PUBLICATIONS OF THE HAZARD PROJECT
30:2019

HAZARD Seaport Risk Assessment Toolbox

Ayman Nagi
Abir Bouraffa
Wolfgang Kersten

EU Strategy for the Baltic Sea Region Flagship
Interreg Baltic Sea Region
European Union – European Regional Development Fund
HAZARD

30:2019

HAZARD Seaport Risk Assessment Toolbox

Ayman Nagi
Abir Bouraffa
Wolfgang Kersten

Turku 2019

ISBN 978-951-29-7654-6

2019

PUBLISHED BY:
HAZARD Project
Turku School of Economics
University of Turku
Rehtorinpellonkatu 3, FI-20014 University of Turku, Finland
http://blogit.utu.fi/hazard/

This publication has been produced with the financial assistance of the European Union. The content of this publication is the sole responsibility of the publisher and under no circumstances can be regarded as reflecting the position of the European Union.

The content of this publication reflects the authors views. The Investitionsbank Schleswig-Holstein is not liable for any use that may be made of the information contained herein.

Photo credits for the cover: Mr. Esko Keski-Oja, Finland

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

Seaports are confronted with risks that may affect the operational, economic and technical dimensions. The types of safety, operational and environmental risks include, for example, leakages of hazardous materials, fires on passenger ships at port, oil spills in port areas as well as explosions of gases or chemicals.

To mitigate the effects of this type of incidents, the HAZARD Project has been running in 2016-2019 to improve the current status of risk management at Baltic Sea Region (BSR) major seaports. A core part of risk management is the identification, analysis and evaluation of risks (See: https://blogit.utu.fi/hazard/). Project HAZARD has been co-funded by EU's BSR Interreg Programme.

Work package 4 of HAZARD, led by Hamburg University of Technology has aimed firstly to analyse the current state of risk assessment in seaports using a comprehensive interview study. The study revealed that there is no standard implemented process for risk assessment. Additionally, stakeholders at the interviewed BSR major seaports use different methods for the identification, analysis and evaluation of risks.

Therefore, it is necessary to install a proper standard risk management process with suitable understandable methods that can be used to proactively identify, analyse and evaluate different sources of risks at seaports. The applicable methods, from the interview study and the cooperation with the OpenRisk[1] Project, have been integrated in the online Toolbox. The other methods have been extracted from a comprehensive literature review for risk assessment methods in seaports.

The **HAZARD Seaport Risk Assessment Toolbox** (available online at: https://hazard.logu.tuhh.de/), enables the selection of suitable risk assessment methods that could be applied in seaports. Different workshops were carried out among the project partners to validate the successful applicability and usability of this Toolbox. This dynamic Toolbox enables its users to suggest new methods or update the current content, which facilitates a continuous improvement process that is necessary when working with emerging risks.

The selected methods for risk assessment are briefly described with regards to their usage and application. The methods are explained with practical examples that can be used by stakeholders to make the process of risk assessment understandable. The detailed description of each method can be viewed as a method card in the online Toolbox. The user guide for the online Toolbox integrated in this guideline elaborates the whole process of risk assessment with screenshots and clear steps.

This report is structured as following. Section 2 presents the methodology used to develop the online Toolbox. Section 3 describes the extracted requirements for the online Toolbox from the

[1] Maritime risk assessment on accidental spills

point view of port operators and rescue services. Section 4 presents the structure of risk categories that are integrated within the Toolbox. Section 5 briefly describes selected risk assessment methods and their main properties. Section 6 elaborates on the structure and design of the Toolbox. Section 7 presents the user manual for the online Toolbox. Finally, section 8 summarises the reasons behind the development, the operational principles and the capabilities of the Toolbox.

2 METHODOLOGY

The **HAZARD Seaport Risk Assessment Toolbox** is developed based on a comprehensive literature and interview studies to examine the different categories of risks and methods for risk assessment in seaports. **Figure 1** displays the chosen approach on how the Toolbox was developed and validated.

Requirements for the development of the online Toolbox were gathered in two HAZARD workshops with different stakeholder categories from major BSR seaports. Focus groups and exercises aimed at gathering the essential requirements for rescue services, academia and seaport operators.

The risk assessment methods were then extracted from comprehensive literature review and interview studies. These methods were analysed and evaluated in a co-operation meeting with rescue service, authorities and knowledge partners. This was in order to examine the degree of applicability linked to the phases of the risk assessment process according to ISO 31000:2018. The process, as aforementioned, comprise identification, analysis and evaluation.

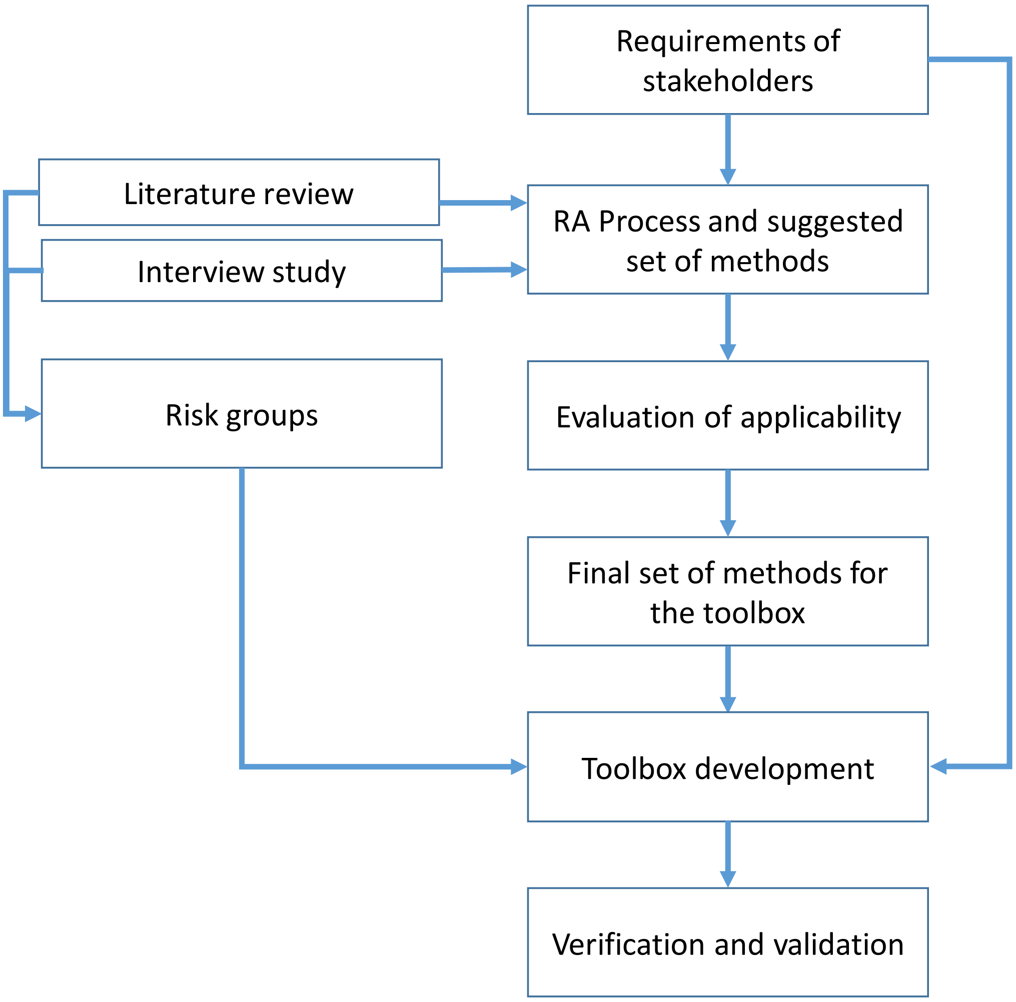


Figure 1*: Approach to develop the online HAZARD Seaport Risk Assessment Toolbox*

Based on the analysis and evaluation, the final set of methods for the Toolbox were selected. One of the most important properties of the Toolbox is the dynamic addition of new methods for risk assessment. The methods described in this guideline can be considered to be the initial set for the online Toolbox.

The risk groups are an essential element of the Toolbox. Each selected risk assessment method can be linked to one of the risk groups in seaports e.g. to operational and environmental risks. A breakdown structure for the risk groups is used to enable a smooth selection and extension of risks. The risk groups, subgroups and their associated examples were extracted from the HAZARD literature and interview studies.

Based on the requirements, selected risk assessment methods and risk groups, the online Toolbox was developed using Drupal content management framework that enables an efficient development process for the further extension and development of the online Toolbox. In order to help the users in the usage of the Toolbox, a user guide with clear step and screenshots is provided.

Initial tests were carried out utilising a co-operation meeting with other Project Partners (PPs) to verify and validate the online Toolbox and extract additional requirements for further refinement of the content, design and properties. The participants represented different stakeholder categories including authorities, terminal operators and knowledge partners from the participating BSR countries. The next section presents the extracted requirements of stakeholders.

3 REQUIREMENTS OF STAKEHOLDERS

It is essential for any project to determine the essential requirements of the core stakeholders that will use the created solutions and suggestions for risk assessment in seaports.

Work package 4 (WP4) organised a workshop in November 2016 in Hamburg, Germany to gather important requirements of port operators, knowledge partners and rescue services regarding the development of the HAZARD Seaport Risk Assessment Toolbox. Such workshops enable WP4 to determine the requirements and specifications for the online Toolbox. Therefore, co-operation among Work packages and Partners of HAZARD is essential to ensure a better understanding, successful support and application of risk assessment methods in order to improve the current status of risk management process in BSR seaports.

