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 Treatment in the Security Risk Management Process

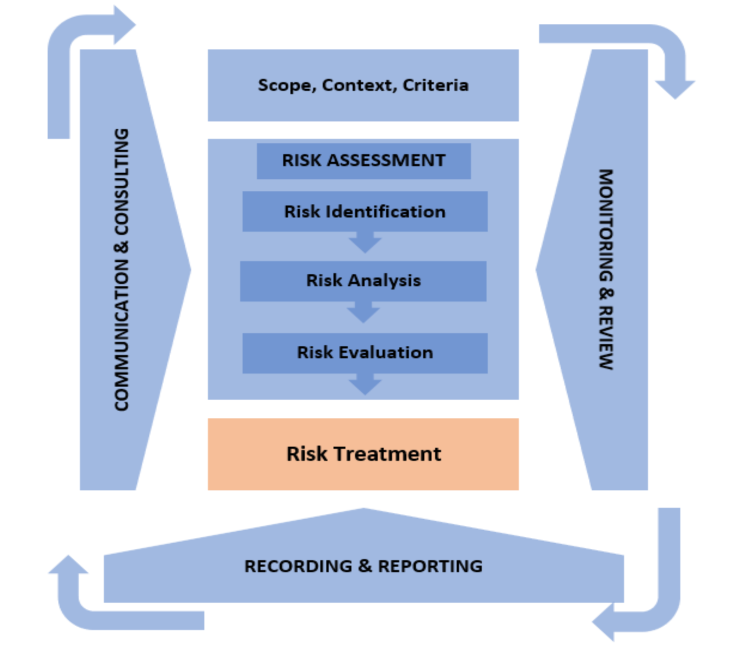
AUTHOR: Raimundas Kalesnykas, Turiba University, Latvia

BACKGROUND:

The security risk management process involves the systematic application of organization’s policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting security risk. All activities of an organization involve risk. Organizations manage security risk by identifying it, analysing it and then evaluating whether the risk should be modified by risk treatment in order to satisfy their risk criteria. Risk treatment is the plan of implementing organization’s strategies and actions to appropriately deal with the security threats and manage it in an effective way. Risk treatment should always go hand in hand with other security risk management processes enlisted in the standard of ISO 31000:2018

REFERENCE TO ISO 31000 STANDRD

According to the ISO 31000:2018 standard, the purpose of risk treatment is to select and implement options for addressing security risk.
Risk treatment involves an iterative security risk management process of: (a) formulating and selecting risk treatment options; (b) planning and implementing risk treatment; (c) assessing the effectiveness of that treatment; (d) deciding whether the remaining risk is acceptable; and (e) if not acceptable, taking further treatment.



GOAL OF THIS EXERCISE

Students will get theoretical knowledge and understand the impact of risk treatment in planning the security risk management process. They will also learn how to formulate and select risk treatment options based on identified threats to the organization, using the security risk matrix, and develop a risk treatment plan according to the requirements of ISO 31000:2018.

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 (police duty station, court buildings and premises, business company for developing critical infrastructure, etc.). As well, the 5x5 risk assessment matrix is presented for each group with identified threats according to the severity of the risk and the likelihood of its occurrence
3. Each students' group is given one method applicable to: a) choose and prioritize high risks along a spectrum from likely and very likely occurrence to significant and severe severity; b) formulate and select risk treatment options / or measures to mitigate risk; c) take action and plan the implementation of risk treatment. Please comply with the requirements set out in Clause 5 of ISO 31000:2018.
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 10 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 (no 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 selecting and implementing options for addressing security risk in accordance with the 31000:2018.
3. Explain the task assigned to each group of students. References to the requirements for security risk treatment are provided in the line of 31000:2018.
4. Assign each group of students with one or mixed the provisions from 31000:2018, i.e. a) choose high risks to the organization's security along a spectrum from likely and very likely occurrence to significant and severe severity; b) prioritize high risks to the organization's security along a spectrum from likely and very likely occurrence to significant and severe severity; c) formulate and select appropriate measures to mitigate risk base on identified

threats to the organization's security; d) plan actions for risk treatment deciding whether the remaining high risk is acceptable or not.

5. Depending on the number of groups of students, the content of the tasks can be narrowed or expanded.

6. 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 (paper document). Explain what outcomes/results are expected according to the given task.

