Funded by
the European Union

secureu
DIGITAL EDUCATION TOOLS
FOR SECURITY RISK MANAGEMENT

ERASMUS+ cooperation partnership

Digital education tools for

SECURITY RISK MANAGEMENT

PRACTICAL TASKS

for higher education institutions teaching security

FOCUS ON SECURITY RISK MANAGEMENT

INTRODUCTION

Over the past few years, security has become a critical issue for many European countries. The world is grappling with a wide range of challenges, including migration, cyber-attacks, and emerging threats such as the crisis caused by the pandemic and the ongoing war in Ukraine.

As a result, there is a clear and urgent need not only for high-quality training for young security specialists but also for training that equips them to better prepare for crises and mitigate numerous threats before they escalate into full-blown crises.

This need led to the formation of a consortium comprising seven partner organizations from six countries. The consortium's primary objective is to develop diverse digital teaching and learning materials focused on security risk management. As part of this initiative, we offer practical tasks designed to train students in security risk assessment, crisis response, and threat mitigation, allowing them to apply their knowledge in realistic scenarios and develop essential problem-solving skills.

ABOUT THE PROJECT

Partners from Latvia, Lithuania, Finland, the Netherlands, Norway, and Spain combined their knowledge and expertise to develop an ERASMUS+ cooperation partnership project, aimed at creating various teaching materials on security risk management.

The project seeks to establish a sustainable network of security specialists capable of long-term cooperation. As part of the project, the partners developed recommendations for universities that train security specialists in Europe. In addition, the partnership created comprehensive, up-to-date digital teaching materials and tools, all gathered on a single web platform. This platform offers the latest information on security risk management, making it accessible to security experts, students, and academics alike.

Find more materials on project website: https://security.turiba.lv/

ABOUT THIS PUBLICATION

This publication is a comprehensive collection of 14 practical tasks designed to enhance students' skills in security risk management. Developed within the SECUREU project, these exercises provide hands-on learning opportunities that allow students to apply theoretical knowledge to real-world security challenges.

The tasks focus on key areas such as risk assessment, crisis response, threat mitigation, cybersecurity, and decision-making in high-risk environments. They are structured to be completed individually or in groups, fostering both independent critical thinking and collaborative problem-solving.

By engaging with these practical exercises, students will develop essential analytical, strategic, and operational skills that are crucial for future security professionals. This publication serves as a valuable educational resource for universities, training institutions, and anyone seeking to strengthen their expertise in security risk management.

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

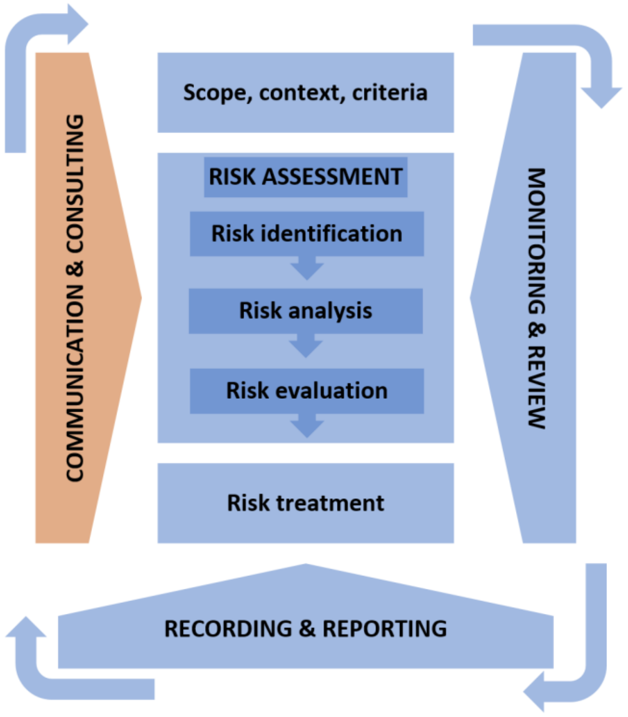
EXERCISE FOR SECURITY STUDENTS

Promotion of knowledge and awareness of security issues in society, organisations and companies

AUTHORS: Uģis Začs, Kristīne Neimane, Turiba University, Latvia

BACKGROUND:

In a study conducted at the end of 2022, experts from six countries emphasized that security specialists lack the knowledge and skills to inform and explain security issues and the importance of security risks to both - their colleagues and society in general. It is clear that without the understanding and involvement of colleagues, ensuring security in an organization or company becomes impossible. If the staff of a company is not aware of the importance of security, it will be challenging to identify and manage risks effectively. Therefore, one of the tasks of a security specialist in an organization or company is to inform, educate, and involve colleagues in identifying and managing security risks. The full report can be found here: https://security.turiba.lv/2022/12/06/what-skills-young-security-specialists-are-missing/

REFERENCE TO ISO 31000 STANDRD According to the ISO 31000 standard, communication is of paramount importance in effective risk management. Communication plays a critical role in all stages of the risk management process, including risk identification, assessment, treatment, and monitoring.	 COMMUNICATION & CONSULTING Scope, context, criteria RISK ASSESSMENT Risk identification Risk analysis Risk evaluation Risk treatment MONITORING & REVIEW RECORDING & REPORTING

GOAL OF THIS EXERCISE:

To provide skills and abilities to develop, formulate and prepare information about security and security risk management in the organization. To develop skills in creating various types of informational materials for colleagues, employees of the organization or company or for the general public.

TASK DESCRIPTION FOR STUDENTS:

1. Individually or in groups, choose a target group for which informational material on security risks management will be created. It can be a real or fictional company or organization (micro-enterprise, SME, public organization, educational institution, etc.) or a group of society (such as children, young people, teachers, seniors, workers, etc.).
   a. If you choose a company - clearly define the company's field of activity;
   b. If you choose a specific group in society – define the framework (age, gender, place of residence, other parameters).
2. Your task now is to develop short informative material (1 - 2 A4 pages) that explains a selected aspect of security or security risk management.
3. It is important to create informative material that is easily understandable and visually attractive. We recommend using visual editing tools such as Canva, Infogram, or Piktochart to create the material. Canva also allows free downloads for the materials created. You can find beginner tutorial videos on YouTube: https://www.youtube.com/playlist?list=PLATYfhN6gQz8GiTG_nUxVar8ycrt9hJxL
4. Present your material and explain the information included in it - why exactly this target group was chosen, why the information included in the material is important for a specific target group and what knowledge the target group will gain by getting acquainted with the informative material.

An illustrative example is attached. The example was created using infogram.com

TASK DESCRIPTION FOR TEACHER / TRAINER:

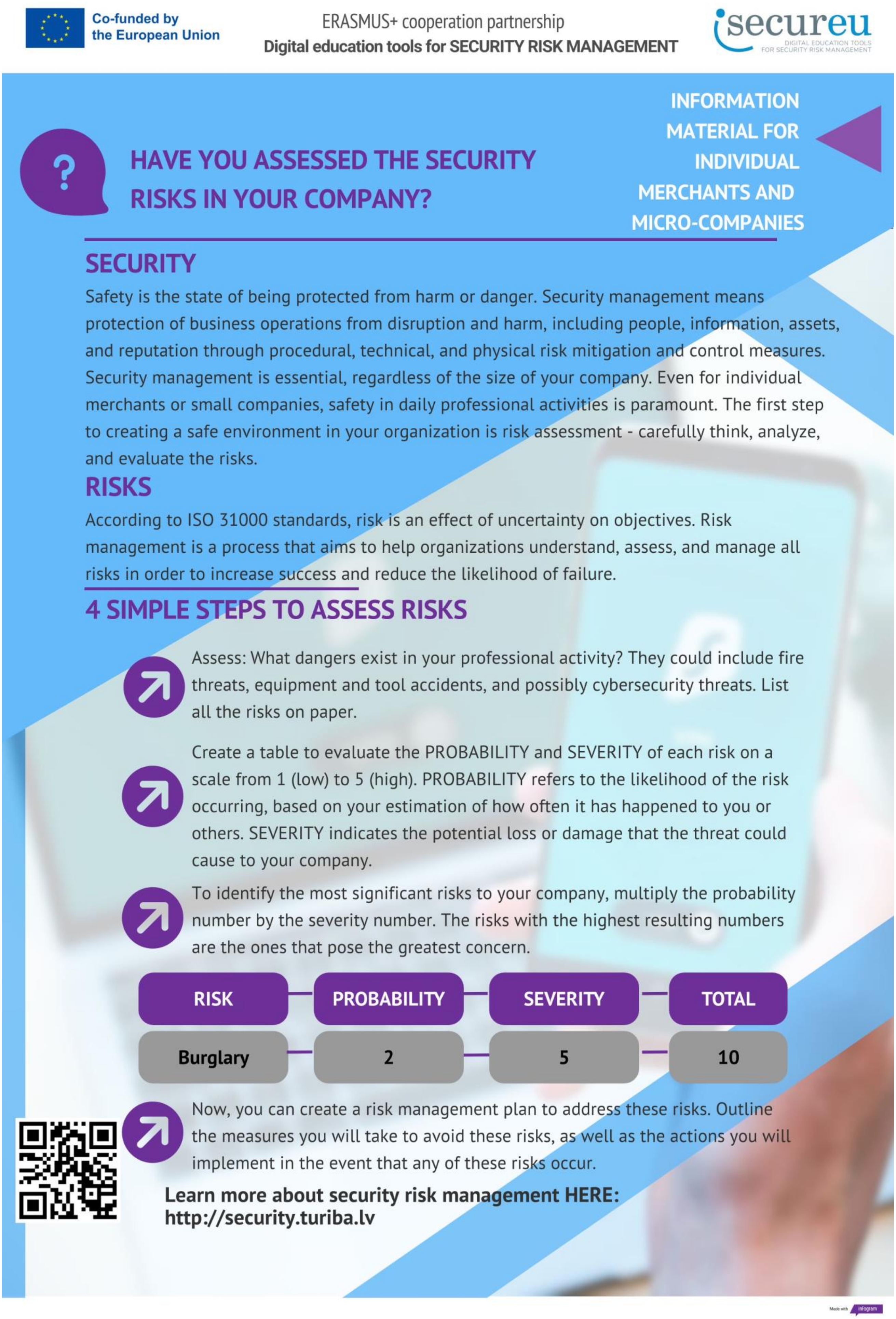
The teacher's tasks are as follows:

1. Create students' groups (not more than 4 people in one group is recommended).
2. Explain the task to the students, emphasizing the importance of developing skills to effectively communicate safety information to colleagues and the public.. It is recommended to present the Study on skills of young security specialists: https://security.turiba.lv/2022/12/06/what-skills-young-security-specialists-are-missing/
3. Assist students in selecting the target group and the focus of informational material. Provide examples and guidance if needed.
4. If students lack experience and skills in using visualization tools such as Canva, Infogram, or Piktochart, provide an introduction and basic training on one of these visual editing tools.
5. Evaluate the informational materials developed by students and discuss their content, providing recommendations for improvements.

ADDITIONAL SKILLS THAT THE STUDENT ACQUIRES THROUGH THIS ASSIGNMENT:

Ability to work in a team; skills to formulate information and opinion, digital skills (visual editing skills).

EXAMPLE



Co-funded by the European Union

ERASMUS+ cooperation partnership

Digital education tools for SECURITY RISK MANAGEMENT

secureu DIGITAL EDUCATION TOOLS FOR SECURITY RISK MANAGEMENT

INFORMATION MATERIAL FOR INDIVIDUAL MERCHANTS AND MICRO-COMPANIES

HAVE YOU ASSESSED THE SECURITY RISKS IN YOUR COMPANY?

SECURITY

Safety is the state of being protected from harm or danger. Security management means protection of business operations from disruption and harm, including people, information, assets, and reputation through procedural, technical, and physical risk mitigation and control measures. Security management is essential, regardless of the size of your company. Even for individual merchants or small companies, safety in daily professional activities is paramount. The first step to creating a safe environment in your organization is risk assessment - carefully think, analyze, and evaluate the risks.

RISKS

According to ISO 31000 standards, risk is an effect of uncertainty on objectives. Risk management is a process that aims to help organizations understand, assess, and manage all risks in order to increase success and reduce the likelihood of failure.

4 SIMPLE STEPS TO ASSESS RISKS

- Assess: What dangers exist in your professional activity? They could include fire threats, equipment and tool accidents, and possibly cybersecurity threats. List all the risks on paper.
- Create a table to evaluate the PROBABILITY and SEVERITY of each risk on a scale from 1 (low) to 5 (high). PROBABILITY refers to the likelihood of the risk occurring, based on your estimation of how often it has happened to you or others. SEVERITY indicates the potential loss or damage that the threat could cause to your company.
- To identify the most significant risks to your company, multiply the probability number by the severity number. The risks with the highest resulting numbers are the ones that pose the greatest concern.

RISK	PROBABILITY	SEVERITY	TOTAL
Burglary	2	5	10

- Now, you can create a risk management plan to address these risks. Outline the measures you will take to avoid these risks, as well as the actions you will implement in the event that any of these risks occur.

Learn more about security risk management HERE:
http://security.turiba.lv

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

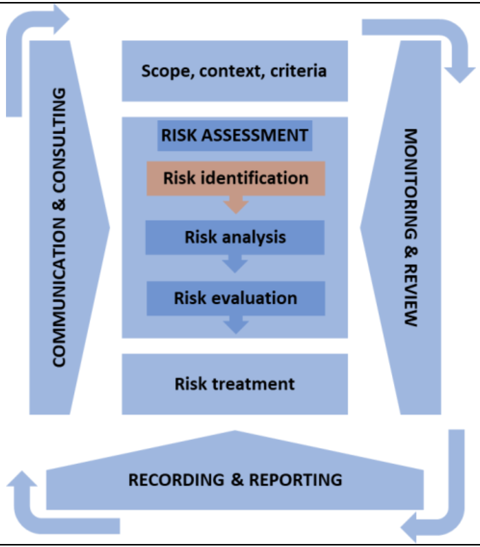
EXERCISE FOR SECURITY STUDENTS

Risk identification toolkit

AUTHORS: Kaci Bourdache, Hanna Iisakkila Rojas

BACKGROUND:

Managing risks requires thorough risk identification as one of the first steps of the process, as described in ISO 31000:2018. Depending on the context and goals of risk management, the most applicable methods should be chosen for that individual case.

REFERENCE TO ISO 31000 STANDRD According to the ISO 31000 standard, risk identification is the first step of a risk assessment.	 Scope, context, criteria RISK ASSESSMENT Risk identification Risk analysis Risk evaluation Risk treatment COMMUNICATION & CONSULTING MONITORING & REVIEW RECORDING & REPORTING

GOAL OF THIS EXERCISE:

Students will familiarise themselves with various risk identification methods from the IEC 31010:2019 standard, test some of them, and conduct comparison between different methods and their applicability in risk management.

TASK DESCRIPTION FOR STUDENTS:

1. Form groups as instructed by teacher
2. Each group is given one method applicable to risk identification from IEC 31010:2019
3. Under guidance from teacher, define a physical target, such as a building or premises or a part of it. The target should be e.g., business premises such as schools, commercial buildings, workplaces, warehouses, etc.
4. Familiarize yourself with the method given to you and prepare a short presentation of that method for your fellow students.
5. Use the method given to identify security risks for your target. In addition to the premises, property and people, be aware of what the activities and operations carried out within them are.
6. Write down the results of your identification as instructed by the teacher. Prepare to present your target and results to fellow students.
7. Present the method (as prepared in step 4), your assigned target, and the results of your risk identification to fellow students (as prepared in step 6)
8. Listen to 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. Would the method give you different results?
9. After all presentations discuss in your group which of the presented methods would be best for your target. Share your thoughts with the class.

TASK DESCRIPTION FOR TEACHER / TRAINER:

1. Before class, estimate the number of students and how many groups of approximately four students they would form. Decide on any method you prefer to assign to them.
2. Before class, for each group choose one method applicable to risk identification from IEC 31010:2019, section “B.2 Techniques for identifying risk”
3. Optionally:
   - If you wish the identification exercise to be carried out as a desktop exercise, you could prepare providing students with blueprints and other information about the targets. They can also use open-source information, such as Google Maps, Google Earth, etc.
   - If you wish the exercise to be carried out in a physical location, make sure you have access and proper facilities within it. You may also want to divide up the facilities for the groups beforehand.
4. In class, assign students into groups of approximately four students.
5. Assign each group one of the methods from IEC 31010:2019.
6. Each student group should have a physical target, such as a building or premises or a part of it. The target should be e.g., business premises such as schools, commercial buildings, workplaces, warehouses, etc. You can assign these yourself or let the students decide. In

any case, it is recommended to approve all the targets so that they are suitable for the assignment.

7. Instruct students to familiarize themselves with the method given to them, and to prepare a short presentation of that method for their fellow students. You can decide the delivery method of the presentation. It is recommended to limit the presentation to max. 5 minutes.

8. Instruct students to use the method given to identify security risks for their target. In addition to the premises, property and people, they should be aware of what activities and operations are carried out within them. The identification can be carried out as a theoretical exercise, as a desktop exercise using information about their target, or as a physical exercise on site – or any combination of these.

9. Instruct students to write down the results of their identification; this can be done on e.g., post-it notes, on the whiteboard, PowerPoint presentation, in an online environment, etc. Instruct students to prepare to present their target and results to their fellow students. You can decide the delivery method of the presentation. It is recommended to limit the presentation to max. 5 minutes.

10. While the students prepare their method presentation, identify risks, and prepare their results presentation, your task is to facilitate their work and assist if they have questions on the method and its use, for example.

11. Instruct students to present their method, their assigned target, and the results of their risk identification to their fellow students.

12. During presentations, make sure to chair the discussion and keep the groups within the given schedule. The process is as follows:
    - Approx. max. 10 minutes for one group presentation
    - After each presentation groups should discuss 2 minutes within their groups if the presented method would have been applicable for their target.
    - Groups are encouraged to share their thoughts with the class. The key question is: would the method give you different results?

13. After all the presentations, lead all students in a discussion about which of the presented methods would be best for their target.

