Funded by the European Union

secureu
DIGITAL EDUCATION TOOLS FOR SECURITY RISK MANAGEMENT

ERASMUS+ cooperation partnership

Digital education tools for

SECURITY RISK MANAGEMENT

BEST PRACTICES 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.

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, titled "European Best Practices on Security Risk Management," serves as a comprehensive resource on various subtopics within the field of security risk management. It provides readers with valuable insights, including articles that showcase best practices, practical case studies, and expert advice.

Within this material, you will find articles covering a wide range of topics, including early-stage security threat identification, security risks associated with public events, the role of artificial intelligence in security risk management, and crisis management strategies.

The target audience for this publication includes students with a strong interest in security risk management, as well as lecturers and professionals actively working in the security field.

Table of Contents

1. IMPLEMENTING SECURITY RISK MANAGEMENT FOR AN ORGANIZATION OPERATING AS AN ELECTRICITY GRID MANAGER IN THE CRITICAL INFRASTRUCTURE

Lambert Bambach / Avans University of Applied Science, the Netherlands / 2023

ABSTRACT

Threats of nation state actors and organized crime are changing the threat landscape of the critical infrastructure in which organizations operate as electricity grid managers. Examples of the threats are hacking, theft, destruction and manipulation of the electricity grid. To deal with these threats, it is important to have an asset protection programme that is up to date. This is achieved by mapping the various assets to be protected in line with the organization's objectives, performing threat and risk analysis in collaboration with government actors at European and National level, competing fellow electricity grid operators at national level and several departments within the organization itself.

Link to ISO 31000

Improvement, design, Implementation, best available information, customized, communication & consulting, risk identification, risk analysis and risk evaluation.

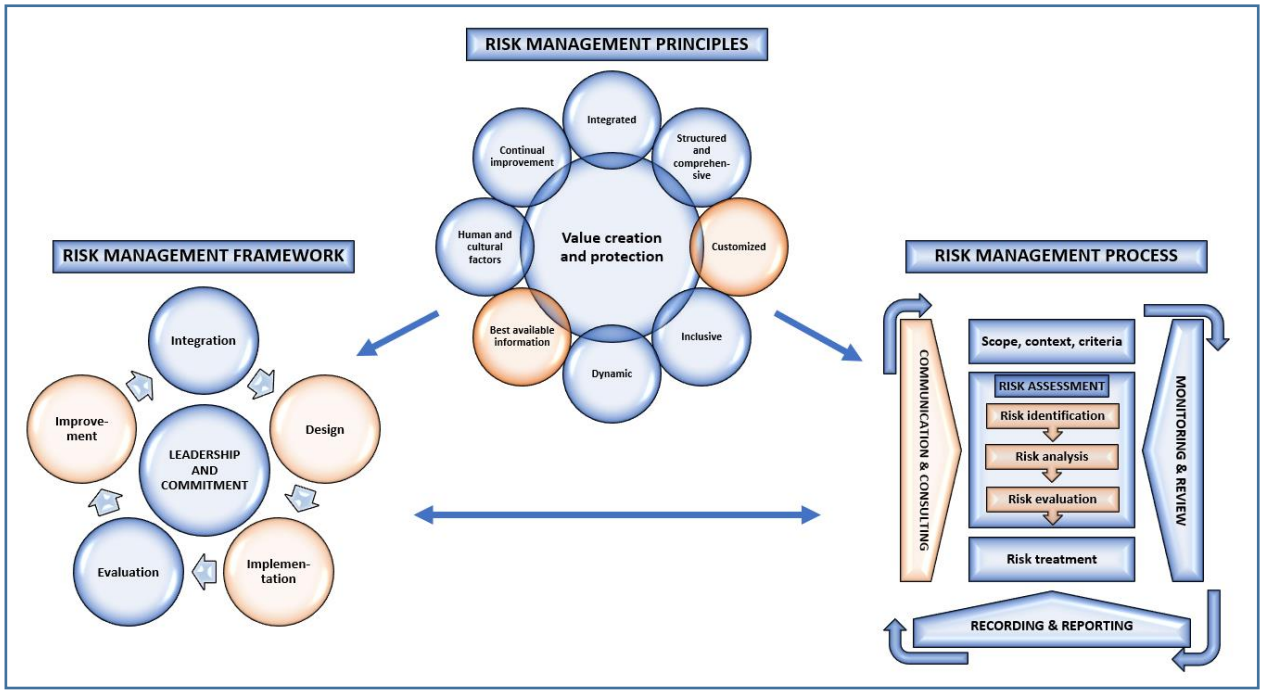


Figure 1. Risk management framework, Risk management principles and Risk management process according to ISO 31000:2018

1. Introduction

A junior security employee in the Asset Protection department of an electricity grid manager, is asked to provide insight into a possible method for renewing the Asset Protection Programme for 40,000 decentralized unmanned assets ranging from low voltage, medium voltage spaces, high-voltage cables and two central locations where large data centers are located.

The interest of the organization is that the asset protection programme must be established in collaboration with internal and external stakeholders to provide protection against threats to assets in the fields of Information Security, Operational Technology and Physical Protection.

With the renewed asset protection programme, a level of security must be realized that, in collaboration with various actors, copes with a changing threat landscape in which State Actors, organized crime and pilferers increasingly pose threats to the realization of the objectives. Also posing a threat to the primary objective of the organization: 'at all times distributing energy across all their grids every single day'.

The organization wonders how the asset protection programme can be achieved.

2. Case

The organization functions as electricity grid manager, responsible for properly distributing energy across all their grids every single day. Through cables and pipes, over three million Dutch households and companies are supplied with electricity. For this, 40,000 decentralized unmanned assets ranging from low voltage, medium voltage rooms, high voltage cables and two central locations where large data centers are located are used. The organization wants its grid to remain among the world's most reliable ones, and maintain dependability, affordability and accessibility of the grid for their customers.

The security risk manager explains that the asset protection programme should be able to cope with the changing threat landscape so that the goals of the organization can continue to be realized. In this changing threat landscape of terrorism, the likelihood of operating systems getting hacked by Nation State Actors and the stealing of valuable materials by organized crime and pilferers is increasing.

The security manager also knows that the number of assets that need to be protected is not only extensive but also diverse in nature. It concerns both assets that are OT and IT related. He has to deal with several stakeholders who play roles and with whom cooperation is required. These actors do not always have the same interests as the organization. It is also not yet clear how the various laws and regulations can best be complied with.

For all these reasons, you are asked to provide insight into a possible method to realize the asset protection programme. In doing so, it is important to take into account: a) the purpose of the organization; (b) threats and risk analysis; (c); (d) various stakeholders.

3. Best practices

3.1 Purpose of the organization

The primary objective of the organization, to be able to distribute energy across all their grids at all times every single day, to keep their grid one of the most reliable ones in the world.

3.2 Different types of assets

The organization has Assets both in the decentralized field and centrally. In the decentralized field, the organization deals with assets such as control cabinets, transformers. Operational Technology (OT) plays an important role in these assets. Operational Technology is characterized by the fact that it is all set up with only one goal: 'It must run for as long as possible and with as little downtime as possible. It is therefore equipment that lasts a long time, which often does not meet the standards that we set today, because it was once built to the standards that applied 30 years ago. In addition, an OT asset cannot protect itself digitally.

Centrally, the organization deals with assets such as office buildings and data centres that are more Information Technology (IT) related. With an IT environment you assume that an information asset must be able to protect itself. You also assume that you need flexibility with IT you are mainly working with it functionally. It must support the business goals and these are all quickly flexible, having short lifespans.

That means that you need to look at OT assets differently than IT assets. As a rule, an OT asset can also be considered as an asset that cannot protect itself, so that means that you must build the measures around it to protect such an asset. However, the three fundamental basic principles of information technology are: integrity, confidentiality and availability. Periodic downtime is accepted. In operational technology, the valuation of these basic principles is different, namely: availability, integrity and finally confidentiality. Downtime is not accepted.

3.3 Threat and risk analysis

3.3.1 Identification and analysis of risks

The main threats are Nation State Actors, organized crime and pilferers which can lead to compromising the primary objective of the organization by hacking, theft, destruction and manipulation of the electricity grid.

3.3.2 Risk Assessment

In the case of the Nation State Actor it is difficult to mitigate this threat because these actors often have unlimited resources. It is an accepted risk. But the critical infrastructure may not be compromised and has to be available all the time, because many other public services and organizations depend on it. For example, the police expect to always keep their communication systems up and running. If the police are no longer able to communicate in times of crisis, then the organization has a problem because this poses a national security problem and the organization does not achieve its primary objective: 'security of supply'. This means distributing energy across all their grids at all times every single day.

In the case of organized crime, the organization needs to take some more security measures. Especially for the OT assets because these assets cannot protect themselves. That also means that measures must be built around them to protect such assets, using camera systems, fences and reinforced access control. For this, the organization is also continuously developing and assessing annually whether the security baseline is still sufficient or not and whether it needs to be adjusted or

not? For the pilferer, the standard measures to mitigate this threat are often sufficient. The pilferer is characterized by the fact that the chance of participating in criminal activities increases if the opportunity is there. So, if the opportunity is limited, there is a high probability that the pilferer will not continue their activities.

3.4 Laws and regulations

3.4.1. Legislation

In the case of this organization, one of the most important stakeholders is the legislature. The organization is supervised by the National Inspectorate of Digital Infrastructure of the Ministry of Economic Affairs and Climate because the organization is regulated under the NIS 1 and will be regulated in the near future under the NIS 2, as they are part of the Dutch vital infrastructure. NIS is the directive on the security of network and information systems (NIS Directive), as ordered by the European Union Agency for Cybersecurity (ENISA).

3.4. 2. Regulation

In addition, the organization has also certified itself in accordance with ISO 27001 together with ISO 27019.

ISO standardizations have helped the physical and information security department to be able to advise objectively. Standardization also helps to speak a universal language internally, for example with management, but also with external actors such as a regulator and it helps in the continuous search for improvements within the organization.

3.5 Stakeholders

The various stakeholders form sources on which the organization relies to map the threat landscape and risk appetite of its own organization and to test whether they are on the right track to gain insights in the threats and to work together to mitigate the threats.

3.5.1 Internal stakeholders

3.5.1.1 Management

Management makes choices as to whether it will actually implement measures. It makes its decisions based on the threat landscape advised to it by the physical and information security department. An ISMS has been set up for this purpose, which falls directly under the Board of Directors. That is the highest body where all the final decisions for the organization are taken. The moment the organization faces an injudicious risk, the physical and information security department can report that to the Board of Directors, after which resources can be shifted to address the problem to be able to do the right things. The questions are: Are we actually going to implement all the measures and in what period of time are we going to do that? Or perhaps we are not going to adjust the requirements accordingly, so that perhaps something will be weakened? Or perhaps even more effort will be made on measures.

3.5.1.2 Department of physical and information security

The physical and information security departments are working together. In the organization, the departments fall directly under the Board of Directors. For the organization it is actually the only place where security belongs and also the only place where the departments can carry out their independent role, because security is on the one hand requirement setting and on the other hand controlling, but never executive. Very often one sees that in organizations it is placed in an executive department, then the security departments can never be independent in the advice to be given.

To establish effective requirements, the organization considers the following: a) What are we actually going to protect? b) What are we protecting at the moment? c) What are our crown jewels?

An important task here is to help staff members become aware of the fact that the threat landscape has actually changed and that this leads to new measures. It is also about involving them in the changes regarding security. We get new information assets, what does this mean for your work as security measures will also change? That does not mean that you merely need to be technically trained for that, but also that we should put other management measures in place and let staff members know why we do that. In this respect enabling security awareness is important.

3.5.2 External stakeholder

3.5.2.1 Europe

The European Network of Transport System Operators of Electricity (ENTSO-E), is the partnership in which all European network operators active in the synchronized network of Europe are represented. The organization is a member of ENTSO-E, in order to exchange knowledge about the changing threat landscape.

3.5.2.2. National Government

To obtain information for the threat and risk analysis, the organization cooperates with the National Cyber Security Center of the Ministry of Justice and Security, the National Coordinator for Counterterrorism and Security of the Ministry of Justice and Security and the General Intelligence and Security Service of the Ministry of the Interior and Kingdom relations. Additionally, it is supervised by the National Digital Infrastructure Inspectorate of the Ministry of Economic Affairs and Climate Policy, which monitors the execution of the imposed tasks.

3.5.2.3 Competing fellow electricity grid operators

The organization works together with 3 network distributors. They share the same interest in protecting the vital infrastructure but are competing organizations as well. They work together to lay down a minimum security baseline that needs to be reviewed periodically, in order to keep in line with the most current threat landscape and to know whether the security measures of the organization itself and the others are in place. From a commercial point of view, it is important to which extent the organization invests in security measures, but also whether your security measures are at least equal to or perhaps better than those of the competitors, because the criminal still looks for the weakest link.

References

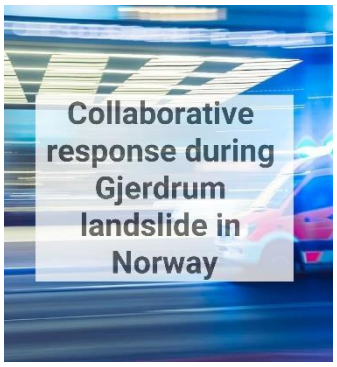
1. Cybersecurity And Nation-State Threats: What Businesses Need To Know. Accessed 31.05.2023 Cybersecurity And Nation-State Threats: What Businesses Need To Know (forbes.com)
2. European association for the cooperation of transmission system operators. Accessed 30.05.2023 Home (entsoe.eu)
3. European Union Agency for Cybersecurity. Accessed 31.05.2023 https://www.enisa.europa.eu/
4. How do OT and IT differ? Accessed 31.05.2023 https://www.cisco.com/c/en/us/solutions/internet-of-things/what-is-ot-vs-it.html
5. Identify Your “Crown Jewels”. Accessed 30.05.2023 https://staysafeonline.org/cybersecurity-for-business/identify-your-crown-jewels/#:~:text=Crown%20jewels%20are%20the%20data,high%2Dvalue%20target%20for%20cybercriminals.

6. Information security management system (ISMS). Accessed 30.05.2023 https://www.techtarget.com/whatis/definition/information-security-management-system-ISMS
7. ISO/IEC 27001. Accessed 31.05.2023 ISO/IEC 27001 - Wikipedia
8. ISO/IEC 27019. Accessed 30.05.2023 https://en.wikipedia.org/wiki/ISO/IEC_27019
9. Information Technology. Accessed 31.05.2023 Information technology - Wikipedia
10. NIS Directive Accessed 31.05.2023 https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new
11. Operational Technology. Accessed 31.05.2023 https://en.wikipedia.org/wiki/Operational_technology

2. COLLABORATIVE RESPONSE DURING GJERDRUM LANDSLIDE IN NORWAY

Ensieh Roud / Nord University, Norway / 2024

ABSTRACT



This article presents some successful elements of collaboration during an emergency response to a landslide which happened in Gjerdrum, Norway. Furthermore, it will shed light on the pivotal role of improvisation versus planning, and formal versus informal connections. This article highlights role of communication and knowledge sharing within organizations, which is important part of ISO 31000:2018 Risk management process. Effective collaboration networks, characterized by discursive properties such as reciprocity, participatory decision making, and collaborative leadership, are identified as successful elements in this incident.

Link to ISO 31000

This article highlights role of communication and knowledge sharing within organizations, which is important part of ISO 31000:2018 Risk management process.

1. Introduction

Countries and communities need to develop solutions for adaptation and implement action to respond to the impacts of climate change that are already happening, as well as prepare for future impacts. These are words from the UN Climate Change Secretariat (UNFCCC, 2021), discussing adaptation to climate change. However, natural disasters are not isolated events, as they are often the result of complex interactions between social and environmental factors (Boin et al., 2020). To address this multifaceted issue, this article will address the ISO 31000 principles and refer to the ASIS handbook 'Domain Seven'.

Collaboration across multiple geographic and organizational boundaries is one of the key parts of enhancing risk management and resilience that enable effective response and recovery activities in a natural disaster (Therrien, Beauregard, & Valiquette-L'Heureux, 2015).

The evaluation reports of several disasters, such as Hurricane Katrina, the California wildfires and the flood in Germany in 2021, indicate that more organized inter-organizational collaboration would have reduced the destructive effects of these events. The dynamic situations in natural disasters and responding to complex events often require emergency organizations to deviate from established organizational structures to address a novel context and new tasks (Andreassen & Borch, 2020). Responding to natural disasters requires organizations to collaborate because a single organisation may not respond independently due to rapid changes in the environment, a lack of experience, the scope of the task, and insufficient resources (Kapucu & Garayev, 2011).

This inter-organizational collaboration can be ensured by the systematic sharing of information possessed by each organization and by combining their goals (Therrien, Beauregard, & Valiquette-L'Heureux, 2015). Therefore, in such collaborative emergency response, several organizations, such as

police departments, paramedic services, and rescue agencies, may be involved. In addition, depending on the scale of the emergency, local authorities, government departments, military forces, and various businesses from different nations may also be engaged. Additionally, resilience enhancement in a natural disaster requires an integrated hazard mitigation and resilience plan that includes inter-organizational collaboration among interdependent organizations (Godschalk, 2003).

This article presents some best practices of the inter-organizational relationships in the landslide event in the small town of Ask in the Gjerdrum municipality in Norway. Due to its coastline and wide mountain ranges, Norway is highly exposed to changing weather conditions. The "Climate in Norway 2100" report, provided by the Norwegian Centre for Climate Services (NCCS, 2017), indicates that gradually increasing temperature, increased precipitation and extreme rainfall, and increased floods in the future climate may cause more quick clay slides in certain areas in Norway (p.34). In addition, some flood and landslide events have been studied with a view to improving risk and crisis management related to natural hazards.

2. Case

The 2020 Gjerdrum landslide occurred in Norway, at Ask village, Gjerdrum's administrative center. This quick clay landslide spanned an area of 300 by 700 meters and caused debris flow to affect an additional 9 hectares. While some individuals were rescued and others evacuated themselves, 10 people lost their lives and several buildings were destroyed, resulting in an estimated economic cost exceeding $100 million (Nikel, 2021). The Joint Rescue Coordination Center (JRCC) report states that during the early phase of the Gjerdrum landslide, the primary challenge was to acquire a comprehensive understanding of its extent and to request appropriate resources (JRCC, 2021).

Emergency situations are often characterized by uncertainty and limited information, and incidents occurring during the night or under adverse weather conditions, such as the Gjerdrum landslide at night during the Christmas period, exacerbate the challenge of gaining an overview. The incident necessitated a demanding search and rescue (SAR) operation due to the significant number of people requiring immediate attention, and the subsequent breakdowns in infrastructure, such as water, sewage, roads, and electricity in the area, added to the complexity of the operation (JRCC, 2021).

3. Best practices

The response to Gjerdrum landslide is considered as fairly successful. It could have ended in larger tragedy. Reviewing the evaluation reports and interviewing the actors involved revealed some elements of great collaboration. In Norway, after the terrorist attack in 2011, several reforms have taken place and collaboration was added to the crisis management principles. Since then, the organizations have gone through exercises together to enhance interorganizational collaboration. The municipality in Gjerdrum planned an exercise based on a landslide scenario but due to the outbreak of Covid, unfortunately, they could not execute it. If they had been able to do that, however, the interorganizational challenges that they faced would have been minimized. This revealed the importance of joint exercises and how it can positively influence ***information dissemination, communication, clarity of roles, establishing common operating terms and allocation of resources***.

During the Gjerdrum landslide, fire brigades invited the Norwegian Directorate for Civil Protection (DSB), to listen to their meeting at the operating center. This is the first time they have done

it and it was identified as an efficient way of passing information to decision makers at a higher level without creating any confusion. However, the DSB believes this should happen by invitation only from the lower level and not through a command from them. This example highlights the importance of flexibility and trust among organizations involved and across levels.

Moreover, having a liaison who has decision making authority was identified as a facilitating element in collaborative emergency response. This might save a huge amount of time during a crisis.

The crisis management structure of Norway was found to function very well during the landslide because the police were the leader of the operation and there was almost no conflict when it came to decision making and clarity of roles.

There were two operation centers - side by side during the days of a rescue operation, one of which continued its operation for two months after the first one ended. One operation center was focused on the rescue operation, the other on all the other tasks that also had to be taken care of, but which did not fall directly under the rescue operation. The tasks that were solved by the second operation center were also very important tasks and had an impact on life and health. There were, for example, farms with several hundreds of animals within the evacuated zone, there was a need for measures to improve infrastructure such as water and roads and there was a need to retrieve important assets from evacuated buildings. This has been identified as an innovative approach to handle crises. It prevents information overload in one center and categorizes the tasks during operations to facilitate collaboration.

This case further revealed how critical is to have personal and informal contact during crises. For example, the municipality explained that due to Covid it faced so many obstacles and all the roads were destroyed, making the transfer of people to a safe place difficult. It was almost impossible to get public transport in order, but the person in charge had some contacts in private transport companies and was able to call them for assistance.

All the examples above are in line with the findings from our Norwegian security experts round table in which it was underlined how significant soft skills such as communication, continuous interaction, cooperation and making innovative decisions are.

References

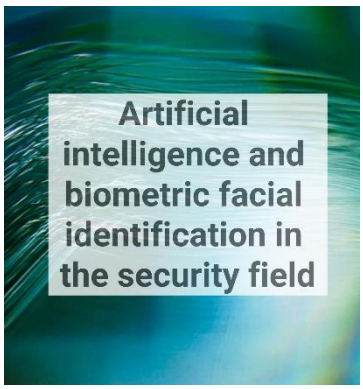
1. ASIS International Board Certification Handbook. Accessed 20.04.2023 https://www.asisonline.org/globalassets/certification/documents/certification-handbook_final.pdf
2. Andreassen, N., Borch, O. J., & Sydnes, A. K. (2020). Information sharing and emergency response coordination. *Safety Science*, *130*, 104895.
3. Boin, A., Ekengren, M., & Rhinard, M. (2020). Hiding in plain sight: Conceptualizing the creeping crisis. *Risk, Hazards & Crisis in Public Policy*, *11*(2), 116-138.
4. Climate in Norway 2100 (2017). Accessed 25.05.2023 https://www.miljodirektoratet.no/globalassets/publikasjoner/M741/M741.pdf
5. Godschalk, D. R. (2003). Urban hazard mitigation: Creating resilient cities. *Natural hazards review*, *4*(3), 136-143.

6. JRCC (2021). Evaluation report of the rescue operation and the emergency management under quick clay landslide at Gjerdrum. Accessed 25.05.2023. https://www.regjeringen.no/contentassets/52d43dc95b5b44fd80293c2b3515713b/rapport-gjerdrum-hovedredningssentralen-03-06-2021-digital-1.pdf
7. Kapucu, N., & Garayev, V. (2011). Collaborative decision-making in emergency and disaster management. *International Journal of Public Administration*, *34*(6), 366-375.
8. Nikel, D. (2021). Norway Landslide Insurance Bill Tops $100 Million [Press release]. Accessed 25.05.2023. https://www.forbes.com/sites/davidnikel/2021/01/08/norway-landslide-insurance-bill-tops-100-million/
9. Therrien, M. C., Beauregard, S., & Valiquette-L'Heureux, A. (2015). Iterative factors favoring collaboration for interorganizational resilience: The case of the greater Montréal transportation infrastructure. *International Journal of Disaster Risk Science*, *6*, 75-86.
10. United nations climate change annual report (2021). Accessed 25.05.2023 https://unfccc.int/sites/default/files/resource/UNFCCC_Annual_Report_2021.pdf

3. ARTIFICIAL INTELLIGENCE AND BIOMETRIC FACIAL IDENTIFICATION IN THE SECURITY FIELD

Javier Dorado / School of Prevention and Integral Safety and security, Spain / 2024

ABSTRACT



The use of biometric facial identification technologies in public and private institutions for security purposes is a reality. Examples are detection and prevention within access control, or the identification of suspects or wanted persons. Nonetheless, the use of these techniques that operate with artificial intelligence and automated decisions presents several problems, not only in terms of regulatory legitimacy from the point of view of the protection of fundamental rights, but also from an operational perspective. In this sense, biometric identification must be approached from a dual analysis: the technical-operational and the legal-regulatory, as both dimensions can entail risks for the organisation and the physical integrity of individuals.