7. Set time limit for the implementation of tasks to each group of students (15 min.)

8. Facilitate students' work and assist if they have questions on the provided assignment.

9. Instruct each group of students to prepare a short presentation of outcomes/conclusions under provided assignment. Presentation can be done orally, post-it notes (flipchart), on the whiteboard, PowerPoint, etc. Time limit for the presentation is up to 10 min.

10. After all presentations, lead all students in a discussion of the rationale for selection of the risk treatment options, including the expected benefits to be gained in managing security risk. Time limit for the discussion is up to 10 min.

11. 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 one's opinion on a case
- Multi-disciplinary skills and critical thinking

SUPPORT MATERIALS

ISO 31000 SECURITY RISK MANAGEMENT PROCESS

6.5. RISK TREATMENT

Is a collective term for organization's security policies and/or strategies chosen to respond to a specific risk, bound to achieve the desired outcome concerning the threat to security

- process to modify security risk
- can create new risks or modify existing risks
- referred to as "security risk mitigation", "security risk elimination", "security risk prevention", "security risk reduction"

RISK TREATMENT PROCESS

STEPS	CRITERIA / REQUIREMENTS
1. BRAINSTORMING AND SELECTION OF RISK TREATMENT OPTIONS	Options for treating security risk may involve one or more of the following: · avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk

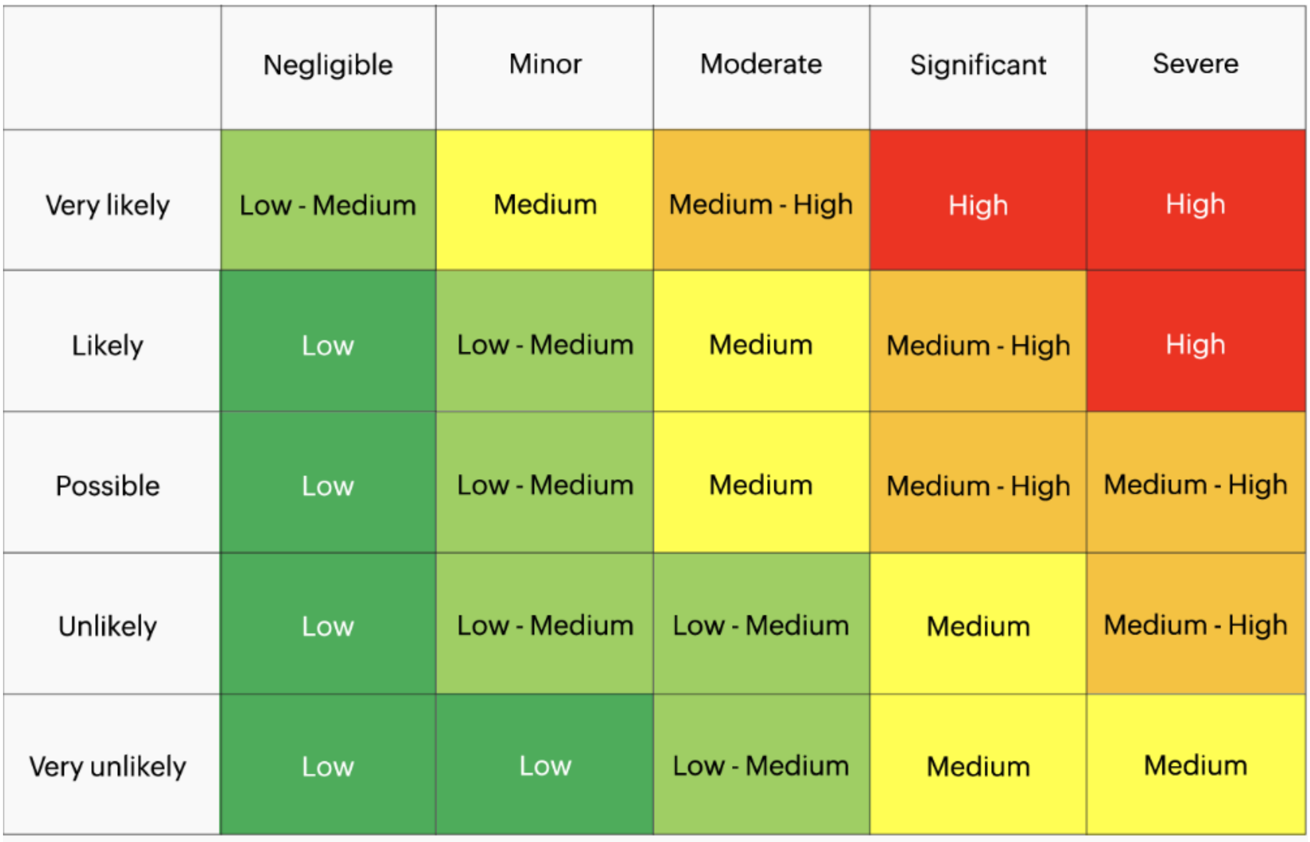
Selecting the most appropriate security risk treatment option(s) involves balancing the potential benefits derived in relation to the achievement of the objectives against costs, effort or disadvantages of implementation.	· taking or increasing the risk in order to pursue an opportunity · removing the risk source · changing the likelihood · changing the consequences · sharing the risk (e.g. through contracts, buying insurance) · retaining the risk by informed decision Risk treatment options should be chosen based on a detailed analysis of the accompanying factors: the overall security risk strategy of the organization, its resources, the objectives of the organisation, as well as predicted costs against the benefits. The selection of security risk treatment options should be made in accordance with the organization's objectives, risk criteria and available resources.