ADDITIONAL SKILLS THAT THE STUDENT ACQUIRES THROUGH THIS ASSIGNMENT:

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

EXERCISE FOR SECURITY STUDENTS

Risk analysis and new technologies

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

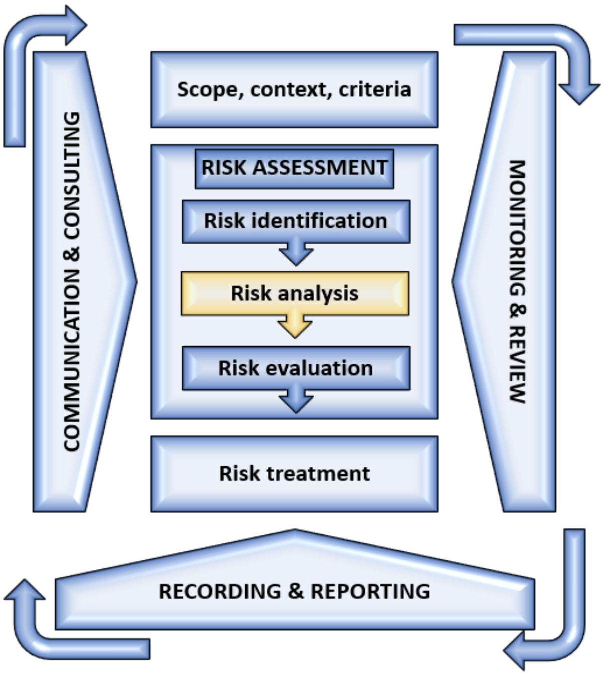
BACKGROUND:

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…).

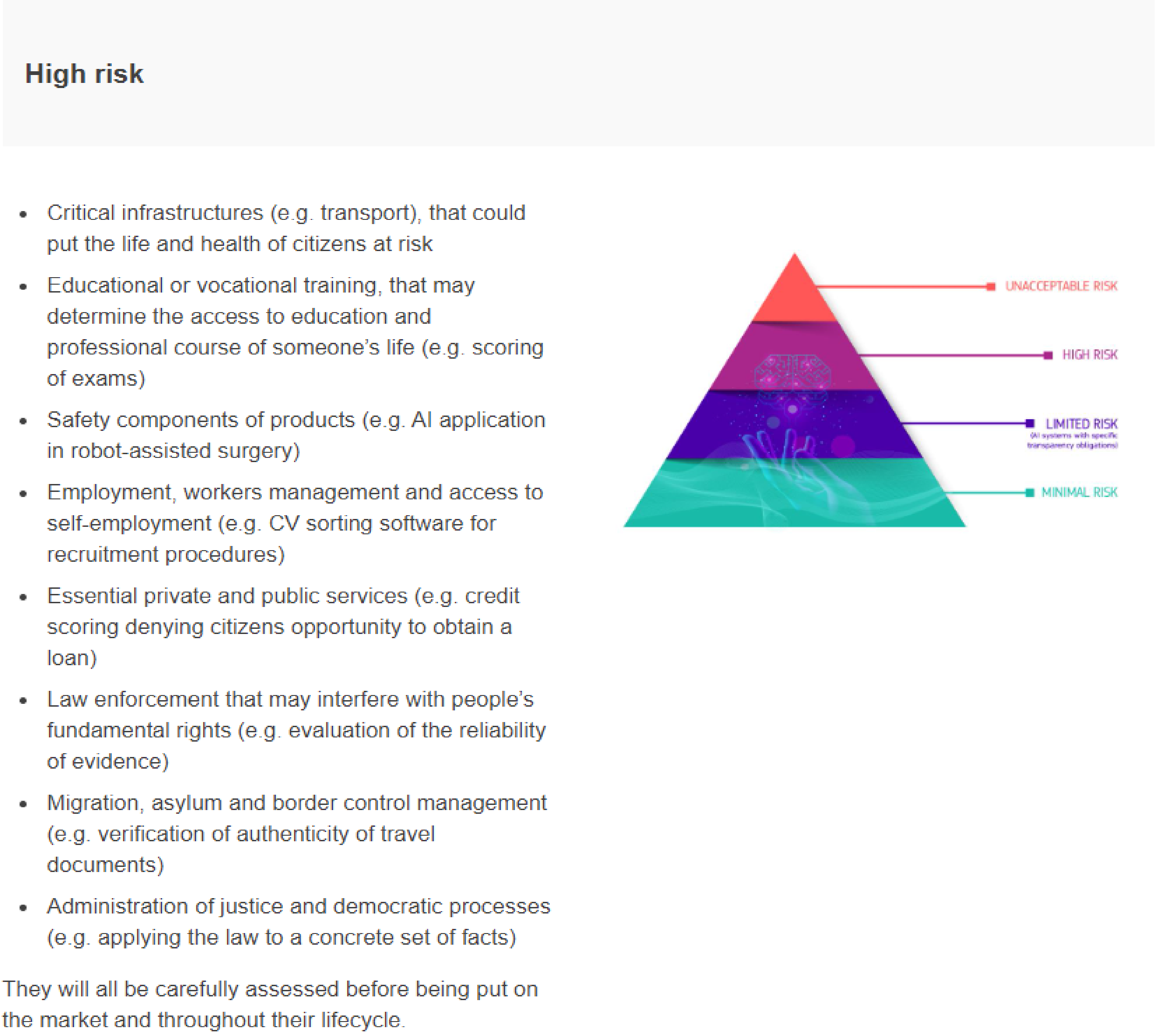
4. Insist on the necessity of specifying the scenario in terms of those w's, before starting to implement the risk analysis procedure.

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

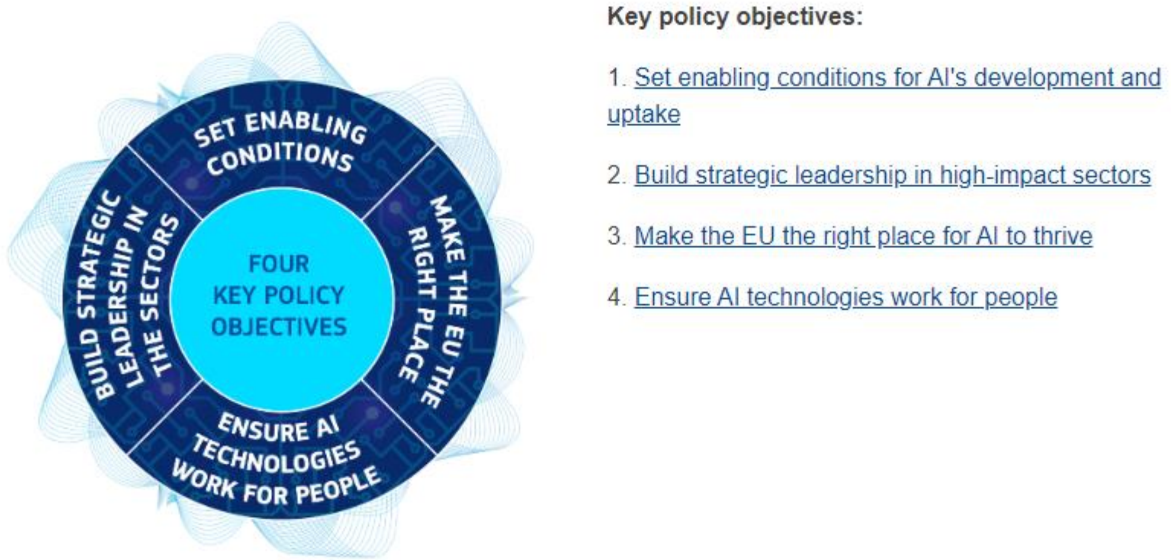


High risk

- 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


FOUR KEY POLICY OBJECTIVES
SET ENABLING CONDITIONS
MAKE THE EU THE RIGHT PLACE
ENSURE AI TECHNOLOGIES WORK FOR PEOPLE
BUILD STRATEGIC LEADERSHIP IN THE SECTORS

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

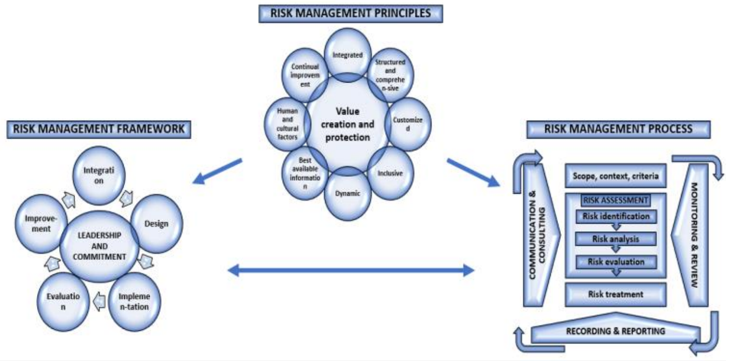
EXERCISE FOR SECURITY STUDENTS

Security Risk Management Cycle based on ISO 31000

AUTHOR: Lambert Bambach

BACKGROUND:

Building a sustainable approach of Security Risk Management requires a thorough comprehension of the building blocks of the ISO 31000:2018. Depending on the context and goals of an organisation, is started with one of the building blocks to realize security risk management. The most applicable building block should be chosen for that individual case.

REFERENCE TO ISO 31000 STANDRD According to the ISO 31000 standard, the main building blocks are Risk management framework, Risk management principles and Risk management process.	 RISK MANAGEMENT PRINCIPLES Integrated Structured and comprehe n-sive Customize d Inclusive Dynamic Best available informatio n Human and cultural factors Continual improvem ent Value creation and protection RISK MANAGEMENT FRAMEWORK Integrati on Design Impleme n-tation Evaluatio n Improve-ment LEADERSHIP AND COMMITMENT RISK MANAGEMENT PROCESS COMMUNICATION & CONSULTING Scope, context, criteria RISK ASSESSMENT Risk identification Risk analysis Risk evaluation Risk treatment MONITORING & REVIEW RECORDING & REPORTING

GOAL OF THIS EXERCISE:

Students will familiarise themselves with the building blocks from the IEC 31000:2018 standard, using three cases, on the basis of which they must indicate substantiated: Where do you start in the Security Risk Management Cycle based on ISO 31000? Why do you start there? What are you going to do? Who will be your allies?

TASK DESCRIPTION FOR STUDENTS:

1. Form groups as instructed by teacher
2. Each group is given three cases to work on
3. Under guidance from teacher, define where do you start in the Security Risk Management Cycle based on ISO 31000? Why do you start there? What are you going to do? Who will be your allies?
4. Familiarize yourself with the building blocks of your choice which you start with and write down the results of your choice for approach, concerning Where do you start in the Security Risk Management Cycle based on ISO 31000? Why do you start there? What are you going to do? Who will be your allies?
5. Prepare a short presentation for your fellow students in the other groups about the results of your choice for approach, concerning: Where do you start in the Security Risk Management Cycle based on ISO 31000? Why do you start there? What are you going to do? Who will be your allies?
6. Present your presentation for your fellow students in the other groups.
7. Listen the presentations of the fellow students. After each presentation discuss 2 minutes with your group if their approach of the cases would have been applicable for you too. Share your thoughts with the class in your turn. Would your approach per case been different knowing due to the new insides given by the other group(s)?
8. After all presentations discuss in your group which of the presented approaches would be best for each case. Share your thoughts with the class.

TASK DESCRIPTION FOR TEACHER / TRAINER:

1. Before class, estimate the number of students and how many groups of approximately four students they would form. Decide on any method you prefer to assign them.
2. Before class, for each group should have a copy of the ISO 31000: 2018; a copy of the case and have read the best practice article Implementing Security Risk Management for an organization operating as an electricity grid manager in de vital infrastructure
3. Optionally:
    - If you wish the exercise to be carried out in a physical location, make sure you have access and proper facilities within it. You may also want to divide the facilities for the groups beforehand.
4. In class, assign students into groups of approximately four students.
5. Instruct students to familiarize themselves with the ISO 31000:2018; The Case; The article and handout.
6. Instruct students to write down the results of their choice for approach this can be done on e.g., post-it notes, on the whiteboard, PowerPoint presentation, in an online environment,

etc. Instruct students to prepare to present their results to their fellow students. You can decide the delivery method of the presentation. It is recommended to limit the presentation to max. 5 minutes.

9. While the students discuss their approach, write down their choice for the approach and prepare their presentation on: Where do you start in the Security Risk Management Cycle based on ISO 31000? Why do you start there? What are you going to do? Who will be your allies? Your task is to facilitate their work and assist if they have questions.

7. Instruct students to present their short presentation for their fellow students in the other groups about the results of your choice for approach, concerning: Where do you start in the Security Risk Management Cycle based on ISO 31000? Why do you start there? What are you going to do? Who will be your allies?

8. During presentations, make sure to chair the discussion and keep the groups within the given schedule. The process is as follows:
    - Approx. max. 10 minutes for one group presentation
    - After each presentation groups should discuss 2 minutes within their groups if the presented method would have been applicable for their target.
    - Groups are encouraged to share their thoughts with the class. The key question is: would the choice for approach give you different results?

9. After all presentations, lead all students in a discussion of which of the presented approach would be best for their target.

ADDITIONAL SKILLS THAT THE STUDENT ACQUIRES THROUGH THIS ASSIGNMENT:

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

CASE SECURITY RISK MANAGEMENT AND THE ADMINISTRATIVE ORGANIZATION

The Logistic Organization

Direction

THE LOGISTIC ORGANIZATION has 14 physical shops (the 'shops'), a webshop and one national distribution centre warehouse. THE LOGISTIC ORGANIZATION has a turnover of € 370,000,000 per year, of which € 270,000,000 for the physical shops and € 100,000,000 for the web shop. THE LOGISTIC ORGANIZATION's position in the market is as strong as its relationship with its customers. The long-term relationship with customers is therefore central to its strategy.

Vision

- Customer experience
- Customer centreed

Mission

- Empathy (feeling): THE LOGISTIC ORGANIZATION knows the individual needs of the customer.
- Expertise (knowing): THE LOGISTIC ORGANIZATION has the knowledge to meet the individual needs of the customers.
- Experience (can): THE LOGISTIC ORGANIZATION introduces you to the best electronic products

Values

- Customer first
- Do what you say
- Realizing ideas
- Always better

Promises

- Better for the customer
- Better for the employee
- Better for the environment

Business model

- Lower costs
- Strong brands
- Wide range of products

Strategic pillars

- Strong customer loyalty
- Broadening of the range of products available
- Online sales
- Attractive products
- Corporate responsibility
- Good for our people

Ambition

- Always better
- Growth in turnover and profit
- Reduction of losses and costs through better control of primary processes

The service level of THE LOGISTIC ORGANIZATION is high. Short delivery times and lowest price including service ensure that THE LOGISTIC ORGANIZATION looks closely at the contribution that products make to profit.

Developments

- Stock is kept to a minimum. Measurability is essential, whether it's advertising campaigns, inventory control or loss prevention;

- The LOGISTIC ORGANIZATION also aims to introduce self-scan of articles to increase convenience for the customer;

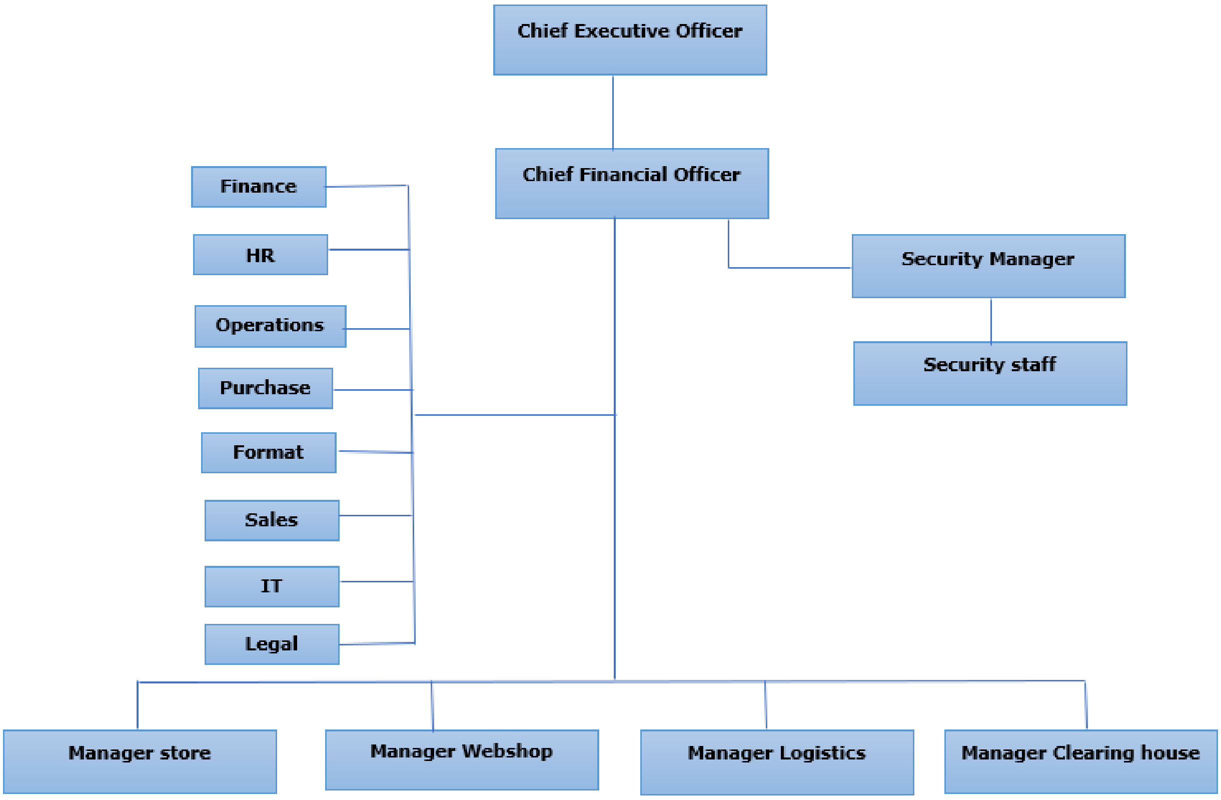
- In addition, THE LOGISTIC ORGANIZATION wishes to achieve a growth in profits by increasing online sales;

- In shop and online, the same price applies. If a consumer can order the desired product cheaper elsewhere, THE LOGISTIC ORGANIZATION will deliver it at that same price. In this way, THE LOGISTIC ORGANIZATION prevents customers from delaying their buying decision;

- THE LOGISTIC ORGANIZATION delivers within 24 hours after ordering the products;

- THE LOGISTIC ORGANIZATION is currently developing THE LOGISTIC ORGANIZATION -Smart. From these smaller hubs in shopping centres, the electronics chain aims to experiment with express delivery. The Smart shops will be located in larger shopping centres where customers can go for a smaller range of products and advice. In the Smart hubs, omnichannel is becoming the norm. Via invisible walls in the shop, customers can check whether a product is available, what it looks like and place orders. As a vision for the future, THE LOGISTIC ORGANIZATION sees that these orders are delivered to the customer's home the same day.