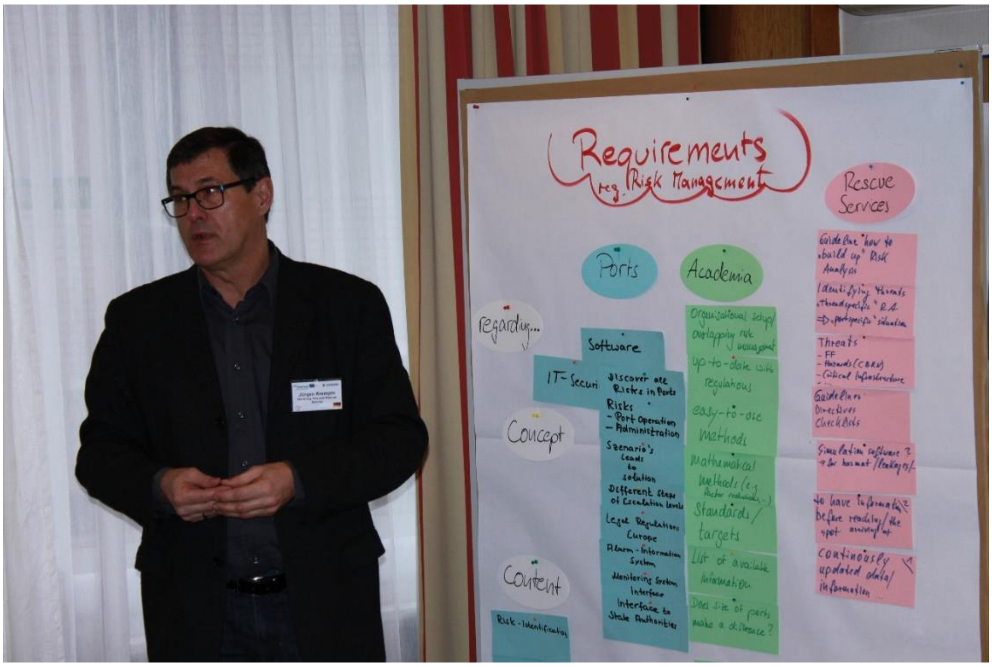


Figure 2: *HAZARD workshop to extract the requirements of stakeholders*

The following requirements have been considered in the development of the Toolbox:

1) **Guideline on how to perform a risk analysis**: the principles, framework and process of ISO 31000 with the associated risk assessment methods and risks would enable stakeholders to perform risk analysis according to their requirements

2) **Identifying threats and hazards**: several methods for risk assessment provide a comprehensive identification of possible threats and hazard sources that could trigger a top event (risk)

3) **Simulation software for hazmat and leakages**: simulation methods are integrated in the Toolbox to enable accurate quantitative analyses of spills and leakages of oil and hazardous materials

4) **Proactive risk management approach**: the process and methods for risk assessment enable the early identification of the causes and consequences of risks in order to define appropriate measures to prevent the occurrence of risks or mitigate the severity of consequences

5) **Dynamic and continuously updated**: one of the most important properties of the online Toolbox is its dynamic behaviour that enable a continuous improvement process by adding risks and methods for risk assessment

6) **Including guidelines, directives and checklists**: the Toolbox is accompanied with clear guideline and user manual to provide clear steps to identify, analyse and evaluate risks that could occur at seaports

The extracted methods for risk assessment were also evaluated in April 2018 in Klaipeda, Lithuania during a co-operation meeting with the other project stakeholders including rescue services and knowledge partners from Estonia, Finland, Germany and Lithuania. The evaluation process was based on the phases of risk assessment process and properties of each method. Each group during the workshop analysed the applicability, complexity and the effort of each risk assessment method. The final set of method along with their properties were integrated to the online Toolbox.

Figure 3: *HAZARD workshop to evaluate the RA methods*

Next section presents the risk groups and the associated breakdown structure that are linked with the risk assessment methods.

4 RISK GROUPS

Risk sources identification is one important step that must be followed in order to effectively assess potential risks in seaports. If a risk source is somehow missed, overlooked or underestimated it might likely produce an inadequate expected top event. This is a reason why it is extremely important to create a comprehensive list of foreseeable risk sources. This is particularly crucial regarding seaports or similar infrastructures as these are important systems, where a series of accidents or catastrophic events could endanger life or the well-being of people and organisations (Nagi et al. 2018).

In port facilities, there are many known and unknown risk sources; the aim was to classify them in an effective and understandable manner, and thus two terms were selected: natural or man-made risk sources (Birkmann 2011; John et al. 2016). Important to mention is that these terms have been successfully used in other transport infrastructures.

Natural risk sources are ordinary occurring processes (Schmidt et al. 2011) which exist in the natural environment (Kaundinya et al. 2016). These risks possess a threat to societies and organisations as they occur due to uncontrollable changes in the physiognomies of the planet such as hydrological, meteorological, seismic, geologic, volcanic or mass movement variations (Kaundinya et al. 2016). For instance, in the past years the world has experienced extremely dangerous natural disasters including tsunamis, hurricanes, and earthquakes (Zhou et al. 2010). Seaports or similar organisations are extremely vulnerable to these risk sources due to their critical location (Yang et al. 2010). These environmental changes have a great potential to cause a negative impact on humans working in ports, in the community and in the related activities or groups.

Unlike natural risk sources, man-made sources are intentional or unintentional actions that have a potential to cause harm to people or organisations (Kaundinya et al. 2016). John et al. (2014) also discussed some of the risk sources related to these type of top events—they, for example, mentioned that the handling of hazardous cargo could lead to cargo spillages. Also, vulnerabilities in port control systems or in critical databases could potentially lead to cyber- or terrorism attacks (John et al. 2014; Polatidis et al. 2018).

For the development of the Toolbox, a three-level categorisation was followed to enable a dynamic extension of possible risks. The risk groups comprise natural disasters, operational, safety, organisational, environmental, as well as technical and technological risks. **Table 1** provides a brief description of each risk group.

Table 1: *Main risk groups (Own illustration)*

Risk group	**Description**
Natural disasters	Natural disaster is a natural change in the Earth's surface or atmosphere potentially having devastating effects.
Operational risks	Operational risks are related to the occurrence of unexpected events or accidents disturbing the flow of routinely conducted operations.
Safety risks	Safety risks are closely related to the continual compliance and monitoring of enforced safety regulations.
Technical and technological risks	Technological risks are related to the potential failure of devices, machinery and the corresponding IT software.
Organisational risks	Organisational risks are related to inadequate or failed internal processes, people and systems.
Environmental risks	Environmental risks are related to potential threats of diverse sources affecting organisms and environment by emissions, leakages etc.

Each risk group has its corresponding risk subgroups. Natural disasters at seaports have three risk subgroups: geophysical, hydrological and meteorological risks. Geophysical risks are associated with the physical properties and processes of the Earth. Hydrological risks are caused by hydrological (i.e. water) processes. Meteorological risks are caused by extreme weather conditions.

Operational risks have two risk sub-groups: containers and dangerous goods. The former represents risks connected to the different operational processes of containers at seaports. The latter represents risks connected to the different operational processes of dangerous goods at seaports.

Safety risks have two risk sub-groups: spills and leakages as well as work-related risks. The former represents risks that are associated with the spills and leakages of oil, gas and other hazardous materials. The latter represents risks that could cause potential danger to the safety of workers at seaports.

Technical and technological risks have two risk sub-groups: machinery and devices as well as software. The former represents risks that could cause harmful failure to essential machinery and devices at seaports. The latter presents risks that can lead to the failure or manipulation of essential software at seaports.