Link to ISO 31000

Parts from ISO 31000:2018 Risk management process referenced in this article – Risk Assessment, Risk Treatment, Monitoring, and Review.

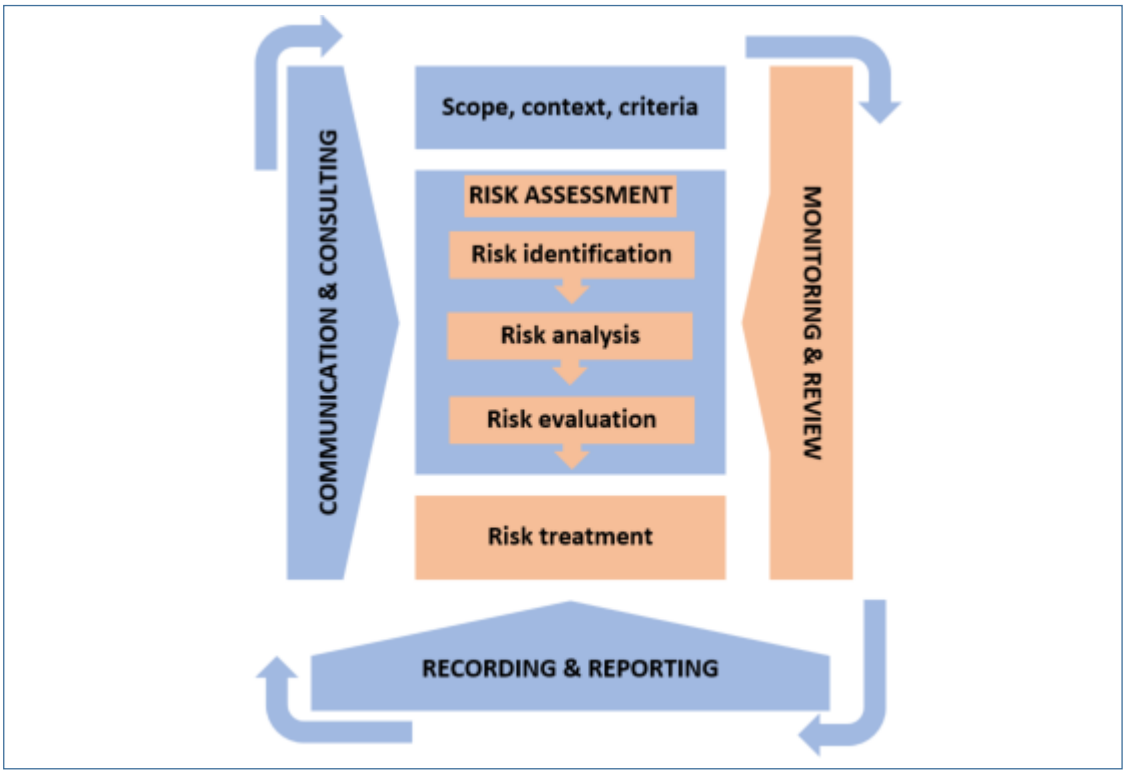


Figure 2. Risk management process (adapted from ISO 31000:2018), Risk assessment, risk treatment, monitoring, and review.

1. Introduction

A company entrusts you with the task of analysing the risks involved in implementing a biometric identification camera for access control purposes on its premises. However, they are not only concerned about the potential failures that this technology might generate, which could endanger private security purposes, but also about the possible administrative sanctions that this could entail within the framework of data protection.

With regard to technical-operational issues, the company needs to detect a number of persons who have previously been convicted of theft or burglary. For these persons, the company has biometric facial identification templates. However, the company has concerns about the possibility of incidents (false positives or false negatives) with this technology.

In terms of regulatory issues, the company is unclear to what extent and under what conditions it can use this technology without incurring a data protection infringement.

2. Case

The company in question is a jewelry shop and, as mentioned above. It has a database with the facial templates of people (15 in total) who have been previously convicted by the criminal courts in the last three years, specifically for theft or burglary in the establishments of this business.

The manager of the jewelry shop explains that the biometric identification camera, if positive, will inform the state security forces and bodies, so that they can go and arrest those identified, as they have a restraining order against the establishments, issued by the criminal jurisdiction.

However, the manager knows that this type of technology sometimes fails, either because of false positives (mistaken identifications) or false negatives (failure to detect the reported person in the database). In the first case, the company does not want to have problems with customers, as a false positive could lead to a complicated situation, as the system is designed to alert the police, when, in this case, the person identified has no criminal record. In the second case, on the contrary, if the identification fails, there would be a potential risk to the physical integrity of the employees, and/or to the company's assets, depending on whether the individuals in question are punished for robbery with violence or theft, respectively.

Furthermore, it is not clear to the company whether they can use this type of technology legally or whether there are risks of sanctions, which could lead to financial problems for the company.

For all these reasons, you are entrusted with the task of issuing a report with a dual perspective: a) a technical-operational report on the risks and advantages that the use of biometric identification cameras for access control purposes may entail; and b) a regulatory report on the conditions under which this technology can be used without violating data protection regulations.

3. Best practices

3.1 Technical-operational risks: a) False positives; b) False negatives

3.1.1 Identification and analysis of risks

The main risks to be reported to the company are indeed the possibility of occurrence failure of the technology such as false positives or false negatives.

3.1.2 Risk assessment

In the first case, it is important that the company providing this technology informs us of the probability of its software generating this type of failure. Once this point has been clarified, and

considering that the bug cannot be neutralised, a two-step protocol should be put in place, in order to ensure that no one who does not meet the requirements is stopped. In this regard, it is recommended that a switchboard should filter out suspicious positives, i.e., those where there is doubt as to the identification of suspects.

In the case of false negatives, it is clear that it is difficult to implement an ex-ante access control process, as it is precisely this that has failed. Therefore, again, human verification is needed. If artificial intelligence fails, human intelligence can make up for it. This could be done by training employees, so that they can appeal to the competent public authority when they suspect that a customer's behaviour is inappropriate and may pose a risk to the physical integrity of employees or the company's assets.

3.2 Regulatory risks: GDPR sanctions

3.2.1 Identification and analysis of risks

On the legal-regulatory level, the company's assignment presents even more problems. The first thing we need to make clear to the company is that Art. 9 GDPR establishes a prohibitive rule regarding the use of "biometric data intended to uniquely identify a natural person". This prohibitive rule is accompanied by a series of assumptions that legitimise the use of personal data through these technologies. These assumptions include a) explicit consent; b) vital interests of the data subject or another natural person; c) exercise of legal actions; d) essential public interest.

3.2.2 Risk assessment

Regarding consent, it can hardly be given, in the terms of the **GDPR** (art. 7), in the context of the establishment. We cannot ask for explicit, specific consent, for the purposes of processing, from every single customer entering the establishment. As for the essential public interest, we must rule it out, as we are in the field of private security.

On the other hand, the other two enabling grounds (vital interests and legal action) can lift the ban on the processing of biometric data for access control purposes.

However, considering the millions of administrative penalties that would result from unlawful use of such data without respecting the principle of lawfulness (Art. 83.5 **GDPR**: administrative fines of up to EUR 20 000 000 or, in the case of a company, an amount equivalent to up to 4% of the total annual global turnover of the previous financial year), we recommend that a consultation with the national data protection agency be carried out. In the meantime, we recommend that the company do not make use of these technologies, as the enabling grounds that may legitimise the use of these technologies may not be sufficient to make a fully lawful use of them.

References

1. ISO 31000 Risk management. In: ManagementMania.com [online]. Wilmington (DE) 2011-2023, 11/11/2016 [cit. 05/30/2023]. Available at: https://managementmania.com/en/iso-31000-risk-management
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.


AI

4. COLLABORATION IN EVENT SAFETY AND SECURITY RISK PREVENTION: CASE RUISROCK

Anja Aatsinki & Hanna Iisakkila Rojas / Laurea University of Applied Sciences, Finland / 2023

ABSTRACT

The purpose of this article is to demonstrate the process of collaboration in event safety and security. The best practice demonstrates the model used by South-West Finland´s authorities when collaborating with event organizers. The process follows the ISO 31000:2018 risk management process. Representatives of the Finnish police and the South-West Finland rescue authority have been consulted and interviewed for this article.

1. Introduction

Event safety and security are heavily legislated in Finland and for that reason planning in time is essential. The most important legislation related in basically every event in Finland includes the Assembly Act, the Rescue Act and the Land Use and Building Act. In every event the organizer is responsible for preventing and managing the risks and collaborating with various actors and authorities. The size and the risk profile of the event affect the requirements of the legislation but basically all events where the risks are considered substantial, an emergency plan is obligatory. The Government Decree on Rescue Services 407/2011 defines which events are considered as such.

This article focusses on event risk management at the Ruisrock summer festival held in Finland. Ruisrock is one of oldest festivals in Finland. It is held on Ruissalo island, which is part of the city of Turku (Ruisrock 2022a). Ruissalo is a unique site for events because its nature is heavily protected and the island location creates its own challenges for risk management. The island is connected to the mainland via one bridge. Ruisrock is a three-day festival and approximately 100,000 people visit the event during the weekend (Ruisrock 2022b). In this article the collaboration model between organizer and different authorities is presented.

2. Case

Planning annual big events like Ruisrock is usually continuous and planning for the next year's event starts right after the previous event is finished. The Finnish Assembly Act (530/1999) regulates that the event organizer needs to notify the police at least five days in advance of the event but in bigger events planning and consulting are practically constant all year round. In Finland The Rescue Act (379/2011) and The Government Decree on Rescue Services (407/2011) requires that all public events that have 200 or more persons present at the same time, draw up an emergency plan. Responsibility lies with the organizer.

Organizing the event also requires collaboration with other stakeholders like the performing artists with their organizations and different companies that offer services at the event. Planning is done in close collaboration with organizers, the event security provider, the police, rescue services and the health service provider. In this article the best practice presented is the model that describesorganizers collaboration with the South-West Finland authorities (Varsinais-Suomen

pelastuslaitos 2019). In this article this model is presented through the ISO 31000:2018 Risk-management framework (Figure 1).

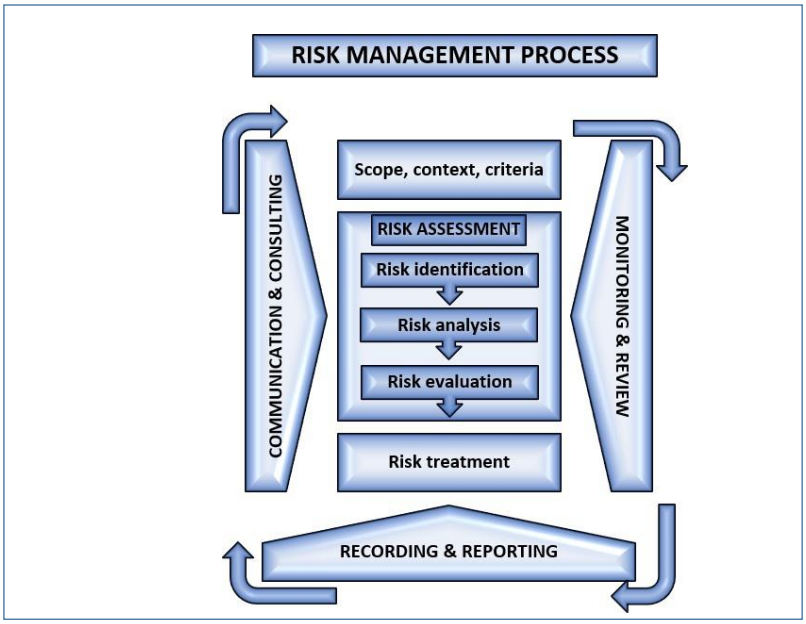


Figure 3. Risk management process (adapted from ISO 31000:2018)

3. Best practice

Communication and consultation

In order to have a safe and secure event, close and immediate multi-authority cooperation is essential, as well as continuous interaction with the event organizer. Due to cooperation with the authorities, expertise is available in a wide area of event safety, which is combined with up-to-date information and expertise with the organizer. Safety and security planning are started early enough by the event organizer. Continuous collaboration also requires and assures that concrete preparations for the event are made in time. For large events it is usually necessary for the event organizer to consult also other experts in safety and security, rather than doing everything by themselves. It is important to be able to recognize the areas where one's own expertise isn't sufficient. The authorities will advise on the basics, but the responsibility lies with the organizer. Besides supervision, authorities also provide information and guidance. Nevertheless, the legal responsibility lays with the event organizer. Therefore, the organizer must submit the rescue plan of the event to the regional rescue authorities no later than 14 days before the start of the event (Rescue Act 379/2011).

Functional safety and security measures are fundamental to successful events, so it is vital that the organizer is motivated and sensitive about a safety and security culture, even though that might mean investing more money or resources.

Scope, context, criteria

When the group for Ruisrock´s risk assessment is formed, the following aspects are considered when gathering enough expertise to cover the specific risks and features:

- The specific characteristics of the area (water, location on an island, heavy traffic, elevation differences, urban environment, public transport, etc.)

- The amount of people participating in the event (environmental maintenance, security stewarding, guidance, services, exits, etc.)
- The nature of the event (whether there are topics or performers that are politically or societally sensitive, people with disabilities, children, the elderly)
- Whether there are any special programs or equipment at the event that require special safety planning and expertise, the availability of the organizer/ resources of public authorities.

According to the Rescue Act (379/2011) the dangers and risks concerning the event need to be identified and assessed. All measures in the emergency plan must be based on this risk assessment. The event organizer must take care that all relevant legislation is taken into consideration.

Risk assessment

The first step in in the risk assessment process is drawing up the overall situational picture. It includes the structures, program, environmental management and placement, human resources, and all other essential factors. Identification of the risks is based on the specific features of the event and the lessons learned from previous years. Analysis of the risks is done by recognizing causes and consequences for each risk. After this, the analysis is used to evaluate the magnitude of risks. All key authorities affecting event safety must participate in this risk assessment, in the form of a joint meeting. The organizer presents the factors affecting the situational picture to the authorities, and together the severity of risks and the level of preparedness for them are considered. The organizer makes a preliminary emergency plan that can be discussed with the authorities.

Recognized causes and consequences are used to create event specific treatment measures. The event organizer needs to have a comparable and reliable criterion for assessing the magnitude of the risk. They should demonstrate that their risk management measures are risk-orientated and compliant with the legislation. Authorities evaluate whether the measures presented in the rescue plan are sufficient and they can ask the event organizer to enhance the event safety and security plan.

In addition, regarding the overall security of society at large, the authorities must then carry out an assessment of the risks posed by the event and how the authorities should prepare for identified risks that are not directly the responsibility of the event organizer. This preparedness may include increasing authorities´ resources, reserving additional spaces, ensuring the internal flow of information, and providing information etc. In addition to the event area, a mega-scale event has a wider impact on society, and the risk assessment generated by its impact is the responsibility of the authorities.

Risk treatment

The risk treatment is a combination of structural, technical and operational measures that are based on the risk assessment. Preventing crimes and other deliberate harmful acts is largely directed by legislation. Various laws regulate the powers of different actors, like security stewards, security guards and police. For example, the security checks and removal from the area and apprehension are regulated by law. In bigger events like Ruisrock multiple other plans must be drawn up beside a rescue plan and they are part of the risk treatment.

Monitoring and review

Monitoring in Ruisrock is done through an official inspection just before the start of the event. During the event onsite monitoring is done by both authorities and the security service provider.

Private security service and health service providers are also obliged to keep a logbook of the service events that help organizer to develop and plan the event for the future. After the event debriefing a session is held with the organizer. Information is also obtained from the media and other public sources. All this information and sources are helping to review and develop the Ruisrock festival.

The authorities always go over the most significant events together afterwards. Often, debriefing is also carried out together with the organizer. If criminal negligence by the organizers is suspected, the matter can be investigated by the police.

Recording and reporting

During all the phases authorities take notes, so that after a year, the shortcomings identified are considered at the planning stage. During the process there are multiple mandatory documents that must be made. These include for example:

- Fire inspection minutes
- Event logs
- Meeting minutes

A dynamic and continuously improving emergency plan also serves as a recording and reporting tool.

References

1. Assembly Act 530/1999. Accessed 10.2.2023. https://www.finlex.fi/fi/laki/kaannokset/1999/en19990530_20020824.pdf
2. Government Decree on Rescue Services 407/2011. Accessed 10.2.2023. https://www.finlex.fi/fi/laki/ajantasa/2011/20110407 (in Finnish)
3. Rescue Act 379/2011. Accessed 10.2.2023. https://www.finlex.fi/en/laki/kaannokset/2011/en20110379.pdf
4. Ruisrock. 2022a. Accecced 3.12.2022. https://ruisrock.fi/en/info/
5. Ruisrock. 2022b. Accessed 3.12.2022. https://ruisrock.fi/en/sold-out-ruisrock-makes-a-stellar-comeback-attracting-a-total-of-105-000-visitors/
6. Varsinais-Suomen pelastuslaitos 2019. Accessed 10.2.2022. https://www.vspelastus.fi/uutinen/2019-10-02_valtakunnallinen-turvallisuuspalkinto-varsinais-suomeen

5. HOW TO DEVELOP AND IMPLEMENT A SECURITY CULTURE IN YOUR ORGANIZATION

Kārlis Apalups / Turiba University, Latvia / 2023

ABSTRACT

The development of a security culture in an organization can be a challenge, but there are some steps for success that should be considered once a decision is made to develop a culture of security. Such a decision should come from the top management, since without such support no significant development of organizational culture can take place. Likewise, it is important to establish clear and consistent security policies to be followed as a standard throughout the organization. Once support and policies are set in place, the next step should be training your organization on the policies and best practices for security. In order to maintain an up-to-date security culture, there also need to be monitoring and measurement of the security culture and this may be achieved by setting in place specific metrics to measure the success of the security culture as well as establishing an ROI.

Link to ISO 31000

ISO 31000:2018 Risk management principles: Human and culture factors.

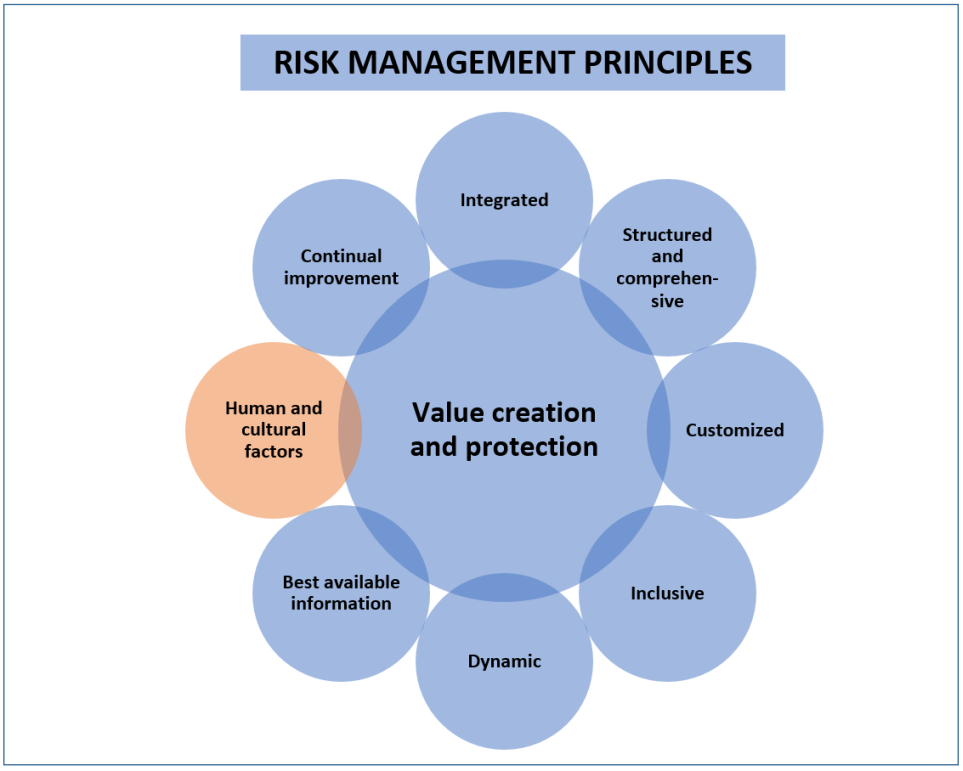


Figure 4. Risk management principles (adapted from ISO 31000:2018)

1. Introduction

Security culture is the set of ideas, customs and social behaviors that influence the security of an organization. It is the most important element in an organization's security strategy, as it affects how employees perceive and respond to security threats and incidents. A strong security culture can reduce risk and save money by preventing data breaches, complying with regulations, and protecting the reputation of the organization.

However, developing and implementing a security culture is not a simple task. It requires a strategic, long-term approach that involves top management support, clear and consistent security policies, effective awareness and training programmes, and continuous measurement and improvement. In this article, we will discuss some best practices for creating and maintaining a security culture in your organization. For the purpose of this article, we will be studying the case of “Latvijas finieris” which works in an international environment and has security as one of its core values.

2. Case

“Latvijas Finieris” is the leading plywood and its products' manufacturer in Baltic States and Finland. The company is also active in forest management, logging and the production of synthetic resins and phenol films.

In 2014 “Latvijas finieris” had a huge fire in one of Rīga-based factories. After this event, the holding company decided to implement a security culture and develop it. A part of its efforts was the creation of a Safety management service (SMS) that managed security risks in such areas as fire safety, occupational health and work safety, environmental protection and physical security. Before the fires there had been a high amount of work related accidents which had led to losses of working power, insurance costs and a decrease in feelings of safety among workers.

The efforts of SMS enabled developing a security culture that drastically lowered work related incidents, increased the ROI from security and safety investment and improved the overall organization culture.

3. Best practices

3.1. Get top management support. Obtaining the support of senior leaders is the first step in building a security culture. It is important that they communicate the significance and value of security and safety to all employees, allocate sufficient resources and budget for security initiatives, and hold themselves and others accountable for security performance. This support can also help create a positive tone at the top, where security is seen as a strategic priority and a shared responsibility, not just another budget expenditure.

3.2. Establish clear and consistent security policies. Security policy is like a standard for the organization. It’s the rules that define the expected behaviour and actions of employees regarding security. The policy should cover topics such as access control, password management, data protection, incident response and compliance requirements. Security policies should be aligned with the organization's goals and values, as well as with the relevant laws and regulations. They should also be written in simple and understandable language, communicated to all employees, and enforced consistently.

3.3. Provide effective awareness and training programmes. Awareness and training programmes are essential for educating employees about the security risks they face, the policies they need to follow, and the best practices they need to adopt. They should be tailored to the specific needs and roles of different groups of employees, such as IT staff, managers, or end users. Awareness and training programmes should be delivered regularly and updated frequently to keep up with the changing threat landscape.

3.4. Measure and improve security culture. Security culture is not a static state, but a dynamic process that needs to be monitored and evaluated over time (just like risk management). There are various tools and methods that can be used to measure security culture, such as questionnaires, surveys, interviews, or audits. These can help to assess the current state of security culture, identify strengths and weaknesses, and track progress and changes. Based on the results of these measurements, security culture can be improved by addressing gaps, reinforcing positive behaviours, rewarding good performance, or correcting bad habits.

3.5. **Get an ROI of security culture.** Security culture is not only a cost centre, but also a value driver for an organization. By developing and implementing a security culture, an organization can achieve various benefits such as:

- Reducing the likelihood and impact of security incidents
- Enhancing customer trust and loyalty
- Improving employee engagement and retention
- Increasing operational efficiency and productivity
- Complying with legal and regulatory obligations
- Gaining competitive advantage in the market

To quantify these benefits, an organization could use metrics such as:

- Number of security incidents prevented or detected
- Amount of money saved or recovered from security incidents
- Customer satisfaction or retention rate
- Employee satisfaction or turnover rate
- Time or resources saved or optimized by security measures
- Compliance status or audit results
- Market share or revenue growth

By measuring these metrics before and after implementing a security culture programme, an organization can calculate the return on investment (ROI) of its security culture efforts.