Arrangement



Organization chart of THE LOGISTIC ORGANIZATION

Managers shops, web shop, logistics and distribution centre warehouse

As far as is known, the managers have no substantive tasks and responsibilities in the field of security, but are responsible for the management of the employees in the field of safety in the shops, the web shop and the distribution centre warehouse.

Manager support departments

As far as is known, the managers of the Finance, Operations, Purchasing, Format, Sales, IT, Legal departments have no substantive tasks and responsibilities in the field of security, but are responsible for managing the employees in their department.

Security

Security is organized at a central level. Security is a staff service. As far as is known, the Chief Financial Officer has no substantive tasks and responsibilities in the field of security, but is still accountable for the Security department and managing the head of the Security. reports to the Chief Executive Officer. The budget of the Security department is set at group level. Every organizational unit of THE LOGISTIC ORGANIZATION can call on the Security department when it deems it necessary. Expenses for investments and costs of maintenance are borne by the THE LOGISTIC ORGANIZATION.

Security Manager

- The Security Manager is responsible for managing, planning and leading the implementation of the security arrangement. This arrangement was developed at the head office, the risk classification process is part of this. In addition, the head of the security department and his department support the national and local management by performing tasks such as conducting investigations, security audits and ensuring that the shops, the web shop and the distribution centre warehouse comply with the legal regulations. In addition, the manager oversees THE LOGISTIC ORGANIZATION security standard, instructions, guidelines, etc.

Security staff

Employees of the Security department perform the following tasks:

- Supporting operational management in the field of security;
- Assisting in preparation for audits (internal assessments, investigations) and supporting in the follow-up and measures;
- Collecting details of incidents and reporting them to local management;
- Supporting in investigations into internal fraud;
- Evaluating industry information and discovering threats;
- Implementing THE LOGISTIC ORGANIZATION security standard, instructions, guidelines, etc. in collaboration with the Security Manager;
- Checking installed physical security equipment for possible defects or malfunctions;
- Providing general security information and the Security Awareness For Employees (SAFE) training, and providing this training for local staff;
- Reporting the results of these activities to the head of the Security department;
- Making risk analyses and adjusting measures accordingly;

The Security department is responsible for:

- Background checks of new employees and contractors;
- Risk inventory & evaluation (work processes, security);
- Management of the external security guards;
- Toolbox meetings on risks;
- Access control;
- Camera surveillance;
- Incident investigation;
- Business continuity planning;
- Risk management;
- Organizing workshops on awareness, insider threat etc.

Shops, web shop, distribution centre warehouse

The current THE LOGISTIC ORGANIZATION consists of 14 shops, a web shop and a distribution centre warehouse which are connected by a logistics process.

THE LOGISTIC ORGANIZATION has its own shops and a franchise formula. Franchisees pay for the use of the formula. For these own shops and franchisees, THE LOGISTIC ORGANIZATION arranges central purchasing, distribution centre warehouse, logistics process, publicity, maintenance, security and the web shop. The franchisee arranges personnel matters, opening hours, shop location, insurance, etc.

The shops

THE LOGISTIC ORGANIZATION has 14 shops. The shops are high end consumer products retailers. The process in the shop is characterized by inbound, storage and removal of products. The flow rate of the goods is tracked by registering old and expired products and products that are still in stock in the shop and which need to be reordered. The shops are supplied once a week. The shops have a mixed assortment. All products are for sale in all shops and are in approximately the same place in all shops. The promotions that the shop has in certain weeks of the year are placed in the headlines of the shop. THE LOGISTIC ORGANIZATION uses an app, a loyalty card and Wi-Fi tracking of customers in the shop.

Shop

THE LOGISTIC ORGANIZATION believes in full integration of offline and online. By integrating the web shop and the physical shops, the products can reach the customer quickly at a competitive price, with personal service. In addition, there are internet-only products.

Distribution centre warehouse

From the distribution centre warehouse, deliveries are made once a week to the shops of THE LOGISTIC ORGANIZATION. In principle, the goods purchased via the web shop are delivered directly from the distribution centre warehouse to the customer. If the customers want to pick up the goods ordered online in the shop, they will be delivered to the shops via the distribution centre warehouse. Those orders are delivered to the shops daily by an external distributor. Just like in the shops, the process in the distribution centre warehouse is characterized by inbound, storage and removal of products. In the distribution centre warehouse, pallets are 'picked' and prepared for transport. This complete process requires good cooperation between, among other things, the shops, the web shop and the distribution centre warehouse with goods receipt (*inbound*) and goods distribution (*outbound*).

Logistics

The shops all have their own stock. To maintain the stock in the shops, three systems are used, namely: SAP, POSFlow and TIB.

To manage the stock, THE LOGISTIC ORGANIZATION uses SAP. SAP is an ERP program with which THE LOGISTIC ORGANIZATION manages all goods flows. All items are recorded in SAP, including the specifications and the purchase, transfer and sales prices.

SAP is linked to POSFlow, the POS system of THE LOGISTIC ORGANIZATION. The POS system makes it possible to process sold goods without delay.

SAP determines on the basis of sales how much need there is for a certain product.

External actors

Two external parties are involved in the ordering and return process: CEVA and DHL

CEVA is one of the world's largest supply chain management companies. CEVA has agreements with THE LOGISTIC ORGANIZATION regarding the storage, shipping and receipt of goods.

DHL is the transport company that transports all goods for THE LOGISTIC ORGANIZATION.
The security manager maintains good contacts with fellow security managers of similar logistics organizations. The security department also has good contact with the national police.

Stock

The Purchasing department determines how much stock should be present in each shop. This way of ordering connects to the Internet of Things (IoT), which means that objects connected to the internet communicate with each other and automatically start a process. The IoT is becoming increasingly important for logistics.

THE LOGISTIC ORGANIZATION has two important processes in the supply chain, namely the automatic ordering process and the return process.

The automatic ordering process

The process by which products are automatically ordered by SAP to maintain stock is also called the automatic ordering process. SAP analyzes the sales data and determines the optimal order moment and the optimal order quantity. The moment SAP detects that there are not enough items in stock in a shop, SAP automatically creates an order for the shop in question. POSFlow provides and SAP with the sales data, so that the stock can be monitored.

The return process

In addition to the automatic ordering process, there is the return process. Every Monday a Return Merchandise Authorization (RMA) is created in the shop. An RMA consists of mandatory returns and Death On Arrival (DOA). Dead on Arrival is a term which indicates that an item or merchandise received by a buyer was found defective or broken on arrival. After creating the RMA, DHL picks up the order and sends it to DHL. There, the products are returned to the third party or shopd in the warehouse.

Direct deliveries by producers

The automatic ordering process supports the supply of 60% of the shops from the distribution centre warehouse. The supply of the remaining 40% of the shops is provided by producers of goods with which THE LOGISTIC ORGANIZATION has concluded a contract. The representatives of these producers themselves go to the shops to inspect and fill the shelves of their products. In addition, they may replenish stocks if the branch needs them. The shops do not check the content of the delivery, they may supplement the shelves with stock that the representatives have delivered there. Employees of the shop sign on the packing slip for receipt of the goods and enter the items into SAP. The same products can also be delivered via the distribution centre warehouse with the same barcode.

In-shop delivery and pick-up

The DHL courier will park their van as close to the shop as possible. They then unload the necessary goods. The moment they enter the shop, everything is recorded by the cameras. The DHL employee walks to an employee of the shop and they then go to the back office to pick up the goods that need to be collected by the courier.

CASES

CASE I

The Financial Director's view on security

Security is a staff service. Due to the 'feel good' character of the shops, the security measures must not disrupt the customer experience. Customers must be able to touch the products, even when it comes to attractive products that would be in a display case at other shops. The director expects shop employees to also play a role in shop security when it comes to being alert to deviant customer behavior, or signaling shoplifting.

In the primary process, a more proactive attitude is expected of the security department: not waiting for an incident to occur, but converting warning signals into preventive action. To this end, it is necessary for the security department to work more information-driven with key performance indicators based on available internal and external information sources.

CASE II

Security policy

Security lacks direction, due to the absence of a clear mission, vision and strategy with regard to security. There is also no policy plan or business objective with regard to security. Due to the lack of security policy, the organization is unable to effectively manage its risks and protect itself against crime. As there is a lack of direction and taking security responsibilities at management level, a reflection of this behaviour has manifested within the operation. This behaviour translates to the fact that employees and managers do not behave in accordance with the rules and procedures and are not aware of the risks they cause.

Case III

Risk inventory

There is no security-oriented risk inventory. The organization monitors its risks with the security audit. However, this instrument does not provide specific information on the nature and extent of risks. This means that no analysis has been made of the threats and what damage they can cause to THE LOGISTIC ORGANIZATION.

There is also no method by which external information and knowledge are inventoried, analyzed and translated into policy. For example, there is a lack of a method with which information or research about crime in the retail sector is translated into security policy. This creates a gap between the development in the field and the position of THE LOGISTIC ORGANIZATION in the field of security.

Due to the lack of an extensive process of a threat and risk inventory, the organization is unable to effectively align security measures with the security risks that the organization runs. The risk inventory is currently not leading when making choices for security measures. Lastly, there is a lack of a complete record of regular inspections and observations.

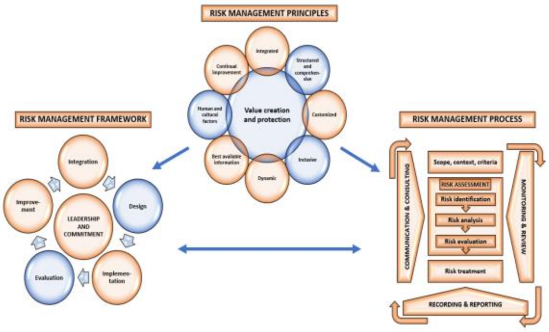
EXERCISE FOR SECURITY STUDENTS

Security Risk Management Cycle and the Administrative Organization (ISO 31000 and COSO)

AUTHORS: Lambert Bambach

BACKGROUND:

The security manager must be aware of the operation of the internal control measures, because he can contribute to the implementation and maintenance of the correct risk control measures based on his specific knowledge of security. Depending on the context and goals of an organisation, is started with one of the building blocks of the ISO 31000:2018 to realize security risk management. The most applicable building block should be chosen for that individual case.

REFERENCE TO ISO 31000 STANDRD According to the ISO 31000 standard, the building block Risk Management Process and the sub-building blocks improvement, integration, implementation, continual improvement, integrated, customized, dynamic, best available information are involved	

GOAL OF THIS EXERCISE:

The students will advise the security division of an organization on the basis of three cases. The advice will be based on Security Risk Management Cycle and the Administrative Organization. They must indicate substantiated:

- What needs to be done with regard to Administrative organization;
- What needs to be done with regard to Information-driven working;
- Where to start in the Security Risk Management Cycle;
- Why do you start there?
- What are you going to do?
- Who will be your allies?

TASK DESCRIPTION FOR STUDENTS:

1. Form groups as instructed by teacher
2. Each group is given three cases to work on
3. Under guidance from teacher, define What needs to be done with regard to Administrative organization: What needs to be done with regard to Information-driven working; Where to start in the Security Risk Management Cycle; Why do you start there?; What are you going to do?; Who will be your allies?
4. Familiarize yourself with the theory of the Administrative organisation and the building blocks of the ISO31000. Also familiarize yourself with the building blocks of your choice which you use for your approach and write down the results of your choice for approach, concerning What needs to be done with regard to Administrative organization: What needs to be done with regard to Information-driven working; Where to start in the Security Risk Management Cycle; Why do you start there?; What are you going to do?; Who will be your allies?
5. Prepare a short presentation for your fellow students in the other groups about the results of your choice for approach, concerning: What needs to be done with regard to Administrative organization: What needs to be done with regard to Information-driven working; Where to start in the Security Risk Management Cycle; Why do you start there?; What are you going to do?; Who will be your allies?
6. Present your presentation for your fellow students in the other groups.
7. Listen the presentations of the fellow students. After each presentation discuss 2 minutes with your group if their approach of the cases would have been applicable for you too. Share your thoughts with the class in your turn. Would your approach per case been different knowing due to the new insides given by the other group(s)?
8. After all presentations discuss in your group which of the presented approaches would be best for each case. Share your thoughts with the class.

TASK DESCRIPTION FOR TEACHER / TRAINER:

1. Before class, estimate the number of students and how many groups of approximately four students they would form.
2. Before class, for each group should have a copy of the ISO 31000: 2018, The case and have read the article on Administrative organisation.
3. Optionally:
   - If you wish the exercise to be carried out in a physical location, make sure you have access and proper facilities within it. You may also want to divide the facilities for the groups beforehand.
4. In class, assign students into groups of approximately four students.

5. Instruct students to familiarize themselves with the ISO 31000:2018; The case and the article on Administrative organisation.

6. Instruct students to write down the results of their choice for approach this can be done on e.g., post-it notes, on the whiteboard, PowerPoint presentation, in an online environment, etc. Instruct students to prepare to present their results to their fellow students. You can decide the delivery method of the presentation. It is recommended to limit the presentation to max. 5 minutes.

9. While the students discuss their approach, they write down their choice for the approach and prepare their presentation on: What needs to be done with regard to Administrative organization: What needs to be done with regard to Information-driven working; Where to start in the Security Risk Management Cycle; Why do you start there?; What are you going to do?; Who will be your allies? Your task is to facilitate their work and assist if they have questions.

7. Instruct students to present their short presentation for their fellow students in the other groups about the results of your choice for approach, concerning: What needs to be done with regard to Administrative organization: What needs to be done with regard to Information-driven working; Where to start in the Security Risk Management Cycle; Why do you start there?; What are you going to do?; Who will be your allies?

8. During presentations, make sure to chair the discussion and keep the groups within the given schedule. The process is as follows:
    - Approx. max. 10 minutes for one group presentation
    - After each presentation groups should discuss 2 minutes within their groups if the presented approach would have been applicable for their approach.
    - Groups are encouraged to share their thoughts with the class. The key question is: would the choice for approach give you different results?

9. After all presentations, lead all students in a discussion of which of the presented approach would be best.

ADDITIONAL SKILLS THAT THE STUDENT ACQUIRES THROUGH THIS ASSIGNMENT:

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

CASE SECURITY RISK MANAGEMENT AND THE ADMINISTRATIVE ORGANIZATION

The Logistic Organization

Direction

THE LOGISTIC ORGANIZATION has 14 physical stores (the 'stores'), a webshop and one national distribution center warehouse warehouse. THE LOGISTIC ORGANIZATION has a turnover of € 370,000,000 per year, of which € 270,000,000 for the physical stores and € 100,000,000 for the web shop. THE LOGISTIC ORGANIZATION's position in the market is as strong as its relationship with its customers. The long-term relationship with customers is therefore central to its strategy.

Vision

- Customer experience
- Customer centered

- **Mission**
- Empathy (feeling): THE LOGISITIC ORGANIZATION knows the individual needs of the customer.
- Expertise (knowing): THE LOGISITIC ORGANIZATION has the knowledge to meet the individual needs of the customers.
- Experience (can): THE LOGISITIC ORGANIZATION introduces you to the best electronic products

Values

- Customer first
- Do what you say
- Realizing ideas
- Always better

Promises

- Better for the customer
- Better for the employee
- Better for the environment

Business model

- Lower costs
- Strong brands
- Wide range of products

Strategic pillars

- Strong customer loyalty
- Broadening of the range of products available
- Online sales
- Attractive products
- Corporate responsibility
- Good for our people

Ambition

- Always better
- Growth in turnover and profit
- Reduction of losses and costs through better control of primary processes

The service level of THE LOGISITIC ORGANIZATION is high. Short delivery times and lowest price including service ensure that THE LOGISITIC ORGANIZATION looks closely at the contribution that products make to profit.

Developments

- Stock is kept to a minimum. Measurability is essential, whether it's advertising campaigns, inventory control or loss prevention;

- The THE LOGISITIC ORGANIZATION also wants to introduce self-scan of articles to increase convenience for the customer;

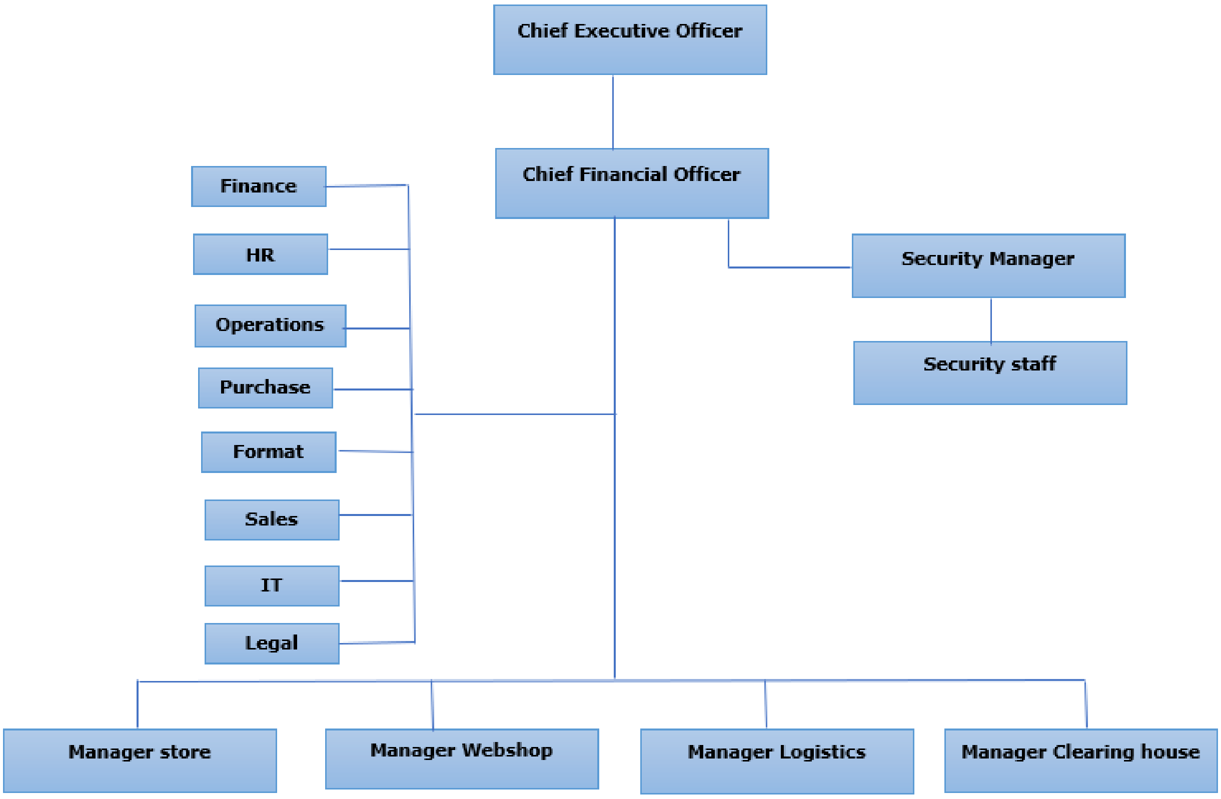
- In addition, THE LOGISITIC ORGANIZATION wants to achieve a growth in profits by increasing online sales;

- In store and online, the same price applies. If a consumer can order the desired product cheaper elsewhere, THE LOGISITIC ORGANIZATION will deliver it for that same price. In this way, THE LOGISITIC ORGANIZATION prevents customers from delaying their buying decision;

- THE LOGISITIC ORGANIZATION delivers within 24 hours after ordering the products;

- THE LOGISITIC ORGANIZATION is currently developing THE LOGISITIC ORGANIZATION - Smart. From these smaller hubs in shopping centers, the electronics chain wants to experiment with express delivery. The Smart stores will be located in larger shopping centers where customers can go for a smaller range of products and advice. In the Smart hubs, omnichannel is becoming the norm. Via invisible walls in the store, customers can check whether a product is available, what it looks like and place orders. As a vision for the future, THE LOGISITIC ORGANIZATION sees that these orders are delivered to the customer's home the same day.