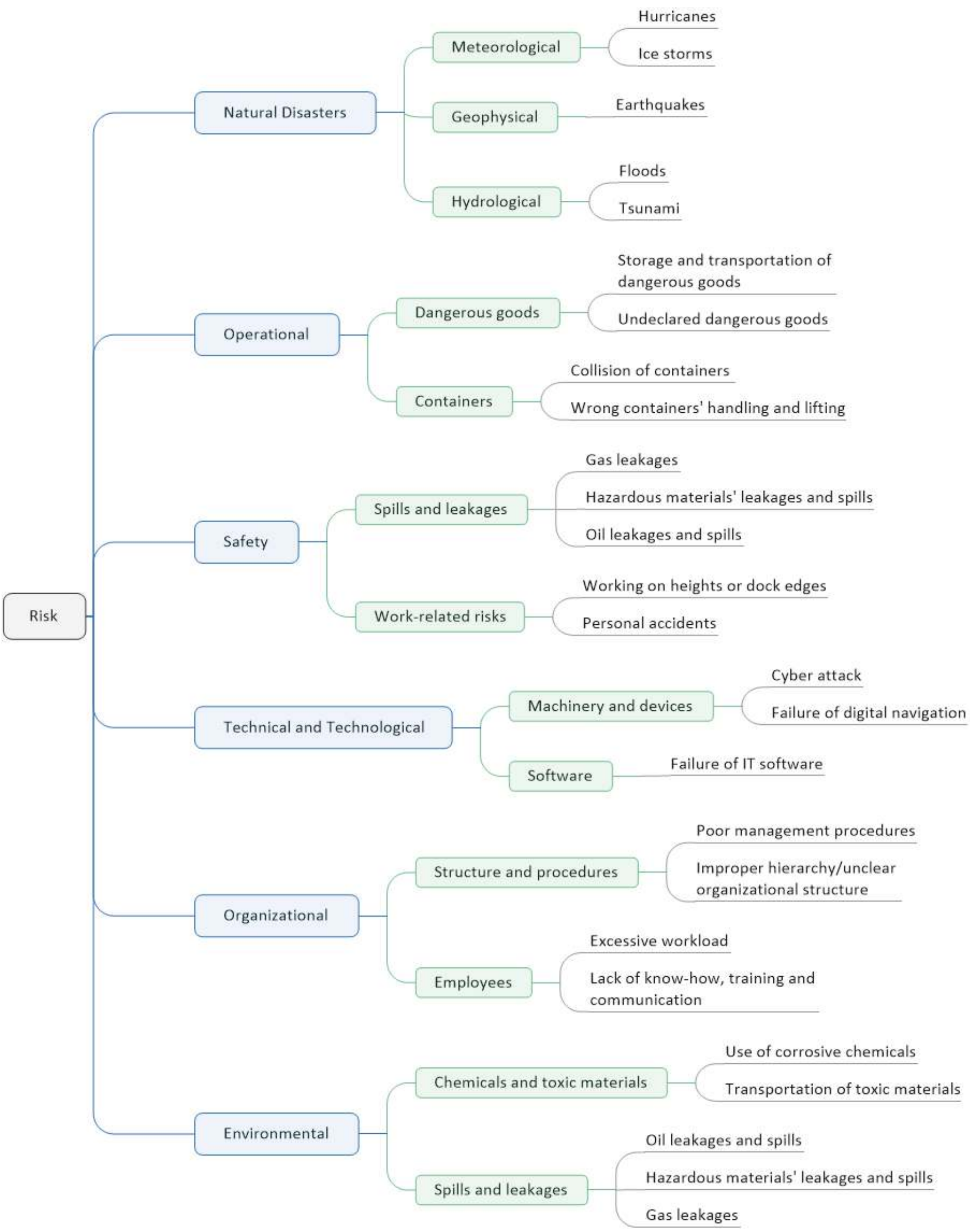


Figure 4: *Breakdown of risk groups*

Organisational risks have two risk sub-groups: employees as well as structure and procedures. The former represents risks that could negatively impact the productivity of employees and their corresponding roles and tasks. The latter represents risks that are related to the structure and procedures of an organisation that could negatively impact the daily operational activities.

Environmental risk groups consist of two sub-groups: chemicals and toxic materials and spills and leakages. Chemical and toxic materials represent risks that are associated with chemical and toxic materials hazardous to the environment. Spills and leakages represent risks that are associated with the spills and leakages of oil and other hazardous materials. **Figure 4** shows the overall breakdown structure of the risk groups that are integrated to the online Toolbox.

5 RISK ASSESSMENT IN SEAPORTS

This chapter gives a guideline on how to implement the risk assessment process in seaports. Section 5.1 presents the overall suggested risk management principles and framework according to ISO 31000. Section 5.2 elaborates the process of risk assessment based on ISO 31000. Section 5.3 presents the suggested set of quantitative, qualitative, semi-quantitative and hybrid methods which can be used to identify, analyse and evaluate different sources of risks

5.1 Risk management principles and framework according to ISO 31000

5.1.1 Principles

The principles aim to create and protect value in line with organisation's objectives and mandate. For risk management to be effective, an organisation should at all levels comply with different set of principles (International Organization for Standardization 2018). The standard stresses on the importance of eight principles that need to be satisfied as follow:

Figure 5: *Risk Management Principles according to ISO 31000:2018*

INTEGRATED

Risk management should be integrated to the main activities and processes of the organisation. It is not a stand-alone activity and should be part of the management's responsibilities and an integral part of all organisational processes, including strategic planning and all project and change management processes.

CUSTOMISED

The organisation's internal and external context as well as risk profile should be considered in the design and implementation of risk management. Based on the scope, goals and context of the organisation, risk management can be customised accordingly.

STRUCTURED AND COMPREHENSIVE

The efficiency to deliver consistent, comparable and reliable results depends on a structured, systematic and timely approach to risk management. The approach should display developed steps, dependencies and associated flows.

INCLUSIVE

Ensuring a relevant and up-to-date risk management process should be based on timely and appropriate involvement of stakeholders and decision makers at all levels of the organisation. This allows the proper representation of stakeholders by taking their views into consideration in determining risk criteria.

DYNAMIC

The dynamic aspect of risk management requires continuous sense and responses to changes. As internal and external events occur, knowledge and context change, reviewing and monitoring of risks take place. This can result in the emergence of new risks, change and/or disappearance of others.

BASED ON BEST AVAILABLE INFORMATION

The proper management of risks requires accurate input that is based on information sources such as observations, historical data, expert judgment and observation. However, the stakeholders and decision makers should take into account any limitations of the models and data used in the management of risks.

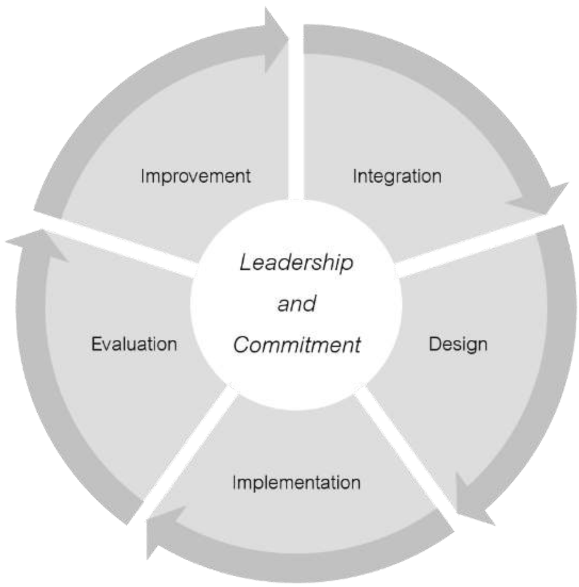


Figure 6: *Risk Management Framework (ISO 31000:2018)*

CONSIDERATION OF HUMAN AND CULTURAL FACTORS

The intention, capabilities and perceptions of internal and external people should be recognised by risk management which can hinder or facilitate the fulfilment of organisation’s objectives.

CONTINUOUSLY IMPROVED

Organisations should design and implement strategies and measures in order to improve the risk management maturity in parallel to all other aspects of their organisation. These development and implementation strategies should fulfil the requirements of core stakeholders.

5.1.2 Framework

The risk management framework was based on ISO 31000:2018. The framework emphasises the strong connection between the risk management process, leadership and commitment. A strong leadership and commitment are required to integrate the risk management process into organisational structure, roles and responsibilities.

The framework of ISO 31000:2018 consists of a set of parts that elaborate the basis and organisational areas for the design, implementation, monitoring, reviewing and continuous improvement of risk management throughout the organisation. The framework is connected to principles and risk management process.

The successful implementation of the framework supports in the effective management of risk by the application of the risk management process at different levels and within specific contexts of the organisation. The framework stresses the adequate reporting of information about risk management that is derived from the implemented risk management process. This information is used as a basis for accountability and decision-making at all relevant organisational levels.

INTEGRATION

Integration into organisational structure and context, roles and responsibilities. The leadership and commitment of top management is required to integrate risk management into the organisational activities.

DESIGN

Design of risk management framework based on legal, policy, operational requirements and needs, as well as the assignment of roles and responsibilities along with the allocation of resources. Internal and external communication and reporting mechanism should also be incorporated during the design phase. This includes an analysis of internal and external stakeholder interests and influences

IMPLEMENTATION

Implementation of risk management framework and process by making specific plans as well as defining responsibilities, accountabilities, decisions about who does what, when and how. Clear communication plan should be created to disseminate the implementation strategy.

EVALUATION AND IMPROVEMENT

Decisions should be carried out, based on the results of monitoring and reviews, on how risk management policy, framework and plan can be improved. These decisions should facilitate the implementation of improvements in the organisation's management of risk and the associated risk management culture.

5.2 Risk assessment process according to ISO 31000

The risk management process aids in the systematic application of management policies, procedures and practices with regards to the activities of communicating—consulting, establishing the context, and assessment, treating, monitoring and reviewing risk. Throughout the process, it is extremely important that the various steps and results are communicated accordingly and comprehensively between the parties involved. The HAZARD guideline and Toolbox focuses on the risk assessment phases comprising identification, analysis and evaluation. **Figure 7** shows the steps of the risk assessment process

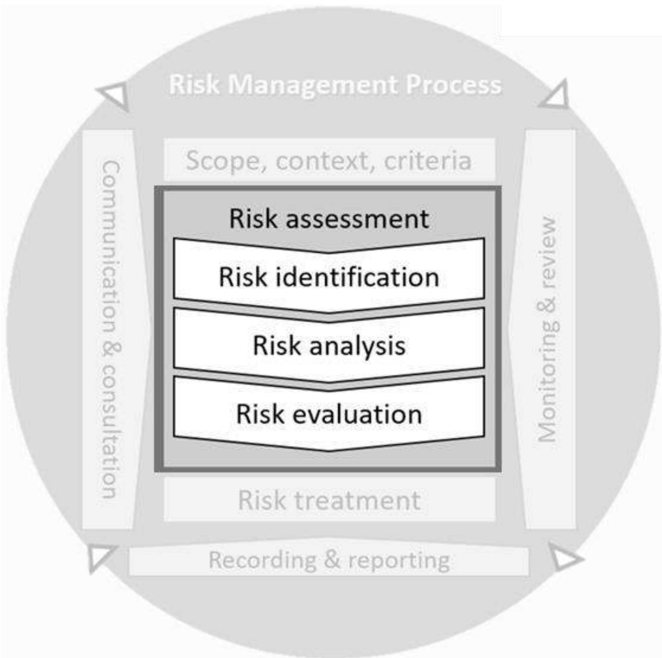


Figure 7: *Risk assessment process (ISO 31000:2018)*

5.2.1 Risk identification

This essential step requires the careful identification of risks based on accurate information. The organisation should identify sources of risk, areas of impacts and their causes and their potential consequences. A comprehensive list of risks should be generated in this step, which might negatively affect the achievement of objectives.

5.2.2 Risk analysis

This step aims at analysing the identified risks based on the associated causes and consequences along with their likelihood and severity respectively. The output of risk analysis is used in the evaluation of risks in order do decide about the risk treatment priorities, and on the appropriate treatment strategies and methods.