By following these best practices, an organization can build and maintain a strong security culture.

References

1. The Importance Of A Strong Security Culture And How To Build One – Forbes https://www.forbes.com/sites/forbesbusinesscouncil/2021/05/27/the-importance-of-a-strong-security-culture-and-how-to-build-one/
2. Building a Culture of Security - ISACA https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/building-a-culture-of-security
3. Developing a cyber security culture: Current practices and future directions - ScienceDirect https://www.sciencedirect.com/science/article/pii/S016740482100211X
4. https://www.finieris.com/en/home
5. https://www.tvnet.lv/4765017/latvijas-finiera-rupnica-liels-ugunsgreks

6. HYBRID THREATS AND SECURITY RISK MANAGEMENT

Prof. dr. Raimundas Kalesnykas / Kazimieras Simonavičius University, Lithuania/ 2023

ABSTRACT

Hybrid threats is one of the most complex challenges in security management systems faced by the European Union (EU) and its Member States, public sector organizations and busineses. States and their organizations are looking for innovative security solutions in order to quickly respond to and be resilient against threats such as cyber-attacks, irregular migration, cross-border crime, disinformation.

The case of instrumentalization of migrants organized by the Belarusian authorities at the EU's Eastern borders is presented in this article. It illustrates that organizations (state border security, private companies implementing security solutions) must establish a security risk management system based on the response mechanism regarding hybrid threats.

The risk management process requires an understanding of external and internal factors in order to assess risk in the field of border protection. Managing risks that pose a threat to border security includes risk identification, analysis and evaluation.

Link to ISO 31000

Establishing the context, defining the external and internal parameters for managing risk, risk assessment, legal and regulatory requirements.

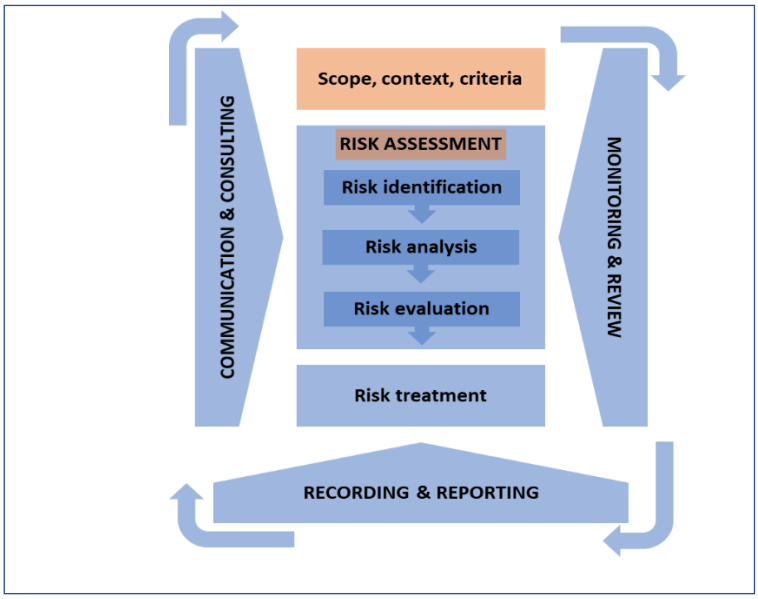


Figure 5. Risk management process (adapted from ISO 31000:2018)

1. Introduction

In recent years, the topic of *Hybrid Threats* has dominated the national security landscape in the EU. The state and institutions that take care of its security are looking for new security tools and technologies to address vulnerabilities across multiple domains. The concept of *Hybrid Threats* has been increasingly transformed from military context to public security realm.

The term *Hybrid Thre*at refers to an action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level. *Hybrid Threats* are characterized as: (a) coordinated and synchronized action that deliberately targets democratic states and institutions' systemic vulnerabilities through a wide range of means (e.g. hybrid attacks using people, technologies, false information), (b) activities that exploit the thresholds of detection and attribution, as well as various interaction points. This means that hybrid threats use tactics that make it difficult to identify and respond to them, often operating across different locations, organizations, or groups of people (e.g. in the context of internal and/or external security , local and or state security, national and/or international security). For example, imagine a scenario where a country uses cyberattacks to disrupt another nation's critical infrastructure, such as power grids. At the same time, they spread disinformation through social media to create confusion and panic among the population. This combination of cyber warfare and psychological manipulation makes it difficult for the targeted nation to respond effectively, as they are dealing with both physical disruptions and misinformation. This illustrates how hybrid threats can operate across different domains, complicating detection and response efforts.

Countering hybrid threats relates to national security and the maintenance of law and order. Efforts to respond to hybrid threats have to be underpinned by a capacity to detect early malicious hybrid activities, internal and external factors, and to understand the possible links between often seemingly unconnected events.

This first changed with the hybrid aggression by Belarus in mid-2021 through the creation of an artificial migration route to EU Eastern countries (Latvia, Lithuania, Poland) - which brought thousands of refugees at the EU's doorsteps, and posed EU/national security and border management challenges for years to come[1]. These may include a rise in human trafficking, especially women and children, an increase in smuggling of weapons and other illegal goods, as well as terrorism and radicalization.

When managing security risks stemming from hybrid threats, organizations (state or non-state) should establish an external and internal environment in which the organization seeks to achieve its security objectives. In this context, it is important to understand and determine external and internal parameters, which should be taken into account when managing risk: (a) social and cultural, political, legal, regulatory, financial, technological and economic environment, whether international, national, regional or local; (b) key drivers and trends having impact on the security objectives of the organization; (c) relationships with stakeholders; (d) governance, organizational structure, roles and accountabilities; (e) policies and the strategies that are in place to achieve security goals; (f) capabilities and knowledge (e.g. budget, people, processes, information systems and technologies), etc.

[1] Irregular border crossings to the EU increased significantly in 2022, as FRONTEX – the EU's border agency – noted a rise of 64% from the previous year estimating "around 330 000 irregular border crossings were detected at EU's external border, according to preliminary calculations. Last year, EU and Schengen associated countries faced unprecedented challenges at their external borders. These have ranged from the state-organized migration perpetrated by Belarus from 2021 onward to Russia's invasion of Ukraine in February 2022.

2. Case

From June 2021 onwards, the number of migrants seeking to cross from Belarus into the territory of neighbouring Latvia, Lithuania and Poland in an irregular manner increased dramatically. The Belarusian authorities contributed by organizing the transfer of refugees and immigrants from Iraq, Afghanistan, and other countries of the Middle East and Africa across the Belarusian-Lithuanian and Belarusian-Polish-Latvian border.

According to statistics, the number of unauthorized attempts to enter Poland stood at 3,500 in August, 7,700 in September and 17,300 in October 2021, and Polish border services recorded approximately 2 thousand attempts to cross the Polish-Belarusian border every month illegally (Statista, 2023).

In 2021, the number of people crossing the Lithuania-Belarus border increased more than thirtyfold compared to the previous year. Between 1 January 2021 and 31 January 2022, 4 150 irregular migrants (including 2 891 persons in July 2021 alone) were de facto detained in Lithuania (State Data, 2023). According to the Lithuanian Border Guard Service, 20,679 migrants were prevented from entering Lithuania between 3 August 2021 and 1 July 2023 (Lithuanian State Border Guard Service, 2023).

In Latvia, the number of persons detained for irregular border crossing was almost 15 times higher in 2021 (446 attempts) compared to 2020 (30 attempts), 10,394 instances of border-crossing deterrence (i.e. push-backs) were recorded from 2021 until 20 July 2023 (Latvia State Border Guard, 2023).

The majority of migrants were citizens from Middle Eastern and African countries (Iraq (Kurds and Yazidis, Iraqi Arabs) Syria, Iran, Afghanistan, Congo, Cameroon, Sri Lanka).

The Belarus–European Union border crisis was recognized as “hybrid attacks” by the Belarusian authorities resulting in increased pressures relating to migration and asylum at the Belarus border with Latvia, Lithuania and Poland (CoE Parliamentary Assembly Resolution 2404 (2021)). The migrant crisis was triggered by the severe deterioration in Belarus–EU relations, following the 2020 Belarusian presidential election, the 2020–2021 Belarusian protests, the Ryanair Flight 4978 incident and subsequent sanctions on Belarus. The “hybrid attacks” began around July 7 2021, when Belarus's President threatened to "flood" the EU with "drugs and migrants". Those who arrived in Belarus were then given instructions about how and where to trespass the EU border, and what to tell the border guards on the other side of the border.

Poland, Lithuania, and Latvia have described the migrant crisis as a “hybrid attack”, using migrants as weapons and calling the migrant crisis an incident of human trafficking of migrants, waged by Belarus against the EU. In the EU agenda, this phenomenon was named as “the instrumentalization of migration” - capacity to control irregular migratory flows (Rashe, 2022), and a response mechanism was initiated by 3 EU Eastern countries in order to establish a risk management system for external border security. Migration is increasingly framed as a security issue because immigrants are presumed to bring risks of terrorism, human trafficking, cross-border crime and illegal immigration (Dekkers et al., 2016). This situation indicates that contemporary security challenges are highly complex and inter-related, requiring more cross-sectoral, transdisciplinary and cross-country cooperation in all risk management phases both at the EU and Member States levels.

3. Best practices on EU external – Eastern borders' security management

3.1. Risk Analysis and Controls

External border security is affected by phenomena such as geopolitics, migration, cross-border crime, terrorism, and hybrid threats that are fluid and multidimensional in nature, thus requiring a flexible approach to their understanding, analysis and management.

Border Security Agencies within EU Member States are using Common Integrated Risk Analysis Model (CIRAM)[2], which focusses on the security threat dimension. The analysis of different risk categories provides a comprehensive picture of challenges and threats that jeopardize the security and functioning of the EU's external borders. Risks are grouped into three broad categories: irregular migration (clandestine entry, document fraud), , secondary movements and returns, and cross-border crime (smuggling of illicit drugs, firearms smuggling, detection of stolen vehicles and vehicle parts, tobacco smuggling, trafficking in human beings).

Security Risk Management is the ongoing process of identifying these border security risks and implementing plans to address them. *Risk Analysis* refers to the systematic examination of components of risks to inform decision-making. For the management of the security of external borders, *risk* is defined as the magnitude and likelihood of a threat occurring at the external borders, given the measures in place at the national borders and within the EU, which will affect the EU internal security and national security of Member States.

Risk in the context of the management of the security of external borders can be viewed as having 3 components: (1) the threat that will be assessed in terms of magnitude and likelihood; (2) the vulnerability to the threat – in other words the level and efficiency of response to the threat; and (3) the impact – should the threat on the EU internal and/or Member States' national security materialize, or on the security of the external borders, as well as the bearing on the efficient management of bona fide border crossing. In the practice of security risk management, magnitude refers to the size or severity of a threat (e.g. a large-scale cyberattack could have a high magnitude), and impact is the effect or consequence of that threat if it occurs (e.g. a high-magnitude threat typically leads to a more significant impact, such as financial loss, or loss of life. In essence, the greater the magnitude of a threat, the more substantial the potential impact it can have on security. Both magnitude and impact are interconnected for assessing risks effectively.

Risks are identified and assessed, in view of their level of threat, vulnerability and impact, and then communicated to the decision-makers. While the analysts are responsible for identifying and assessing the threat, decision-makers are responsible, within the remit of their decision-making capacities, for managing the risks. Risk analysis implies a reference period – a day, a week, a month or a year – consistent with the level of decision-making it is intended to inform.

[2] Common Integrated Risk Analysis Model (CIRAM) developed by FRONTEX, the European Border and Coast Guard Agency. The purpose of the CIRAM is to establish a clear and transparent methodology for risk analysis in order to facilitate efficient information exchange and cooperation in the field of border security. See: Common Integrated Risk Analysis Model (CIRAM): summary booklet, Version 2.1 (2021), FRONTEX - European Border and Coast Guard Agency, https://prd.frontex.europa.eu/document/common-integrated-risk-analysis-model-2-1/

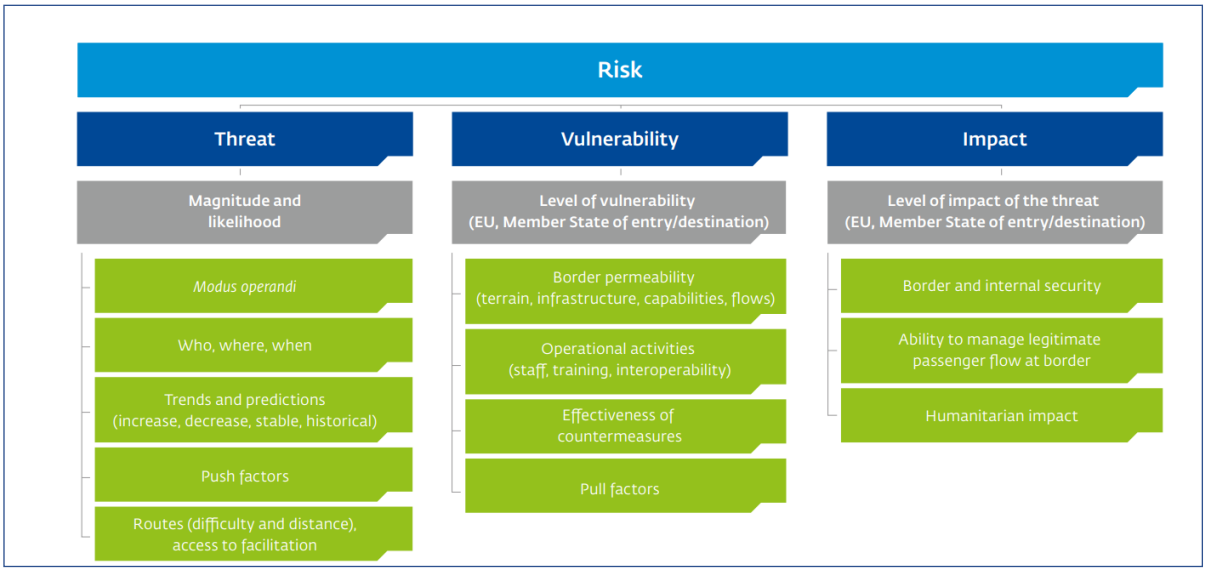


Figure 6. Scheme for the Risk Analysis using CIRAM tool[3]

Example of Controls. Risk analysts of national border security agencies communicate risks to the Management Board, so that it can take informed decisions about annual budget allocation regarding a variety of risks. Risk analysts at border crossing point (BCP) level communicate operational risks to the head of the BCP, so that he or she can take informed decisions when allocating staff for controls and surveillance. Risk analysts should state that the threat of illegal border-crossing between BCP X and BCP Y is very likely, given evidence from the past and intelligence currently available, whereas it is unlikely between BCP Y and BCP Z. This information enables decision-makers to allocate resources as well as to the area between BCP X and BCP Y as a priority.

National integrated border surveillance systems driven by risk analysis should have a stable capacity (organizational, administrative and technical) and in a continuous state of alert. This is necessary to prevent and detect unauthorized border crossings, to apprehend persons who have crossed the border illegally and to ensure that such persons are subject to coherent and comprehensive referral procedures (i.e. screening procedures) that respect their fundamental rights, to intercept transportation means, such as vessels, used for illegal border crossing, to counter cross-border crime, such as smuggling, human trafficking and terrorism, as well as to respond to threats of a hybrid nature.

3.2. Response to Hybrid Threats

3.2.1. Operational support by EU agencies

In the peak of irregular migration influx (July 2021), the Lithuanian Government requested support from specialized EU agencies – FRONTEX (European Border and Coast Guard Agency) and the EUAA (EU Agency for Asylum). FRONTEX and EUAA in dealing with irregular migrants related problems are aimed at preventing the flow of irregular migrants through Lithuania to Western EU countries.

FRONTEX quickly launched a Rapid Border Intervention in order to bring immediate assistance to an EU Member State that is under urgent and exceptional pressure at its external border, especially related to large numbers of non-EU nationals trying to enter its territory illegally. During the Rapid Border Intervention, FRONTEX deployed about 120 officers, 36 patrol cars and 2 helicopters to conduct border surveillance and control activities in support of the Lithuanian State Border Guard Service

[3] Common Integrated Risk Analysis Model (CIRAM): summary booklet, Version 2.0 (2013), FRONTEX - European Border and Coast Guard Agency, https://frontex.europa.eu/what-we-do/monitoring-and-risk-analysis/ciram/

(SGBS). FRONTEX officers also assisted in data gathering on irregular border crossings and exchange of operational information.

The EUAA has been providing operational support and deployed 73 personnel working in the areas of registration and processing of asylum applications – including by conducting interviews and drafting opinions – and enhancing the capacity to manage the reception of applicants. Also, the Lithuanian State Border Guard Service (SBGS) received support to enhance management of the first line reception, in particular onsite management, communication, information provision, as well as assistance in expanding reception capacities.

3.2.2. Physical Barrier

By implementing the Law on Installation of a Physical Barrier (2021), the Lithuanian Government approved the installation of a physical barrier at the end of August in 2021, after the Belarusian regime launched a hybrid attack against Lithuania, resulting in an influx of illegal migrants into the country. The physical barrier is being installed in accordance with the requirements of the State Border Guard Service (SBGS) – a concertina prism was installed on the national border, and fence segments topped with concertina spiral coil are being built next to it. The total height of the fence with the concertina is approximately 4 meters above ground. During the construction of the physical barrier, 530 kilometers of new fence segments were installed, and 357 kilometers of concertina prism were built. The total length of the Lithuanian border with Belarus is 679 kilometers. More than 100 kilometers of the national border runs along the banks of rivers and lakes, where there are no plans to install physical barriers.

3.2.3. Automated state border surveillance system

In order to maximize a state border protection, it is essential to ensure that the entire section of the border with Belarus is monitored using the latest technologies. Lithuania has installed the automated state border monitoring system, equipped with CCTV cameras and motion detectors, on a 640 km stretch and will monitor 100% of the state borders with Belarus. Also, the Lithuanian State Border Guard Service uses drones, reconnaissance aircraft, offshore sensors and satellite remote sensing to track illegal migration.

3.2.4. Refuse entry

In early July 2021, the Lithuanian Parliament declared that the country is in a state-level emergency due to a massive influx of migrants. The Lithuanian Parliament adopted amendments to the Law on the State Border and Protection (25 April 2023), legalizing the turning away of irregular migrants at the border under a state-level extreme situation regime or a state of emergency.

The amendments to the Law on the State Border and Protection (2023) introduce a possibility to refuse entry to Lithuania during a state-level extreme situation, and due to an influx of foreigners; also to those foreign nationals who intend to cross or have crossed the state border at places that are not designated for that purpose or at places designated for that purpose but having violated the procedure for crossing the state border. The officers of the Lithuanian State Border Guard Service (SBGS) have the right to turn away irregular migrants only along the border – up to 5 km inland.

The provision on turning away migrants applied individually to each foreigner and would not apply in certain cases to ensure entry or humanitarian access to Lithuania's territory for foreigners fleeing military aggression or persecution. An assessment of the need for assistance was carried out for foreigners who had not been allowed to enter. If found to be in need, migrants would have to be provided with necessary urgent medical or other assistance.

The amendments to the Law on the State Border and Protection (2023) make a clear distinction between natural migration and the instrumentalized migration facilitated by the Belarusian regime and that the legislation is necessary to safeguard Lithuania's national security interests.

3.3. Legal Framework for Risk Management of Border Security

In October 2021, the European Council invited the Commission to propose any necessary changes to the EU's legal framework to respond to the state-sponsored instrumentalization of people at the EU's external border with Belarus. Article 78(3) of the Treaty on the Functioning of the European Union (TFEU) provides for the adoption of provisional measures in emergency migratory situations at the EU's external borders. The objective of the proposal is to support Latvia, Lithuania and Poland by providing for the measures and operational support necessary to manage in a humane, orderly and dignified manner, fully respectful of fundamental rights, the arrival of persons being instrumentalized by Belarus.

The main features of the emergency migration and asylum management procedure at the EU external borders (Lithuania, Latvia, and Poland) are:

- possibility for the Member States concerned to register an asylum application and offer the possibility for its effective lodging only at specific registration points located at the vicinity of the border including the border crossing points designated for that purpose
- registration deadline for applications for international protection extended to up to four weeks
- possibility to apply the accelerated procedure at the border for all applications, and thus limiting the possibility for Belarus to target for instrumentalization third-country nationals to whom the border procedure cannot be applied
- return procedure at the external borders
- material reception conditions –to cover only basic needs. Latvia, Lithuania and Poland need to ensure that any actions respect basic humanitarian guarantees, such as providing third-country nationals on their territory with food, water, clothing, adequate medical care, assistance to vulnerable persons and temporary shelter

The European Commission's proposal is in line with the comprehensive approach set out in the New Pact on Migration and Asylum. The Pact is designed to establish a common approach to migration and asylum that is based on solidarity, responsibility, and respect for human rights. The Pact has delivered various outcomes, e.g. determined an EU mechanism for preparedness and management of crises related to migration, developed an early warning and forecasting system allowing prompt identification of migration situations, enabling effective preparedness and response, addressed situations of crisis and force majeure in the field of migration and asylum, established the EU integrated border management system – a coordinated framework ranging from border surveillance to anti-smuggling and to returns of migrants.

The European Commission's forthcoming proposals to reform the Schengen Borders Code will include strengthening the EU's legal framework to give better tools to Member States to protect the external borders in situations of instrumentalization of migrants, while ensuring full respect for fundamental rights. They will also contain measures that will help those Member States who see unauthorized movements of migrants including the repercussions of instrumentalization far away from the external border.

The European Commission's proposal is the latest in a series of coordinated EU actions that include: targeted measures for transport operators that facilitate or engage in smuggling; diplomatic and external action; stepping up humanitarian assistance and support for border security and migration management.