Arrangement



Organization chart of THE LOGISITIC ORGANIZATION

Managers stores, web shop, logistics and distribution center warehouse

As far as is known, the managers have no substantive tasks and responsibilities in the field of security, but are responsible for the management of the employees in the field of safety in the stores, the web shop and the distribution center warehouse.

Manager support departments

As far as is known, the managers of the Finance, Operations, Purchasing, Format, Sales, IT, Legal departments have no substantive tasks and responsibilities in the field of security, but are responsible for managing the employees in their department.

Security

Security is organized at a central level. Security is a staff service. As far as is known, the Chief Financial Officer has no substantive tasks and responsibilities in the field of security, but is still accountable for the Security department and managing the head of the Security. reports to the Chief Executive Officer. The budget of the Security department is set at group level. Every organizational unit of THE LOGISITIC ORGANIZATION can call on the Security department when it deems it necessary. Expenses for investments and costs of maintenance are borne by the THE LOGISITIC ORGANIZATION.

Security Manager

The Security Manager is responsible for managing, planning and leading the implementation of the security arrangement. This arrangement was developed at the head office, the risk classification process is part of this. In addition, the head of the security department and his department support the national and local management by performing tasks such as conducting investigations, security audits and ensuring that the stores, the web shop and the distribution center warehouse comply with the legal regulations. In addition, the manager oversees THE LOGISITIC ORGANIZATION security standard, instructions, guidelines, etc.

Security staff

Employees of the Security department perform the following tasks:

- Supporting operational management in the field of security;
- Assisting in preparation for audits (internal assessments, investigations) and supporting in the follow-up and measures;
- Collect details of incidents and report them to local management;
- Support in investigations into internal fraud;
- Evaluating industry information and discovering threats;
- Implementing THE LOGISITIC ORGANIZATION security standard, instructions, guidelines, etc. in collaboration with the Security Manager;
- Check installed physical security equipment for possible defects or malfunctions;
- Provide general security information and the Security Awareness For Employees (SAFE) training, and provide this training for local staff;
- Reporting the results of these activities to the head of the Security department;
- Making risk analyses and adjusting measures accordingly.

The Security department is responsible for:

- Background check of new employees and contractors;
- Risk inventory & evaluation (work processes, security);
- Management of the external security guards;
- Toolbox meetings on risks;
- Access control;
- Camera surveillance;
- Incident investigation;
- Business continuity planning;
- Risk management;
- Organizing workshops on awareness, insider threat etc.

Shops, web shop, distribution center warehouse warehouse

The current THE LOGISITIC ORGANIZATION consists of 14 stores, a web shop and a distribution center warehouse which are connected by a logistics process.

THE LOGISITIC ORGANIZATION has its own stores and a franchise formula. Franchisees pay for the use of the formula. For these own stores and franchisees, THE LOGISITIC ORGANIZATION arranges central purchasing, distribution center warehouse, logistics process, publicity, maintenance, security and the web shop. The franchisee arranges personnel matters, opening hours, store location, insurance, etc.

The shops

THE LOGISITIC ORGANIZATION has 14 stores. The stores are high end consumer products retailers. The process in the store is characterized by inbound, storage and removal of products. The flow rate of the goods is tracked by registering old and expired products and products that are still in stock in the store and which need to be reordered. The stores are supplied once a week. The stores have a mixed assortment. All products are for sale in all stores and are in approximately the same place in all stores. The promotions that the store has in certain weeks of the year are placed on the headlines of the store. THE LOGISITIC ORGANIZATION uses an app, a loyalty card and Wi-Fi tracking of customers in the store.

Shop

THE LOGISITIC ORGANIZATION believes in full integration of offline and online. By integrating the web shop and the store, the products can reach the customer quickly at a competitive price, with personal service. In addition, there are internet-only products.

Distribution center warehouse

From the distribution center warehouse, deliveries are made once a week to the stores of THE LOGISITIC ORGANIZATION. In principle, the goods purchased via the web shop are delivered directly from the distribution center warehouse to the customer. If the customers want to pick up the goods ordered online in the store, they will be delivered to the stores via the distribution center warehouse. Those orders are delivered to the stores daily by an external distributor. Just like in the stores, the process in the distribution center warehouse is characterized by inbound, storage and removal of products. In the distribution center warehouse, pallets are 'picked' and prepared for transport. This complete process requires good cooperation between, among other things, the stores, the web shop and the distribution center warehouse with goods receipt (*inbound*) and goods distribution (*outbound*).

Logistics

The stores all have their own stock. To maintain the stock in the stores, three systems are used, namely: SAP, POSFlow and TIB.

To manage the stock, THE LOGISITIC ORGANIZATION uses SAP. SAP is an ERP program with which THE LOGISITIC ORGANIZATION manages all goods flows. All items are recorded in SAP, including the specifications and the purchase, transfer and sales prices.

SAP is linked to POSFlow, the POS system of THE LOGISITIC ORGANIZATION. The POS system makes it possible to process sold goods without delay.

SAP determines on the basis of sales how much need there is for a certain product.

External actors

Two external parties are involved in the ordering and return process: CEVA and DHL

CEVA is one of the world's largest supply chain management companies. CEVA has agreements with THE LOGISITIC ORGANIZATION regarding the storage, shipping and receipt of goods.

DHL is the transport company that transports all goods for THE LOGISITIC ORGANIZATION.

The security manager maintains good contacts with fellow security managers of similar logistics organizations. The security department also has good contact with the national police.

Stock

The Purchasing department determines how much stock should be present in each store. This way of ordering connects to the Internet of Things (IoT), which means that objects connected to the internet communicate with each other and automatically start a process. The IoT is becoming increasingly important for logistics.

THE LOGISITIC ORGANIZATION has two important processes in the supply chain, namely the automatic ordering process and the return process.

The automatic ordering process

The process by which products are automatically ordered by SAP to maintain stock is also called the automatic ordering process. SAP analyzes the sales data and determines the optimal order moment and the optimal order quantity. The moment SAP detects that there are not enough items in stock in a store, SAP automatically creates an order for the store in question. POSFlow provides and SAP with the sales data, so that the stock can be monitored.

The return process

In addition to the automatic ordering process, there is the return process. Every Monday a Return Merchandise Authorization (RMA) is created in the store. An RMA consists of mandatory returns and Death On Arrival (DOA). Dead on Arrival is a term which indicates that an item or merchandise received by a buyer was found defective or broken on arrival. After creating the RMA, DHL picks up the order and sends it to DHL. There, the products are returned to the third party or stored in the warehouse.

Direct deliveries by producers

The automatic ordering process supports the supply of 60% of the stores from the distribution center warehouse. The supply of the remaining 40% of the stores is provided by producers of goods with which THE LOGISITIC ORGANIZATION has concluded a contract. The representatives of these producers themselves go to the stores to inspect and fill the shelves of their products. In addition, they may replenish stocks if the branch needs them. The stores do not check the content of the delivery, they may supplement the shelves with stock that the representatives have delivered there. Employees of the store sign on the packing slip for receipt of the goods and enter the items into SAP. The same products can also be delivered via the distribution center warehouse with the same barcode.

In-store delivery and pick-up

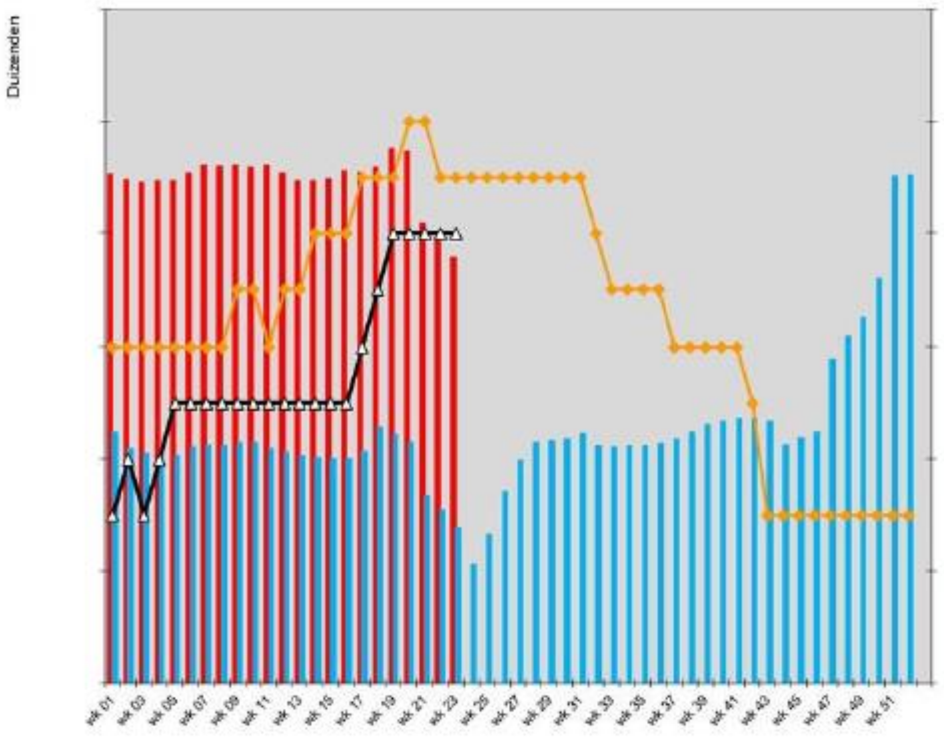
The DHL courier will park the bus as close to the store as possible. He then unloads the necessary goods. The moment he enters the store, everything is recorded by the cameras. The DHL employee walks to an employee of the store and he then goes to the back office to pick up the goods that need to be taken by the courier.

CASES

CASE I

Suspicion of loss due to organized crime

There are suspicions that organized crime is a problem for the organization. The Chief Financial Officer wants security measures to be taken. The financial analyst indicates that undefined leakage is a major problem within THE LOGISTIC ORGANIZATION. Theft accounts for 33% of the entire leakage. There is a large increase in the area of undefined leakage compared to last year. Undefined leakage indirectly affects the mapping of organized crime. Undefined leakage means that the leak has not been mapped by THE LOGISTIC ORGANIZATION and is only detected later. This creates a less concrete picture of what the leakage figures consist. This contributes to the inability or impairment of organized crime. If (more than) half of the leakage cannot be mapped, it cannot be clearly described how big the impact of organized crime actually is on the leakage figures. Overall leakage rates have increased by 6.41% compared to the same period last year. The LOGISTIC ORGANIZATION has a target of 0.20% in terms of leakage. That is the total amount (at purchase price) that was stolen divided by the total gross turnover.



Sales 2023 Sales 2022 Shrinkage 2023Shrinkage 2022

The figure shows that the percentage of leakage is lower compared to last year, but that this is due to the increased turnover. In absolute terms (amounts), thefts, and therefore leakage, have increased. If the turnover this year had been the same as last year, the leakage rate might have doubled.

CASE II

Registration of deviations

It appears that the procedures are not being followed structurally at the moment. In some cases, the reports do not go through the Logistics department. As a result, they are not always aware of these reports. In other cases, the Logistics Department does not follow through on the reports for various reasons. These factors influence the registration of deviations in such a way that a precise number of deviations cannot be mentioned by all parties. Logically, this entails dark numbers.

Goods are regularly booked by an 'unauthorized' person. An unauthorized person is understood to mean a flex worker who books goods using the store's login details. Just as with booking, the booking must be done by an employee with his or her own cash register code. It is not checked whether the stores still use the shop login. It is noteworthy that the RMA number is not communicated to DHL. The remarkable thing about this is that there is no control mechanism.

Case III

Risk inventory

There is no security-oriented risk inventory. The organization monitors its risks with the security audit. However, this instrument does not provide specific information on the nature and extent of risks. This means that no analysis is made of the threats and what damage they can cause to THE LOGISTIC ORGANIZATION.

There is also no method by which external information and knowledge are inventoried, analyzed and translated into policy. For example, there is a lack of a method with which information or research about crime in the retail sector is translated into security policy. This creates a gap between the development in the field and the position of THE LOGISTIC ORGANIZATION in the field of security.

Due to the lack of an extensive process of a threat and risk inventory, the organization is unable to effectively align security measures with the security risks that the organization runs. The risk inventory is currently not leading when making choices for security measures. There is a lack of a complete record of regular inspections and observations.

EXERCISE FOR SECURITY STUDENTS

Scope, Context, Criteria in Security Risk Management Process

AUTHOR: Raimundas Kalesnykas, Kazimieras Simonavičius University, Lithuania

BACKGROUND:

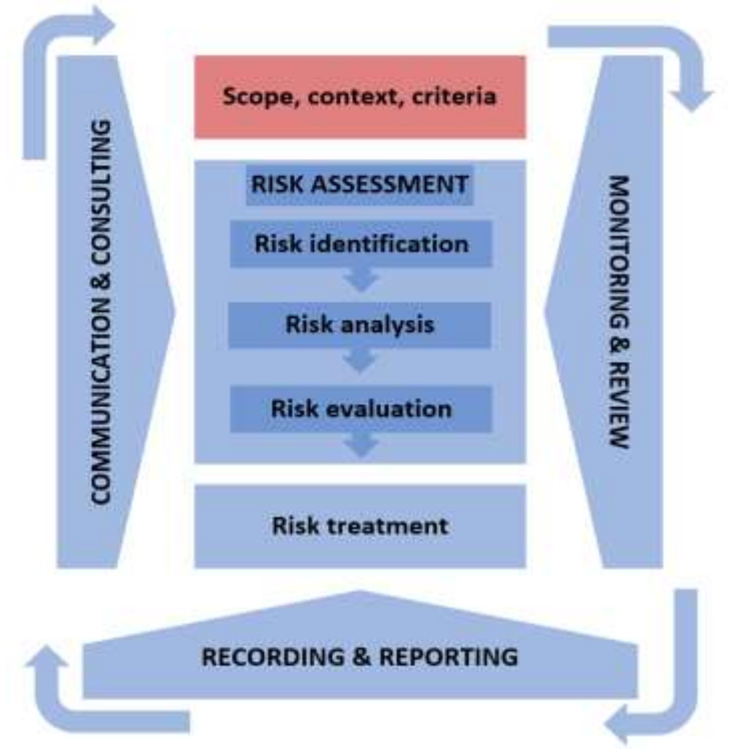
The success of security risk management will depend on the effectiveness of the management framework, which assists in managing security risks effectively through the application of the risk management process at varying levels and within specific contexts of the organization.

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.

REFERENCE TO ISO 31000 STANDRD

According to the ISO 31000 standard, the purpose of establishing the scope, the context and criteria is to customize the risk management process, enabling effective risk assessment and appropriate risk treatment.

Scope, context and criteria involve defining the scope of the process, and understanding the external and internal context of the organization.



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

Economic
Political
Social
PESTLE
Environmental
Technological
Legal

Common factors to consider when understanding the context of the organisation in relation to external factors can be assessed using the PESTLE acronym:

- Political
- Economic
- Social
- Technological
- Legal
- Environmental

More: https://pestleanalysis.com/pest-analysis-template/

ISO 31000 SECURITY RISK MANAGEMENT PROCESS

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	INTERNAL
· 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	· 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

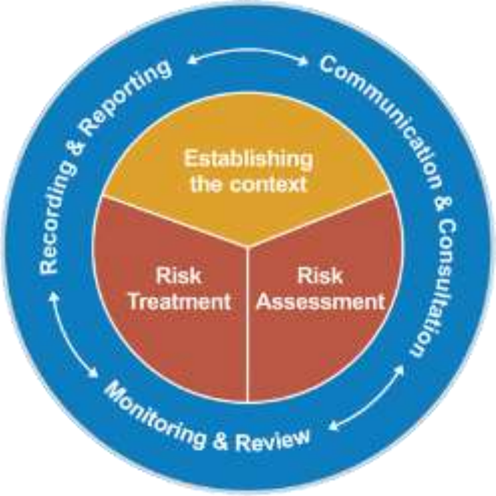
Defining Risk Criteria

- 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



Step 1: IDENTIFY
Identify the threats.

Step 2: EVALUATE
Evaluate the threats and rate your organization's risk level (vulnerability).

Step 3: DEVELOP
Develop strategies to reduce risk and vulnerability.