5.2.3 Risk evaluation

This step aims at the prioritisation of the identified risk that has been analysed in the analysis phase. This is in order to assist in making decisions about the risks in need of urgent treatment. Risk evaluation involves comparing the level of risk determined during the analysis process with the established risk criteria.

5.3 Risk assessment methods

There is no "ideal" risk assessment that will suit all seaports; as the investigation revealed, most of the time, the selected method depends on the information available, the people involved, the degree of knowledge/expertise and the type of risks that will be assessed. For instance, there were authors concentrating on assessing operational or security risks, whereas other focused on natural disaster threats, pollution risk or cyberattacks.

A multidisciplinary team is normally required to take part in the risk assessment—the people designated to undertake this evaluation should be competent and have an understanding of the general approach to be used. The employers participating in the risk evaluation should co-operate in the identification and assessment of risks. The stakeholder engagement and understanding during this process is imperative. Therefore, it is believed that the best suitable methods for this evaluation should comply with the characteristics of the risk assessment team involved.

The risk assessment methods integrated to the online Toolbox can be categorised to quantitative, qualitative and semi-quantitative methods. Each method has a different application complexity level and might require low, medium or high resources and time. The quantitative methods are normally more complex than the qualitative and semi-quantitative methods since certain software, programs and specific knowledge are required. Certain risk assessment methods can have a combination of quantitative, qualitative and semi-quantitative applications. This increases the degree of flexibility to apply the method according the available data. **Table 2** displays a summary of the selected methods for the online Toolbox.

Table 2*: Overview of the selected Risk Assessment methods*

Method	Type	Corresponding ISO 31000 phase	Recommended application
ALARP	• Quantitative • Qualitative • Semi-quantitative	• Risk evaluation	• General
Bow-Tie	• Qualitative • Quantitative	• Risk Identification • Risk analysis: Causes/threats; Consequences;	• Dangerous goods • Risks associated with machinery and devices • Software failures • Spills and leakages
Brainstorming	• Qualitative	• Risk identification	• General
Cause-consequence analysis	• Quantitative • Semi-quantitative	• Risk analysis: Causes/threats; Consequences; Likelihood; Severity	• Dangerous goods • Chemicals and toxic materials • Spills and leakages
Checklist	• Qualitative	• Risk Identification • Risk analysis: Causes/threats; Consequences;	• Dangerous goods • Organisational risks • Container risks
Cost-benefit analysis	• Quantitative	• Risk evaluation	• Organisational risks
Delphi Method	• Quantitative • Qualitative	• Risk Identification • Risk analysis: Likelihood; Severity • Risk Evaluation	• General
Event Tree Analysis (ETA)	• Quantitative • Qualitative • Semi-quantitative	• Risk analysis: Consequence; Likelihood	• Natural disasters • Dangerous goods • Safety risks
Fault Tree Analysis (FTA)	• Quantitative • Qualitative • Semi-quantitative	• Risk analysis: Causes/threats; Likelihood;	• Dangerous goods • Safety risks • Container risks
Failure Mode and Effect Analysis	• Semi-quantitative	• Risk Identification • Risk analysis: Causes/threats; Consequences; Likelihood; Severity	• Risks associated with machinery and devices • Software failures
Hazard diamond	• Semi-quantitative	• Risk analysis: Consequence; Severity	• Spills and leakages • Dangerous goods
Monte Carlo simulation	• Quantitative	• Risk analysis: Likelihood; Severity	• Spills and leakages • Geophysical risks

Method	Type	Corresponding ISO 31000 phase	Recommended application
Monte Carlo simulation	• Quantitative	• Risk analysis: Likelihood; Severity	• Spills and leakages • Geophysical risks
Preliminary Hazard Analysis	• Semi-quantitative	• Risk Identification • Risk analysis: Causes/threats; Consequences; Likelihood; Severity	• Dangerous goods • Containers risks • Spills and leakages
Risk matrix	• Qualitative • Semi-quantitative	• Risk analysis: Likelihood; Severity • Risk evaluation	• General
SeaTrack Web	• Quantitative	• Risk analysis: Consequences	• Oil spills
Scenario analysis	• Quantitative • Qualitative	• Risk analysis: Causes/threats; Consequences; • Risk evaluation	• Natural disasters • Cyberattacks
SWOT analysis	• Qualitative	• Risk Identification • Risk analysis: Causes/threats	• Organisational risks

The methods and their applications are presented in the upcoming sub-sections based on their type following quantitative, qualitative, semi-quantitative or hybrid approach.

5.3.1 Quantitative methods

Quantitative methods are often characterised by the use of probabilistic information in regards of potential events and their consequences.

Cost-benefit analysis

The cost-benefit analysis is about comparing the costs and benefits of a project or a major activity and using this comparison as a basis for decision-making for the implementation of the project/activity. The costs and benefits are in most cases described in monetary terms to allow comparison. However, it is sometimes difficult to express welfare gains, for example, as a monetary unit. If at the end of the analysis the benefit is higher than the total cost, a project/activity should be implemented. Experience and expected values are used to determine costs and benefits in advance (Sen 2000).

Application

This method can be utilised to evaluate organisational risks such as poor management procedures, improper hierarchy/unclear organisational structure and lack of know-how.

Monte Carlo Simulation

Monte Carlo simulation belongs to the stochastic simulation methods, in which random numbers are used to calculate scenarios within certain ranges. Further types of simulation methods are static, dynamic and deterministic simulations, which are selected according to the complexity of the structure to be simulated. Today, almost exclusively stochastic and dynamic methods are used to assess risks or make decisions under uncertainty. Using the Monte Carlo simulation and synthetic data, the effects of different decisions and their probability of occurrence can be estimated. It is a calculation method to simulate extreme cases, but also to secure everyday decisions. Thus, it is usable for the most diverse industries.

Application

This method can be applied to analyse natural disasters such as earthquakes and spills and leakages of oil and hazardous materials. The analysis phase of the Monte Carlo simulation comprises the calculation of the occurrence probability and consequences' severity. Na and Shinozuka (2009) used the Monte Carlo simulation the evaluate the potential damages and disruptions in seaports due to earthquakes.

SeaTrack Web

The Seatrack Web system comprises three main parts with an oil drift model that has been jointly developed by the Swedish Meteorological and Hydrological Institute (SMHI) and the Danish Maritime Safety Administration (DAMSA). The model is executed whenever a Seatrack Web user requests a simulation. The graphical user interface has been developed at SMHI and is based on open-source GIS-server technology i.e. the user interacts with geo-referenced data in a map (Liungman & Mattsson 2011).

Application

The SeaTrack Web tool can be used to analyse the consequences of an oil spill drift to a particular sea area to determine where does the oil spill drift to in the sea area. The method is selected based on the co-operation with the OpenRisk Project. The tool can be accessed at https://stw.smhi.se. Access can be provided upon sending an email to seatrackweb@smhi.se. Provide information about your institution and inform us why you want to access SeaTrack Web.

5.3.2 Qualitative methods

This technique tends to be used in a wide majority of industries due to its easiness of use and comparative characteristics, which can help rank a risk (Pasman et al. 2017). This approach is a simple rapid assessment, where even a single person can gather the necessary information to conclude the analysis. Moreover, this type of method is used whenever there is a lack of adequate information, resources and/or time.

SWOT analysis

The SWOT analysis is an instrument of strategic corporate management with which strengths and weaknesses of the company or its supply chain as well as the opportunities and threats in the environment can be uncovered. The resulting findings can be used to identify risks by comparing the requirements of the market with the potential of the company or supply chain. Finally, identified weaknesses are to be regarded as risks, whereby these can be both strategic and operational in nature.

Application

This method can be used to identify and analyse risks. The analysis phase comprises the identification of possible causes/threats

Checklists

Checklists are a very simple way to identify risks. As a rule, checklists consist of standardised questionnaires that help to systematically record risks. In general, it can be stated that checklists and questionnaires determine the actual status of a particular system. They can contain open or closed questions, whereby closed questions are better suited for the identification of risk potentials, since the evaluation of the answers is simpler and thus leads faster to concrete results. The questions mostly arise when using creative techniques. Workshops, brainstorming, etc. are most commonly used in the creation process. It is advisable to consult experts as they have the greatest access to information and knowledge.

Application

This method can be used qualitatively to identify risks at seaports.

Brainstorming

Brainstorming is probably the best known and most widespread creativity technique, which basically aims to activate thought processes and identify as many ideas or risks as possible by promoting the creative potential of a group or individuals. Brainstorming is used to identify risks in all industries and functional areas due to its methodological simplicity and its versatility (Hogganvik & Stølen 2006).

Basically, brainstorming is a method that is carried out in a group of 5–10 people. A large number of risks are to be generated by spontaneous statements on concrete questions and problems. The open utterance in front of the group and parallel visualisation of the utterances, e.g. on a flipchart, stimulates further ideas.

Application

This method can be used qualitatively to identify risks at seaports.

5.3.3 Semi-quantitative methods

The semi-quantitative method provides an intermediary technique between the “word-based” evaluation of qualitative risk assessment and the “numerical” evaluation of quantitative risk assessment.

Failure Mode and Effect Analysis

The Potential Failure Mode and Effects Analysis is a cross-industry established method to identify and eliminate potential failures, problems, errors and risks of a system, design or process before adverse consequences reach the internal/external customer.

The basic idea of the FMEA is thus the preventive risk identification and error prevention instead of a subsequent correction. Accordingly, an FMEA can be used to identify risks and derive a high benefit for a company e.g. lower error costs, smoother product launches, higher customer satisfaction and ultimately, a better market position (Stamatis 2003).

Application

This method can be applied to identify and analyse technical and technological risks, such as failure of IT software, failure of digital navigation and cyberattacks. The analysis phase of the FMEA comprises the identification of causes, consequences along with calculating the occurrence probability and consequences’ severity.