References

1. Amendments to the Law on the State Border and Protection, adopted by the Parliament of the Republic of Lithuania, 25 April 2023, No. XIV-1891, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/ff701250e35a11eda305cb3bdf2af4d8?jfwid=fwi8z9chx
2. Blažytė, G. et al. (2022). Comparative report on the influx of irregular migrants across the Belarus border: the response by the Governments of Lithuania and Latvia. *Diversity Development Group and PROVIDUS Center for Public Policy*, https://ec.europa.eu/migrant-integration/library-document/niem-comparative-report-influx-irregular-migrants-across-belarus-border_en
3. Building walls, restricting rights: Lithuania's response to the EU-Belarus border 'crisis', *Statewatch, 1 February 2022,* https://www.statewatch.org/analyses/2022/building-walls-restricting-rights-lithuania-s-response-to-the-eu-belarus-border-crisis/
4. Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a New Pact on Migration and Asylum (COM/2020/609 final), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0609
5. Communication from the European Commission to the European Parliament the Council on Establishing the multiannual strategic policy for European integrated border management (COM(2023) 146 final), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023DC0146
6. Dekker R., et al. (2016). The use of online media in migration networks. *Population, Space and Place, 22, 539–551.*
7. Evans, J. (2021). "Belarus dictator threatens to 'flood EU with drugs and migrants'". *The Week, 28 May 2021,* https://www.theweek.co.uk/news/world-news/europe/952979/belarus-dictator-threatens-flood-eu-with-drugs-migrants-avoid-sanctions
8. FRONTEX - European Border and Coast Guard Agency: Risk Analysis for 2022/2023 (2022), https://frontex.europa.eu/publications/risk-analysis-for-2022-2023-RfJIVQ
9. Giannopoulos, G. et al. (2021). The Landscape of Hybrid Threats: A conceptual model. *Publications Office of the European Union, Luxembourg.*
10. Hybrid Threats as a Concept. *The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE),* https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/
11. Joint Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Responding to state-sponsored instrumentalization of migrants at the EU external border (JOIN(2021) 32 final), https://commission.europa.eu/document/4d0c173e-709f-4832-b12f-31792cd10bff_lt
12. Joint Communication from the European Commission to the European Parliament and the Council on Joint Framework on countering hybrid threats - a European Union response (JOIN/2016/018 final), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018
13. Latvia State Border Guard. Statistics at the state border and within the country (from 1 August 2021 to 1 July 2023), https://www.rs.gov.lv/en
14. Law on Installation of a Physical Barrier in the territory of the Republic of Lithuania near the External Border of the European Union with the Republic of Belarus, adopted by the Parliament of the Republic of Lithuania, 10 August 2021, No. XIV-513, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/4763ca32fa7211ebb4af84e751d2e0c9?positionInSearchResults=1&searchModelUUID=e617cf00-5855-4e3f-afc8-d9021687a307
15. Lithuanian State Data Management IS. Monitoring of illegal migration (from 01.01.2011) & Registered illegal migrants, https://ls-ospsdg.maps.arcgis.com/apps/dashboards/9b0a008b1fff41a88c5efcc61a876be2
16. Parliamentary Assembly of the Council of the Europe Resolution 2404 (2021) “Instrumentalised migration pressure on the borders of Latvia, Lithuania and Poland with Belarus”, https://pace.coe.int/en/files/29537/html

17. Rashe, L. (2022). The instrumentalization of migration – how should the EU respond? *Jacques Delors Centre, Hertie School, Germany,* https://www.delorscentre.eu/en/publications/the-instrumentalisation-of-migration
18. Sari, A. (2023). Instrumentalized migration and the Belarus crisis: Strategies of legal coercion. *The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)*
19. Statista. Number of attempts to illegally cross the Polish-Belarusian border in Poland from August 2021 to June 2023, https://www.statista.com/statistics/1271292/poland-attempts-of-illegal-crossing-of-the-polish-belarusian-border/
20. The European Commission's proposal for a Council Decision on Provisional emergency measures for the benefit of Latvia, Lithuania and Poland (COM/2021/752 final), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A752%3AFIN&qid=1638547296962

7. PREVENTION OF SEXUAL VIOLENCE IN A NIGHTCLUB

Elisabet Garcia Rull / School of Prevention and Integral Safety and Security, Spain / 2023

ABSTRACT

Risk assessment in relation to prohibited acts of a sexual nature, such as sexual harassment, sexual aggression and rape in crowds and at large events such as at nightclubs or music festivals, involves not only private security but also public authorities. This article examines best practices for improving safety and minimising sexual violence in a nightclub. It is relevant to adapt the risk assessment process according to ISO 31000 to the specific law applied. The article is based on the protocols regarding "WE WON'T KEEP QUIET" and the "Security protocol against sexual violence in leisure spaces" of the Government in Catalunya.

Link to ISO 31000

ISO 31000:2018 processes: Scope, context, criteria, risk analysis, risk assessment and risk treatment.

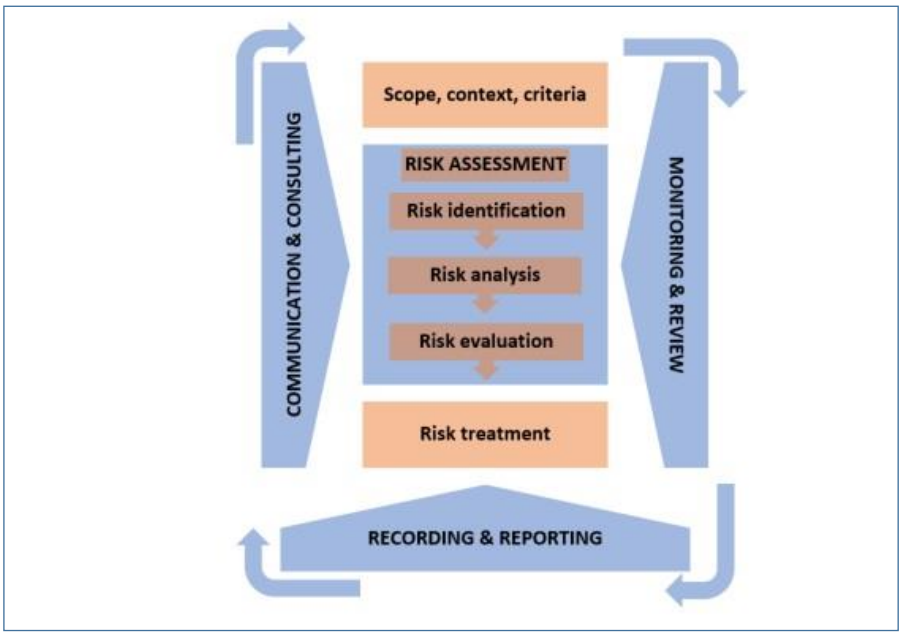


Figure no. 7. Risk management process (adapted from ISO 31000:2018)

1. Introduction

Nightclubs, festivals and other large gatherings where alcohol and drug use are common have been statistically shown to be places where prohibited sexual activities such as harassment, sexual aggression and rape occur. In recent years there have also been cases of chemical submission. The World Health Organization (WHO) defines sexual violence as: “Any sexual act, attempt to obtain a sexual act, unwanted sexual comments or advances, or acts to traffic or otherwise directed against a person’s sexuality using coercion, by any person regardless of their relationship to the victim, in any setting, including but not limited to home and work” (World Health Organization [WHO], 2010).

In a high percentage of cases, the alleged victim is a woman, and the alleged perpetrator is a man. A gender perspective is therefore essential. The immediate, rapid, and efficient action of the organisation can be crucial for the criminal justice process in order to quickly locate the alleged perpetrator.

Prevention is essential in order to protect the individuals who support the event, to avoid reputational and economic damage to the company/organisation, and to avoid criminal, administrative and civil liability for the company/organisation.

The Prevention Protocol will apply to all types of acts related to sexual violence, whether or not they are criminal offences.

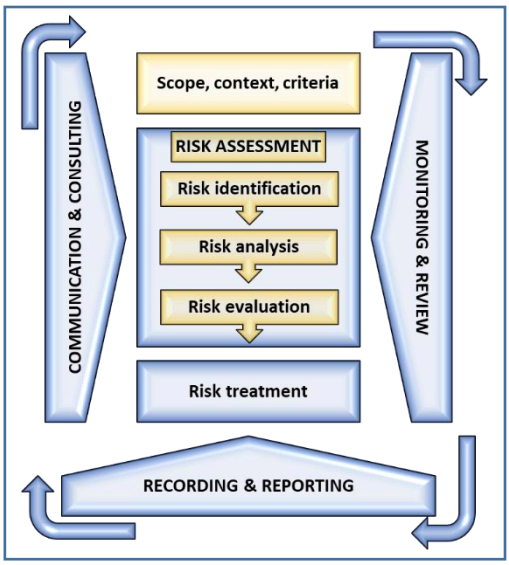
2. Case

A local nightclub company, located in a town in the province of Barcelona, requests a general risk assessment regarding prohibited acts of a sexual nature, such as harassment, sexual abuse/aggression, etc. In their direct experience, such prohibited acts have recently increased, especially in the nightclub's toilets, and they now have a bad reputation in the media and are facing the opening of administrative proceedings against the nightclub. As a direct result, the nightclub has lost female customers, which has had a negative economic impact. The company has a policy of free entry for women and paid entry for men. The general age of the company's customers is between 18 and 25 years. The club is generally open every Friday and Saturday between 00.00 and 6.00.

The nightclub requests a specialist to carry out an integral assessment where the assailants are men in order to decrease the prohibited acts in its space and to improve its public image.

3. Best practices

SCOPE, CONTEXT, CRITERIA AND RISK ASSESSMENT



Good practice includes prevention and giving an efficient and effective response in cases of crimes against sexual freedom, which will also be crucial in preventing unwanted events in the future.

For prevention, the **context** is a nightclub with young attendees under 25. The attendees may be under the influence of alcohol and drugs.

Social-human origin. The person directly affected is an individual or a group. The assets affected are the health/life, emotional health of the clients on the one hand, and the finances and reputation of the company on the other. The origin of the risk cannot be predicted because the studies show that many factors are involved.

Depending on the **risk identification**, some of the aspects could be a list of previous cases. The company should contact the authorities to gather information and check records. Based on the information, the specialist will try to profile the victim/offender and check whether drugs and alcohol increase the likelihood of the risk. The lack of gender equality policies may also be an aspect to consider.

The information gathered can be used to study the possibilities, especially if there are certain areas where there are more cases, such as the toilets. Therefore, it is relevant to check if there are opportunities created by the various spaces of the nightclub or “black spots”. The specialist will notice that in the toilets there is a lack of cameras so as to respect the privacy of the attendees and that this can create opportunities for the perpetrators.

RISK ANALYSIS AND EVALUATION

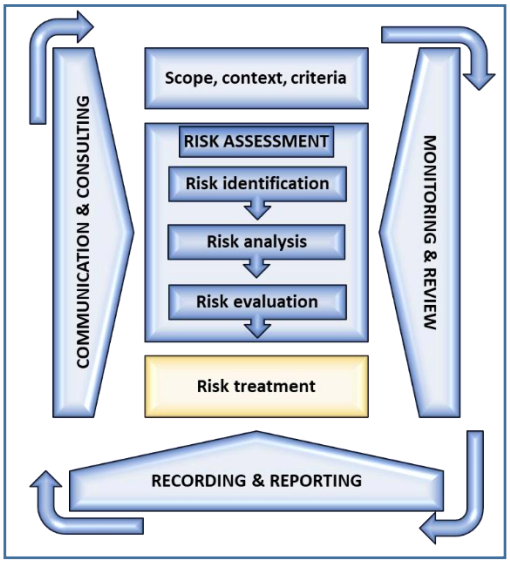
The **risk analysis** will result in a probability of the unwanted event happening, the nature and magnitude of the consequence, whether or not there is effectiveness of the pre-existent controls, and also what the level of sensibility and trust is.

Subsequently, the purpose of the **risk evaluation** is to reduce the unwanted acts in the nightclub as much as possible.

The basis on which risk management will operate are the laws and protocols of the region in which the nightclub is located. In this case. The main ones are the Spanish Constitution, the Statute of Autonomy of Catalonia, the Organic Law 10/2022, of 6 September, on the Comprehensive Guarantee of Sexual Freedom, the Law 5/2014, of 4 April, on Private Security, the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), the "Security Protocol against Sexual Violence in Leisure Spaces".

The applicable law changes in each country, except for the General Data Protection Regulation. The student must study the specific legislation applicable to his/her country.

RISK TREATMENT



After the risk assessment, the next step is the **risk treatment**:

PREVENTIVE ACTIONS

In order to minimize the risk, the nightclub needs to:

Safe space

Make the toilets a safer place by making the necessary architectonic changes and installing cameras that can easily identify people going in and out of the toilets.

Avoid having areas which put users in a situation of danger because they are dark or hidden. And if those are necessary, use video-security.

There should be clear wall posters with information about the video-security and the surveillance vigilance, in accordance with the applicable Laws and as a dissuasive method.

Create new policies from a gender respectful perspective.

Towards the users:

- Entrance policies: charging men and women the same entrance fee, no gender discriminatory attitude towards the clothing or look of the users and denying access to anyone who sexually harasses or assaults while waiting to enter in the nightclub.
- Prohibiting activities that promote or encourage gender or sexual diversity discrimination.

Respectful and non-discriminating dress code for staff.

Creating a point of contact, such as a purple space in the club to report any act of sexual violence, providing a WhatsApp telephone number and an email address that users can use to report situations of sexual violence. There should be wall posters with this information.

Every night there should be a **specific assistance person** in the nightclub in charge of prevention, detection and response to sexual violence acts, but it is a general responsibility of all the staff.

Control of alcohol and drugs. The nightclub can refuse alcoholic beverages to a user who is at a high alcoholic or drugs level.

Appropriate specific training for nightclub staff, especially security staff, to equip them with the skills to prevent, detect and respond to any case of sexual violence and to coordinate with the police.

There will also be **information posters on the wall explaining some of the club's policies**, specifically the purple space, and the cameras installed, as well as the total rejection of any kind of sexual violence in the nightclub.

REACTIVE AND INTERVENING MEASURES

Prevention is linked to the correct detection and response in the event of an incident, as the nightclub demonstrates its policy of not accepting prohibited acts on its premises and creates a deterrent effect which has a positive impact on its image. Good practice in response and intervention is essential to avoid secondary victimisation.

The staff will find possible witnesses to the facts and write down the specific time period to check the images recorded by the surveillance cameras.

The nightclub will have 2 separate secure areas.

Vis-à-vis the alleged victim:

- A member of staff will meet the alleged victim, offer them a safe place to wait and ask if they have a safe contact person to accompany them.
- The member of staff in charge of the matter shall provide the alleged victim with written information about her/his rights handing him/her an already prepared information leaflet.
- The staff member shall collect all information related to the facts of the case that the victim may verbalise.
- The staff member will contact the police and medical services, respecting the victim's willingness to report or not to report the facts that have occurred. If the person is not fit to verbalise his/her wishes, contact the police and medical services. At the same time, it is important for the member of staff to go to a medical centre as soon as possible to receive emotional support for any harm caused by the assault and to record any evidence of it.

Towards the suspected perpetrator:

- The private security guards of the nightclub will identify the suspected perpetrator(s), gather information and keep him/her in a secure area until the police arrive to decide if the reported act might be a criminal offence, respecting his/her presumption of innocence. If there is more than one person involved, the private security guards will try to keep them apart.

The private security guards will make sure the alleged victim and the suspected perpetrator won’t see each other until the police arrives.

The details of victims and alleged perpetrators will be kept confidential by the nightclub staff.

There will be regular coordination meetings between the nightclub manager, the town hall and the local police. At least once a year, statistics will be analysed in order to improve and adapt the protocol.

The effectiveness of the risk management process should be continuously monitored with new accurate data, and the prevention protocol must be reviewed at least once a year.

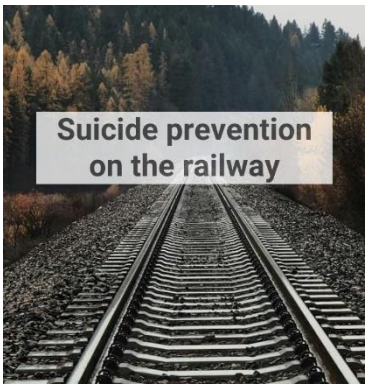
References

1. Barcelona Hall Town. Protocol “We won’t keep quiet” campaign against sexual assault and harassment in private night-time leisure venues. Last accessed 24.7.2023 https://ajuntament.barcelona.cat/dones/sites/default/files/documents/protocol_oci_nocturn_eng_0.pdf
2. Government of Catalonia. Department of Interior. Security Protocol against sexual violence in leisure spaces. Accessed 12.7.2023 file:///C:/Users/1319529/Documents/SECUREU_Juliol%202023/PROTOCOL%20GENCAT.pdf
3. Law 5/2014, of the 4th of Abril, of Private Security. State official newsletter 83 of 5.4.2014, 28975 to 29024
4. Organic Law 10/1995, of the 23th of November, Criminal Spanish Code. State official newsletter 281, of 24.11.1995, 33987 to 34058 https://www.boe.es/eli/es/lo/1995/11/23/10/con
5. Organic Law 6/2006, of the 19th of July, Autonomy Statute of Catalonia. State official newsletter 172 of 20.07.2006, 27269 a 27310 https://www.boe.es/eli/es/lo/2006/07/19/6/con
6. Organic Law 10/2022, of the 6th of September, on the comprehensive guarantee of sexual freedom. State official newsletter 215, of 7.9.2022, 124199 to 124269 https://www.boe.es/eli/es/lo/2022/09/06/10/con
7. Quigga, Z. Biglanda, C. Hughes, K., Duchc, M., Juan M. Sexual violence and nightlife: A systematic literature review. Aggression and Violent Behavior. Volume 51, March–April 2020, 101363
8. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data
9. Spanish Constitution. State official newsletter 311 of 29.12.1978, 29313-29424. https://www.boe.es/buscar/doc.php?id=BOE-A-1978-31229; https://www.boe.es/eli/es/l/2014/04/04/5/con
10. WHO. Understanding and addressing violence against women. Accessed 24.7.2023 https://apps.who.int/iris/handle/10665/77432
11. WHO. Preventing violence against women. Accessed 21.7.2023 https://www.who.int/news-room/fact-sheets/detail/violence-against-women

8. SUICIDE PREVENTION ON THE RAILWAY

Elisabet Garcia Rull / School of Prevention and Integral Safety and Security / 2024

Abstract



Suicide is defined as death caused by harming oneself with the intention of dying. One in 100 deaths is by suicide, according to the WHO. Suicides are recognized as a major public health problem. "More than 700,000 people die by suicide each year. Furthermore, for each suicide there are more than 20 suicide attempts" according to the WHO. Suicides are preventable. Moreover, often occur in railways across Europe causing transportation concerns, as well. Therefore, the prevention of suicides must focus on suicides that occur in railways, and this requires an effort from all private and public organizations and institutions involved. We will apply the guidelines of the WHO, experts and the ISO 31000 to create a general prevention guide as a basis for generating safety risk management in this area.

1. Introduction

"Among young people aged 15-29, suicide was the fourth leading cause of death after road traffic injuries, tuberculosis and interpersonal violence. In Catalonia, there has been a decrease in the average age at first episode of suicidal behavior.

According to the WHO, more than twice as many men as women die by suicide.

For decades, suicide was silenced by institutions and the media. Today, however, suicide is recognized as a **public and global health problem**. Most importantly, the WHO and experts recognize that these deaths are preventable.

Many suicide attempts and effective suicides take place on railways throughout Europe and the world.

Despite this, there is a great lack of data on suicide attempts on Spanish railways and there are no statistics at all.

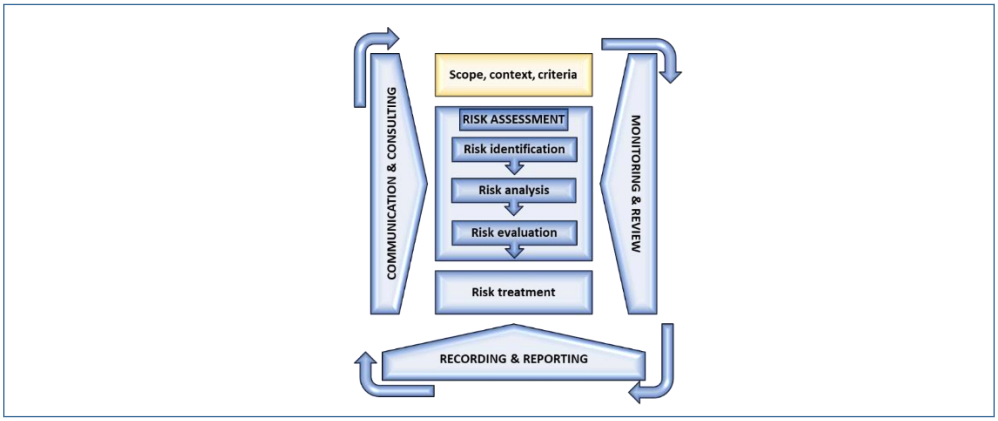


Figure no. 8. Risk management process (adapted from ISO 31000:2018), Scope, Context, criteria.

2. Case

The causes of suicide are many and often related to mental health problems, but remain unclear as a whole. The risk factors are classified in systemic and social, community, relational factors and individuals.

Risk factors include mental disorders, especially depression; personality disorders; addictive behaviours; exposure to family violence, including physical or sexual abuse; social dislocation or loneliness; recent release from prison or jail; stressful life events and chronic pain; direct or indirect exposure to the suicidal behavior of others; and previous suicide attempts.

Suicide has continued to be socially stigmatized. The exact number of suicides on the railways is unclear due to lack of statistics, but that type of suicide does exist.

The consequences are multiple and very varied:

- The loss of a person
- Serious injuries in the attempt
- The suicide leaves the loved ones of the suicide victim with difficult grief.
- Trauma to those who witness the event and all those who are directly or indirectly involved in a suicide can suffer trauma: from the train driver to the dispatcher and the staff involved in maintenance and cleaning up after the event.

Economically, suicides are also negative for the state: the dead person doesn't work anymore; the costs of burial and funeral can be covered by the state; possible liability of public authorities; those close to the suicide may need medical help and leave from work; if the person was the breadwinner, the state will also have to offer economic help to the family, such as orphan's pensions; the workers involved may also suffer and need medical help and even leave from work.

When the suicide is committed on the railways, it produces delays and some workers may need psychological support, leaves, and even job changes after such events.

It is therefore a must to prevent suicides, both for human rights reasons relating to life and health, and for economic reasons.

3. Best practices

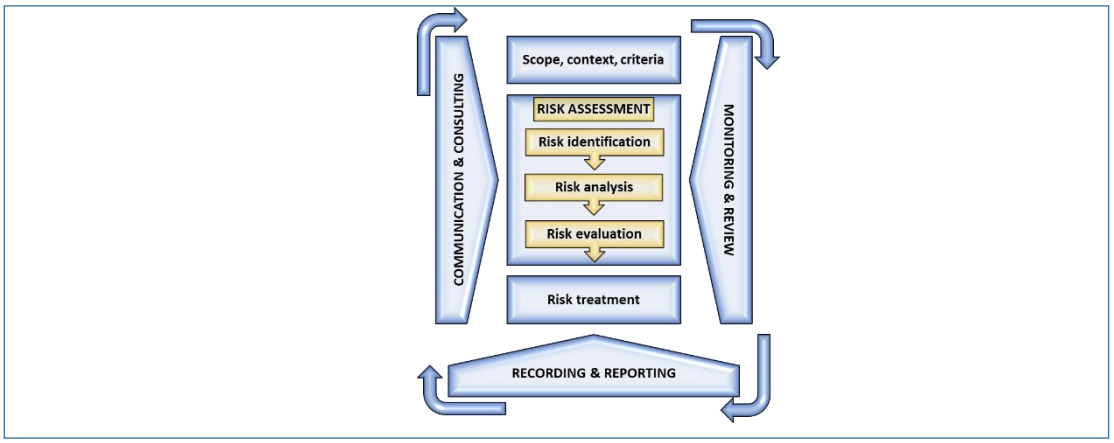


Figure no. 9. Risk management process (adapted from ISO 31000:2018), Risk assessment.

The foundation of the WHO are situation analysis, multisectoral collaboration, awareness raising, capacity building, financing and, as well, surveillance, monitoring and evaluation.

RISK ASSESSMENT

Risk assessment participants:

- Operational director of the organization
- Future staff member involved in the Suicides Prevention programme of the organization
- Media officer of the organization
- Train drivers' representative
- Train dispatchers' representative
- People who have attempted suicide on the railways
- Specialist psychiatrist

The views of people who have actual experience of trying to commit suicide on the railways, also called survivors or suicide loss survivors, will be heard, and valued to design the prevention plan.

RISK ANALYSIS, EVALUATION, AND TREATMENT

Impossibility of access to the means of suicide (the railways) decreases the number of suicides.

IDENTFY THE RISK

Risk assessment includes identifying the risk:

From a psychosocial approach:

- Where a person is more likely to commit suicide
- Who is more likely to commit suicide, to find out about the "who", whether there are more men than women, whether there is an age pattern,
- Whether the suicidal person has been under the influence of drugs
- Whether there have been previous suicide attempts.
- When it is more likely to happen, whether there are certain months/dates of the year with more suicides
- To identify the previous behavior of people who are about to commit suicide and whether they can be divided into 2 groups: those who go straight to the point of action and those who spend time and hesitate before the attempt.

From a technical approach:

- Where suicides and suicide attempts occur: to identify where the suicides and attempted suicides have been occurring and where there is a high likelihood of it happening. It will be very different for the metro than for the trains. The risk control is to identify which are the black points such as stations near hospitals, and which are the places where a person can commit suicide and where the investigation will come from.
- By observing the places where a person might commit suicide. New technologies such as drones can be very useful.