Identify Threats
Violent Threats
Organizational Threats
Environmental Threats

Violent Threats	**Organizational Threats**	**Environmental Threats**
- Targeted armed attack - Non-targeted armed conflict - Kidnapping - Terrorism - Carjacking - Sexual violence - Civil unrest - Religious violence - Crime - Other types of violence	- 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	- 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/

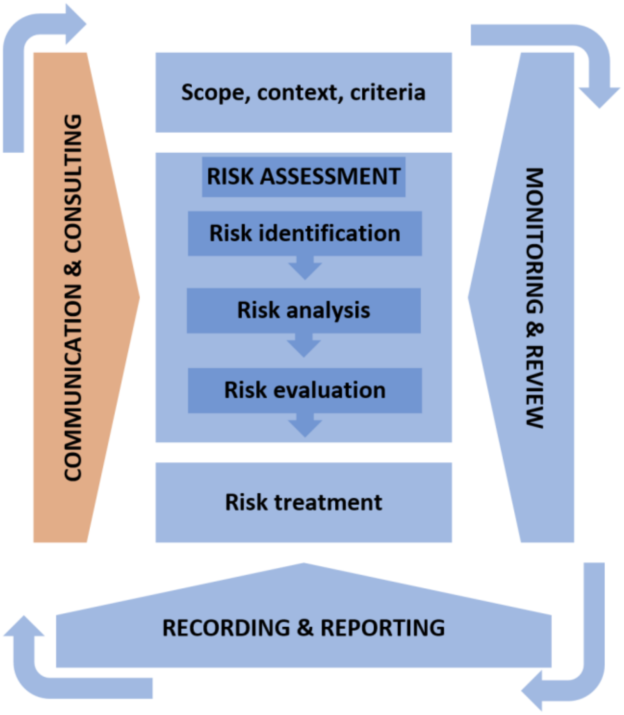
EXERCISE FOR SECURITY STUDENTS

Terrorism Risk Assessment of Public Spaces

AUTHORS: Elisabet Garcia Rull, School of Prevention and Integral Safety and Security, Spain

BACKGROUND:

In accordance with ISO 31000, the EU has published the article "Terrorism Risk Assessment of Public Spaces for Practitioners", which is a very useful tool for the city official or security operator. It presents the EU Vulnerability Assessment Checklist for Public and Security Authorities. The checklist is a very useful tool (https://ec.europa.eu/newsroom/pps/items/674909/en Published 22-4-2020)

REFERENCE TO ISO 31000 STANDRD According to ISO 31000, the risk analysis of the risk assessment includes the vulnerability assessment. The EU Vulnerability Assessment Checklist for Public and Security Authorities specifies some vulnerability aspects to be considered	

GOAL OF THIS EXERCISE:

Students will become familiar with vulnerability assessment in the risk analysis process in the field of terrorism.

TASK DESCRIPTION FOR STUDENTS:

1. Form groups as instructed the teacher

2. Your task now is to choose a large famous square in your city/town and we will simulate that there is a high risk of a terrorist attack with a vehicle as a weapon and with this information each group will have to analyse the vulnerability of the chosen square according to the checklist in the attached article.

3. It is important to create informative material that is easily understandable and visually attractive. We recommend using visual editing tools such as Canva, Infogram, or Piktochart to create the material. Canva also allows free downloads for the created materials. You can find beginner tutorial videos on YouTube: https://www.youtube.com/playlist?list=PLATYfhN6gQz8GiTG_nUxVar8ycrt9hJxL

4. Present your material and explain the information included in it:
Why exactly this target group was chosen, why the information included in the material is important for a specific target group and what knowledge the target group will gain by getting acquainted with the informative material.

TASK DESCRIPTION FOR TEACHER / TRAINER:
The teacher's tasks are as follows:

1. Create students' groups (not more than 4 people in one group is recommended).

2. Explain the task to the students, emphasizing the importance of developing skills to effectively communicate safety information to colleagues and the public. It is recommended to present the Study on skills of young security specialists: https://security.turiba.lv/2022/12/06/what-skills-young-security-specialists-are-missing/

3. Assist students in selecting the target group and the focus of informational material. Provide examples and guidance if needed.

4. If students lack experience and skills in using visualization tools such as Canva, Infogram, or Piktochart, provide an introduction and basic training on one of these visual editing tools.

5. Evaluate the informational materials developed by students and discuss their content, providing recommendations for improvements.

ADDITIONAL SKILLS THAT THE STUDENT ACQUIRES THROUGH THIS ASSIGNMENT:

- Working in a group
- Working under time pressure
- Presenting and arguing
- Multidisciplinary and critical thinking skills
- Ability to work in a team
- Ability to communicate effectively
- Digital skills (visual editing skills)
- Familiarity with the EU Vulnerability Assessment Checklist for Public and Security Authorities

https://ec.europa.eu/newsroom/pps/items/674909/en

- **“Vulnerability Assessment**

Vulnerabilities are the inherent weaknesses of a potential target. Critically assessing vulnerabilities in the context of attack scenarios will inform decision-makers on effective deterrence and mitigation measures, strategies to minimize exposure, emergency management plans and enhanced resilience. Vulnerabilities are threat-specific, setting-specific and time-specific.

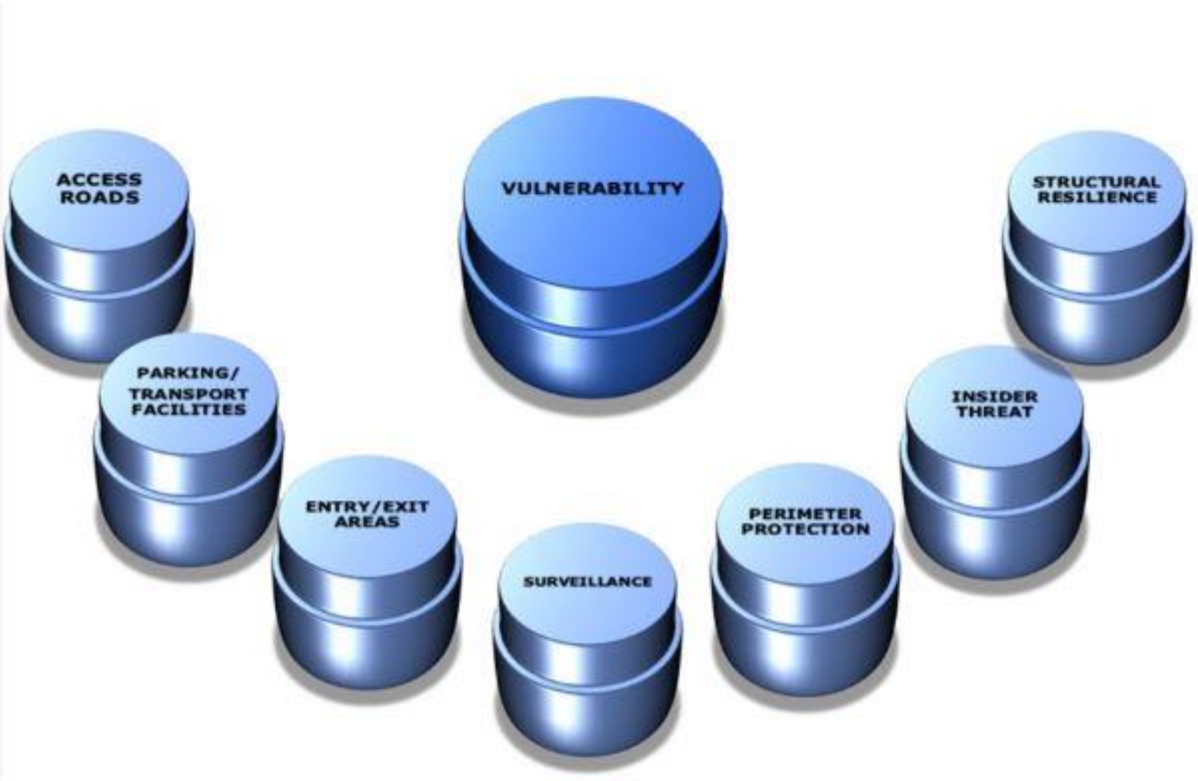


Figure 4: Vulnerability Assessment Components

The *EU Vulnerability Assessment Checklist* [16] provides a set of factors to consider and practical questions to ask during the vulnerability assessment of different types of public spaces across a broad range of identified threats.

Public space vulnerabilities are categorized according to the different access/entry/exit phases to a public space and are linked to possible attack scenarios and considerations. There are additional vulnerability assessment matrixes for insider threats and drone attacks. The vulnerability aspects to consider are:

- Access roads to venue
    - bottlenecks (possible vehicle-borne explosion impact, also for adjacent pedestrian traffic)
    - alternative access/exit roads
    - proximity to major road infrastructure, residential areas, other transport infrastructure

    - access to large/heavy vehicles

- Parking and transport facilities
    - Particularities of the entry flows (tunnels, shuttles, narrow lanes)
    - Adjacent public places
    - Situation of the parking/transport facilities in respect to the public place

- Pedestrian access
    - bottlenecks (possible person-borne IED, active shooter incidents)
    - Surrounding structures that may be used by terrorists
    - Public transport

- Entry / exit points
    - crowd conglomeration
    - vulnerability to attacks outside the protected perimeter
    - emergency exits
    - electronically operated equipment (lifts, mobile barriers, etc.)

- Access controls
    - Positioning of access controls in a way not causing crowd conglomeration
    - Possibility to break through access controls

- Open access public places
    - possibility to re-channel the crowd flow
    - vulnerability of crowds at entry and exit points outside of the public space
    - presence of shelter from a possible shooting/vehicle ramming attack
    - protection form drone attacks

- Structural resilience
    - Possibility of fragments /structural parts collapsing
    - Other buildings/structures in proximity

- Internal security measures
    - Means to check / stop attackers
    - Control of service staff/vehicles
    - Insider threat and internal controls

Systematic and continuous terrorism risk assessment for public spaces is essential for the prioritization, planning and implementation of effective mitigation solutions. In practice, there are no attack-proof solutions and there will always be the acceptable risk factor to weigh in on the decision-making process. Still, the aim of terrorists is to achieve the highest degree of havoc with their attack, thus they would naturally be attracted to exploiting the exposed vulnerabilities of public spaces. **The implementation of mitigation measures which address systematically analysed risks will provide increased resilience in case of a terrorist attack and its presence will in itself act as a dissuasion for terrorist targeting.”**

EXERCISE FOR SECURITY STUDENTS

Communication in Crisis Situations

AUTHORS: Uģis Začs, Turiba University, Latvia

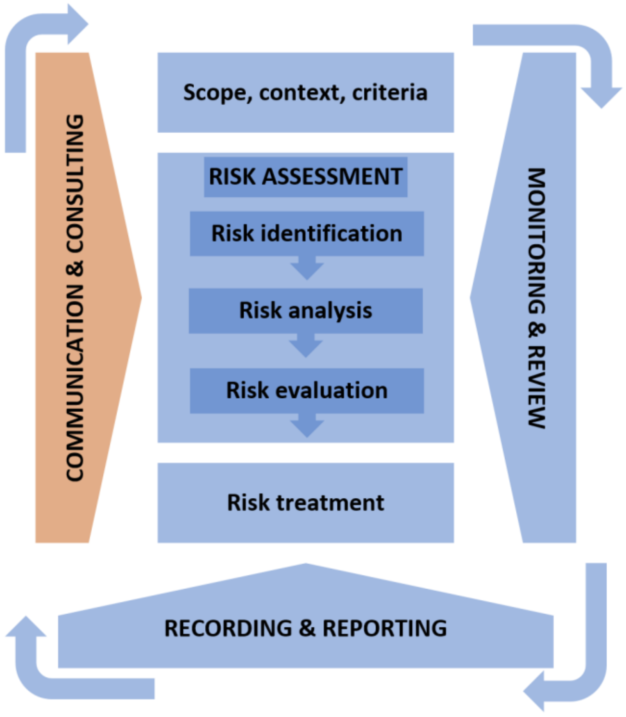
BACKGROUND:

In a study conducted at the end of 2022, experts from six countries emphasized that security specialists lack the knowledge and skills to inform and explain security issues and the importance of security risks to both - their colleagues and society in general. It is clear that without the understanding and involvement of colleagues, ensuring safety in an organization or company becomes impossible. Even more it is important in the crises situation. Therefore, one of the tasks of a security specialist in an organization or company is to be able to ensure proper communication in the situation of crises.

The full report on skills can be found here: https://security.turiba.lv/2022/12/06/what-skills-young-security-specialists-are-missing/

REFERENCE TO ISO 31000 STANDRD

According to the ISO 31000 standard, communication is of paramount importance in effective risk management. Communication plays a critical role in all stages of the risk management process, including risk identification, assessment, treatment, and monitoring.



GOAL OF THIS EXERCISE:

One of the most important aspects of security risk management is knowing how to organize quick and accurate communication in crisis situations. The task of this exercise is to train the students to communicate the crisis situation in a short and concise manner and to prepare an understandable message.

TASK DESCRIPTION FOR STUDENTS:

1. Prepare your smart device.
2. Agreed with the teacher on the method of communication (SMS, messengers, WhatsApp or otherwise).
3. Watch the video with the teacher.
4. Imagine that you (student) are the head of Security. You should prepare an informative message detailing what is important to inform all employees of the company, including what to do, how to act, and what not to do if such a crisis occurs and information about the company appears in the media.

TASK DESCRIPTION FOR TEACHER / TRAINER:

The teacher's tasks are as follows:

1. The teacher agrees with the students on the method of communication—SMS, messenger, WhatsApp, or otherwise. The teacher provides the number or name for the communication channel.
2. The teacher demonstrates a YouTube video - https://www.youtube.com/watch?v=xaNuE3DsJHM.
   This video also can be found on YouTube by searching "Domino pizza crisis, Dirty Dirty Dominos pizza."
3. Watch this video with the students. Alternatively, the teacher can find and demonstrate a similar video to the students.
4. The teacher asks students to prepare and send a message through the pre-selected channel, as if they were the head of security, detailing what and how they would inform the company's employees after the appearance of such a video in the media.
5. After receiving messages from students, the teacher can analyse the answers and provide feedback and suggestions on whether the communication was clear, if the guidance for employees was clear and consistent, and if it was evident from the message what to do, how to act, and how to communicate with the media if approached.

ADDITIONAL SKILLS THAT THE STUDENT ACQUIRES THROUGH THIS ASSIGNMENT:

Ability to take decisions; skills to formulate information and opinion.

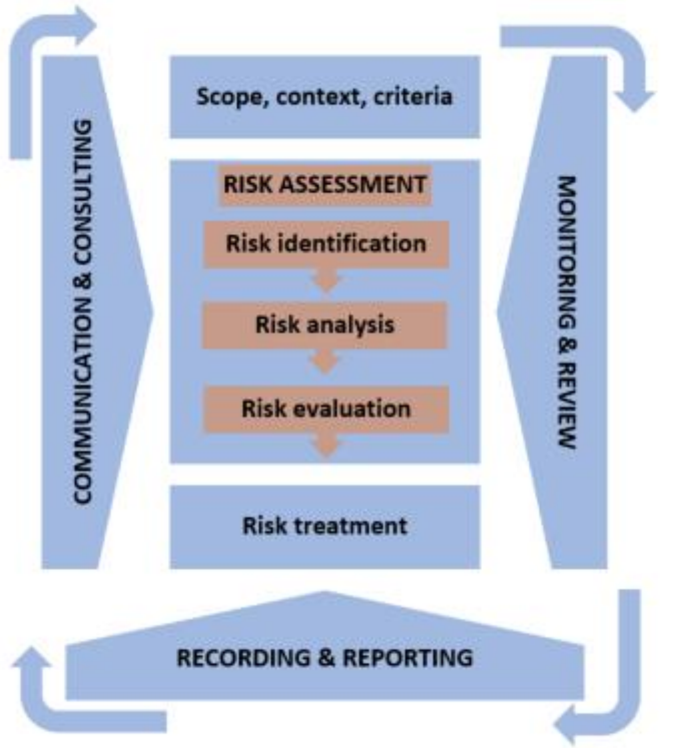
EXERCISE FOR SECURITY STUDENTS

Identification and Prioritization of the Risks

AUTHORS: Uģis Začs, Kristine Neimane, Turiba University, Latvia

BACKGROUND:

Managing risks requires thorough risk identification as one of the first steps of the process, as described in ISO 31000:2018. Subsequent steps include the analysis and evaluation of risks, which necessitate the ability to prioritize them.

REFERENCE TO ISO 31000 STANDRD According to the ISO 31000 standard, risk identification is the first step of a risk assessment. Next steps are risk analysis and evaluation.	 Scope, context, criteria RISK ASSESSMENT Risk identification Risk analysis Risk evaluation Risk treatment COMMUNICATION & CONSULTING MONITORING & REVIEW RECORDING & REPORTING

GOAL OF THIS EXERCISE:

One of the most important aspects of security risk management is the ability to identify and prioritize risks. To develop and enhance these skills, training is essential. The purpose of this task is to have students identify potential security risks associated with various stationary objects and learn how to prioritize them. By doing so, students can put themselves in the shoes of security service managers and understand how to effectively mitigate these risks.

TASK DESCRIPTION FOR STUDENTS:

1. Students choose one object for themselves.
2. Students identify 20 security risks that could be related to the specific object.
3. Students evaluate these risks according to two criteria: probability and consequences. Use a scale from 1 to 5, where 1 represents "impossible/small consequences" and 5 represents "will definitely happen/big consequences, potentially causing the organization to shut down."

Example:

Risk	Probability	Consequences	Coefficient
Fire at the facility	2	4	8

The risk coefficient is calculated by multiplying the probability and consequences.

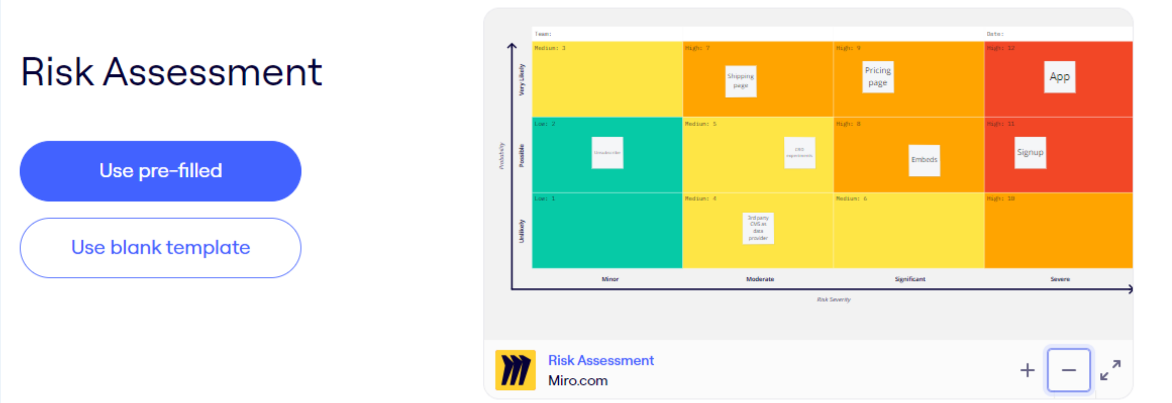
4. Based on the coefficients, identify the five most important risks and determine how they could be reduced. Present the completed work.