Hazard diamond

The Hazard diamond is used to identify and analyse the different risks associated with hazard sources. The Hazard diamond or the so-called fire diamond is defined in the NFPA (704) which is the Standard System for the Identification of the Hazards of Materials for Emergency Response. The four divisions of the diamond are color-coded to represent flammability (red), health hazard (blue), chemical reactivity (yellow) and special hazards (white). The Hazard diamond is normally used to identify the risk associated with hazardous materials and dangerous goods (National Fire Protection Association 2017).

Application

This method can be applied to identify and analyse the associated risks of hazardous materials, leakages and dangerous goods. The analysis phase of the Hazard diamond comprises the identification of consequences along with calculating the consequences’ severity. Rescue services and fire brigades usually use this method to evaluate dangerous materials and define the corresponding adequate measures.

Preliminary Hazard Analysis

The Preliminary Hazard Analysis (PHA) is a semi-quantitative risk analysis method that is used to identify potential hazards and the corresponding top events (risks). The PHA sheet identifies the required measures and follow-up actions as well to control the hazard sources. The PHA should consider hazardous components, facilities, safety-related equipment and environmental constraints (Rausand 2005).

Application

This method can be applied to identify and analyse the associated risks of hazardous materials, leakages and dangerous goods. The analysis phase of the PHA comprises the identification of causes, threats, consequences along with calculating the occurrence probability and the consequences' severity.

5.3.4 Hybrid methods

These are methods that can be applied in a combined manner, i.e. quantitative and qualitative; qualitative and semi-quantitative etc. This gives an advantage to apply the same method based on the given situation as well as the available resources and data.

Cause-Consequence analysis

The Cause-Consequence Diagram is developed from a certain initiating top event, i.e. an event that initiates a specific operational sequence or an event which activates certain safety systems. The Cause-Consequence Diagram consists of two reliability analysis methods previously elaborated, the FTA (Fault Tree Analysis) and ETA (Event Tree Analysis) methods (Andrews & Ridley 2002).

Application

This method can be applied to analyse environmental risks and the risk associated with dangerous goods. The analysis phase of the cause-consequence analysis comprises the identification of causes/threats and consequences as well as the calculation of the occurrence probability and the consequences' severity. The analysis approach be carried out quantitatively or semi-quantitatively.

ALARP

The ALARP (As Low as Reasonably Practicable) principle is based on the fundamental thinking of "acceptable" or "tolerable" risks. It allows analysts and decision makers to define boundaries to combine probability-consequence scales. These boundaries can be used to delineate acceptable and intolerable risks. This allows decision makers to evaluate whether a system or process poses certain risks which need to be treated using risk-control options. The ALARP principle can easily be combined with tools such as Risk Matrices to graphically represent the boundaries of risk tolerability (Laine et al. 2018).

Application

This method can be applied to evaluate the identified risks. The evaluation approach of ALARP can be carried out quantitatively, qualitatively or semi-quantitatively based on the defined evaluation criteria.

Risk Matrix

In a qualitative approach, risks are usually categorised into "high", "medium" and "low", and are represented in a risk matrix. This risk matrix represents the possibility and severity of a risk in order to integrate the potential accident scenarios that were identified in the threat identification stage. Inside the matrix, the criticality of a risk can identified by using colours. The results provided by this matrix can be used to compare risks and identify improvement and mitigation measures.

A risk matrix can also be used in a semi-quantitative method. The main difference to a qualitative one is that instead of using linguistic labels (low, medium, high) to assess the severity and probability of a risk, established numerical values are used. For instance, the rows could represent the increasing likelihood of consequences, and the columns the increasing severity of the correspondent consequences. After that, the quantification of the risk is performed, by the multiplication of probability and severity.

Application

This method can be applied to analyse and evaluate risks. The analysis phase of the risk matrix comprises the calculation of the occurrence probability and consequences' severity. The analysis approach is to be carried out qualitatively or semi-quantitatively. Belamarić et al. (2016) analysed the pollution risk of the Port of Šibenik due to oil spill scenarios because of collision, impact and grounding. The assessment of the impact and probability of risks was performed using a risk matrix with numerical and linguistic elements.

Fault Tree Analysis (FTA)

The FTA (fault tree analysis) is a scientific method for detailed fault analysis. It serves the systematic identification and documentation of possible causes for errors or misconduct. Found causes are broken down as precisely as possible.

Application

This method can be applied to analyse operational and safety risks such as handling of dangerous goods, personal accidents and collision of containers. The analysis phase of the FTA comprises the identification of causes/threats as well as the calculation of the occurrence probability. The analysis approach be carried out qualitatively, quantitatively or semi-quantitatively. Hamka (2017) utilised the Fault-Tree Analysis (FTA) methodology to evaluate safety regarding loading and unloading activities in container terminals.

Event Tree Analysis (ETA)

Event Tree Analysis (ETA) is a method that examines the consequences of a particular event. Starting from an initial event, the tree is divided into two branches, whereby the upper one represents a positive and the lower one a negative development (event trees are usually drawn from left to right). Repeated branching of the tree shows possible effects of an initial event on a system. The aim of ETA is the identification of possible damage events.

Application

This method can be applied to analyse natural disasters as well as operational and safety risks e.g. hurricanes, handling of dangerous goods, personal accidents and collision of containers. The analysis phase of the ETA comprises the identification of consequences as well as the calculation of the occurrence probability. The analysis approach be carried out qualitatively, quantitatively or semi-quantitatively. Many applications integrate the ETA with the Bow-Tie analysis and the cause-consequence analysis (Mokhtari et al. 2011).

Bow-tie

The BowTie method can be considered a combination of earlier developed Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) methods. The first BowTie diagrams seem to have appeared in the Imperial Chemistry Industry course in Australia 1979, but how and when the method found its exact origin is not completely clear. A significant milestone in the history of BowTie was the catastrophic incident on the Piper Alpha platform in 1988, which shook the oil and gas industry. In the early 1990s, the Royal Dutch Shell adopted the BowTie method as part of its methodological Toolbox for managing risks. The method rapidly gained support throughout the industry as the BowTie diagrams appeared to be a suitable visual tool. Nowadays, the BowTie method is also used for risk management related to different transport modes such as maritime and aviation (Mokhtari et al. 2011; Laine et al. 2018) .

Application

This method can be applied to identify and analyse operational, environmental, safety and technological risks such handling of dangerous goods, oil leakages, cyberattack and failure of digital navigation. The analysis phase of the BTA comprises the identification causes/threats and consequences of the corresponding identified risks. The analysis approach be carried out qualitatively or quantitatively. (Mokhtari et al. 2011) applied the bow-tie method as a framework for risk management in seaports and offshore terminals.

Scenario Analysis

Originally, the scenario technique came from the military field, but today it is also frequently used to help solve economic and social issues. Basically, the scenario technique combines quantitative and qualitative forecasting elements. Thus, no pure linear projection is made on the basis of historical data. The aim of the procedure is to prepare companies for future developments in order to improve their ability to act.

The complexity is reduced by the calculation and exclusion of inconsistent future developments. The scenario technique provides consistent future projections based on the information collected during the process. For these scenarios, corporate strategies can be developed that react adequately to future risks.

Application

This method can be applied to analyse and evaluate the risks associated with natural disasters as well as technological risks. The analysis phase of the scenario analysis comprises the identification of causes/threats and consequences. The analysis approach can be carried out qualitatively or quantitatively. Kwesi-Buor et al. (2016) used the scenario analysis for disaster preparedness of port and maritime logistics risk management.

Delphi Method

The term Delphi in the name of the instrument refers to the famous oracle in ancient Greece, which was consulted before all important political decisions. The actual method originates from the USA, where the method was developed in the 1950s by American scientists. The Delphi method was developed against the background of military national defence in order to identify possible targets in the USA during the Cold War. It is a structured group communication process with the aim of answering questions or finding a consensus on facts about which uncertain and incomplete knowledge naturally exists. Selected experts from various disciplines are involved in this communication process (Laine et al. 2018).

Application

This method can be applied to identify, analyse and evaluate risks. The analysis phase of the BTA comprises the identification causes/threats and consequences of the corresponding identified risks. The analysis approach be carried out qualitatively or quantitatively.

6 HAZARD SEAPORT RISK ASSESSMENT TOOLBOX

The online Toolbox is available as a website and accessible for all potential users. The main functionality of the Toolbox is to guide and inform the users through the process of choosing an appropriate risk assessment method based on their specific needs and the type of risk they are facing.

The Toolbox has been designed with simplicity in mind. This is mirrored in the structure chosen arranging and presenting the information in question. This structure is depicted in **Figure 8**.

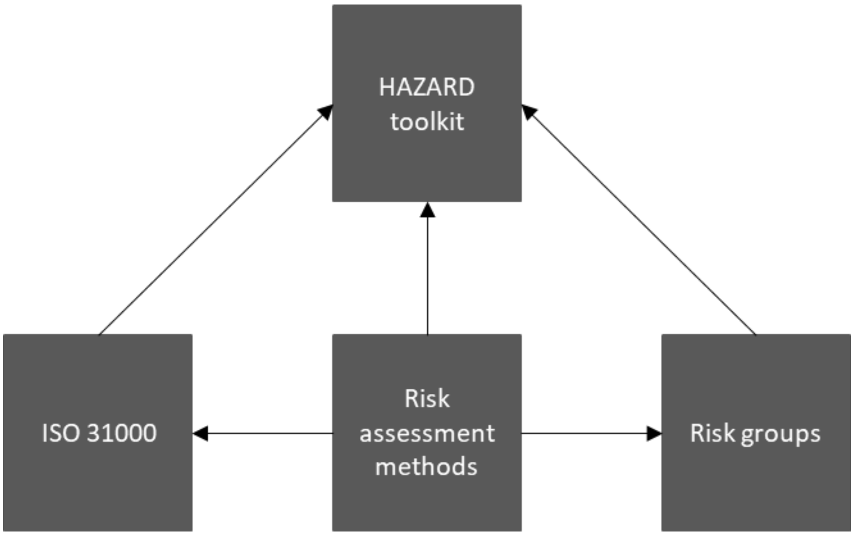


Figure 8: *General structure of the HAZARD Seaport Risk Assessment Toolbox*

6.1 ISO 31000 section of the Toolbox

This section offers a concise introduction to the ISO 31000:2018 standard describing the most recent risk management guidelines.

a. *Principles*
   Outlines the set of principles an organisation should comply with to meet the standard. An example hereof is the continuous improvement of risk management within an organisation
b. *Framework*
   The framework offers the foundations and crucial steps towards implementing an effective risk management process within an organisation
c. *Process*
   The process describes the actual steps included in the ISO 31000 guideline. These include three phases constituting the main focus of the Toolbox: Risk Identification, Risk Analysis and Risk Evaluation. The risk assessment methods described in the following section are sorted according to their usefulness in these three steps of the risk assessment process.