The organization should gather the information from the participants, their data records and video-surveillance, working jointly with public authorities. There will be a system to guarantee the anonymity of the people who have committed suicide.

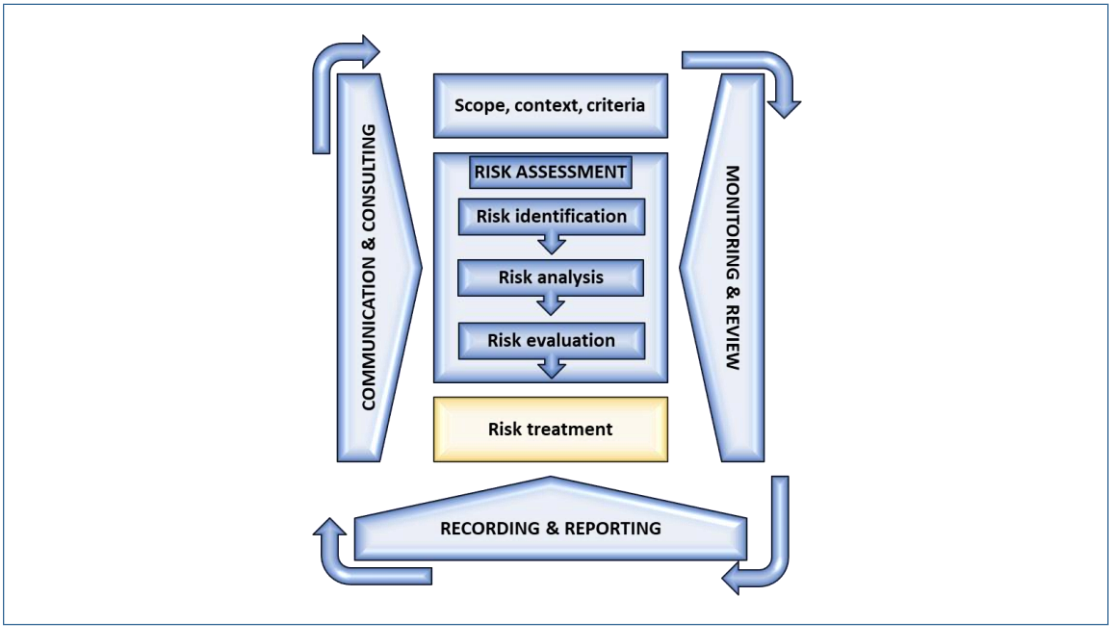


Figure no. 10. Risk management process (adapted from ISO 31000:2018), Risk treatment.

TECHNICAL APPROACH PREVENTION

A. DISCOURAGING OF TRESPASSING

a) Adequate lighting, decoration and spaces with music and social activity in all stations
b) Use of lighting to dissuade entry to the track.

B. PREVENTING SUICIDE IMPACTS

<u>Means of preventing access to the tracks</u>

a) Physical barriers: once these have been analyzed, the organization needs to consider whether there are physical barriers to prevent the person from attempting suicide or methods to minimize the risk. If there are physical barriers, are they effective? If not, are these places easily accessible to the citizens? If it is possible to add/improve the physical barriers, the organization should do so. If this is not possible, for example because the area is too large, the organization will need to prevent access by other means, such as:
b) Partial physical barriers as a minimum to be installed at all stations on railway lines that have high-speed trains passing by
c) Vegetation
d) People detectors

e) Monitoring of track trespassing

C. PREVENTING SUICIDE INJURIES

a) Installing of anti-suicide pits in the new train stations and, according to the budget, installing these at those stations where relatively more suicides and accidents occur

PSYCHOSOCIAL APPROACH.

A. TARGETED PREVENTION: TOWARDS THE PERSON WHO WANTS TO COMMIT SUICIDE

This type of prevention will be carried out by the public health system, following WHO guidelines.

- However, the organization should display signs with the number for the Suicide and Crisis Lifeline and phrases of hope, in coordination with the regional health department.
- There might be specific active awareness campaigns during the months/dates with the highest rate of suicides.

B. PREVENTION BY A THIRD PERSON

a) By the staff

The organization shall train its whole staff who come into contact with passengers to recognize a life crisis and to contact the emergency services if they recognize a vulnerable person who is in distress and may be contemplating suicide.

The organization should train and have staff specialized in recognizing life crises and providing comfort until the emergency services arrive.

b) By relatives and friends

The organization will facilitate a telephone number or e-mail address where relatives and friends of passengers who often go by that transport can communicate that someone may commit suicide.

c) By passengers and citizens

Both passengers and other citizens can help prevent suicide. The Suicide and Crisis Lifeline (in Spain number 024, created in 2022) will also be useful for anyone to provide information regarding a person who may be about to attempt suicide and receive an immediate and prompt response. The passengers/citizens will also be able to inform any staff member who will:

1. Immediately contact the emergency services,
2. Immediately contact the internal suicide prevention hotline
3. Activate private security if necessary to protect the person

The organization will also provide a safety button to stop the train if someone is already on the track.

MEDIA COMMUNICATION

The Ministry of Health and the Ministry of Transport should communicate the number of suicides and attempted suicides that have occurred on the railways in a coordinated manner in a public act every year, reporting them as a public health issue, including helpful resources and messages of hope and recovery.

The communication of each suicide will follow the responsible guidelines on reporting suicides.

Financing: the prevention plan will need to be well funded, with the various budgets established.

In each train/underground station there should be a suicide prevention officer who will be especially trained and who will have maximum responsibility for implementing and monitoring the protocol.

The effectiveness of the risk management process requires full coordination between health and transport departments/ministries.

Finally, the effectiveness of the risk management process will be continuously monitored, and the prevention plan will be reviewed.

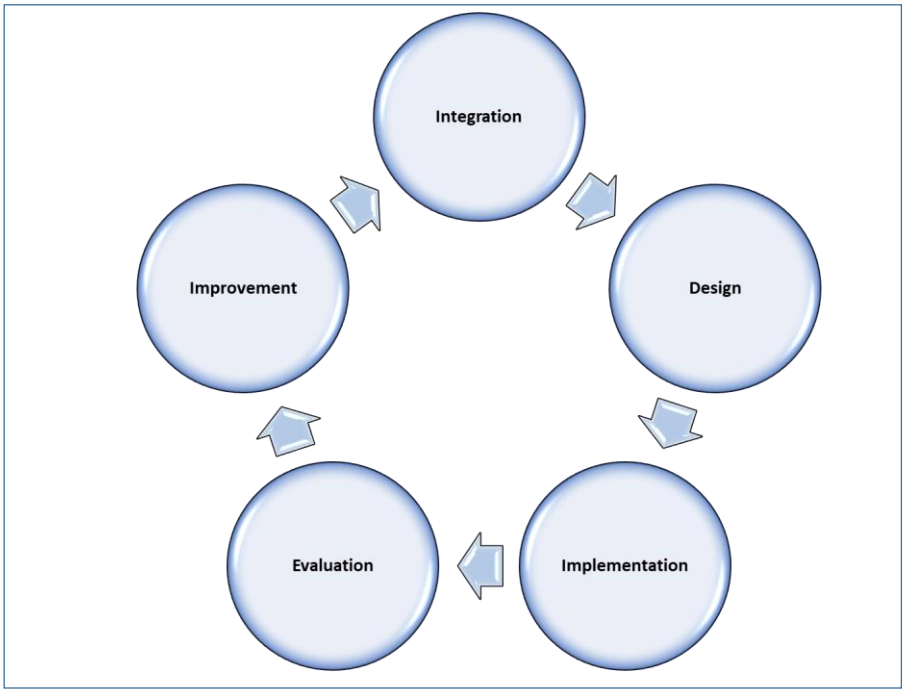
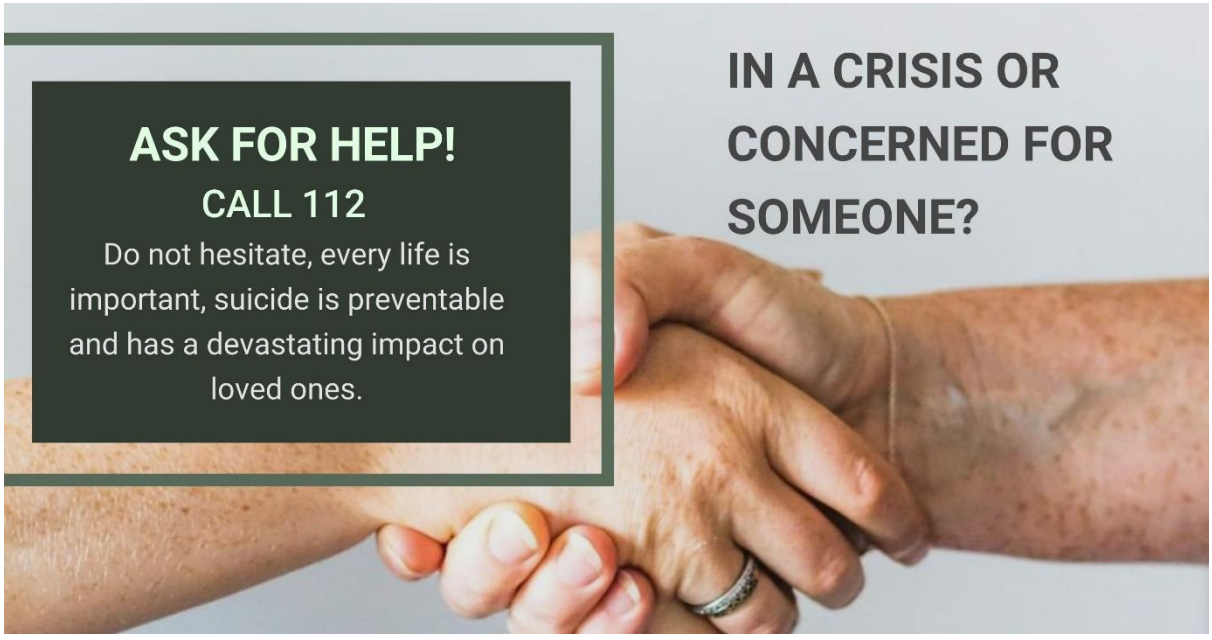


Figure no. 11 Risk management framework (from ISO 31000:2018).



References

1. AI and Suicide Prevention. Mishara B, Chavarriaga R, Till B, Sinyor M, Kirtley O, Mörch C., Accessed 30.10.2023, https://aiforgood.itu.int/event/ai-and-suicide-prevention/ https://www.youtube.com/watch?v=SdOjLLZp3xs
2. Association of Survivals. After the suicide. Accessed 12.7.2023, https://www.despresdelsuicidi.org/es/inicio/
3. Connecting for life. Accessed 20.7.2023, https://www.hse.ie/eng/services/list/4/mental-health-services/connecting-for-life/
4. Cristino Sanchez, I. (2023). *Psychosocial risk factors and their impact on reliability. Psychosociological study of the train dispatcher position*. Unpublished final Degree Thesis, School of Prevention and Integral Safety and Security
5. Erazo N, Baumert JJ, Ladwig K-H. Factors associated with failed and completed railway suicides. Journal of Affective Disorders 2005; 88: 137–143
6. Health Department of Catalonia. Suicide prevention plan in Catalonia 2021-2025. Accessed 20.7.2023 https://scientiasalut.gencat.cat/handle/11351/6319
7. Hallewell MJ, Ryan B, Hughes N, Coad N. Conceptualising innovative lighting interventions for suicide, trespass and risky behaviour on the railway. Lighting Res. Technol. 2023; 55: 79–99
8. Improving Suicide Prevention. Program CRS. Accessed 9.4.2024, https://codirisc.org/home
9. LifeSpan lived experience framework. Black Dog Institute (Australia). Accessed 20.7.2023 https://www.blackdoginstitute.org.au/wp-content/uploads/2020/04/bdi_lived-experience-summit-2018_final.pdf
10. National Institute of Mental Health. NIH Publication No. 23-MH-6389. (2023). Frequently Asked Questions About Suicide. Accessed 20.7.2023 https://www.nimh.nih.gov/health/publications/suicide-faq
11. Railway Suicide Prevention and reduction of negative consequence. Accessed 30.10.2023 https://railwaysuicideprevention.com/prevention-of-railway-suicide/overview.html
12. Reporting On Suicide. Recommendations for Reporting on Suicide. Accessed 12.7.2023 https://reportingonsuicide.org/
13. Spanish Foundation for the Prevention of Suicide. https://www.fsme.es/ Accessed 19.7.2023
14. Spanish National Statistics Institute. Accessed 19.7.2023, https://www.ine.es/en/index.htm
15. Suicide prevention on the railway. Accessed 21.7.2023, https://www.networkrail.co.uk/communities/safety-in-the-community/suicide-prevention-on-the-railway/
16. Timms, K. 10 October 2018. Train driver describes the harrowing reality of rail suicide. PlaymouthLive. Accessed 20.7.2023, https://www.plymouthherald.co.uk/news/local-news/rail-suicide-train-driver-interview-2074583
17. 024. Suicidal Behaviour Hotline. Accessed 19.7.2023, https://www.sanidad.gob.es/linea024/home.htm, https://www.ine.es/
18. U.S. DOT Volpe Center. Rail Suicide Prevention Resource Page. Last updated: Thursday, March 23, 2023. Accessed 20.7.2023, https://www.volpe.dot.gov/rail-suicide-prevention
19. World Health Organization. 17 June 2021. LIVE LIFE: An implementation guide for suicide prevention in countries. Accessed 19.7.2023, https://www.who.int/publications/i/item/9789240026629
20. World Health Organization. One in 100 deaths is by suicide. World Health Organization. Guidance to help the world reach the target of reducing suicide rate by 1/3 by 2030. Accessed 19.7.2023, https://www.who.int/news/item/17-06-2021-one-in-100-deaths-is-by-suicide

9. SELECTION OF CYBERSECURITY TECHNOLOGIES BASED ON RISK MANAGEMENT PROCESSES

Jyri Rajamäki / Laurea University of Applied Sciences, Finland / 2023

ABSTRACT

By following the principles of ISO 31000:2018, organizations can make informed decisions about the selection, implementation, and ongoing management of cybersecurity technologies to effectively mitigate risks and protect their information assets. Drawing on the results of the DIMECC Cyber Trust programme, this article provides a structured approach to choosing the necessary security technologies based on risk management processes, which is crucial in the context of ever-evolving cybersecurity threats.

Link to ISO 31000

Parts from ISO 31000:2018 Risk management process referenced in this article Risk Assessment, Risk Treatment, Monitoring and Review, Recording and reporting, Communication and Consultation.

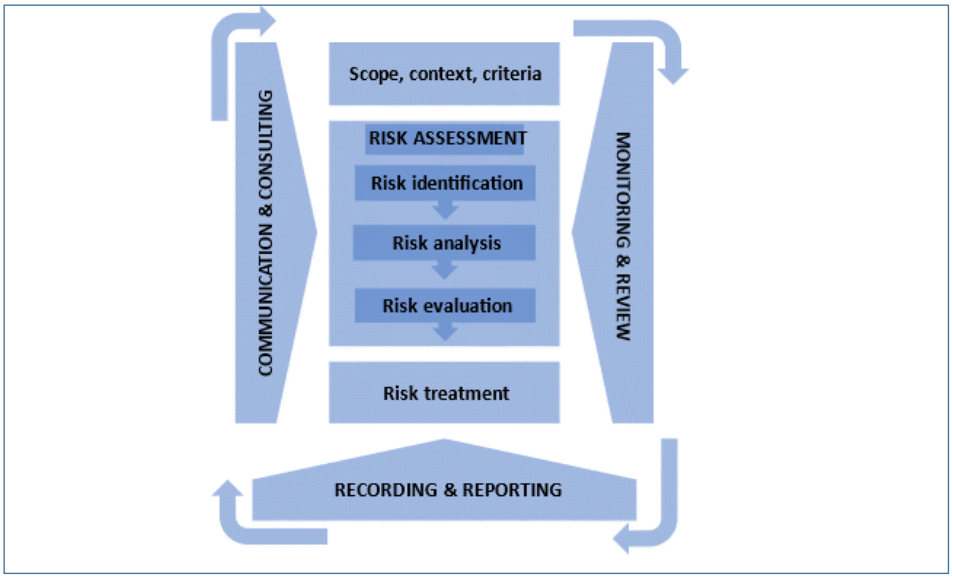


Figure 12. Risk management process (adapted from ISO 31000:2018)

1. Introduction

Risk management is an essential part of setting strategy, achieving objectives, and making decisions at different levels of the organization. ISO 31000:2018 provides guidelines and principles for effective risk management in any organization. Risk management has a vitally important role in any management system. For example, in practice, cybersecurity management is a risk management procedure as the Figure below illustrates.

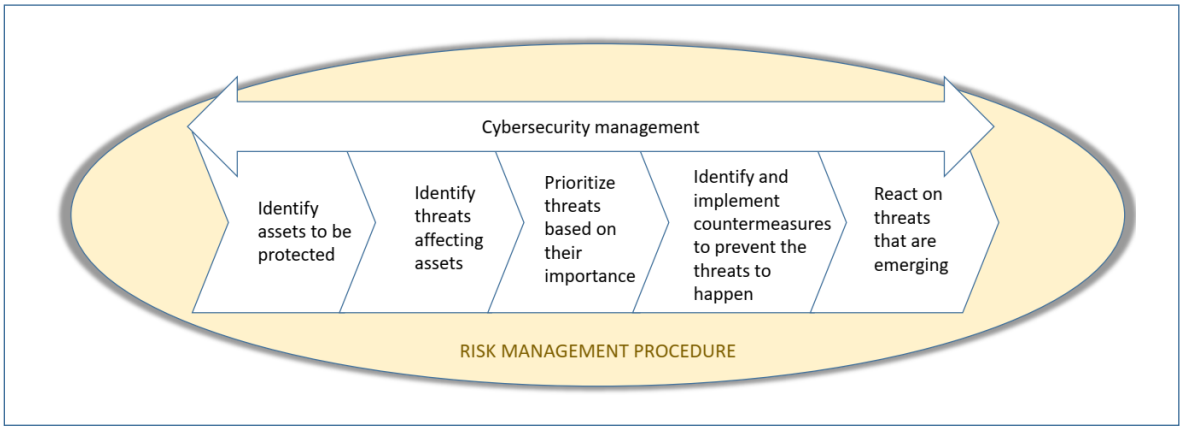


Figure 13. Cybersecurity as a risk management procedure (adapted from Rajamäki & Nevmerzhitskaya, 2018)

Security technologies encompass technical means for achieving cybersecurity, including secure system architectures, protocols, and tools. They enable the protection of infrastructures, platforms, devices, services, and data. Key aspects include user identification, authorization, and access rights. Common security technology standards include ISO/IEC 27033 for network security and ISO/IEC 27034 for application security. While ISO 31000 doesn't specifically address cybersecurity technologies, its principles and framework can be applied to the selection and implementation of cybersecurity technologies within an organization.

2. Case

The DIMECC Cyber Trust Programme created a foundation for Finnish research and industry to address needs emerging within cybersecurity. The main research objective of the DIMECC Cyber Trust programme was to improve privacy, trust, and decision-making within digital infrastructure. The consortium consisted of 19 companies and 8 research institutes and universities. The programme published over 130 research articles on cyber security and how to protect privacy.

Cybersecurity serves as a key enabler of trust development in the digital world, to ensure resilience in all operational systems and infrastructures. DIMECC outlines four key themes within cybersecurity, namely security management, situational awareness, security technologies, and resilience of operational systems.

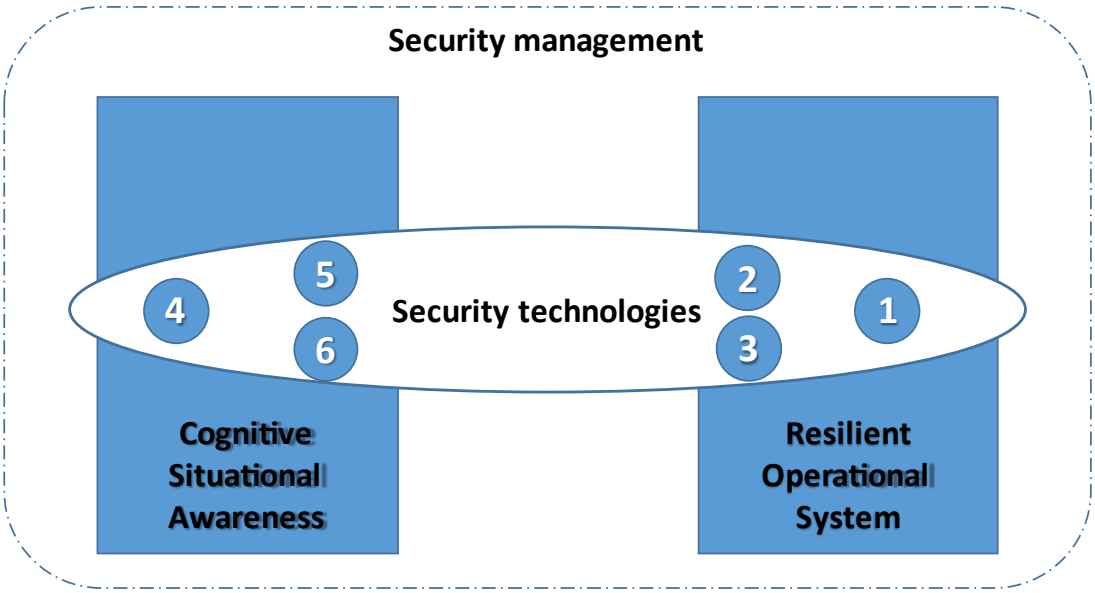


Figure 14. Categories of cybersecurity technologies (adapted from Rajamäki, 2022)

Security technologies can be divided into six different categories according to their goal:

1. Technologies for Improving the security of the operational system, such as system architectures, protocols, implementations, development tools, and development platforms.
2. Protection technologies, such as user identification and authorization, firewalls, antivirus programmes, intrusion protection systems (IPS), and security information and event management (SIEM) systems.
3. Technologies for producing security data, such as sensors (firewall logs, system event logs, antivirus, and packet capture) network traffic analyzers, intrusion detection systems (IDS), and open-source intelligence (OSINT) technologies.
4. Technologies for analyzing security data. These technologies can be divided into three levels:
1. Level1 - History: Forensic
2. Level2 - Comprehension of the current situation (Data fusion, SIEMs)
3. Level3 - Projection of future status
5. Technologies for visualising the situational picture, including technologies for human machine interface.
6. Technologies for cyber threat intelligence sharing between organizations, such as early warning systems, Malware Information Sharing Platform (MISP), Cortex, and TheHieve.

It must be noted, though, that several technologies belong to more than one category.

3. Best practices

By combining the information security technologies mentioned with the ISO 31000 processes, a solid cyber security framework can be created. Here are the main aspects of this integrated approach:

1. Risk Identification, Assessment, and Treatment:

- Risk Identification (ISO 31000 - Clause 5):
    - Utilize technologies for producing security data (sensors, network traffic analyzers, IDS, OSINT) to identify potential threats and vulnerabilities.

    - Leverage open-source intelligence technologies for understanding the cybersecurity landscape.
- Risk Assessment (ISO 31000 - Clause 6):
    - Combine technologies for analyzing security data (Forensic, Data Fusion, SIEMs) to assess the likelihood and impact of identified risks.
    - Utilize technologies for visualizing the situational picture to comprehend the current cybersecurity situation.
- Risk Treatment (ISO 31000 - Clause 7):
    - Select and implement protection technologies (firewalls, antivirus, IPS, SIEM) based on the cybersecurity risks assessed.
    - Use technologies for cyber threat intelligence sharing (early warning systems, MISP, Cortex) to stay informed about evolving threats.

2. Monitoring and Review:

- Monitoring and Review (ISO 31000 - Clause 8):
    - Employ technologies for continuous monitoring of the security infrastructure (sensors, IDS).
    - Analyze security logs using technologies for analyzing security data (SIEMs) to identify anomalies.
    - Regularly review and update cybersecurity measures based on the evolving threat landscape.