TASK DESCRIPTION FOR TEACHER / TRAINER:

The teacher's tasks are as follows:

1. If there are six or more students, they must be divided into pairs. If there are fewer, then each student works individually.
2. Assign or randomly allocate one of the following stationary objects to each student or pair: Bank, Shopping Center, School, Gas Station, Grocery Store, Car Service, Casino, Restaurant, Hotel, Night Club, Sawmill, Embassy, Airport, Railway Station, Office Building, Sports Hall, Customer Service Center, Cinema, Yacht Club, Dairy Factory, Zoo, Car Showroom, Hospital.
3. After the students have completed their assignments, the teacher can analyze the Risk Evaluation matrix and coefficients calculated by the students. The teacher can determine whether the coefficients are realistic or if, in some specific cases, the assessment of probability and consequences is not realistic. Additionally, the teacher can provide feedback on the risk reduction proposals made by the students.

4. You might suggest that students use a digital risk assessment matrix. For example, Miro.com offers a template for risk assessment.



Risk Assessment

	Minor	Moderate	Significant	Severe
Very Likely	Medium: 3	High: 7 Shipping page	High: 9 Pricing page	High: 12 App
Possible	Low: 2	Medium: 5	High: 8 Embeds	High: 11 Signup
Unlikely	Low: 1	Medium: 4 3rd party CMS as data provider	Medium: 6	High: 10

You can read more about the Probability-Severity Risk Matrix here: https://www.vectorsolutions.com/resources/blogs/risk-matrix-calculations-severity-probability-risk-assessment/

ADDITIONAL SKILLS THAT THE STUDENT ACQUIRES THROUGH THIS ASSIGNMENT:

Working in a group, comparison skills and critical thinking.

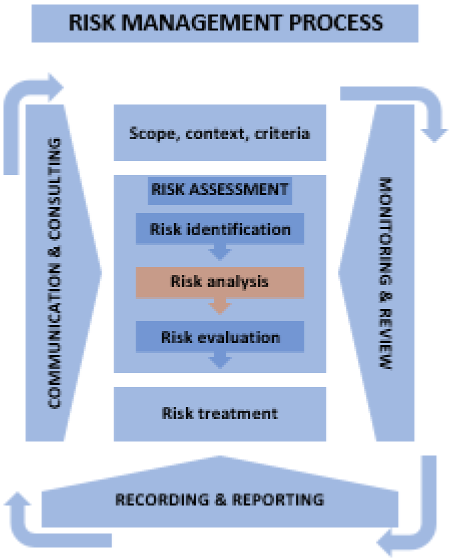
EXERCISE FOR SECURITY STUDENTS

Analysis of risks

AUTHORS: Oskari Lahtinen, Laurea University of Applied Sciences, Finland

BACKGROUND:

Effective management of risks calls for the correct analysis of the identified risks. This is the middle step in risk assessment, according to the ISO 31000:2018 standard. It is always important to use a variety of tools for effective risk analysis.

REFERENCE TO ISO 31000 STANDRD In the ISO 31000:2018 standard risk analysis is depicted as the middle step of risk assessment and the core process as a whole.	 RISK MANAGEMENT PROCESS COMMUNICATION & CONSULTING Scope, context, criteria RISK ASSESSMENT Risk identification Risk analysis Risk evaluation Risk treatment MONITORING & REVIEW RECORDING & REPORTING

GOAL OF THIS EXERCISE:

Students will familiarize themselves with risk analysis methods and tools presented in the IEC 31010:2019 standard and choose three tools, for one of the three areas of the analysis, them being consequence, likelihood and level of risk. The students will then test them and compare their effectiveness and usage.

TASK DESCRIPTION FOR STUDENTS:

1. Form groups of 4 to 5 people.
2. Each group will be given three tools, one for each category (consequence, likelihood and level of risk) as presented in the IEC 31010:2019 standard.
3. With the guidance of the teacher, you will be given a target and a list of risks.
4. Study your given tools and prepare to hold a short presentation on them, along with presenting the results of your analysis to the class after the analysis.
5. Use your given tools to analyze the risks given to you, keeping in mind the targets' activities and operating environment in your analysis. You can choose which tool you use for which risk, do not analyze every risk with every tool.
6. Write down the results of your analysis and prepare to present it to the class.
7. Present the tools you used, assigned target and the results of your analysis to the class.
8. Listen to the other presentations, and after each one prepare comments and questions for the presenter about how your methods differ from each other and which you believe to be the best and why.
9. Lastly, when all presentations are over there will be time to discuss with your own group about the differences between the tools and at the end of it each group will present their thoughts for the rest of the class.

TASK DESCRIPTION FOR TEACHER / TRAINER:

The teacher's tasks are as follows:

1. Before class estimate the number of groups there will be and prepare enough risk analysis tools that fit the assignment and chosen scenario for each category, for each group from table A.3 of the IEC 31010:2019 standard.
2. Before class prepare a fictional location and a list of at least 4 risks that have been identified. A blueprint of the facility and a description of its operations are enough. Or you can use the example ones provided in the attachments.
3. In class, instruct students to form groups of 4 to 5 people, optionally you can use any desired method to divide the students yourself.
4. Assign the groups their 3 analysis tools as well as the prepared target and identified risks.
5. Instruct the students to study their 3 given tools and familiarize themselves with them. Inform the students that they should use their given tools to analyze the risks of the fictional property given to them and remind them of the importance of reading the description of operations and taking that into account in their analysis. Remind the

students that they should choose which tools they use for which risk and advise them not to analyze every risk with every tool.

6. Inform the students that they will present their 3 tools and their results in front of the class when the time to analyze is up. Choose any method of presentation you see fit. Presentations should be a maximum of 5 minutes in length (depending on the number of students this can be shorter or longer if needed) and a maximum of 6 slides or two pages depending on chosen method.

7. Remind the students to write down their findings in their chosen method. All presentable ways are acceptable, for example Word, Miro, pen and paper or PowerPoint.

8. While the students are analyzing risks and preparing their presentation, your task is to oversee the process and help anyone who has any questions on the matter of the presentation method or the tools, for example.

9. Instruct the students to present their 3 tools and the results of their risk analysis. Inform them of the presentation order and schedule of 5-minute presentations and 2 minutes of time for comments between each.

10. During the presentations your task is to watch the clock and stop anyone from going to too much overtime, give feedback during the commenting time and direct the conversation. In a case where the students do not start the commenting spontaneously you can give a comment as a first example and give the students some examples of what to comment on. If this does not work structure the entire commentary section by appointing turns by pointing out, a student at a time, who will give out a comment.

11. After all presentations are complete give the students time to converse in their groups and then direct a conversation in class about the differences of the tools and which each group sees as the best.

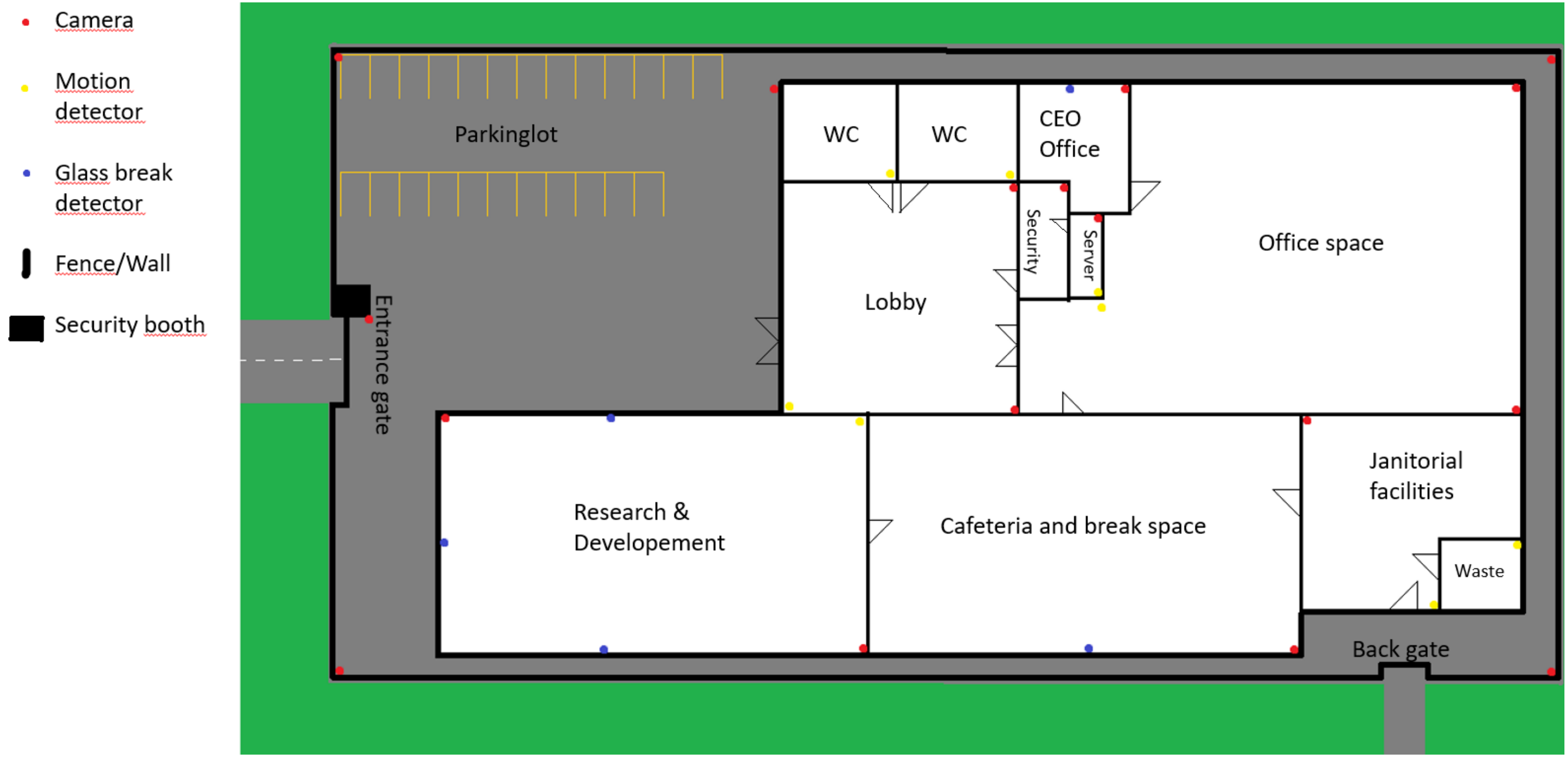
ADDITIONAL SKILLS THAT THE STUDENT ACQUIRES THROUGH THIS ASSIGNMENT:

Group work, Communication within a group, Presentation, Working under time constraint, Comparison and giving constructive feedback.

ATTACHMENTS, MATERIALS

1. Blueprint 1
2. Blueprint 2
3. Description for company in the blueprint and identified risks 1
4. Description for company in the blueprint and identified risks 2

Blueprint 1


● Camera
● Motion detector
● Glass break detector
▮ Fence/Wall
■ Security booth
Parkinglot
WC
WC
CEO Office
Security
Server
Office space
Lobby
Entrance gate
Research & Developement
Cafeteria and break space
Janitorial facilities
Waste
Back gate

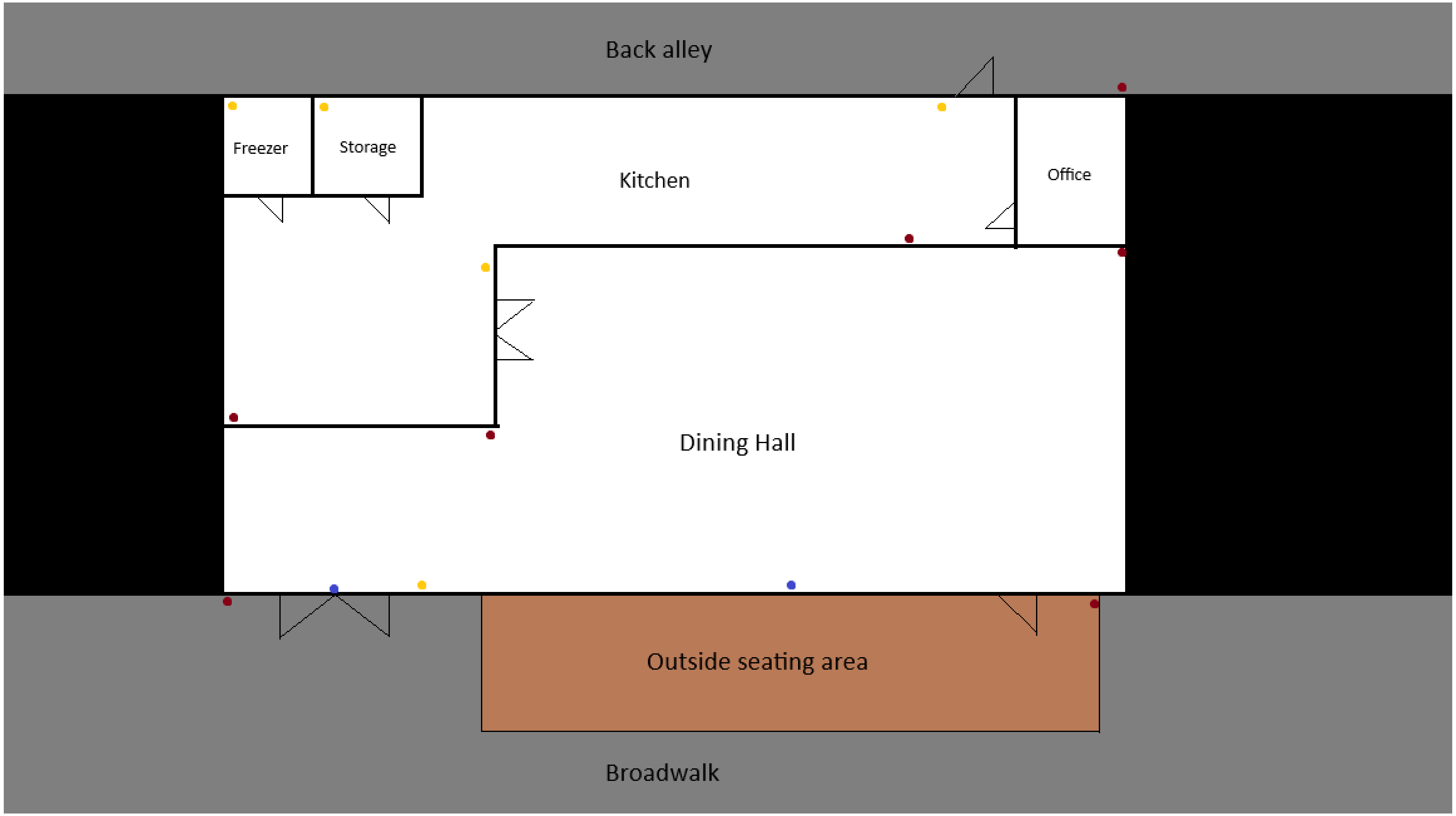
Blueprint 2

● Camera

● Motion detector

● Glass break detector

▨ Wood



Description for company in the blueprint and identified risks 1

A small specialty technology manufacturer with 30 employees.
The building is in southern Finland and is surrounded by forest and an industrial district.
It is about a 15-minute drive away from a city center and the surrounding businesses are mainly car manufacturing and metal working related.

Identified problems:

- Slipping hazard in front of the back gate in winter.
- Subpar safety equipment for employees in the R&D department.
- No security present outside of office hours and the arrival time of police from alarm is about 20 minutes.
- Door between Lobby and Office space is not locked. Risk of intruders, shoulder surfing and other forms of physical spying.

Description for company in the blueprint and identified risks 2

The company is a casual restaurant with good food and alcohol served.
The restaurant it is located in the very heart of the city of over 10 million people, in a a warm climate. The surrounding businesses are mostly fashion boutiques of cafes.

Identified problems:

- Dining hall fire alarm is blocked by a table.
- Back-alley door has a damaged lock. It does lock but can be shook open.
- Raw meat stored next to cooked meat in freezer.
- The varnish of the terrace wood gets extremely slippery in the rain.

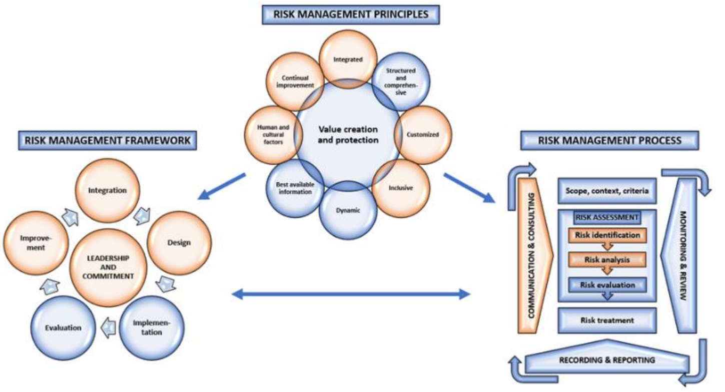
EXERCISE FOR SECURITY STUDENTS

Security Risk Management and Resilience

AUTHOR: Lambert Bambach, AVANS University of Applied Science, The Netherlands

BACKGROUND:

To gain insight in the contribution by Security Risk Management to enable resilience within the organization, it requires comprehension of the six steps *(Discuss for failure, Consider the connections, Understand what is important, Set impact thresholds, Make strategic choices and Conduct stress testing)* that can be taken to support resilience. Although the context and goals of an organization may vary, the students follow the six steps in this assignment as a guide to understand the organization and find out where the opportunities lie for Security Risk Management to contribute.

REFERENCE TO ISO 31000 STANDARD According to the ISO 31000 standard, the main building blocks are Improvement, integration, leadership and commitment, design, human and cultural factors, continual improvement, customized, inclusive, communication & consulting, risk identification and risk analyses.	

GOAL OF THIS EXERCISE:

Students will familiarise themselves with the six steps. Students will be able to determine what is the needed from Security Risk Management to contribute to the organizational mindset towards resilience. Students can apply the six steps and the questions that go with it. See Annex 1.