6.2 Risk assessment methods section of the Toolbox

As mentioned previously, the Toolbox offers a catalogue of risk assessment methods gathered from academic literature and consolidated with qualitative analysis of the status quo in practice. To make it easier for the user to navigate the so-described catalogue, the Toolbox offers a categorisation by the following related factors:

1. *ISO 31000 Step:*
   As mentioned in the previous section, each risk assessment method is assigned to one or more of the ISO Steps: Risk Identification, Risk Analysis and Risk Evaluation with varying levels of granularity. This assignment expresses that the method in question can be applied in the corresponding ISO 31000 step.

2. *Method properties*
   Additionally, it is possible to filter the risk assessment methods by the following descriptive properties:

I. <u>Complexity</u>
   The application complexity and skills the method demands for the successful usage and application. High complex methods could deliver accurate outcomes and less subjectivity compared to less complex methods.

II. <u>Effort</u>
   The resources and time effort required to gather all important data for the successful application of the corresponding method. Several methods require more input, which increases the required effort.

III. <u>Method Type</u>
   According to academic literature, risk assessment methods fall into three categories defined as:
   a. *Qualitative*
      Based solely on the outcome of human interactions and the communication of expert knowledge through natural language by conducting interviews, surveys etc.
   b. *Quantitative*
      Based solely on numerical data analysis and formal or mathematical models
   c. *Semi-Quantitative*
      A hybrid approach of the previous method types capturing the strengths of both, mainly offering the opportunity to assert the formal models with experience reports

6.3 Risk groups section of the Toolbox

In addition to the catalogue of risk assessment methods, the Toolbox offers a hierarchical definition of the most commonly encountered risk types. The hierarchy is defined in the following:

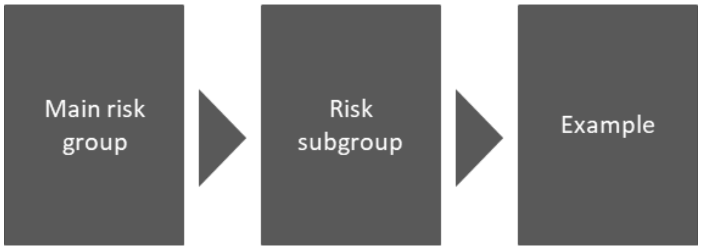


Figure 9: *Breakdown structure of the risk groups*

The hierarchy (shown in **Figure 9**) is organised in a way such that the upper most elements are generic risk groups, which get more and more specific in the subgroups. The last layer of the so-constructed risk tree are most concrete examples of potential risks. These elements are linked directly to the assessment methods addressing them to ensure maximum level of detail and orientation towards the user's risk situation.

6.4 HAZARD Toolkit section

The HAZARD toolkit is the main component of the web-tool. It is mainly organised as a layered form, which needs to be filled by the user to narrow down the risk assessment methods based on the selected criteria. These criteria are geared towards the user needs in terms of required effort, complexity and type of method as well as the risk he/she is attempting to address.

The form contains the following steps:

1. Risk Groups:
   At this level, the user may choose one or more elements of the highest level in risk type hierarchy that is of interest.

2. Risk Subgroups:
   At this level, the user may choose one or more elements of the second level of the risk type hierarchy that is of interest.

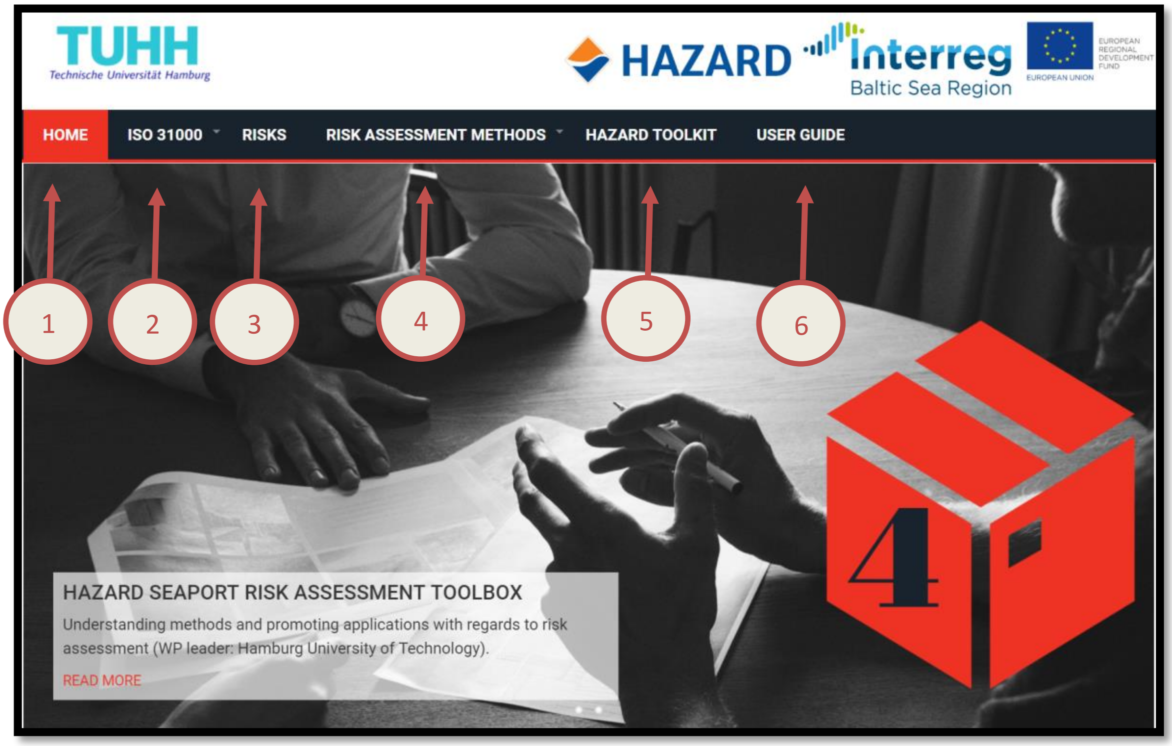
3. Risks:
   At this level, the user may choose one or more concrete risks based on the previous two steps.

4. Method Properties:
   This step permits the user to narrow down their search domain of risk assessment methods based on their needs in terms of complexity, effort and methodology they are most comfortable adopting.

5. Output:
   The output of the Toolbox is a list of risk assessment methods tailored to the previously chosen criteria. The output only shows the procedural steps defined by the method for risk assessment as well as a file attachment(s) of useful resources.

7 USER MANUAL OF THE HAZARD SEAPORT RISK ASSESSMENT TOOLBOX

The user manual gives the user a step-per-step instruction on how to use the Toolbox based on actual screenshots from the website. The website is available through the link https://hazard.logu.tuhh.de.