2. PLANNING AND IMPLEMENTING RISK TREATMENT · *The purpose of security risk treatment plan is to specify how the chosen treatment options will be implemented, so that arrangements are understood by those involved, and progress against the plan can be monitored.* · *The security risk treatment plan should clearly identify the order in which risk treatment should be implemented.* · *The security risk treatment plan should be integrated into the security risk management strategy and processes of the organization, in consultation with appropriate stakeholders.*	The information provided in the security risk treatment plan should include: · the rationale for selection of the treatment options, including the expected benefits to be gained; · those who are accountable and responsible for approving and implementing the plan · the proposed actions · the resources required, including contingencies · the performance measures · the constraints · the required reporting and monitoring; · when actions are expected to be under taken and completed
3. ASSESSING THE EFFECTIVENESS OF RISK TREATMENT It involves evaluating how well the security risk treatment plan and measures implemented to manage security risks are working. This process ensures that the risk treatment is reducing security risks to acceptable levels and achieving the desired outcomes	Assessing the effectiveness of risk treatment involves: · measure performance, i.e. use metrics and indicators to assess how well risk treatment are performing, also include tracking the frequency and impact of security risk events · evaluate residual risk, i.e. assess the level of security risk that remains after the risk treatment have been applied · compare against organisation's objectives, i.e. check if the residual security risk levels align with the organization's risk appetite and objectives · monitor, review and adjust, i.e. the risk treatment is not effective, identify new strategies or adjust existing ones to better manage security risk
4. DECIDING WHETHER THE REMAINING RISK IS ACCEPTABLE	The process of deciding whether the remaining security risk is acceptable include: · determination the level of security risk that remains after implementing risk treatment