TASK DESCRIPTION FOR STUDENTS:

0. Homework: Before starting this exercise as a group, the student has individually surveyed and gathered information in his/her organization – based on the six steps and the accompanying questions – about resilience
1. Form groups as instructed by teacher
2. Each group consists of three to four students
3. Under guidance from the teacher, define how you interpreted the six steps? Rank the steps in difficulty according to the effort it took to obtain the answers to the questions? Reflect on why it possibly was that difficult or not? Rethink what this means for the support from Security Risk Management to resilience in the organization?
4. Prepare a short presentation for your fellow students in your group about the results of your survey. At a minimum the presentation should contain: The six steps, Which step(s) was/where the easiest to gather information about and why?, Which step(s) was/were the hardest to gather information about and why? What does this mean, in your opinion, for the support from Security Risk Management to resilience in the organization? Make clear how Security Risk Management should contribute, what should be the approach?
5. Give your presentation to your fellow students in the other groups.
6. Listen to the presentations of the fellow students. After each presentation discuss for 2 minutes within your group whether the presented approach would have been applicable for you too and why?
7. After all presentations discuss in your group which of the presented approaches you favour as a group and why?. Share your thoughts with the class.

TASK DESCRIPTION FOR TEACHER / TRAINER:

1. Before class, check if the homework is done. Only allow students in that have tried to or have finished the homework. Students that have not, can use the time to do the homework.
2. Before class, estimate the number of students and how many groups of maximum four students they would form. Decide on any method you prefer to assign them to groups.
3. Before class, each group should have a copy of the best practice article on Security Risk Management and Resilience
4. Optionally:
    - If you wish the exercise to be carried out in a physical location, make sure you have access and proper facilities within it. You may also want to divide the facilities for the groups beforehand.
5. In class, assign students into groups of approximately four students.
6. Instruct students to familiarize themselves with the six steps and the accompanying questions.

7. Instruct students to write down the results of their discussions on e.g., post-it notes, on the whiteboard, in a PowerPoint presentation, in an online environment, etc. containing: How did you interpret the six steps? Rank the steps in difficulty according to the effort it took to obtain the answers to the questions? Reflect on why it possibly was that difficult or not? Rethink what this means for support by Security Risk Management to resilience in the organization?

   Instruct students to prepare to present their results to their fellow students. You can decide on the delivery method of the presentation. It is recommended to limit the presentation to 5-10 minutes.

8. Instruct students to give their short presentations about the results of their survey to their fellow students in their group. At a minimum the presentation should contain: The six steps, Which step(s) was/were the easiest to gather information about and why?, Which step(s) was/were the hardest to gather information about and why? What does this mean, in your opinion, for the support from Security Risk Management to resilience in the organization? Make clear how Security Risk Management should contribute, what should be the approach?

9. During the presentations, make sure to chair the discussion and keep the groups within the given schedule. The process is as follows:
   - Approx. max. 10 minutes for one group presentation
   - After each presentation discuss for 2 minutes with your group whether the presented approach would have been applicable for you, too, and why?
   - Groups are encouraged to share their thoughts with the class. The key question is: would the choice of approach be applicable for your organization and/or give you a different opinion about the support that Security Risk Management could give to enable resilience within the organization?

10. After all presentations, lead all students in a discussion about the various approaches and what might be applicable for them.

ADDITIONAL SKILLS THAT THE STUDENT ACQUIRES THROUGH THIS ASSIGNMENT:

- Working in a group
- Working under time pressure
- Giving a presentation and arguing their approach
- Comparison skills and critical thinking

Appendix 1

Discuss for failure to avoid complacency and instill 'future thinking'. Ask what if? Ask what next? Encourage your people to speak up.	**Consider the connections** between the 'five capitals' to understand the potential impact of disruption on stakeholders, organization and on wider society .	**Understand what is important** to stakeholders and to society, the 'essential outcomes' (EOs). that require a high degree of resilience.	**Set impact thresholds** for EOs to determine tolerable limits that should not be breached, considering the impact on all five capitals.	**Make strategic choices** about resilience interventions by balancing control, agility, efficiency and innovation.	**Conduct stress testing** to determine whether you are able to remain within the impact thresholds irrespective of the threat.
What assumptions do people in the organization hold about failure?	What contribution will the enhanced resilience of the organization make to the overall resilience of your sector, community and society?	How is the EO delivered?	What would constitute an intolerable impact to the EO?	How progressive or defensive is the mindset in the organization?	How will the EOs be achieved during stress or disruption?
Do people openly discuss future failure, potential issues and mistakes?	How might the action or inaction of the organization impact the five capitals now and in the future (natural, human, social, built and financial?)	What might prevent the delivery or recovery of the EO?	How would disruption to an EO impact different customer groups, the organization, and the wider sector system?	How flexible or consistent is the design in the organization towards resilience?	What assurance do you have that alternative means and contingencies will enable you to meet EOs within impact tolerance under severe but plausible scenarios?
How are people tasked with spotting challenges, changes or potential disruptors on the horizon?		Could the EO be delivered by alternate means?		How do you balance tensions and leverage a 'both/and' mindset?	How will you test future opportunities and the choices you should (or should not) make today? How might those choices limit your options some years down the line?
Which future trends might provide new opportunities for the organization? What advantages could you develop?		Do we have sufficient flexibility to deliver the EO even in severe or extreme scenarios?		What further investment is required to maintain EOs within acceptable tolerance thresholds?	

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

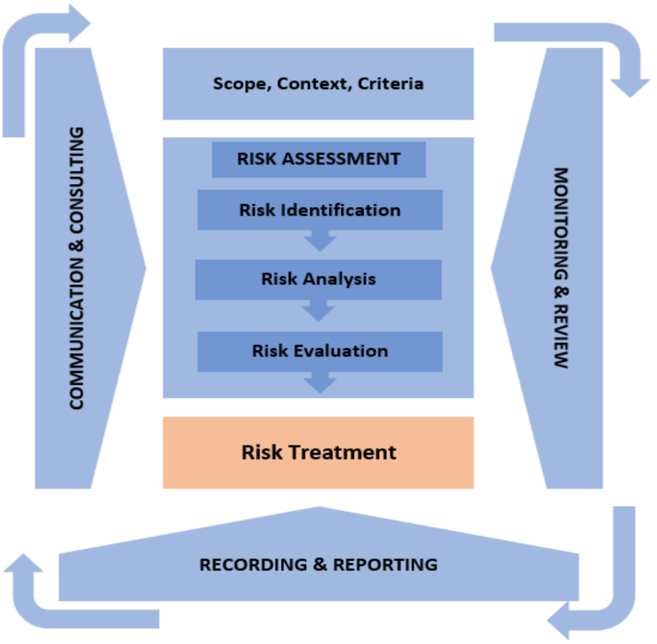
AUTHOR: Raimundas Kalesnykas, Turiba University, Latvia

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

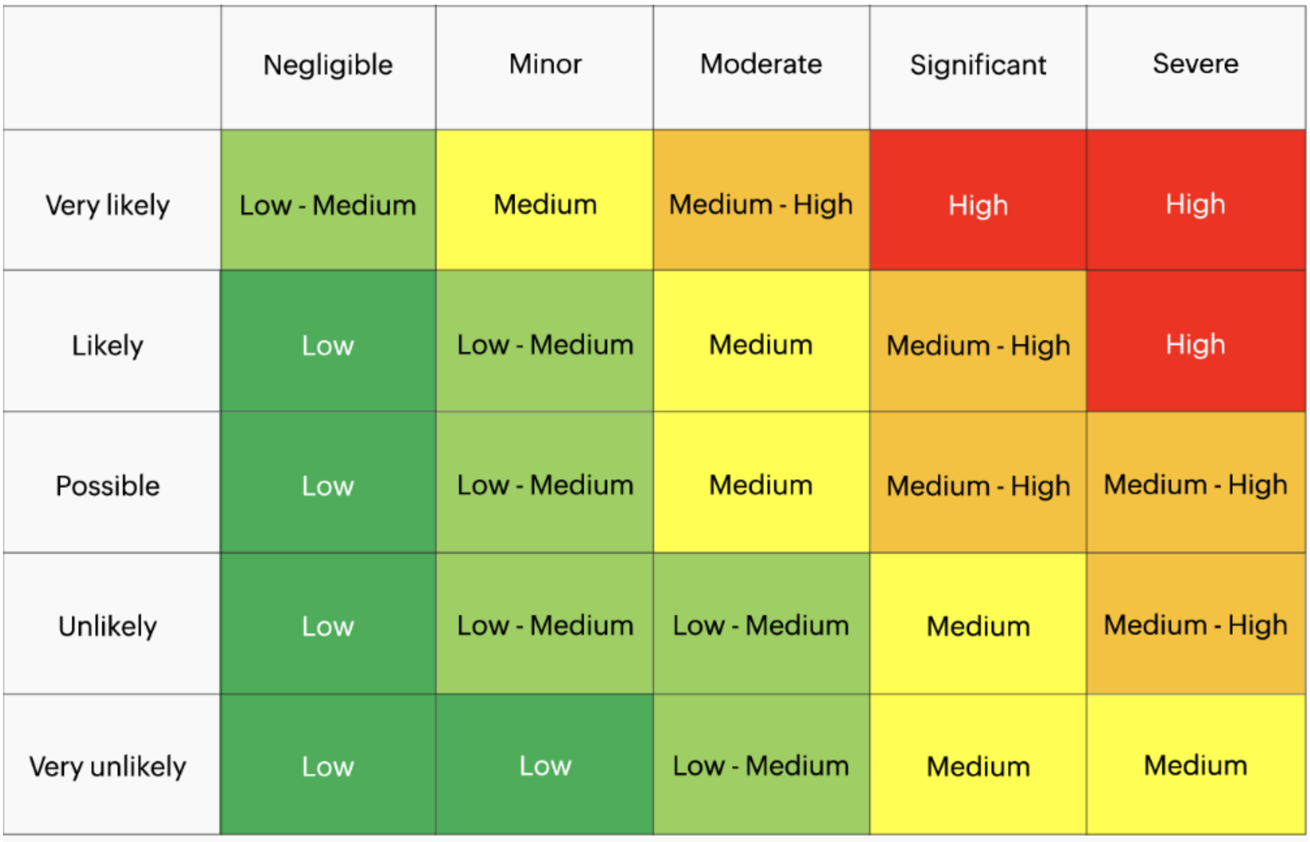
Selecting the most appropriate security risk treatment option(s) involves balancing the potential benefits derived in relation to the achievement of the objectives against costs, effort or disadvantages of implementation.	· taking or increasing the risk in order to pursue an opportunity · removing the 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

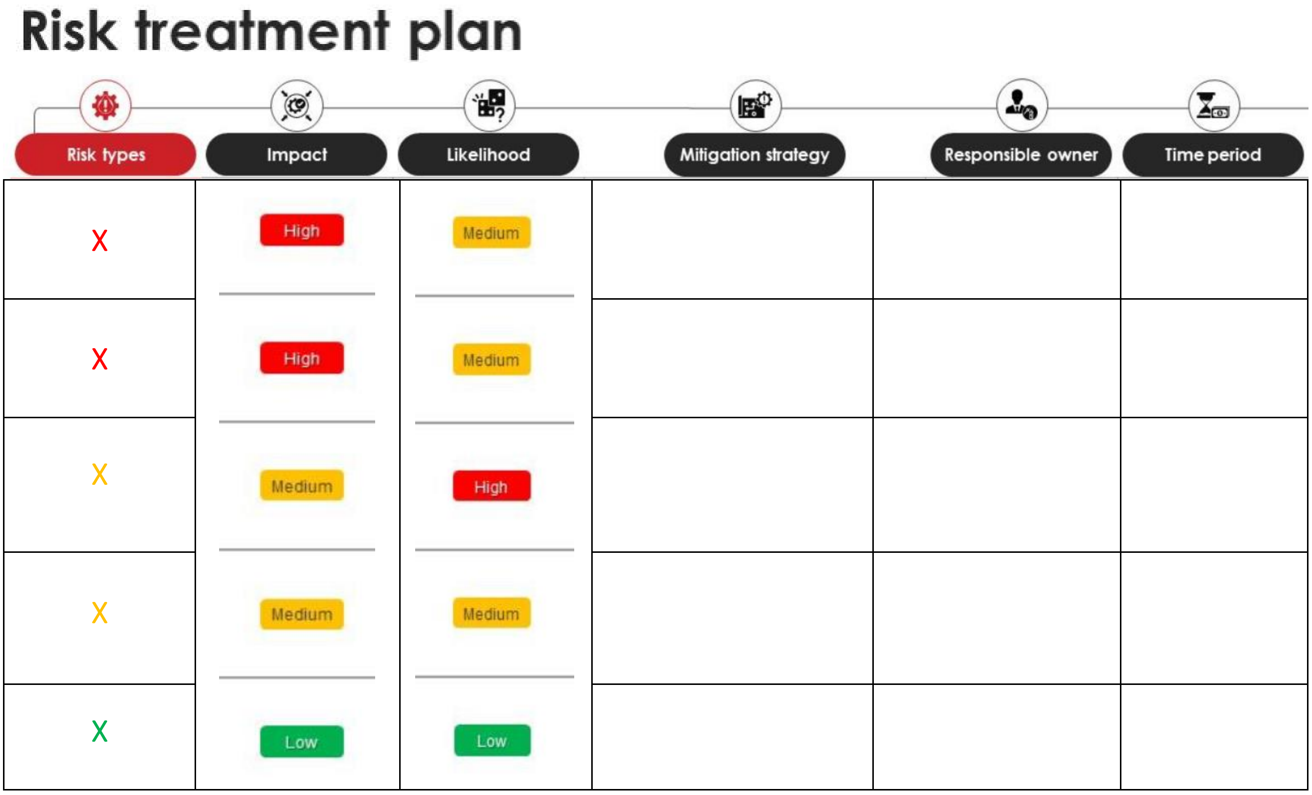
SECURITY RISK ASSESSMENT MATRIX

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

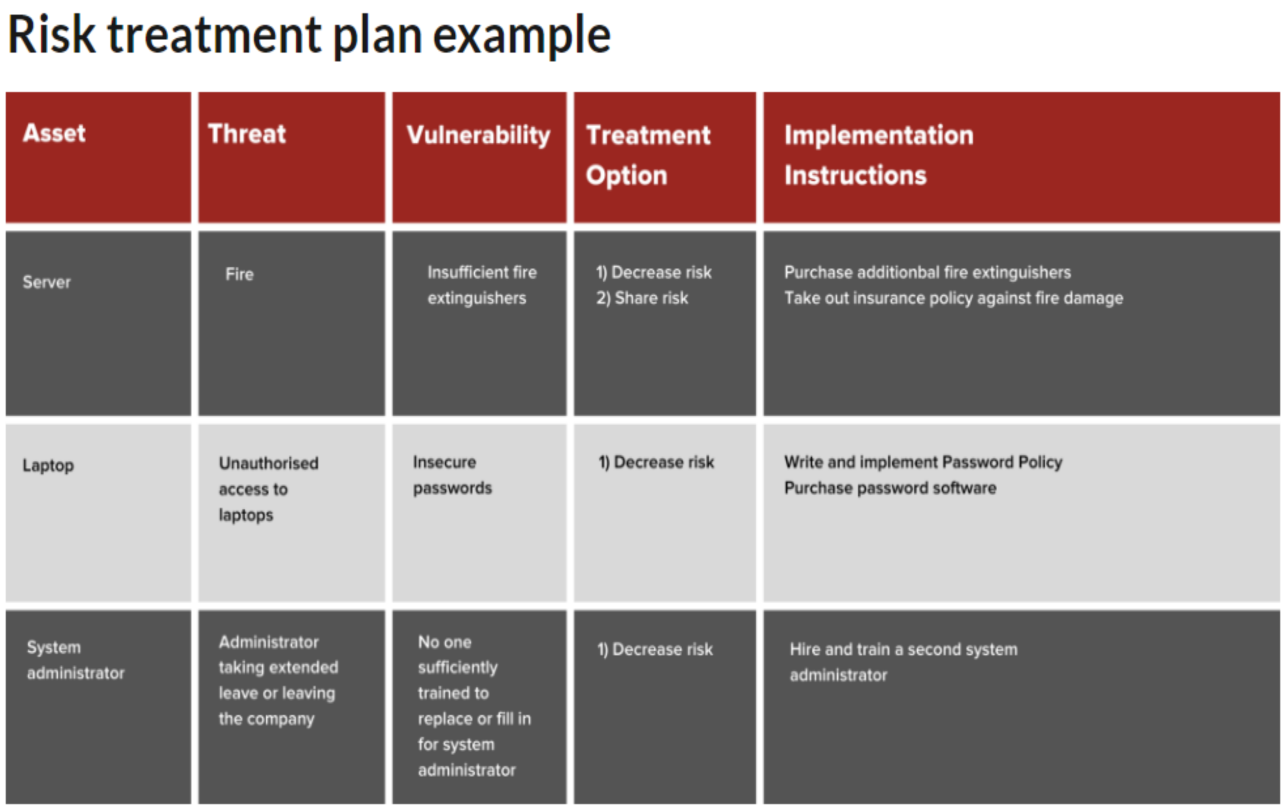
SAMPLE



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

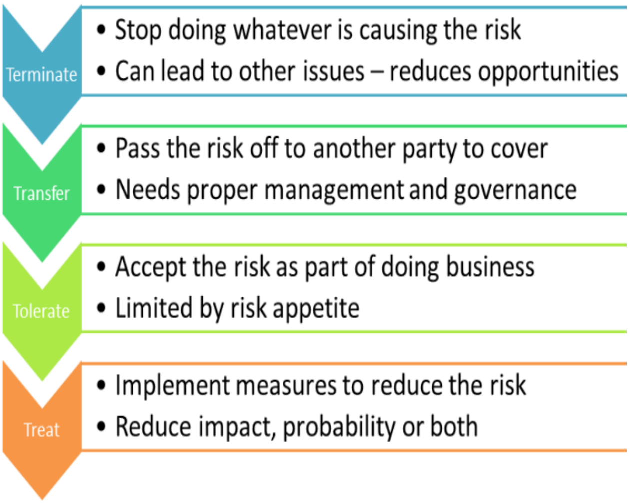


Risk treatment plan example

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

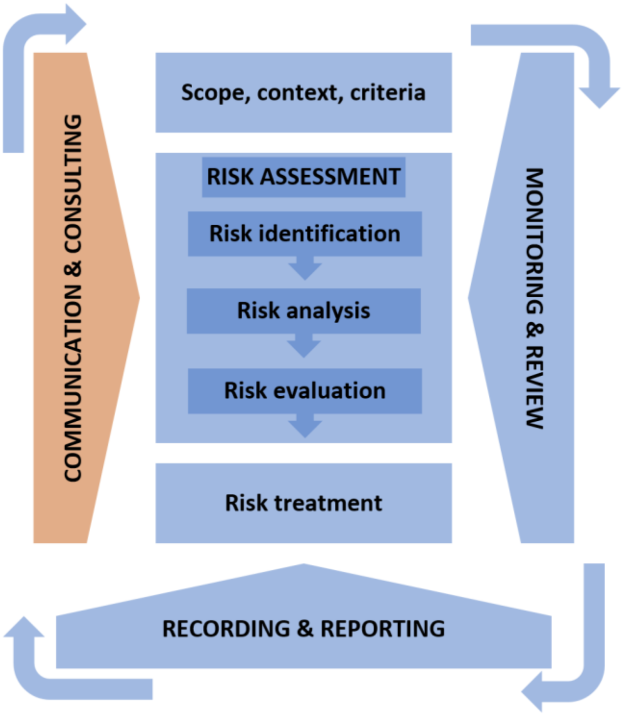
EXERCISE FOR SECURITY STUDENTS

Crisis typology and success factors in crisis management

AUTHORS: Ensieh Roud, Nord University, Norway

BACKGROUND:

Crisis managers must have a clear understanding of the type of crisis they are facing and its potential consequences. Effective crisis management requires balancing improvisation with pre-planned strategies, and leveraging both formal and informal networks. This exercise emphasizes the critical role of communication and knowledge sharing within organizations, aligning with principles outlined in the ISO 31000:2018 Risk Management framework. Successful crisis response focuses on building effective collaboration networks, characterized by key elements such as reciprocity, joint decision-making, and collaborative leadership. These factors are involved in navigating the complexities of a crisis and ensuring a coordinated response.