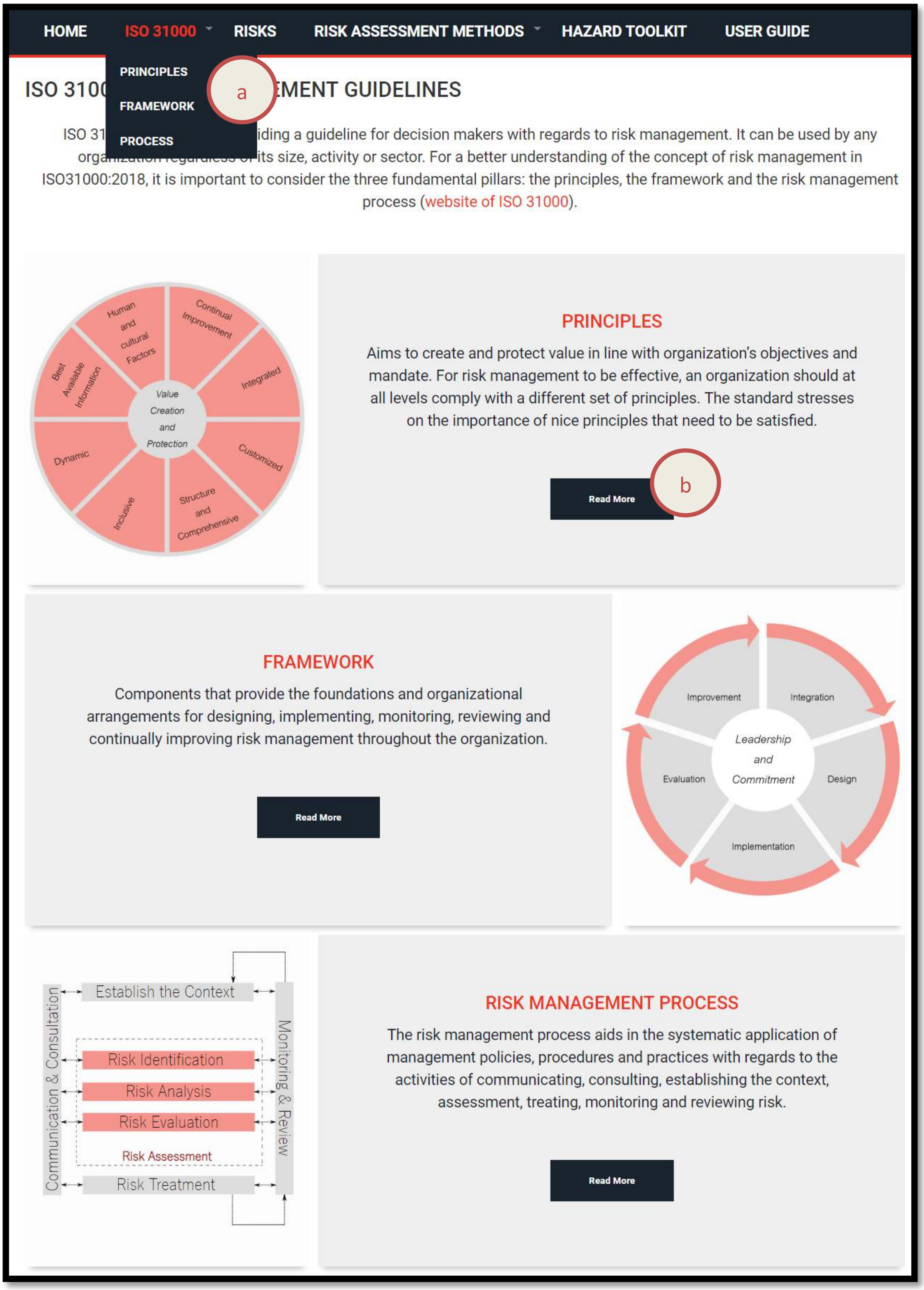


1 **Project Description:**

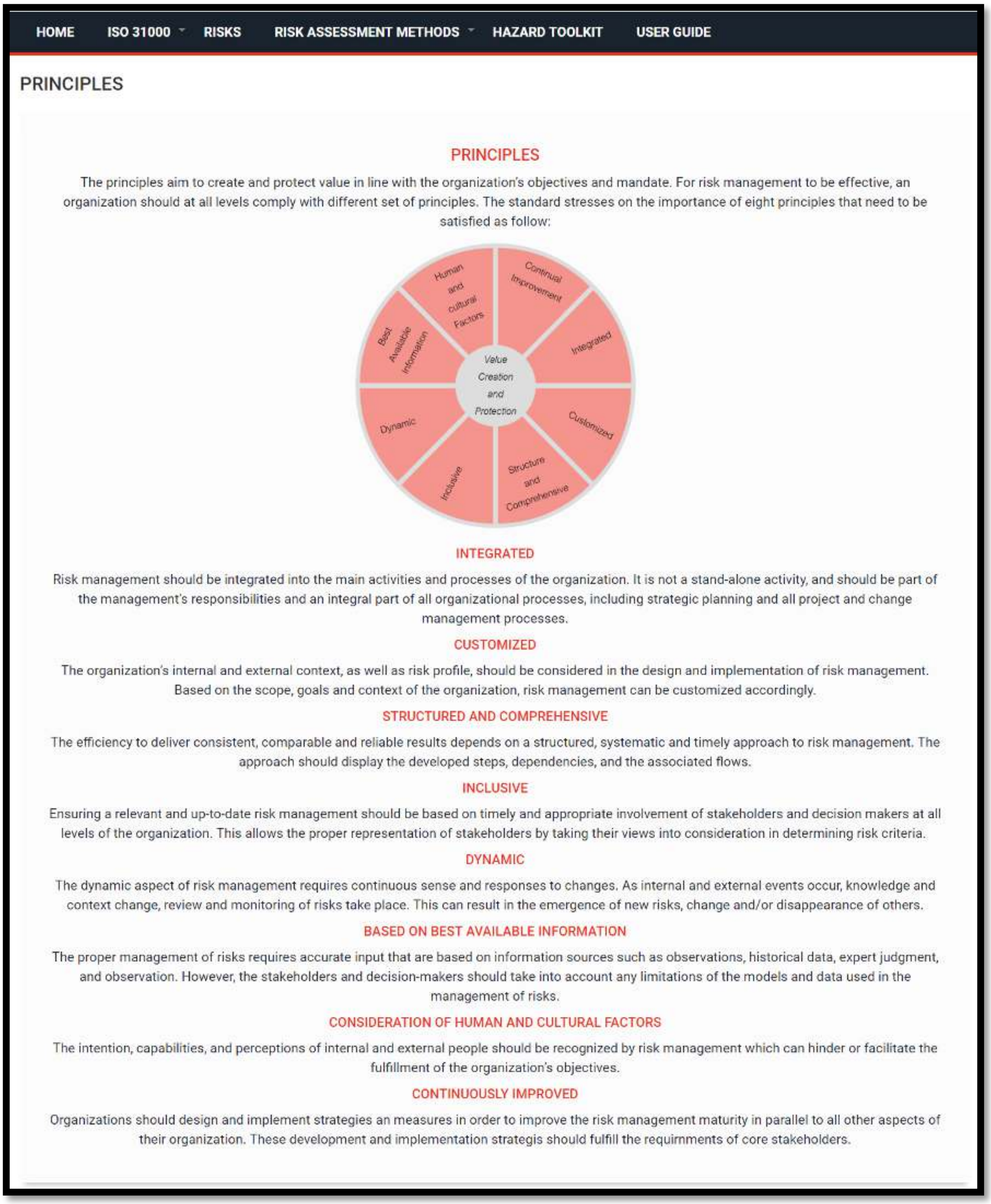
The welcome page of the HAZARD tool offers a short introduction of the HAZARD Project and its scope. Furthermore, it defines the tasks agreed upon and to be delivered by Work package 4, of which the Toolbox represents a crucial part.

2 **ISO 31000:**

The second menu tab in the main navigation offers a short overview of the different components defined in the ISO 31000 standard. These can be accessed either directly through the dropdown menu (a) or by clicking on the *Read More* button (b) in the corresponding section.



For example, by clicking on *Principles*, one is redirected to a webpage with further details about this construct:



PRINCIPLES

The principles aim to create and protect value in line with the organization's objectives and mandate. For risk management to be effective, an organization should at all levels comply with different set of principles. The standard stresses on the importance of eight principles that need to be satisfied as follow:

INTEGRATED

Risk management should be integrated into the main activities and processes of the organization. It is not a stand-alone activity, and should be part of the management's responsibilities and an integral part of all organizational processes, including strategic planning and all project and change management processes.

CUSTOMIZED

The organization's internal and external context, as well as risk profile, should be considered in the design and implementation of risk management. Based on the scope, goals and context of the organization, risk management can be customized accordingly.

STRUCTURED AND COMPREHENSIVE

The efficiency to deliver consistent, comparable and reliable results depends on a structured, systematic and timely approach to risk management. The approach should display the developed steps, dependencies, and the associated flows.

INCLUSIVE

Ensuring a relevant and up-to-date risk management should be based on timely and appropriate involvement of stakeholders and decision makers at all levels of the organization. This allows the proper representation of stakeholders by taking their views into consideration in determining risk criteria.

DYNAMIC

The dynamic aspect of risk management requires continuous sense and responses to changes. As internal and external events occur, knowledge and context change, review and monitoring of risks take place. This can result in the emergence of new risks, change and/or disappearance of others.

BASED ON BEST AVAILABLE INFORMATION

The proper management of risks requires accurate input that are based on information sources such as observations, historical data, expert judgment, and observation. However, the stakeholders and decision-makers should take into account any limitations of the models and data used in the management of risks.

CONSIDERATION OF HUMAN AND CULTURAL FACTORS

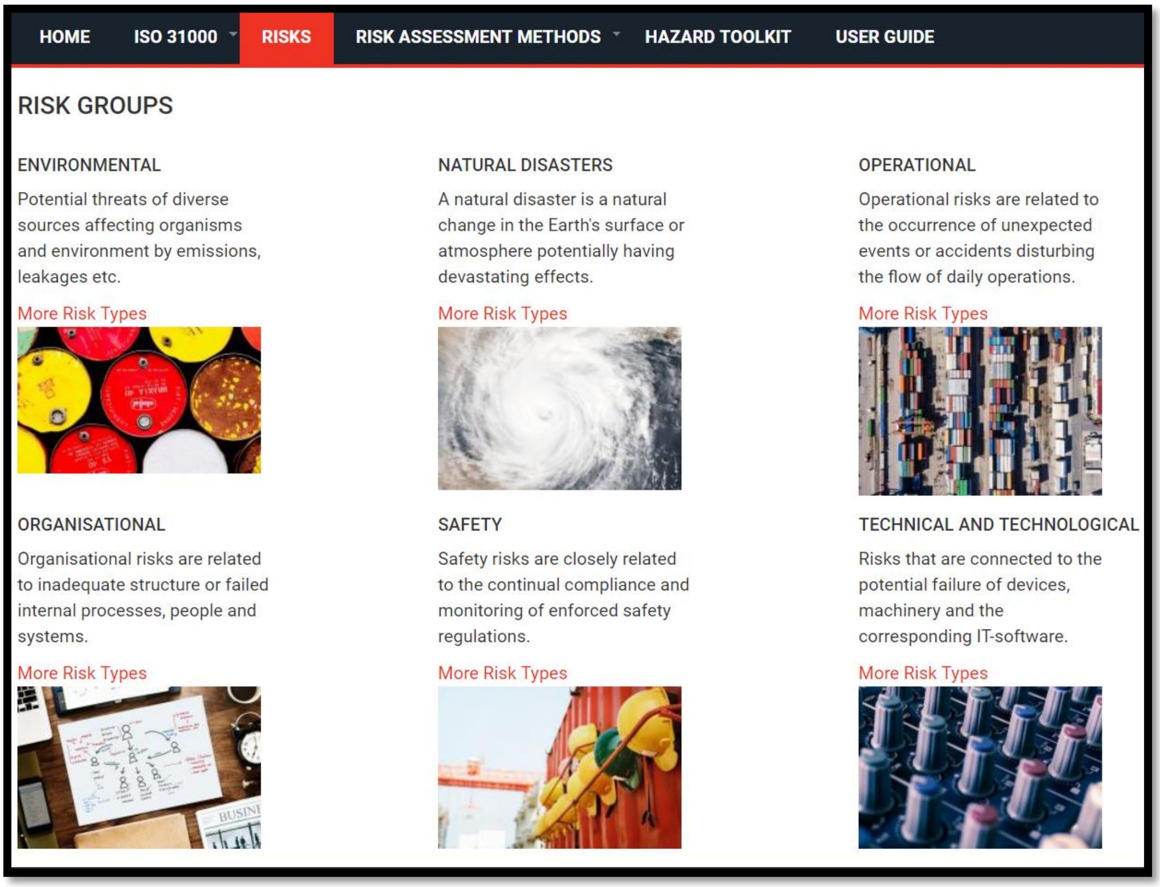
The intention, capabilities, and perceptions of internal and external people should be recognized by risk management which can hinder or facilitate the fulfillment of the organization's objectives.