3. Communication and Consultation:

- Communication and Consultation (ISO 31000 – Clauses 2 and 3):
    - Establish a human-machine interface using technologies for visualizing the situational picture to facilitate communication.
    - Use technologies for cyber threat intelligence sharing to exchange threats and mitigation strategies with other organizations.

4. Integration with Overall Management:

- Integration with Overall Management (ISO 31000 - Clause 4):
    - Integrate cybersecurity risk management into the overall governance using technologies for improving the security of the operational system.
    - Align cybersecurity considerations with business objectives using protection technologies and risk treatment options.

This integrated approach ensures a comprehensive cybersecurity strategy that combines the strengths of various security technologies and aligns with the ISO 31000 processes for risk management. Regular updates and communication channels help in adapting to the dynamic nature of cybersecurity threats.

References

1. DIMECC Cyber Trust Program. In: dimecc.com [online] [cit. 12/11/2023] Available at: https://cybertrust.dimecc.com/
2. ISO 31000 Risk management. In: ManagementMania.com [online]. Wilmington (DE) 2011-2023, 11/11/2016 [cit. 12/11/2023]. Available at: https://managementmania.com/en/iso-31000-risk-management
3. Jyri Rajamäki (2022). Turvallisuusteknologiat kyberympäristön luottamuksen työkaluina. In: *Jatkuvuutta turvaamassa – LaureanYAMK opiskelijoiden näkökulmia*, ed. Harri Ruoslahti, Laurea-ammattikorkeakoulu, pp. 55-64.
4. Jyri Rajamäki and Julia Nevmerzhitskaya (2018). Cybersecurity in an organization. In: *Organization and individual security*, ed. Ivita Kīsnica, Nordplus, Riga, pp. 539-554.

10. SECURITY DESIGN

Kārlis Apalups / Turiba University, Latvia / 2024

ABSTRACT

Designing security training for universal risk readiness is essential for any organization. The process begins with a commitment from top management, recognizing that without their backing, no substantial progress in training design can occur. Establishing clear and consistent security policies is crucial, as these will serve as the foundation for the training content. Once these policies are established, the organization must focus on educating its members about these policies and the best practices for mitigating security risks. To ensure the training remains relevant, ongoing monitoring and evaluation are necessary. This can be achieved by implementing specific metrics to assess the effectiveness of the security training and to evaluate the return on investment. By following these steps, an organization can create a robust security training programme that prepares its members to handle security risks effectively.

Link to ISO 31000

ISO 31000:2018 Risk management principles referenced in this article: Human and culture factors.

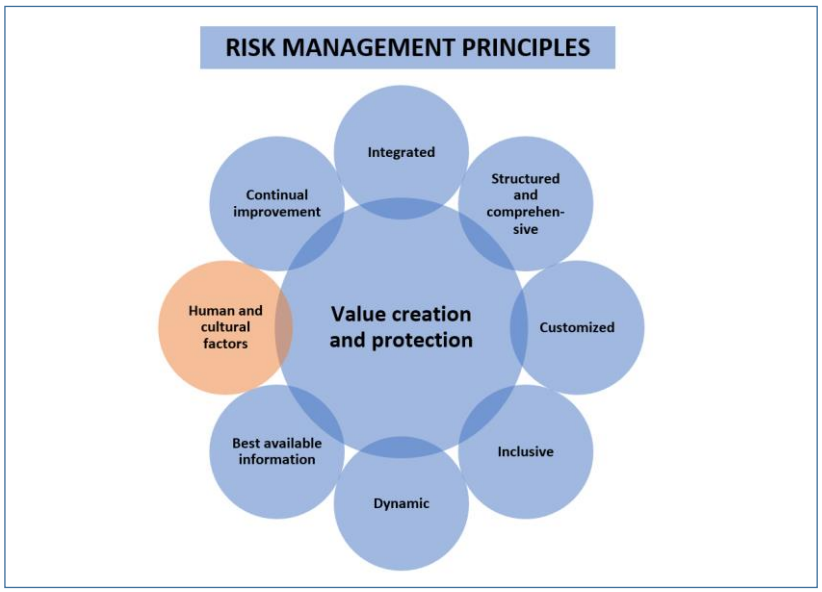


Figure 15. Risk management process according to ISO 31000:2018

1. Introduction

Security training encompasses a range of practices aimed at enhancing the knowledge and skills necessary to protect sensitive information and physical assets.

The design of security training programs is a critical aspect that ensures the training is effective and relevant to the needs of the organization. It includes the development of a curriculum that covers essential topics such as data and record management, password safety, fire safety, evacuation and other crisis procedures. Security training design also involves creating a governance model to drive accountability during development and after the programme is rolled out, ensuring that the training objectives align with the organization's security policies and regulatory requirements.

Moreover, it is not just about the content but also about the delivery methods, which can range from workshops, crisis scenarios and cosplay to online courses, and the evaluation of training effectiveness through assessments and feedback mechanisms. Effective security training design is a proactive approach to safeguarding an organization, emphasizing the importance of continuous learning and adaptation in the face of evolving threats. It is a strategic investment in the human element of security risk management, equipping individuals with the tools and understanding necessary to act as the first line of defense against potential breaches and incidents.

2. Case

“Latvijas Finieris” is the leading plywood and its products' manufacturer in Baltic States and Finland. The company is also active in forest management, logging and the production of synthetic resins and phenol films.

In 2014 “Latvijas finieris” had a huge fire in one of Rīga-based factories. After this event, the holding company decided to implement a security culture and develop it. Part of its efforts was the creation of Safety management service (SMS) that managed security risks in such areas as fire safety, occupational health and work safety, environmental protection and physical security. Before the fire there had been a high amount of work-related accidents which led to losses of working power, insurance costs and a diminished sense of safety or security among workers.

The efforts of SMS allowed to develop such a security culture that drastically lowered work-related incidents, increased the ROI from security and safety investment and increased the overall organization culture. One of the core aspects of the security culture and risk management, was the development of training programmes.

3.Best practices

Good security training design relies upon 3 basic pillars - 1) Panic (self) control 2) Preparedness for the unknown 3) Overcoming of fear. For this to be achieved, creating a security training design for universal security risk readiness involves several key steps:

3.1. Assessment of Security Risks: Begin by identifying and assessing potential security threats and vulnerabilities within the organization or environment. This includes analyzing past incidents, current security measures, and potential future risks. A good security training design relies on a relevant Security risk analysis.

3.2. Defining Training Objectives: Clearly outline what the security training programme aims to achieve. Objectives may include enhancing awareness, improving response strategies, and ensuring compliance with security policies. Also it might include refreshing knowledge.

3.3. Developing a Curriculum: Design a comprehensive curriculum that covers all necessary topics, such as risk identification, prevention strategies, emergency response, and recovery plans. With the curriculum - a scenario also has to be created or put forward.

3.4. Incorporating Diverse Learning Methods: Utilize a mix of learning methods including lectures, interactive workshops, simulations, and e-learning modules to cater to different learning styles and to ensure better retention of information. For the best practical training, it is recommended to use simulations of diversified scenarios of the same risk - people should not get accustomed to the foreseeable, but rather be trained to be prepared for the unexpected.

3.5. Customization for Different Roles: Tailor-made training modules for various roles within the organization, ensuring that each employee receives relevant information according to their responsibilities and level of access. Be aware of the need for specific training for essential workers - they will also be outlined during the security risk analysis.

3.6. Regular Updates and Revisions: Keep the training material up-to-date with the latest security trends, technologies, and practices. Regularly review and revise the content to maintain its relevance and effectiveness.

3.7. Evaluation and Feedback: Establish metrics to evaluate the effectiveness of the training programme. Collect feedback from participants to identify areas for improvement and adjust the training accordingly. It's good to include focus groups for employees in high risk environments and talk about their fears in the workplace.

References

1. UNSMS Security Policy Manual – Security Training and Certification https://policy.un.org/sites/policy.un.org/files/files/documents/2024/Apr/spm_-_chapter_v_section_c_-_learning_and_training.pdf
2. Designing a Successful Security Awareness Training Program https://www.infosecinstitute.com/resources/security-awareness/designing-security-awareness-training-program/
3. https://www.finieris.com/en/home
4. https://www.tvnet.lv/4765017/latvijas-finiera-rupnica-liels-ugunsgreks

11. LEARNING FROM EXPERIENCES OF THE NORTHGUIDER GROUNDING

Natalia Andreassen & Rune Elvegård / Nord University, Norway /2024

ABSTRACT

This article presents a case of learning from experience of the Northguider accident and implementing improvements in the emergency preparedness systems. The article starts with the description of the grounding and crisis management operation, and then proceeds by presenting the case of an emergency preparedness exercise that was based on the scenario of this incident.
In relation to the ISO 31000 standard, the Improvement principle is mentioned, and development of emergency preparedness exercises is suggested for continual learning and improvement.

Link to ISO 31000

The ISO 31000 standard specifies the guidelines for risk management principles. ISO 31000 is an important and useful tool for security risk professionals to develop risk management strategies. As International Organization for Standardization puts it, the long-term success of an organization relies on many things, from continually assessing and updating their offering to optimizing their processes. As if this weren't enough of a challenge, they also need to account for the unexpected in managing risk.

However, the security risk professionals need to extract and integrate the guidance which is most relevant to their organizations and improve risk management process and performance according to their experience.

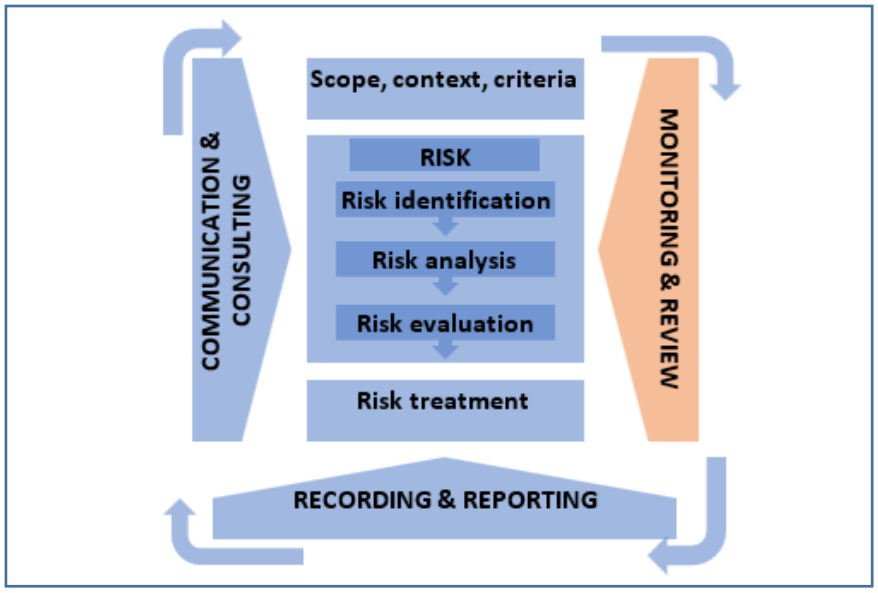


Figure 16. Risk management process according to ISO 31000:2018

The last principle in ISO 31000 is Continual Improvement. This principle confirms that the risk management arrangements should ensure continual improvement. Risk management is continually improved through learning and experience.

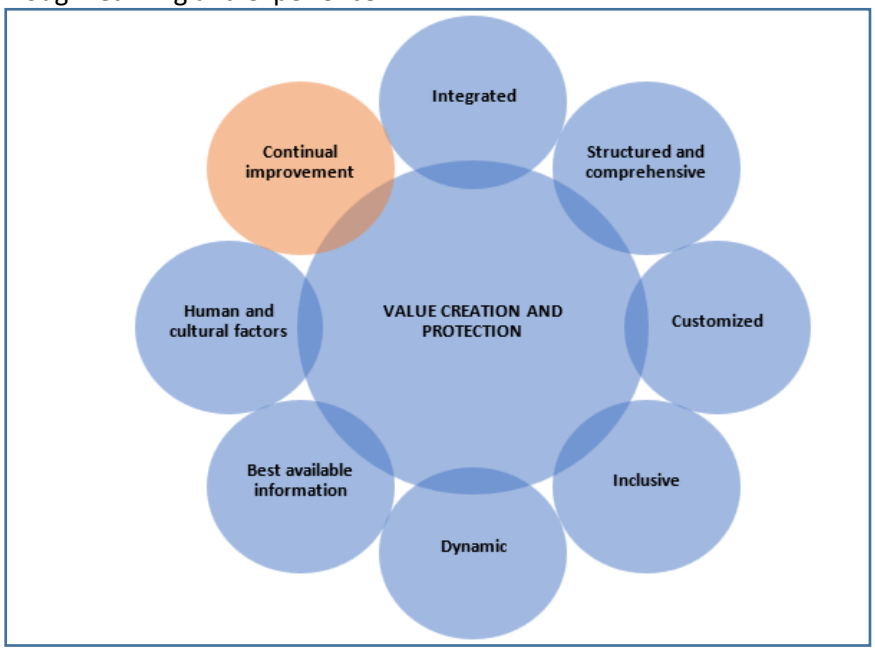


Figure 17. Risk management principles according to ISO 31000:2018

The ISO 31000 framework describes that organizations should evaluate own practices and existing processes for risk management. The last framework component is Improvement, which includes value of risk management, adapting the framework and integration of risk management activities according to organizational needs.

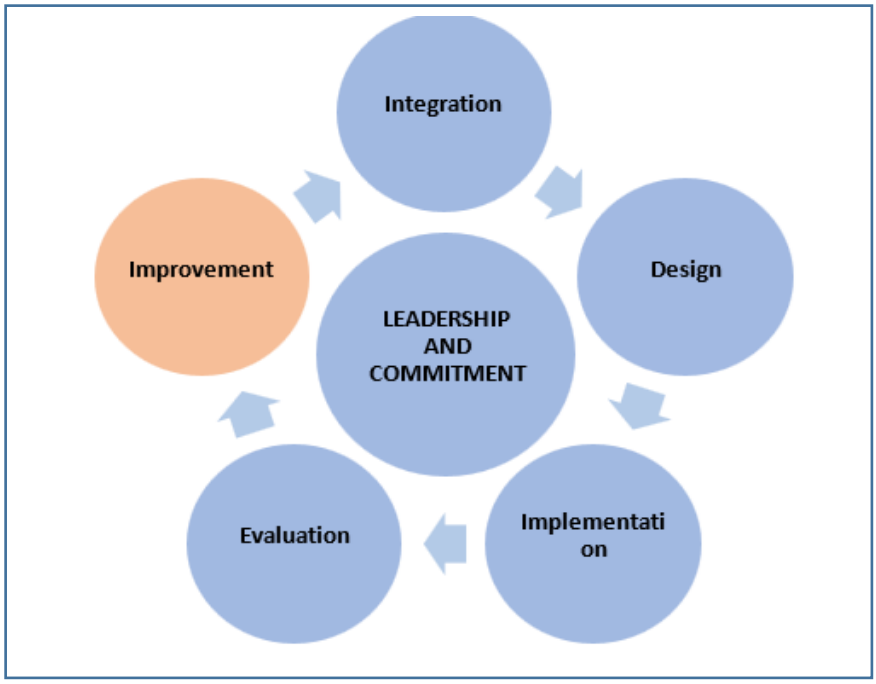


Figure 18. Risk management framework according to ISO 31000

Organization should continually improve and strengthen it's framework for risk management through learning and review of experiences.

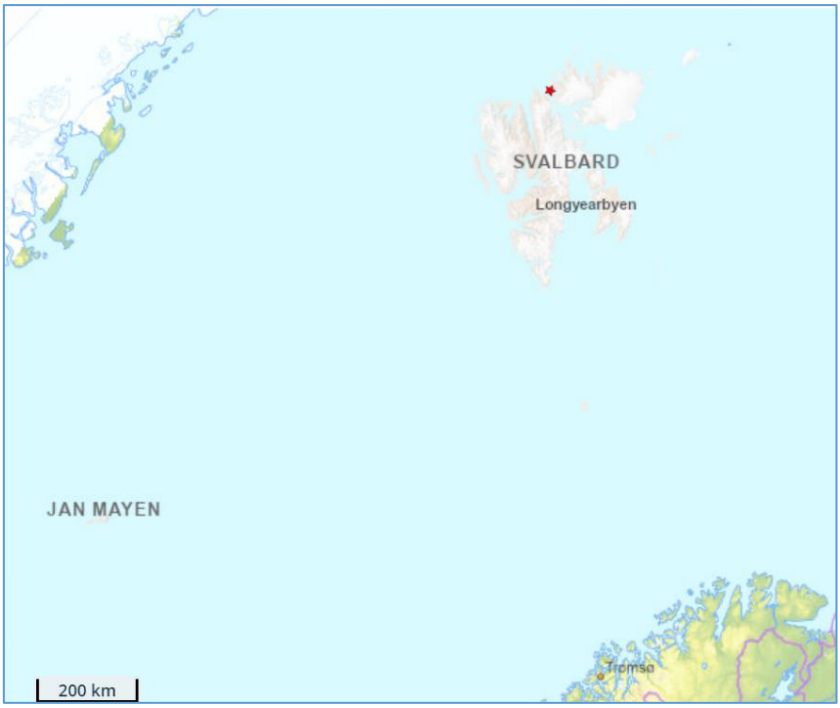
1. Introduction

The article describes the case of the Northguider grounding, which was a very complex search and rescue and marine environmental response operation. The scenario was later utilized in emergency preparedness exercises for improvements of the risk and crisis management systems in the Arctic. One such exercise is presented in this case study, as best practice example, to learn from experience of own emergencies and from others.

2. Case

During the Christmas season, December 28, 2018, the Norwegian trawler Northguider was fishing for shrimp in the Svalbard archipelago with a crew of 14 persons. At approx. 13:00 hrs it ran agroundin the narrow northern part of the Hinlopen Strait. There were no other ships in the area. The Northguider sent out a mayday via its emergency beacon and MF/HF radio. The Northguider did not receive any response to the distress signal, but the message was intercepted by the Norwegian Coastguard Vessel “Barentshav”, which was located near the island Bjørnøya. The Barentshav sailed towards Hinlopen but had to turn back due to ice conditions.

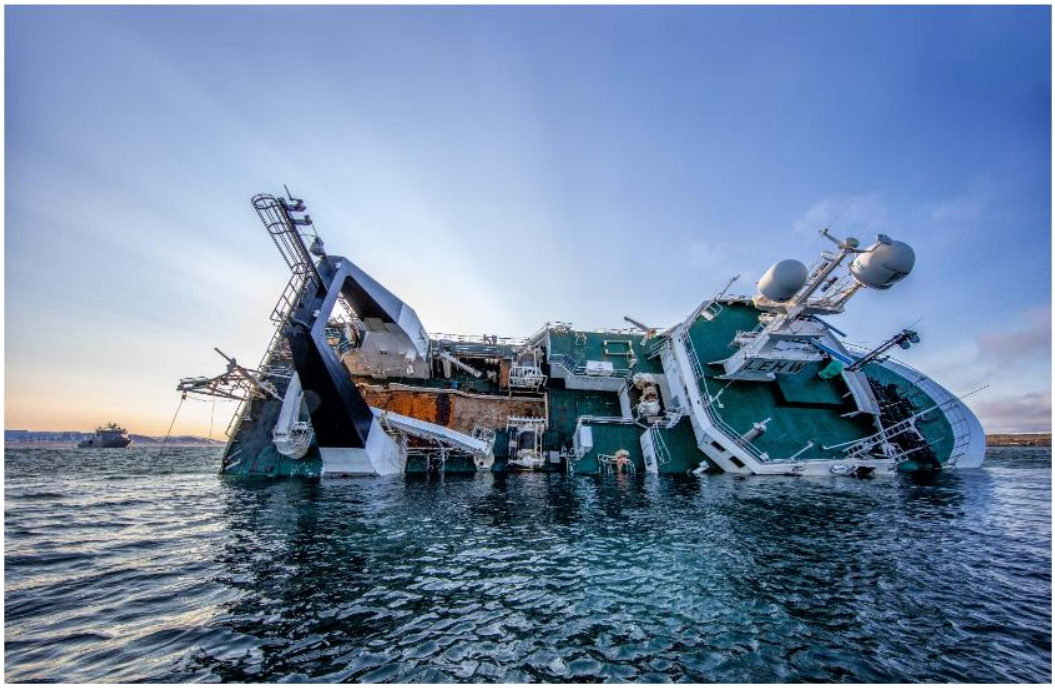
After several hours, the entire crew was rescued by 2 helicopters from the Governor of Svalbard in a very tough rescue operation in bad weather. Lifting in Arctic conditions is a challenge in itself, but this operation was at the limit of what is possible in -20 degrees Celsius temperature, darkness and strong winds.



Picture 1. Location of the Northguider grounding

After the SAR operation had been completed, the Norwegian Coastal Administration took over the responsibility for the response. Due to ice conditions, it was decided that the Norwegian Coastguard vessel Svalbard could assess the situation for further work. The ship was of ice class and was able to handle multi-year ice. On 9 January 2019 emergency unloading of the bunker fuel was started to reduce the enormous environmental consequences in case the trawler should begin to leak.

In February 2019, the Northguider was emptied of all fuel and environmentally hazardous substances. From August to October 2019, a contracted professional salvor made an attempt to raise and tow the ship without success. Because of the ice situation, the harsh climate and remote position, the salvor had to postpone the salvage operation to the summer season of 2020. By September 2020 eventually, the ship was scrapped on the spot and removed.



Picture 2. Northguider, photo: Håkon Kjøllmoen

Remoteness, limited infrastructure and harsh climatic conditions are challenging for maritime activity in the Arctic (Kruke & Auestad, 2021). Emergency response management operations often involve a wide range of actors with specialized tasks and roles related to information sharing, decision-making, and front-end personal command (Bigley & Roberts, 2001). The on-scene command of response operations relies on managers and the systems that are behind them, such as procedures, protocols, formal structures etc. In volatile and complex environments, coordination is less dependent on the pre-planned design than on the current skills, solving emerging tasks and challenges (Andreassen et al., 2020).

The case showed that it is important to pre-plan the roles and responsibilities for both SAR and marine environmental response incidents. This ensures that the key contacts of local, regional, and national authorities collaborate well at the time of the incident. Besides, the initial assessment is vital, the necessary measures must already be taken during the SAR phase.

In November 2021, the table-top exercise “Oil in Ice” took place under the auspices of ARCSAR, the Arctic and North Atlantic Security and Emergency Preparedness Network, which was a large EU-funded innovation project. The exercise was facilitated by Nord University’s NORDLAB, the emergency preparedness management laboratory (ARCSAR, 2022). The main purpose of the Oil in Ice 2021 tabletop exercise was to discuss how oil spill preparedness and response is organized in the case of a large-scale operation in the Svalbard region, as well as to identify lessons from other locations and agencies in the Arctic and North Atlantic regions.

Picture 3. ARCSAR exercise Oil in Ice, photo: Center for Crisis Management and Collaboration, photo: Center for Crisis Management and Collaboration – Nordlab

The scenario for this exercise was based on the Northguider grounding case, with the virtual difference that the spill actually happened. The situation in the Svalbard area is quite challenging, as there are multiple actors from the SAR and marine environmental response sectors who need to collaborate to handle the incident. This includes marine environmental response, the rescue operation, and securing the vessel and the environment.

To learn and discuss potentially necessary improvements the training audience was divided into three groups: the main training audience – those who would be involved in case if there were oil spill; the secondary training audience – the parallel organizations in other Arctic countries, and observers – all other relevant or interested stakeholders. The exercise contributed to deeper understanding of the needs for skills, assessment systems and competences to deal with Arctic marine environmental incidents.

3. Best practices

There is a written joint handover procedure between Joint Rescue Coordination Center and Norwegian Coastal Administration in Norway. However, it is important to understand how to use the procedure and continually improve the systems. This exercise was an important contribution to sharing knowledge and experience on how a serious incident and subsequent oil pollution can be handled under extreme circumstances in the Arctic (Kystverket, 2021). This exercise contributed to the improvements, understanding of relevant procedures, and assessment of new risks and new competences needed to deal with Arctic incidents.