Deciding whether the remaining security risk is acceptable involves evaluating the residual risk, which is the risk that remains after all risk treatment measures have been applied. If the residual security risk is deemed acceptable, it means the organization is willing to live with the remaining risk given the benefits and costs of further risk treatment.	· comparison of residual risk with the organization's risk appetite and tolerance levels · analysis of the potential impact and likelihood of the residual security risk, that helps in understanding the severity and probability of the risk occurrence · make a decision whether the residual security risk is acceptable or if further actions are needed to mitigate security risk further
5. IF NOT REMAINING RISK ACCEPTABLE, TAKING FURTHER ACTIONS FOR RISK TREATMENT It means that the residual security risk level is still too high and could potentially harm the organization or its objectives. In such cases, further actions are necessary to reduce the risk to an acceptable level.	Decision makers in the organization should be aware of the nature and extent of the remaining security risk after risk treatment. The remaining security risk should be documented and subjected to monitoring, review and, where appropriate, further treatment.

SAMPLE

SECURITY RISK ASSESSMENT MATRIX

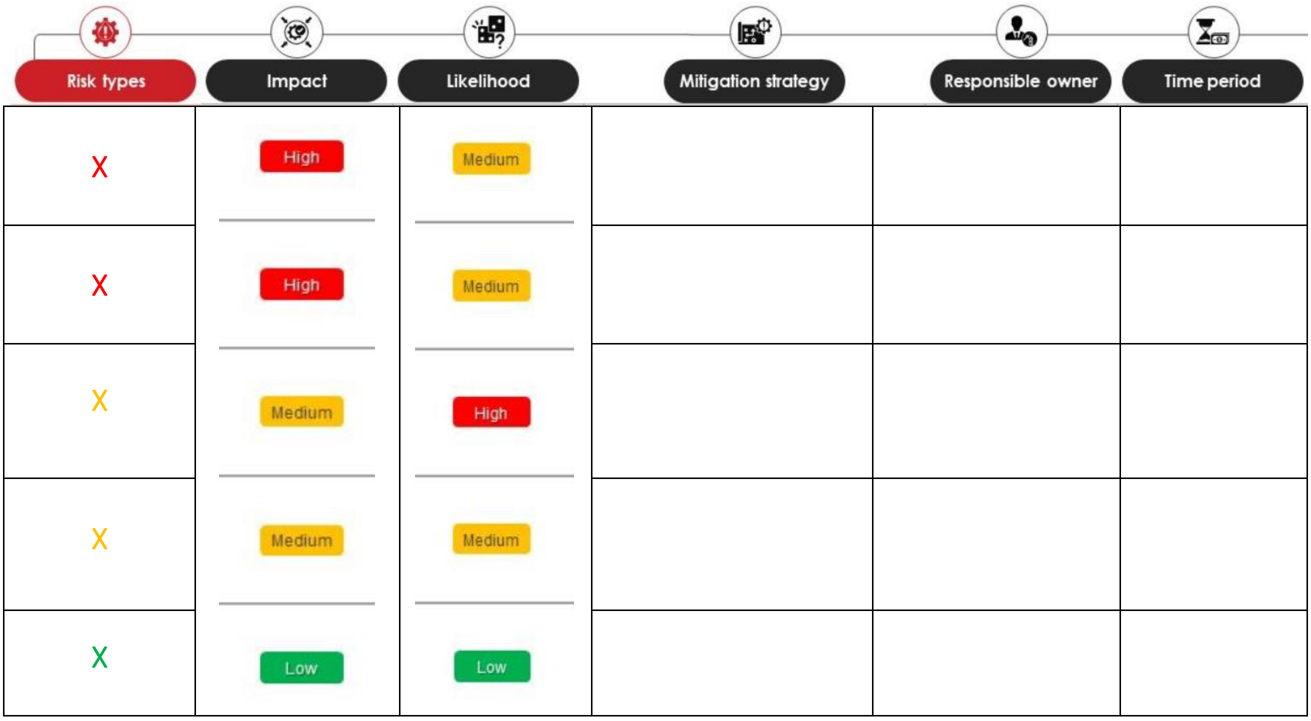
The 5x5 security risk assessment matrix includes five rows and columns, with the columns representing the severity of the risk and the rows representing the likelihood of its occurrence. Risks can be categorized into 25 different cells, based on the severity of the risk and its likelihood. The spectrum varies from unlikely and not severe to highly likely and severe.



	Negligible	Minor	Moderate	Significant	Severe
Very likely	Low - Medium	Medium	Medium - High	High	High
Likely	Low	Low - Medium	Medium	Medium - High	High
Possible	Low	Low - Medium	Medium	Medium - High	Medium - High
Unlikely	Low	Low - Medium	Low - Medium	Medium	Medium - High
Very unlikely	Low	Low	Low - Medium	Medium	Medium