REFERENCE TO ISO 31000 STANDRD According to the ISO 31000 standard, communication is of paramount importance in effective risk management. Communication plays a critical role in all stages of the risk management process, including risk identification, assessment, treatment, and monitoring.	 COMMUNICATION & CONSULTING Scope, context, criteria RISK ASSESSMENT Risk identification Risk analysis Risk evaluation Risk treatment MONITORING & REVIEW RECORDING & REPORTING

GOAL OF THIS EXERCISE:

To equip students with a deeper understanding of key factors involved in effective collaboration and communication during the crisis response phase. By first identifying the type of crisis, its scope, and potential consequences, students will develop critical skills in assessing and managing crisis situations. Through a case study, they will practice categorizing incidents and pinpointing essential success factors for efficient crisis management.

TASK DESCRIPTION FOR STUDENTS:

1. Form groups (3-4) as instructed by teacher.
2. All the groups are given a case study to work on.
3. Familiarize yourself with crisis typologies under guidance from teacher.
4. Prepare a short presentation in your group where you answer the following questions:
   a) Categorize this crisis based on the typologies given
   b) Why this could be considered as successful response?
   c) What was the challenging issues in this event?
5. Present your presentation for your fellow students in the other groups.
6. After all presentations, discuss and share your thoughts with class.

TASK DESCRIPTION FOR TEACHER / TRAINER:

The teacher's tasks are as follows:

1. Before class, estimate the number of students and how many groups of approximately four students they would form. If you use digital platform, using breakout rooms could be suitable.
2. Before the class, the case and the crisis typology material should be send to students for example in Canvas. To familiarize students with crisis typology, you can suggest they watch the video titled 'Crisis Management' available here: https://security.turiba.lv/video/
   You can choose and case which reflects crises situation. T "Two examples of crisis situations can be found in the best practice articles: 'Collaborative Response During the Gjerdrum Landslide in Norway' and 'Learning from the Experiences of the Northguider Grounding'. Both articles are available here: https://security.turiba.lv/best-practice-cases/
3. Instruct student on preparing a presentation with a template.
4. During presentations, make sure to chair the discussion and keep the groups within the given schedule. The process is as follows:
   a) Approx. max. 5 minutes for one group presentation,
   b) After all presentations, groups should discuss 10 minutes with the class.
5. You might use a digital tool like LearnLab to make a visual summary of the students presentations and share with them

ADDITIONAL SKILLS THAT THE STUDENT ACQUIRES THROUGH THIS ASSIGNMENT:

- Engaging in effective group work to solve complex crisis scenarios.
- Navigating tasks efficiently under time constraints, simulating real-world crisis response.
- Delivering presentations and defending their analysis and decisions with well-founded arguments.
- Enhancing skills in comparing different crisis responses, assessing strategies, and thinking critically to determine best practices.

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

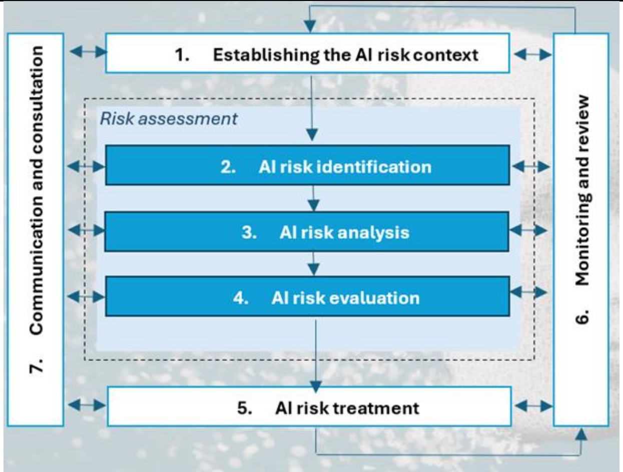
EXERCISE FOR SECURITY STUDENTS

AI Risk Assessment and Treatment Using ISO 31000

AUTHOR: Rita Lankauskienė, Kazimieras Simonavicius University, Lithuania

BACKGROUND:

The fast growth of generative artificial intelligence (AI) technology and the widespread use of creative AI solutions have led to the quick appearance of new risk types. This makes the already complicated processes of creating and implementing AI even less predictable. More and more problems are happening because of the (mis)use of AI (e.g., AI Incident Database, 2024; AIAAIC, 2024). These problems affect a lot of people, groups, and governments at all levels (national, international, and global). Using a risk management method to find risks, analyse them, rate them, and treat them is how risk management practices try to deal with core uncertainties. In this exercise, the ISO31000 standard methodology is modified and applied to assess the AI risk in real life AI cases to model the AI risk treatment scenarios.

REFERENCE TO ISO 31000 STANDRD The ISO 31000 standard offers a systematic methodology for risk management that may be tailored to the particular requirements of AI security, for implementing an AI risk assessment in particular circumstances.	

GOAL OF THIS EXERCISE:

The students will learn to apply the ISO31000 standard methodology-based logic to assess the AI risk in selected real life AI cases and to model the AI risk treatment scenarios.

TASK DESCRIPTION FOR STUDENTS:

1. Form the groups as instructed by teacher and allocate the responsibilities within the group:
    - Who will guide throughout the discussion process, following the task questionnaire and supportive material?
    - Who will fix the discussion summary highlights in written form?
    - Who will present the final group work outcomes to the class?

2. Familiarize yourself and your groupmates shortly with the core building blocks of risk assessment logic, embedded in the ISO31000 standard. On demand, check for additional material for the best practice guidelines, developed by the Internet of Things Security Institute (IoTSI), on how to conduct an AI security risk assessment using ISO 31000. (Available at: https://iotsecurityinstitute.com/iotsec/index.php/iot-security-institute-blog/155-conducting-an-ai-security-risk-assessment-using-iso-31000.) You may also read the material, presented in the

3. Select the case of a (mis)use of AI from AI Incident Database (2024): https://incidentdatabase.ai/. Remember to fix the general details regarding the selected case, as given in the questionnaire guidance.

4. Conduct an AI security risk assessment using ISO 31000 methodology: step-by-step implement all security assessment steps for your selected case of a (mis)use of AI. Carefully follow the questionnaire. Be flexible in forming supportive questions on demand.

5. Discuss withing a group and select one identified risk to prepare a risk treatment scenario.

6. Agree on the final outcome of your group, and prepare up to 10-minute presentation, which include the following aspects:
    - Title and source of the selected case;
    - Team members, who worked on the output;
    - The general description of the selected case of a (mis)use of AI (up to 5 sentences);
    - The internal and external context of a (mis)use of AI;
    - AI risk assessment core steps: identification, analysis and evaluation;
    - Risk treatment plan (scenario building) for selected risk: actions, resources and responsibilities.
    - Summary feedback on the most complicated and most successful stages of applying ISO31000 methodology for AI risk assessment and treatment planning.

7. Listen to other presentations of other groups. After each presentation, engage in a two-minute discussion with your group to determine whether their approach to the selected cases would have been pertinent to you as well. In your turn, articulate your views to the class.

8. Discuss in your group which of the presented approaches would be most appropriate for each case after all presentations have been completed. Please share your thoughts with the class.

TASK DESCRIPTION FOR TEACHER / TRAINER:

The teacher's tasks are as follows:

1. Estimate the number of students and the number of groups of approximately up to 5-7 students that will be formed prior to the commencement of the class.
2. Each group should have access of the supportive material (depending on the live/remote mode):
   - AI security risk assessment table, based on ISO 31000 guidelines (Annex 1);
   - ISO 31000: 2018 framework (Annex 2);
   - internet to select the case of a (mis)use of AI from AI Incident Database (available at: https://incidentdatabase.ai/) prior to the commencement of the class;
   - A1 format paper sheet, colourful post-it notes and markers (or equivalent software in a distanced mode).
3. Distribute students into groups of approximately up to 5-7 students.
4. Instruct students to familiarise with the ISO 31000:2018 standard, as well as the case on “AI Security Challenge and Risk Assessment Using ISO 31000”.
5. Instruct the students how to record the outcomes of their preferred approach, following the “AI security risk assessment table, based on ISO 31000 guidelines”, provided in Annex 1. Remind, that this table is elaborated from the case on “AI Security Challenge and Risk Assessment Using ISO 31000”, which the students must be already familiar. Discussion outcomes might be accomplished through various methods, such as post-it notes, a PowerPoint presentation, a whiteboard, or an online environment. Students should be advised on how to prepare for the presentation of their findings. Provide instructions, what the presentation should include (see above). Remind students, that the presentation may last to a maximum of 10 minutes.
6. During the presentations, ensure that the discussion is chaired and that the groups remain within the designated time frame during presentations. The procedure is as follows:
   - One group presentation is expected to last no more than 10 minutes.
   - Following each presentation, groups should engage in a two-minute discussion within their respective groups to determine whether the approach that was presented would have been pertinent to their own approach.
   - The class is encouraged to hear the perspectives of the other groups.
   - The fundamental inquiry is: are the elaborated risk treatment plans lead to expected outcomes?
7. Follow each presentation with a discussion among all students regarding the most effective approach.

ADDITIONAL SKILLS THAT THE STUDENT ACQUIRES THROUGH THIS ASSIGNMENT:

- Working in a group
- Working under time pressure
- Giving presentation and arguing the case
- Comparison skills and critical thinking

This activity focuses on risk assessment, with the primary purpose being a comprehensive evaluator of the risks associated with the increasing adoption of AI in certain contexts. Through this process, the students will not only become acquainted with the ISO31000 standard methodology and logical framework, but will also learn to adapt it by critically evaluating the implications and effects of AI challenge in real life cases, in different spheres of human activity.

SUPPORT MATERIALS

Relevant references:

- AI Incident Database (2024). Available at: https://incidentdatabase.ai/
- IoT Analytics. State of IoT, Summer 2024. Market Report. Available at: https://iot-analytics.com/product/state-of-iot-summer-2024/
- Conducting an AI security risk assessment using ISO 31000 (2024). IoTSI. Available at: https://iotsecurityinstitute.com/iotsec/index.php/iot-security-institute-blog/155-conducting-an-ai-security-risk-assessment-using-iso-31000
- ISO 31000:2018. Risk management – Guidelines (2018). Available at: https://www.iso.org/obp/ui/en/#iso:std:iso:31000:ed-2:v1:en

Annex 1

AI security risk assessment table, based on ISO 31000 guidelines

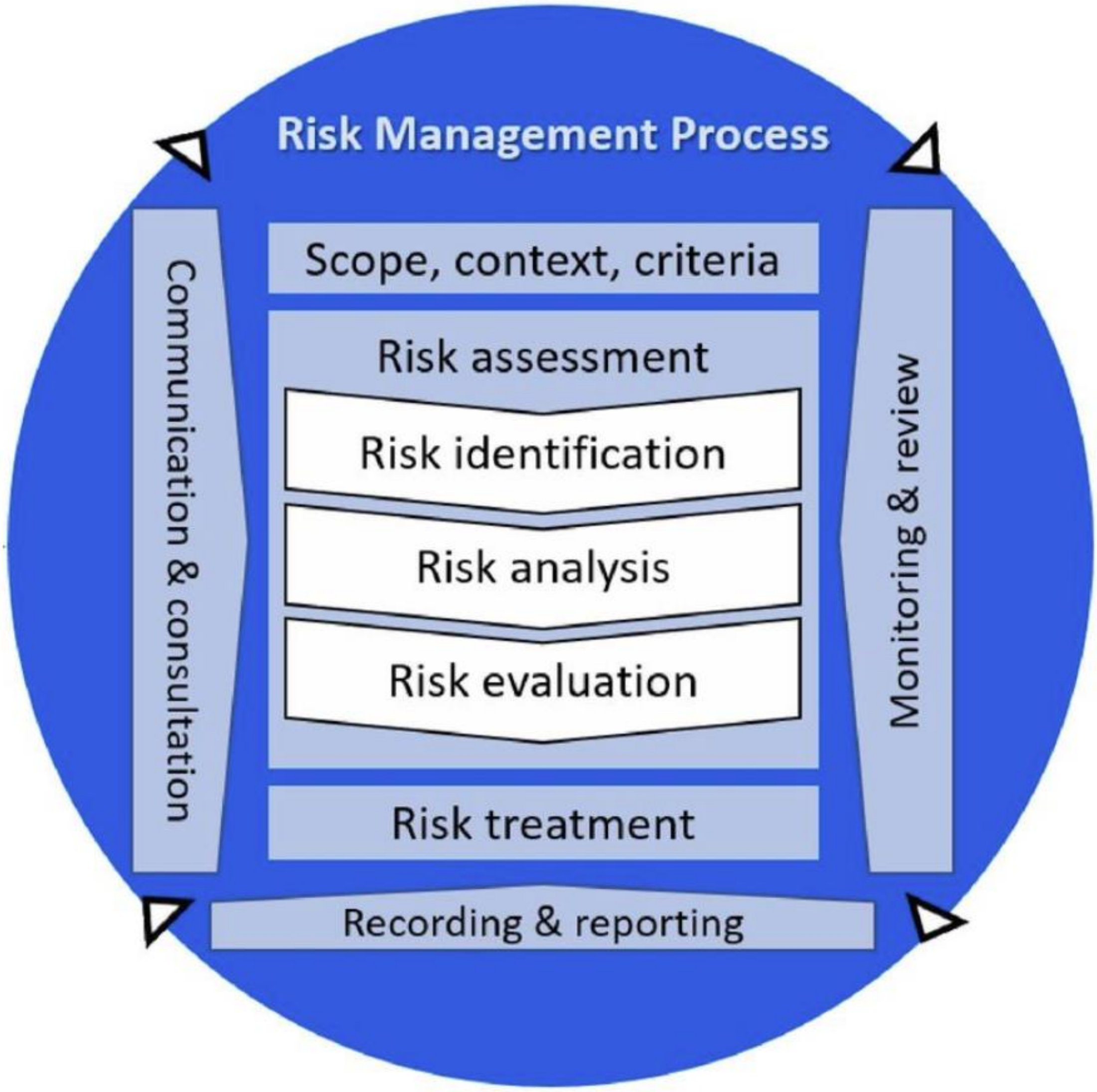
Case data: - Title: - Link to the selected case: - Date of access:		
Group data: - Moderator: - Raporteur: - Output-generating actors:		
AI SECURITY RISK ASSESSMENT PROCEDURE		
	Contents	*Notes*
Establishing the context		
Internal context:	- Regulatory landscape; - Market and technological trends; - Threat landscape.	
External context:	- Organizational structure; - Risk management policies; - Risk appetite and tolerance.	
AI Risk Assessment		
AI risk identification	*Data risks:* - *breaches,* - *data poisoning,* - *data integrity.* *Model risks:* - *adversarial attacks,* - *model stealing,* - *model bias.* *Operational risks:* - *system failures,* - *security configuration,* *third-party risks.*	
AI risk analysis	*Impact assessment:* - *financial impact,* - *operational impacts*, - *reputational impact*, Likelihood assessment: - *historical data*, - *vulnerability analysis,* - *threat actor capability.*	
AI risk evaluation	*Risk matrix:* - High - Moderate - Low *Decision-making:* - everyone involved, - sepatare stakeholders involved, - stakehoder groups invoved.	

Risk Treatment Plan		
The *objective* - define clearly what a particular treatment is supposed to do, like lowering the risk of data leaks or weakening the effects of hostile attacks.	Objective:	
The *actions* - specify to tell the people what they need to do, like putting in place multi-factor login, encrypting data, or doing regular security checks.	Actions:	
Equip the risk treatment measures with reasonable *resources*, staff, and technology they need to be put into action.	Resources:	
Clearly assign *responsibilities* for executing the treatment plan, ensuring accountability and oversight	Responsibilities:	
Risk treatment plan example: To mitigate the risk of model bias, a treatment plan may encompass diversifying training data, applying fairness metrics, and performing regular audits to identify and rectify biases.		

Source: elaborated by author, based on IoTSI guidance (2024). Conducting an AI security risk assessment using ISO 31000. Available at: https://iotsecurityinstitute.com/iotsec/index.php/iot-security-institute-blog/155-conducting-an-ai-security-risk-assessment-using-iso-31000.

Annex 2

ISO 31000: 2018 framework



Source: ISO 31000:2018. Risk management – Guidelines (2018). Available at: https://www.iso.org/obp/ui/en/#iso:std:iso:31000:ed-2:v1:en .