4. Insist on the necessity of specifying the scenario in terms of those w's, before starting to implement the risk analysis procedure.

5. The last step of the task (see point 5 in the previous box, task description for students) can start by asking specific questions such as: Are these technologies effective? What unexpected risk may be associated with their use? Normative risk? Risk for the physical integrity of the persons? Risk for the procedure that your department must guarantee (in this example, access control)?

ADDITIONAL SKILLS THAT THE STUDENT ACQUIRES THROUGH THIS ASSIGNMENT:

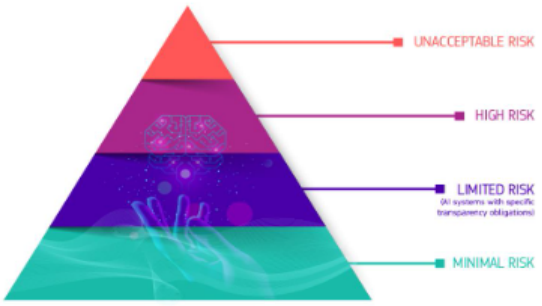
Since this task centres around risk analysis, the main objective of this exercise is to thoroughly assess the risk related to the growing use of new technologies in specific scenarios. By doing this, the students not only become familiar with the ISO standard, but also learn to critically reflect on the consequences and impact that new technologies have both in the private and public sector.

SUPPORT MATERIALS

High risk

- Critical infrastructures (e.g. transport), that could put the life and health of citizens at risk
- Educational or vocational training, that may determine the access to education and professional course of someone's life (e.g. scoring of exams)
- Safety components of products (e.g. AI application in robot-assisted surgery)
- Employment, workers management and access to self-employment (e.g. CV sorting software for recruitment procedures)
- Essential private and public services (e.g. credit scoring denying citizens opportunity to obtain a loan)
- Law enforcement that may interfere with people's fundamental rights (e.g. evaluation of the reliability of evidence)
- Migration, asylum and border control management (e.g. verification of authenticity of travel documents)
- Administration of justice and democratic processes (e.g. applying the law to a concrete set of facts)

They will all be carefully assessed before being put on the market and throughout their lifecycle.



Building trust through the first-ever legal framework on AI. European Commission. Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/excellence-and-trust-artificial-intelligence_en

Key policy objectives:

1. Set enabling conditions for AI's development and uptake
2. Build strategic leadership in high-impact sectors
3. Make the EU the right place for AI to thrive
4. Ensure AI technologies work for people

Boosting excellence in AI. European Commission. Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/excellence-and-trust-artificial-intelligence_en