SAMPLE

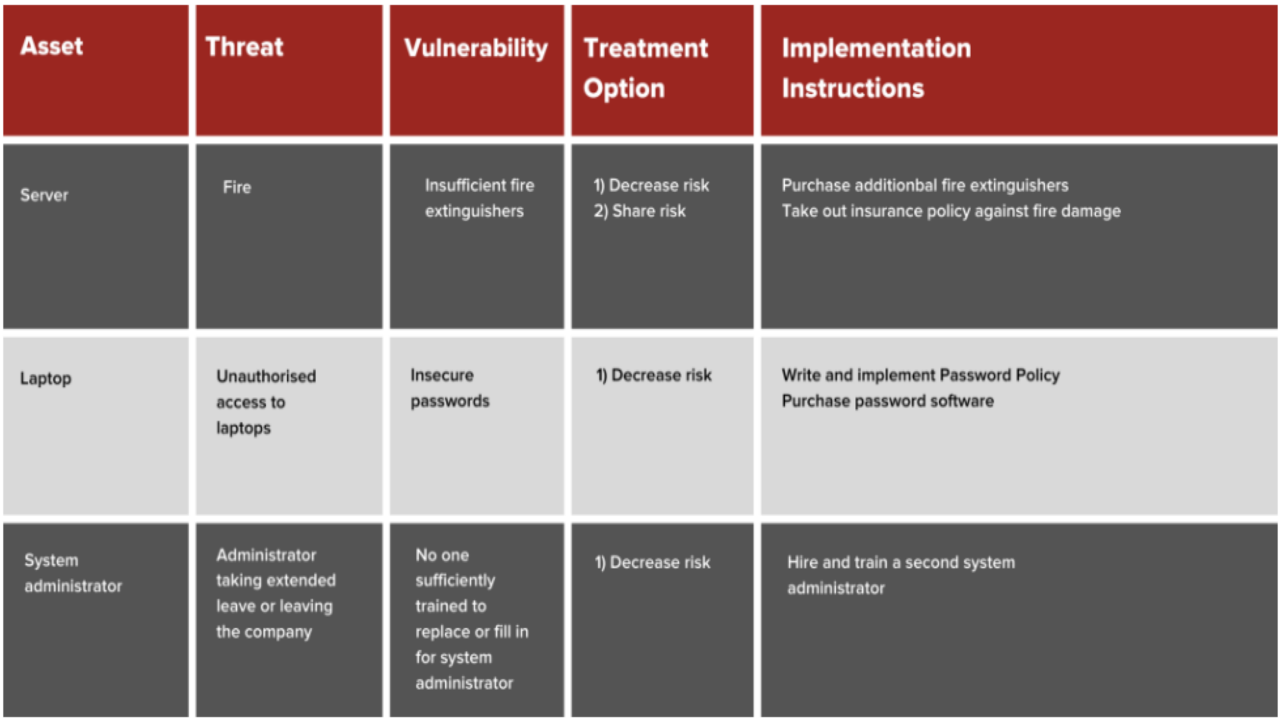
Risk treatment plan



Risk types	Impact	Likelihood	Mitigation strategy	Responsible owner	Time period
X	High	Medium			
X	High	Medium			
X	Medium	High			
X	Medium	Medium			
X	Low	Low			

SAMPLE

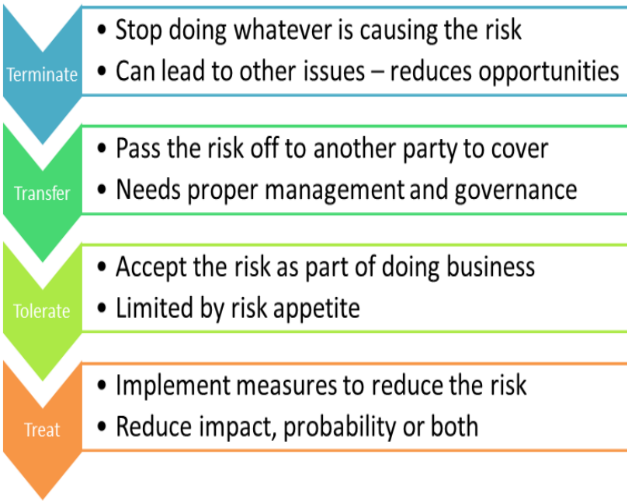
Risk treatment plan example



Asset	Threat	Vulnerability	Treatment Option	Implementation Instructions
Server	Fire	Insufficient fire extinguishers	1) Decrease risk 2) Share risk	Purchase additionbal fire extinguishers Take out insurance policy against fire damage
Laptop	Unauthorised access to laptops	Insecure passwords	1) Decrease risk	Write and implement Password Policy Purchase password software
System administrator	Administrator taking extended leave or leaving the company	No one sufficiently trained to replace or fill in for system administrator	1) Decrease risk	Hire and train a second system administrator

SAMPLE

SECURITY RISK TREATMENT OPTIONS

 Terminate • Stop doing whatever is causing the risk • Can lead to other issues – reduces opportunities Transfer • Pass the risk off to another party to cover • Needs proper management and governance Tolerate • Accept the risk as part of doing business • Limited by risk appetite Treat • Implement measures to reduce the risk • Reduce impact, probability or both	Risk Avoidance: avoid the activities that are causing the risk; this might mean discontinuing a project or changing a process that is too risky. Risk Reduction: implement additional controls or measures to reduce the likelihood or impact of the risk, i.e. this could involve improving safety protocols, enhancing security measures, or upgrading technology. Risk Transfer: shift the risk to another party, such as through insurance or outsourcing, i.e. the financial impact of the risk is borne by another entity. Risk Sharing: distribute the risk among multiple parties, i.e. this can be done through partnerships or joint ventures where the risk is shared.

More: https://continuity2.com/blog/risk-treatment-with-examples