The scenario was based on the real case, so the realism during tabletop- and game exercise provided valuable opportunities for demonstrating relevance of the risks and challenges to various groups of stakeholders. Advanced tabletop exercises like these require good pedagogical planning with a focus on different backgrounds and needs of the various participants. The most important is to facilitate the learning of each individual and organization involved and exchanging ideas on how to

deal with a complex event in demanding conditions (Elvegård & Andreassen, 2022).

As the ISO 31000 suggests, crisis or risk management is continually improved through learning and experience. Both framework component and one of the principles focus on continuous improvement of the systems, learning, and updating the routines and competence. Emergency preparedness exercises serve as a particularly effective learning method for assessing enhanced knowledge, facilitating learning and implementing knowledge in organizations (Andreassen et al., 2024). Exercises contribute to enhancing security risk management capabilities, building trust and collaboration between involved stakeholders (Elvegård et al., 2024). By creating conversational spaces, team members can reflect on their collective experiences and discuss potential response actions. For more recommendations for the development of study and training programmes, particularly on various exercise methods, see Chapter 5 of the SECUREU project report "Recommendations for higher education institutions teaching security risk management" (Neimane et al., 2024).

References

1. Andreassen, N., Borch, O.J. & Sydnes, A.K. (2020). Information sharing and emergency response coordination, *Safety Science*, Volume 130, 104895, https://doi.org/10.1016/j.ssci.2020.104895.
2. Andreassen, N., Elvegård, R., Villanger, R. & Johnsen, B.H. (2024). Enhancing cognitive motivation: an evaluation model for emergency preparedness exercises, *The Learning Organization*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/TLO-06-2023-0100
3. ARCSAR (2022) *Tabletop Exercise ARCSAR TTX 2021 "OIL IN ICE". Exercise Report*. WP3 T3.2, https://arcsar.eu/wpcontent/uploads/2018/11/ARCSAR-TTX-2021-OIL-IN-ICE.pdf
4. Bigley, G. A., & Roberts, K. H. (2001). The incident command system: High reliability organizing for complex and volatile task environments., *Academy of Management Journal*, 44(6), 1281–1299.
5. Elvegård, R. & Andreassen N. (2022). Internasjonalt samarbeid med fokus på oljevern i Arktis, *High North News*, https://www.highnorthnews.com/nb/internasjonalt-samarbeid-med-fokus-pa-oljevern-i-arktis?fbclid=IwAR020Lb75C6x9q6yfRzRuw7u4JrLZCveQPU2BqB9_4De37Lmp5kTTkixUl0
6. Elvegård, R., Andreassen, N. & Badu, J. (2024). Building collaboration and trust in emergency preparedness: a model for planning collaboration exercises. *Safety in Extreme Environments,* https://doi.org/10.1007/s42797-024-00107-w
7. ISO 31000:2018 *Risk management — Guidelines* (Edition 2, 2018)
8. Kruke, B.I. & Austad, A.C. (2021). Emergency preparedness and rescue in Arctic waters, *Safety Science*, Volume 136, 105163, https://doi.org/10.1016/j.ssci.2021.105163.
9. Kystverket [Norwegian Coastal Administration] (2021) Ledet og deltok på øvelse med fokus på nordområdene, *Kystverkets Nyhetsarkiv* 11.1.2021, https://kystverket.no/nyheter/2020/ledet-og-deltok-pa-ovelse-med-fokus-pa-nordomradene2/
10. Neimane, K., Začs, U., Apalups, K., Andreassen, N., Elvegård, R., Kibsgaard, D., Bambach, B., Goffin, B., Bergman, J., Dorado, X., Garcia, E., Aatsinki, A., Rojas, H.I., Kalesnykas, R. (2024). *Recommendations for Higher Education Institutions Teaching Security. Focus on Security Risk Management*., SECUREU report, EU Erasmus+, https://security.turiba.lv/recommendations/

12. HOW SECURITY RISK MANAGEMENT CAN CONTRIBUTE TO ACHIEVING RESILIENCE WITHIN ORGANIZATIONS

Lambert Bambach / Avans University of Applied Science, the Netherlands / 2024

Abstract

The management of a maritime company realizes that organizational resilience incorporating Business Continuity Management requires more than a reliance on procedures to recover assets. What if they can't be recovered within reasonable timeframes, or at all? The management wants to gain insight in the steps that are necessary to enable organizational resilience in a progressive way. Building the capacity for agility, adaptation, learning, and regeneration to ensure that the organization is able to deal with more complex and severe events (such as a pandemic, climate change, or cyber-attacks) and be fit for the future.

Link to ISO 31000

Improvement, integration, leadership and commitment, design, human and cultural factors, continual improvement, customized, inclusive, communication & consulting, risk identification and risk analysis.

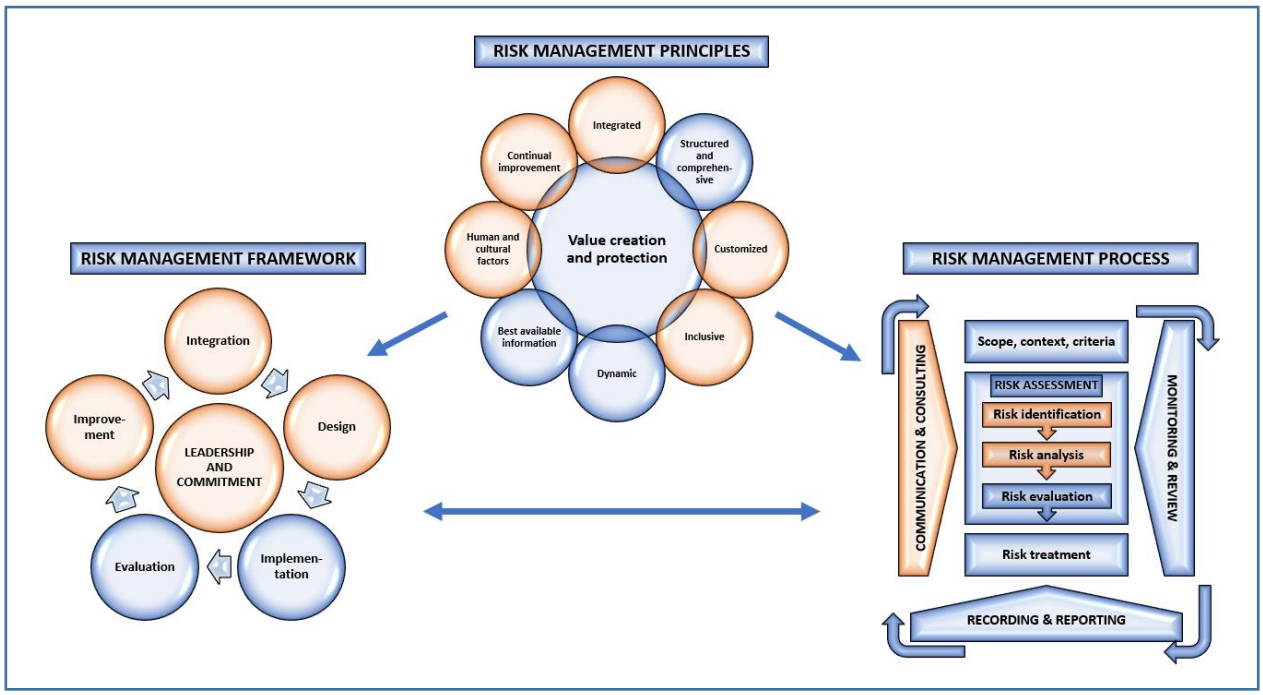


Figure 19. Risk management framework, Risk management principles and Risk management process according to ISO 31000:2018

1. Introduction

A Dutch maritime contracting company that specializes in dredging, land reclamation, and constructing man-made islands experiences that relying on a reactive strategy is not enough on its own to meet the potential scale and pace of change imposed by sudden shocks and future challenges. The management realizes that organizational resilience incorporating Business Continuity Management requires more than a reliance on procedures to recover assets. And what if they can't be recovered within reasonable timeframes, or at all?

2. Case

The management expects that a next crisis might be very different from the COVID-19 pandemic, and another government bailout may not be forthcoming. Therefore, companies must take more responsibility for their resilience and must invest in future resilience.

The management have asked you to look into the steps that are necessary to enable organizational resilience in a progressive way. Building the capacity for agility, adaptation, learning, and regeneration to ensure that the organization is able to deal with more complex and severe events (such as a pandemic, climate change, or cyber-attacks) and is fitter for the future.

3. Best practices

3.1 Goal of the organization

The organization aims for maritime ingenuity for a sustainable and secure future.

3.2 Risk Assessment

The organization identifies risks and translates them into effective and practical solutions. The organization identifies threats and risks in the field of Security Risk Management that directly influence their primary process, as well as trends in threats that arise from geo-political tensions, such as climate change, that can indirectly affect their primary processes. The organization continuously supports the operation in assessing whether the organizational security baseline is still sufficient or not and whether it needs to be adjusted, as well as in the further development of security measures to support resilience for the organization.

3.3 Steps that help to enable resilience within the organization

In the further development of security measures to support resilience the following steps should be taken into account to enable organizational resilience in a progressive way.

3.3.1 Discuss future failure

Resilient organizations accept that their design, plans and operations, are fallible – they ask what if? They also anticipate and make less complacent assumptions about future issues – they ask what next? With this mindset one allows people to speak up who might remain silent for fear of being labelled a pessimist or being punished for speaking up with a dissenting view. It helps dampen excessive optimism about security of the operation, when one assumes the incident has already occurred instead of pretending it might happen. Moreover, it helps people to overcome blind spots – it forces people to see things from different perspectives, especially when you have sufficient cognitive diversity in the room.

3.3.2 Consider connected impacts

No organization is resilient unless the system is resilient. The five capitals model can be used to allow organizations to examine five connected impacts (Table 1) for every severe but plausible

scenario. The model can also help organizations examine their connected resilience and consider what needs to be done to maximize the value of the five capitals, manage 'trade-offs, and avoid weakening them, to minimize any key impacts. In many organizations, these impacts are labelled people, reputational/regulatory, operational, environment and financial. Although the model can help to examine the connected resilience it is a mistake to assume that specific issues in one of the capitals will have a corresponding impact in others. Specifically, reputational impacts can be unpredictable.

Five capitals	Key impacts
Human capital (e.g. skills, capabilities, experience, know-how, tacit knowledge)	People impact (e.g. harm, wellbeing, health absenteeism, turnover)
Social capital (e.g. networks, norms, values and understandings that facilitate cooperations, collaboration and community)	Reputation/regulatory impact (e.g. reputation, confidence, trust, complaints, customer loyalty, regulatory fines, contractual penalties, market integrity)
Built capital (e.g. building, water processing, manufacturing and processing plants, energy, transportation, communications infrastructure, technology)	Operational impact (e.g. machine downtime, system outages, capacity utilization, on-time delivery, yield, data loss)
Natural capital (e.g. materials, soil, air, water, plants and animals)	Environmental impact (e.g. biodiversity loss, pollution, deforestation)
Financial capital (e.g. cash, assets, credit, and other forms of funding that build wealth)	Financial impact (e.g. profitability, liquidity, cash flow, solvency, valuation)

Table 1. Five Capitals Model

3.3.3 Understand Essential Outcomes (EOs)

Often resilience is thought of as the absence of disruptions (or as an acceptable level of risk). In this perspective, resilience is defined as a state, where as few things as possible go wrong. Crucially, this view does not explain why Essential Outcomes (EOs) almost always go right. An alternative to the conventional approach of trying to make *'as few things as possible go wrong'* is to try to make *'as many things as possible go right'*.

To gain the insights for the organization to do this, a visual representation of an EO can be produced by journey mapping and resilience (service) blueprinting involving diverse contributions from a multi-disciplinary team. The benefits of (service) blueprinting are shown below (Table 2).

The benefits of service blueprinting
▪ Forming a stable, shared understanding of an essential outcome
▪ Assembling the contributing factors into a coherent causal diagram
▪ Examining single points of failure/lack of alternative paths, crucial interfaces, critical steps (points of no return), and 'risk important' actions
▪ Exploring how factors are interconnected across borders and boundaries
▪ Incorporating different worldviews and data from diverse sources
▪ Producing a rich, visual picture to share with colleagues
▪ Highlighting problems areas that should be addressed to prevent incidents from occurring in the future

Table 2. The benefits of service blueprinting

3.3.4 Define a resilience threshold based on the impact tolerance approach

Organizations can define their own resilience thresholds, which ultimately entails quantifying how a disruption could impact the organization, different customer groups, and the wider sector and system. To enable organizational resilience in a progressive way organizations should adopt the impact tolerance approach instead of the traditional risk-based approach. Below (Table 3) the impact tolerance approach is compared to the traditional risk management approach.

Traditional risk-based approach	Impact threshold approach
Primarily internal – impact on the organization's objectives	Primarily external – impact to an external stakeholder and broader system
Focus on named risk types	Focus on essential outcomes
Appetite for and classification of risks: minor, moderate, high or severe	Thresholds of what is tolerable/acceptable
Likelihood of the risk occurring	Assumes that risk has occurred
Defines effects and actions or interventions which would reduce the inherent exposure	Defines effects and actions or interventions which would reduce the inherent exposure and factors in recoverability
Often uses words such as 'significant', 'substantial', 'some', 'extensive', 'damage', that are open to interpretation and cannot be quantified	Provides essential outcome measures
Updated and reviewed periodically (quarterly, annually)	Ongoing monitoring and review of the essential outcome. In some organizations, this involves feeding in live information to anticipate and prevent disruptions

Table 3. The impact tolerance approach vs the traditional risk management approach

3.3.5 Balance strategic choices

When thresholds are identified for the EOs it is possible to examine each EO and make choices and changes to enhance resilience based on the four resilience intervention choices and four outcomes of resilience – 4Rs: readiness, responsiveness, recovery and regeneration. The choices include (Table 4):

Intervention choices and outcomes of resilience	
Controls to increase *readiness*	e.g. safeguards, add new plans or procedures, add codes of conduct, ensure compliance, find an fix errors, increase supervision/oversight/audit
Flexibility to increase *responsiveness*	e.g. add redundancy, add diversity, create flexibility (by design) empower people by giving them the freedom and discretion to act, develop teamwork and communication
Optimization to improve *recovery*	e.g. clarify existing roles and responsibilities, improve existing processes, reduce cost, improve monitoring, fix gaps in knowledge and skills
Innovation to increase *regeneration*	e.g. create safe spaces for experimentation, encourage informal networking , developing new capabilities, resources and ways of working, design thinking workshops

Table 4. Intervention choices and outcomes of resilience

3.3.6 Stress test thresholds

Organizations are tested every day by issues like near misses and incidents, which are learning opportunities. Resilient organizations review their successes and failures, assess them systematically, and record the lessons in a form that employees find open and accessible.

Incidents not only cause harm, service loss, or emergency but also generate surprise and shock. These incidents can create a mismatch between people's way of thinking (e.g. what is safe, secure, acceptable, ethical, tolerable, standard?) and their environment. Therefore, recovering from an

extreme event requires a “full cultural readjustment … of beliefs, norms and precautions, making them compatible with the new understanding of the world”. This can be supported by adaptive leadership from management, using design thinking in multidisciplinary teams. With many incidents, organizational learning often stops with the publication of ‘lessons learned’, overlooking ‘lessons applied’. Without making changes in the way that work is done, only the potential for improvement exists.

3.4 Standards

There are various standards and norms for strengthening an organization's resilience. The five standards named below are the most common to be adopted by organizations to strengthen their resilience. It is important to note that the implementation of these standards should be tailored to the specific context and needs of each organization.

ISO 22301: This is the international standard for business continuity management. It provides a framework for planning, setting up, implementing, monitoring, assessing, maintaining, and continuously improving a documented system to prepare for, respond to, and recover from disruptive events as they occur.

ISO 27001: This is the international standard for information security management. It helps organizations manage the security of their information assets, such as financial information, intellectual property, employee data, or information entrusted by third parties.

ISO 31000: This is the international standard for risk management. It provides principles and guidelines for effective risk management in any organization, regardless of size, activity, or sector.

ISO 22316: This is the international standard for organizational resilience. It provides guidance on how to improve an organization's resilience by increasing its ability to respond to, and adapt to, changes and disruptions.

ISO 22320: This is the international standard for emergency management. It provides incident response guidance, including aspects of planning, setting up, leading, coordinating, executing, ending, and evaluating an incident.

3.5. Contribution by Security Risk Management to support the steps that help to enable resilience within the organization

Security Risk Management can support the steps to enable resilience within the organization by helping to create a mindset that building resilience cannot be assumed to be a one-time effort. Resilience is a moving target, ever-changing in response to the changing requirements of the context in which the organization works and the changing conditions it faces concerning its EOs. In supporting the mindset towards resilience, Security Risk Management can apply the 6 steps below and the questions that go with it (Table 5).

Therefore an answer to the management in this case can be to follow the steps below, which are necessary to enable organizational resilience in a progressive way. Following these steps can help in building the capacity for agility, adaptation, learning, and regeneration to ensure that the organization is able to deal with more complex and severe events (such as a pandemic, climate change, or cyber-attacks) and is fitter for the future.

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?	

Table 5. Steps that help to enable resilience within the organization

References

1. Adaptive leadership: Stress-Test Your Strategy: The 7 Questions to Ask (hbr.org) / Accessed 11072024
2. Design thinking: Design thinking, explained | MIT Sloan / Accessed 11072024
3. ISO 22301: ISO 22301:2019 - Security and resilience — Business continuity management systems — Requirements / Accessed 11072024
4. ISO 22316: ISO 22316 Security and Resilience | BSI Middle East and Africa (bsigroup.com) / Accessed 11072024
5. ISO 22320: ISO 22320:2018 - Security and resilience — Emergency management — Guidelines for incident management / Accessed 11072024
6. ISO 27001: What is ISO 27001? A detailed and straightforward guide (advisera.com) / Accessed 11072024
7. ISO 31000: ISO - ISO 31000 — Risk management / Accessed 11072024
8. Journey mapping: Journey mapping 101: What it is and why it's important | Valtech / Accessed 11072024
9. Lessons learned: Triple Loop Learning - NPC (thinknpc.org) / Accessed 11072024
10. (Service) blueprinting: Service Blueprints: Definition (nngroup.com) / Accessed 11072024
11. Stress test: Stress-Test Your Strategy: The 7 Questions to Ask (hbr.org) / Accessed 11072024
12. The five capitals model: The Five Capitals - a framework for sustainability | Forum for the Future / Accessed: 11072024
13. Why Organizations Need to Measure Resilience: https://www.rmmagazine.com/articles/article/2024/07/09/why-organizations-need-to-measure-resilience / Accessed: 11072024

13. AI SECURITY CHALLENGE AND RISK ASSESSMENT USING ISO 31000: THE IOTSI GUIDANCE

Rita Lankauskienė/ Kazimieras Simonavicius University, Lithuania /2024

ABSTRACT

The expansion of generative Artificial Intelligence (AI) technologies across various sectors presents substantial advantages while simultaneously posing intricate security challenges. Managing these risks effectively is essential for maintaining the integrity, reliability, and safety of AI systems. The ISO 31000 standard offers a systematic methodology for risk management that may be tailored to the particular requirements of AI security. This article outlines the emerging cyber security issues with AI challenges at the forefront, which occur due to the unpredictably rapid expansion of the Internet of Things (IoT) industry, accelerated by digital transformation. Based on the Internet of Things Security Institute's (IoTSI) best practice, a step-by-step explanation is given of how to empower the ISO 31000 standard in an AI security risk assessment, encompassing comprehensive methods, technical analysis, and illustrative examples.

Link to ISO 31000

This article explores the application of the ISO 31000 standard systematic methodology and process framework for generative Artificial Intelligence (AI) Security Risk Assessment in organizations.

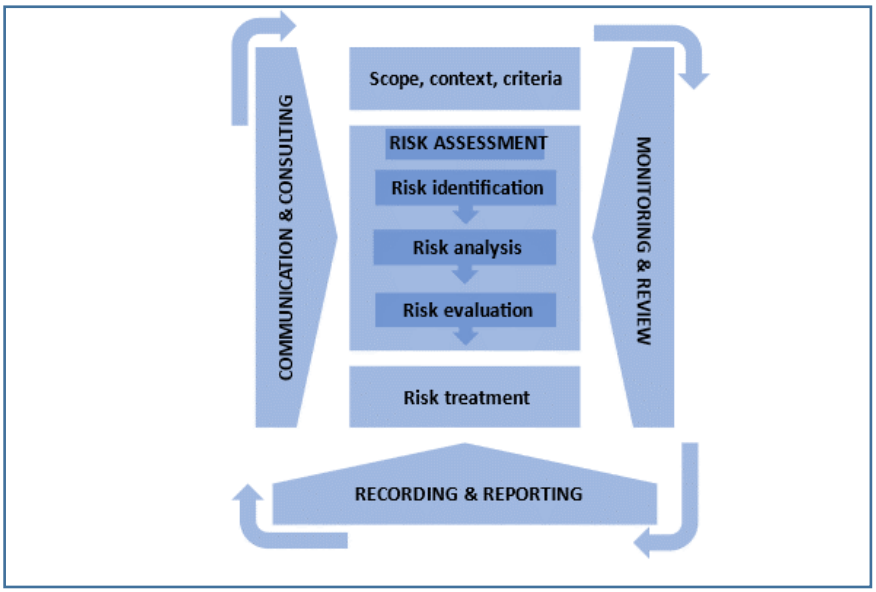


Figure 20. Risk management process according to ISO 31000:2018

1. Introduction

Emerging technologies with generative Artificial Intelligence (AI) at the forefront have widely become recognized as significant catalysts for digital transformation and innovation worldwide (Thorat et al., 2024). Plenty of evidence is collected proving the tremendous benefits, gathered from the numerous applications of different AI tools in different spheres of human activity and technological developments (e.g., Ghobakhloo et al., 2024; Kanbach et al., 2024; Sedkaoui & Benaichouba, 2024, etc.).

The swift development of AI technology and the widespread use of creative AI solutions lead to the rapid emergence of new risk types, which further increases the unpredictability of the already complex procedures involved in AI creation and implementation (Golpayegani et al., 2022). The increasing number of incidents (AI Incident Database, 2024; AIAAIC, 2024) brought on by the (mis)use of AI increasingly bothers a broad range of stakeholders from the general public, organizations, and governments at different – national, international, and global levels (Herani & Angela, 2024).

Numerous initiatives are being undertaken internationally, as well as globally to limit the negative effects of AI, ranging from standards for risk management and regulatory frameworks to guidelines encouraging reliable development and use. Among the most relevant recently issued regulatory frameworks in Europe is the European Commission's Artificial Intelligence Act (AI Act, 2019). The AI Act (2019) is the world's first all-encompassing legal framework around AI. The regulations seek to promote trustworthy AI in Europe and beyond, aiming to guarantee that AI systems adhere to fundamental rights, safety, and ethical standards, and addressing the risks associated with extremely potent and significant AI models.

The core premise behind the AI Act (2019) is that it guarantees Europeans confidence in the potential of AI. Certain AI systems present risks that should be managed to prevent unfavorable consequences, even if the majority of AI systems are low- to non-risk and can help solve many social issues. For instance, it is frequently impossible to determine the rationale behind an AI system's decision, forecast, or action. Therefore, determining whether someone has been unfairly disadvantaged - for example, in an employment decision or during an application for a public benefit program - may become challenging.

Even if current laws offer some protection, they are not enough to handle the unique difficulties that AI systems can present. The AI Act is well-known because it regulates the development and application of AI in systems in a risk-oriented manner. By implementing a risk management system for risk detection, analysis, evaluation, and treatment, risk management practices seek to handle core uncertainties. In this case, the uncertainties of AI systems and their dangers are to be handled following ISO risk management standards. There is collected evidence on how the safe and reliable development and use of AI systems depend on the proper implementation of ISO 31000 in any entity‘s risk management activities.

The ISO 31000 series of standards offers actions, guidelines, and principles to help organizations manage risk. The primary standard that offers general guidelines, a framework, and procedures for handling risks that organizations encounter during their lifecycle is ISO 31000:2018 Risk Management - Guidelines. Another relevant member of this family is ISO 31073:2022 Risk Management – Vocabulary (2022), which enables a common understanding across various business units and organizations, ISO 31073:2022 offers a list of general terms in risk management together with their meanings.

This article presents guidance on best practise, developed by the Internet of Things Security Institute (IoTSI), on how to implement a step-by-step AI security risk assessment procedure in an organization, using the ISO31000 framework.

2. Case

Digital transformation results appear in the unpredictably rapid expansion of the Internet of Things (IoT) industry. More and more devices becoming connected and providing new features and increased convenience in both the personal and professional spheres. According to the IoT Analytics' data (2024), by the end of 2023, 16.6 billion IoT devices were connected, and it was a 15% increase over 2022. And by the end of 2024, IoT Analytics (2024) projects that this will have increased by 13% to 18.8 billion, and will keep increasing further (see figure 21).

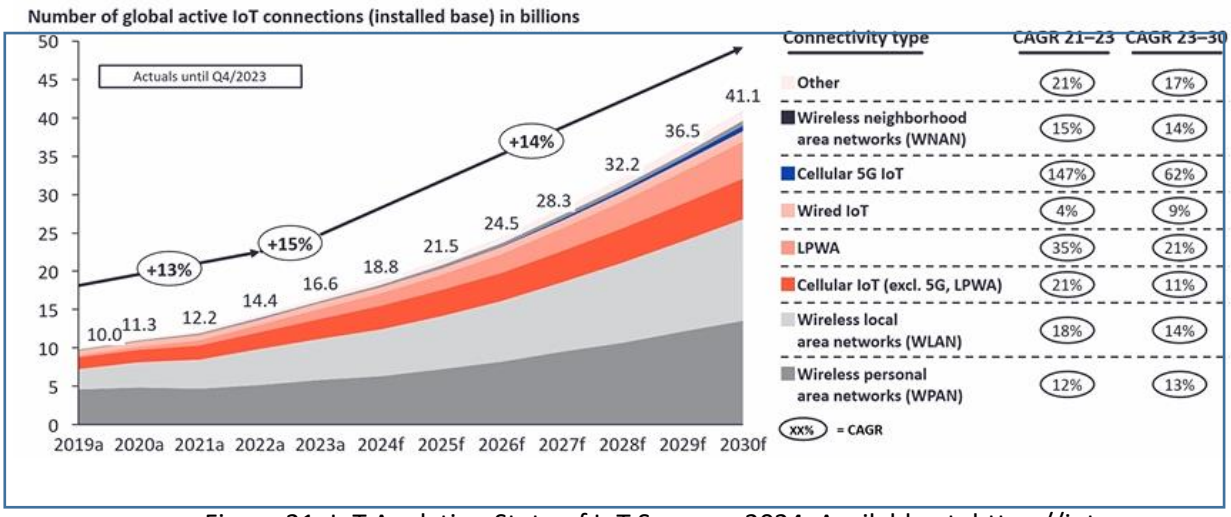
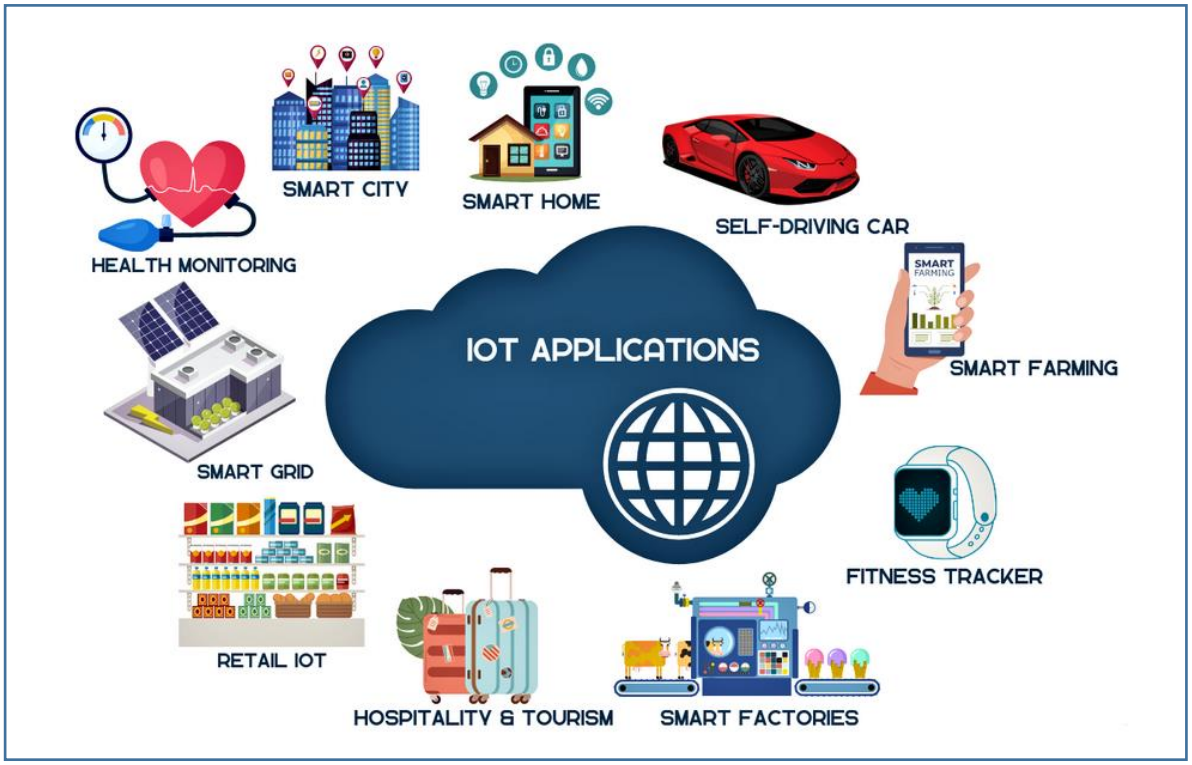


Figure 21. IoT Analytics, State of IoT Summer 2024. Available at: https://iot-analytics.com/product/state-of-iot-summer-2024/

Alongside the growing number of IoT devices and systems, their complexity and sophistication are also rising, offering numerous advantages to a wide range of sectors, such as manufacturing, healthcare, smart cities, home automation, and many more (see picture 4).



Picture 4. Internet of Things (IoT) applications' areas - AI security challenge. Source: Techjury.net, 2024.Available at: https://techjury.net/blog/internet-of-things-statistics/

At the same time, IoT application areas and the widespread adoption of AI technology in many sectors yield substantial advantages while simultaneously presenting intricate security issues. According to the best practice in the field, the above-outlined security issues are successfully manageable following the principles embedded in the ISO 31000 standards' family.

Due to the increasing complexity of the issue, a particular academic and cyber industry think tank has been established - the Internet of Things Security Institute (IoTSI, 2024). IoTSI is focused on delivering security frameworks, instructional resources, and cybersecurity courses to facilitate the best practices in the management of security in Smart Tech, IoT (Internet of Things), and IIoT (Intelligent Internet of Things) ecosystems.

IoTSI suggests using the ISO 31000 standard's systematic framework for risk management, which may be well tailored to the particular requirements of AI security. It is further described in detail, how to apply the ISO 31000-based methodology for an AI security risk assessment, encompassing comprehensive methods, technical analysis, and illustrative examples.

3. Best practices

ISO 31000 is an international standard that establishes risk management guidelines to guarantee that risks are managed consistently and systematically at all organizational levels (ISO31000:2018). It comprises three primary elements: 1) principles, 2) framework, and 3) process. The framework provides the structural elements for implementation, the principles ensure that risk management is a component of decision-making and adds value, and the process entails steps for identifying, assessing, and mitigating risks.

According to IoTSI guidance, an AI security risk assessment, using ISO 31000, is a step-by-step procedure, which consists of several complementary steps (see figure 22).

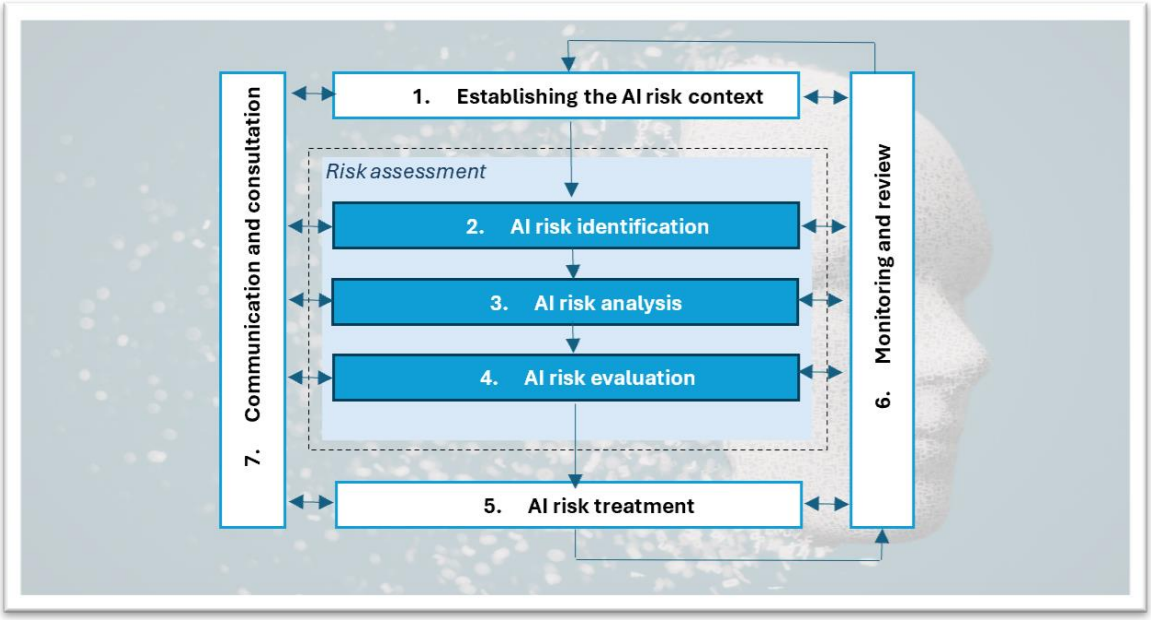


Figure 22. AI security risk assessment, using ISO 31000. Source: Adapted from IoTSI guidance (2024).

3.1. Establishing the context

The foundational step in the ISO 31000 process is the establishment of context, which provides the necessary background to comprehend the environment in which the AI system operates. It is necessary to consider the environment from the two core contexts: external and internal.

While establishing the internal context, it is necessary to focus on the 3 core things:

1) Regulatory landscape - find the rules and laws that relate to data handling, privacy, and security, such as GDPR, CCPA, and HIPAA. As an example, GDPR rules must be followed by any AI system that handles personal data in the EU.
2) Market and technological trends - learn about the changes in the market and in technology that might affect the security of the AI system. For instance, if adversarial attack methods get better, defenses may need to be updated.
3) Threat landscape - look at the current danger landscape. This should include known cyber threats that target AI systems, like data poisoning or model inversion attacks.

The external context refers to the following core themes:

1) Organizational structure - explain who is responsible for what when it comes to managing and protecting AI systems. Find the important people, like IT, legal, safety, and business units.
2) Risk management policies - check the current risk management policies to see if they match the risks that come with AI and the ISO 31000 rules.
3) Risk Appetite and Tolerance - name the company's risk appetite and tolerance levels, especially when it comes to system security, data breaches, and theft of intellectual property.

Once the environmental context is established, it is necessary to define the risk criteria. You should come up with specific ways to judge risks. For example, you may first define the impact metrics, such as financial loss, reputational damage, operational disruption, and legal consequences. Then consider the likelihood metrics, including frequency of threat occurrence, vulnerability exploitability, and control effectiveness. And finally, it is necessary to establish risk categorization i.e., low, medium, and high, based on the above – their impact and likelihood.

3.2. AI Risk Assessment Procedure

The next step is AI Risk Assessment (see picture 2), which is composed of several components. ISO 31000 lists three main components for assessing risk: risk identification, risk analysis, and risk evaluation. The goal of this part is to fully understand all the possible threats and weak spots in the AI system.

3.2.1. AI risk identification

In the risk identification phase, it is necessary to consider all potential sources of risk, including data risks, model risks, and operational risks.

Data risks consist of data breaches, data poisoning, and data integrity. Data breaches are related to unauthorized access to private or secret data, which could result in fines and a loss of trust. Data poisoning is hacking training data to change how an AI model acts in a bad way. For example, changing how accurate a spam blocker is by adding false data to its training set. Data integrity are risks that come from the correctness and thoroughness of the data, which can affect how well and reliably the AI model works.

Model risks entail adversarial attacks, model stealing, and model bias. The adversarial attacks cause changes to input data that are meant to trick the AI model, like changing pictures to force an image recognition system to make wrong decisions. Model stealing occurs when hackers can get into the structure or settings of an AI model without permission, which can lead to theft of intellectual

property or the creation of competing models. Model bias becomes relevant since AI models can have unintended biases that can lead to unfair results. This is especially important in sensitive areas like loans or hiring.

Operational risks overwhelm system failures, security configuration, and third-party risks. System failures come with hardware or software problems that can stop an AI system from working. Security configuration causes problems with the AI system's security, like not enough access controls or gaps that haven't been fixed, which can let attackers in. Finally, third-party risks come from sellers or third-party services, like cloud providers, which can make data less safe and systems less available.

3.2.2. AI risk analysis

The essence of risk analysis is to look carefully at each risk you've found in the previous stage, to learn what it is, how it might affect you, and how likely it is to happen, i.e. perform an impact assessment and likelihood assessment. It is advised by best IoTSI practice to find out about risks by using both numeric and qualitative methods.

During the impact assessment, first consider the financial impact by figuring out how much data breaches could cost in terms of fines, court fees, and fixing problems. Then consider operational impacts, i.e., think about how system downtime, loss of usefulness, and changes to business processes might affect things. And finally analyze reputational impact, considering how this will affect the company's reputation, customer trust, and position in the market over the long run.

In the likelihood assessment, first, consider the historical data, by looking at past events and weaknesses to figure out how likely it is that they will happen again. Then perform the vulnerability analysis by assessing the AI system’s exposure to identified threats, considering factors like the system’s complexity and the robustness of existing security measures. And finally, analyze threat actor capability, i.e., evaluate the capability and motivation of potential attackers, such as hackers, malicious insiders, or competitors.

For example, to assess the danger of adversarial assaults on sensor data in an AI-based autonomous car system, take into account the impact on passenger safety and system reliability.

3.2.3. AI risk evaluation

The following risk evaluation procedure is implemented by ranking the risks and comparing the ones that have been studied to the set standards for risks. This helps decide where to put resources and what risks are the most important.

IoTSI best practices advice using the risk matrix for sorting the risks into groups based on how likely they are to happen and how bad they could be. This visual tool helps you put risks in order of importance and make smart choices about how to treat risks. The decision-making will be more effective by getting everyone involved in figuring out what amounts of risk are acceptable and how to prioritize risks. When making decisions, people may have to weigh the costs and benefits of reducing danger.

3.3. Risk Treatment

Risk treatment is the process of choosing and putting into action ways to change dangers. ISO 31000 says that this can mean avoiding, transferring, reducing, or taking risks.

To manage the process, it is necessary to develop risk treatment plans. A thorough risk treatment plan should be developed for each significant risk. From the best practices, each plan should define the objective, actions, and resources and allocate responsibilities. The objective must define clearly what a particular treatment is supposed to do, like lowering the risk of data leaks or weakening

the effects of hostile attacks. The actions must be specified to tell the people what they need to do, like putting in place multi-factor login, encrypting data, or doing regular security checks. It is necessary to equip the risk treatment measures with reasonable resources, staff, and technology they need to be put into action. And finally, every plan must clearly assign responsibilities for executing the treatment plan, ensuring accountability and oversight.

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.

The next step of risk treatment plan implementation entails putting the risk treatment steps into action and making sure they are part of how the organization works and how it is managed. Technical controls usually are performed by using high-tech security tools like encryption, firewalls, intrusion detection systems, and programs that look for strange behavior. Procedural controls are ensured by setting up or improving processes for managing data, controlling who can see it, and responding to incidents. For example, setting up a way to check for and update security patches daily. And organizational controls are devoted to creating a mindset of security awareness through training programs, campaigns, and making sure that the IT and business units work together.

Risk treatment plan implementation example: establishing a zero-trust security framework for an AI-driven cloud service, incorporating stringent access limits, ongoing surveillance, and thorough audit trails.

3.4. Monitoring and review

Regular reviews and ongoing monitoring are necessary to make sure that risk management methods keep working and adapt to new risks.

First, best practice highlight the necessity of establishing a way to keep an eye on the AI system and its surroundings all the time so that you can quickly spot and deal with new risks. Security Information and Event Management (SIEM) solutions are used to gather and study data about security, sending alerts in real-time for possible security incidents. Another essential part is the model monitoring to continuously monitor the performance of the AI model all the time, aiming to find strange things, like output patterns that don't make sense, which could be a sign of an attack or model change. Finally, incident management is used for setting incident response plans with roles, communication channels, and recovery steps to deal with security incidents quickly.

Continuous monitoring example: using AI-based monitoring tools to find strange trends of data access in a financial AI system could mean that there are threats from inside the company or outside the company.

To ensure a well-running monitoring system, periodic reviews are necessary. The best practice advice is to review the treatment plans and risk management process often to make sure they are still useful and effective. This is performed by internal audits, scenario analysis, and stakeholder engagement. It is advised to do internal audits to see if risk management methods are adequate and working well. This includes checking to see if the rules and policies of the company are being followed. Scenario analysis is useful when testing how well the AI system can handle made-up threats like a coordinated cyberattack or a big data breach, you should do scenario analysis. Stakeholder engagement is helpful for reviews: talking to stakeholders helps reconsider the results of risk management, make changes to risk factors, and improve plans for risk treatment.

Periodic review example: evaluating and revising the risk evaluation of an AI-driven healthcare diagnostic instrument following recent regulatory directives regarding patient data privacy.

3.5. Communication and consultation

Effective communication and consultation are essential components of the ISO 31000 process, guaranteeing transparency and stakeholder engagement. The best practice in the field takes into account both internal and external communication.

Internal communication deals with risk management actions and results, that should be shared regularly with all internal stakeholders that need to know, such as the board of directors, management, and operational staff. Reporting is necessary for giving thorough reports on incidents, risk assessments, and efforts to lower risks. It advised to include important metrics like the level of risk, how well the controls are working, and the state of compliance. And finally, internal communication is concerned with training and awareness. It is necessary to teach the staff regularly about best practices for security, new threats, and how they can help control risk.

Internal communication example: holding meetings for engineers and data scientists to talk about safe ways to build AI and how important it is to think about data quality and ethics.

External communication is used to tell outside groups, like customers, partners, and regulatory bodies, about the efforts to handle risks and follow the rules. It is important to consider the transparency principle, i.e., be clear about the AI system's security measures, especially when it comes to privacy and data protection. Another important part is reporting incidents. It is necessary to establish rules for telling regulators and people touched by security incidents about them, making sure that the information is given correctly and on time.

External communication example: after a security breach in a consumer app driven by AI, a public statement should be made explaining the steps that were taken to protect user data and stop future breaches.

3.6. Recording and reporting

For accountability, openness, and constant growth, it's important to keep detailed records and reports. Documentation is the first important component of this. Best practices advise to write down everything that you do during the risk management process, such as finding risks, analyzing them, making treatment plans, and keeping an eye on things. To create records management, it is necessary to set up a method for managing records to store and organize paperwork so that it is easy to find and that you are following the law. Audit trails are applied to maintain full records of all risk management activities, such as choices made, actions taken, and results reached so that they can be easily checked.

Documentation example: develop comprehensive documentation of a risk assessment procedure for an AI system, encompassing data sources, risk criteria, analytical methods, and mitigation options.

Reporting is based on preparing regular reports: periodic reports and compliance reports. They are used to inform stakeholders about the status of AI security risk management. It is advised to produce regular periodic reports that summarize the most important risks, how they are being managed, and security events, including measurements and trends to get a full picture of the risk exposure. Compliance reports help ensure that you follow all the rules and laws that apply by writing reports that show you did so, like data security rules.

Reporting example: generating a yearly risk management report for an AI-driven financial system, emphasizing significant risks, the efficacy of controls, and opportunities for enhancement.

Summing up, the best practice, proposed by IoTSI for conducting AI security risk assessment using ISO 31000, is worth applying for several reasons. The ISO 31000 framework offers a

comprehensive and methodical strategy for addressing the distinct security threats linked to AI systems. Organizations can reduce possible dangers, guarantee regulatory compliance, and protect their AI assets by adhering to a disciplined approach that includes establishing context, conducting risk assessments, executing treatment plans, and regularly monitoring and reviewing. Efficient communication and comprehensive documentation enhance transparency, accountability, and ongoing enhancement in AI security risk management. As AI technologies and their associated risks develop, it will be imperative for enterprises to implement a comprehensive risk management framework such as ISO 31000 to effectively navigate the intricate environment of AI security.

References

1. AI Act (2019). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689.
2. AI Incident Database (2024). Available at: https://incidentdatabase.ai/.
3. AIAAIC - AI, Algorithmic and Automation Incident and Controversy Repository (2024). Available at: https://www.aiaaic.org/home.
4. 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.
5. Ghobakhloo, M., Fathi, M., Iranmanesh, M., Vilkas, M., Grybauskas, A., & Amran, A. (2024). Generative artificial intelligence in manufacturing: opportunities for actualizing Industry 5.0 sustainability goals. *Journal of Manufacturing Technology Management*, *35*(9), 94-121.
6. Golpayegani, D., Pandit, H. J., & Lewis, D. (2022). Airo: An ontology for representing AI risks based on the proposed EU AI act and ISO Risk management standards. In *Towards a Knowledge-Aware AI* (pp. 51-65). IOS Press.
7. Herani, R., & Angela, J. (2024). Navigating ChatGPT: catalyst or challenge for Indonesian youth in digital entrepreneurship?. *Journal of Entrepreneurship in Emerging Economies*. Vol. ahead-of-print No. ahead-of-print. Available at: https://doi.org/10.1108/JEEE-05-2024-0181.
8. IoT Analytics. State of IoT, Summer 2024. Market Report. Available at: https://iot-analytics.com/product/state-of-iot-summer-2024/.
9. IoTSI (Internet of Things Security Institute) (2024). Available at: https://iotsecurityinstitute.com/iotsec/index.php/about.
10. ISO 31000:2018. Risk management – Guidelines (2018). Available at: https://www.iso.org/obp/ui/en/#iso:std:iso:31000:ed-2:v1:en .
11. ISO 31073:2022 Risk Management – Vocabulary (2022). Available at: https://www.iso.org/obp/ui/en/.
12. Kanbach, D. K., Heiduk, L., Blueher, G., Schreiter, M., & Lahmann, A. (2024). The GenAI is out of the bottle: generative artificial intelligence from a business model innovation perspective. *Review of Managerial Science*, *18*(4), 1189-1220.
13. Petrov Ch. (2024). 26 Insightful Internet of Things Statistics 2024. Techjury.net. Available at: https://techjury.net/blog/internet-of-things-statistics/.
14. Sedkaoui, S., & Benaichouba, R. (2024). Generative AI as a transformative force for innovation: a review of opportunities, applications and challenges. *European Journal of Innovation Management*, Vol. ahead-of-print No. ahead-of-print. Available at: https://doi.org/10.1108/EJIM-02-2024-0129.
15. Thorat, S. R., Tingare, B. A., Deshmukh, S. R., Dabhade, V. D., William, P., Rakshe, D. S., & Verma, A. (2024). Analysis Of Generative Ai's Impact On Industry 4.0 And Digital Transformation. *Library Progress International*, *44*(3), 13379-13390.