CONTINUOUSLY IMPROVED

Organizations should design and implement strategies an measures in order to improve the risk management maturity in parallel to all other aspects of their organization. These development and implementation strategis should fulfill the requirmments of core stakeholders.

3 **Risk Groups:**

Under the Risks tab, the user can get an overview of the existing risk groups. By clicking on *More Risk Types*, one can navigate the risk hierarchy form the generic types such as Natural Disasters all the way down to concrete risk types such as floods.

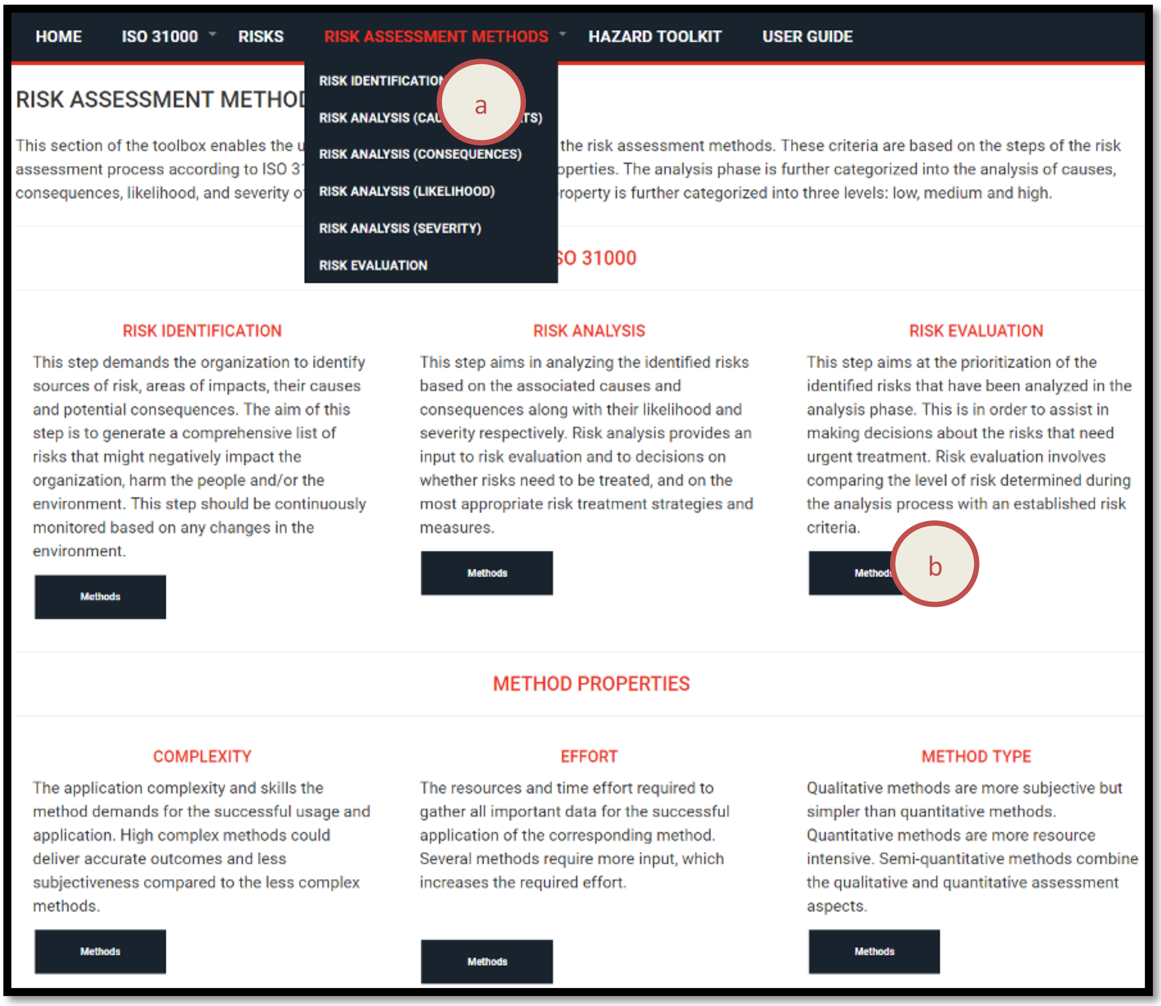


4 **Risk Assessment Methods:**

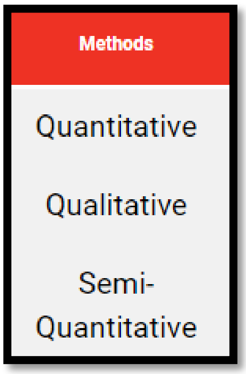
The risk assessment methods menu can be accessed through the fourth tab in the main navigation.

As it is clear from the following screenshot, this page offers a compact representation of risk assessment methods filtered by the phase of the risk assessment process: Risk Identification, Risk Analysis, Risk Evaluation and the method properties: Time required, complexity and method type.

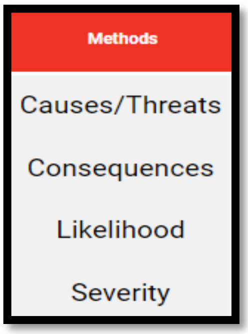
Here again, the filtered view of the methods can either be accessed either through the drop-down menu (a) or by clicking on the *Methods* (b) button.



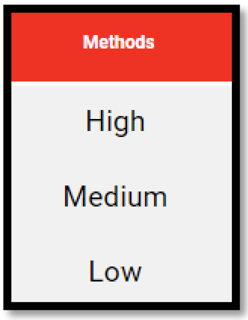
The buttons are sub-divided as to offer a granular filtering of the methods. For example, when hovering over the button under methods type, further filtering options appear:



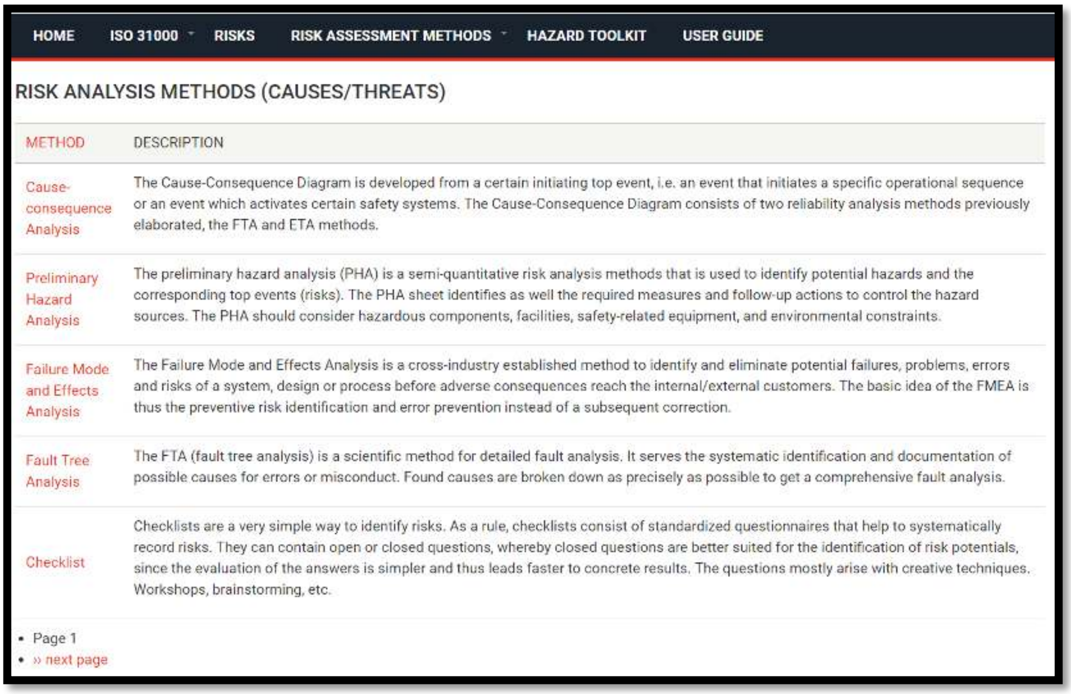
The methods under risk analysis are further subdivided into the following risk analysis categories:



For the rest of the method properties, following options are made available:



For example, when choosing the methods for risk analysis for causes and threats, one gets redirected to a summary table displaying all methods falling under these categories:

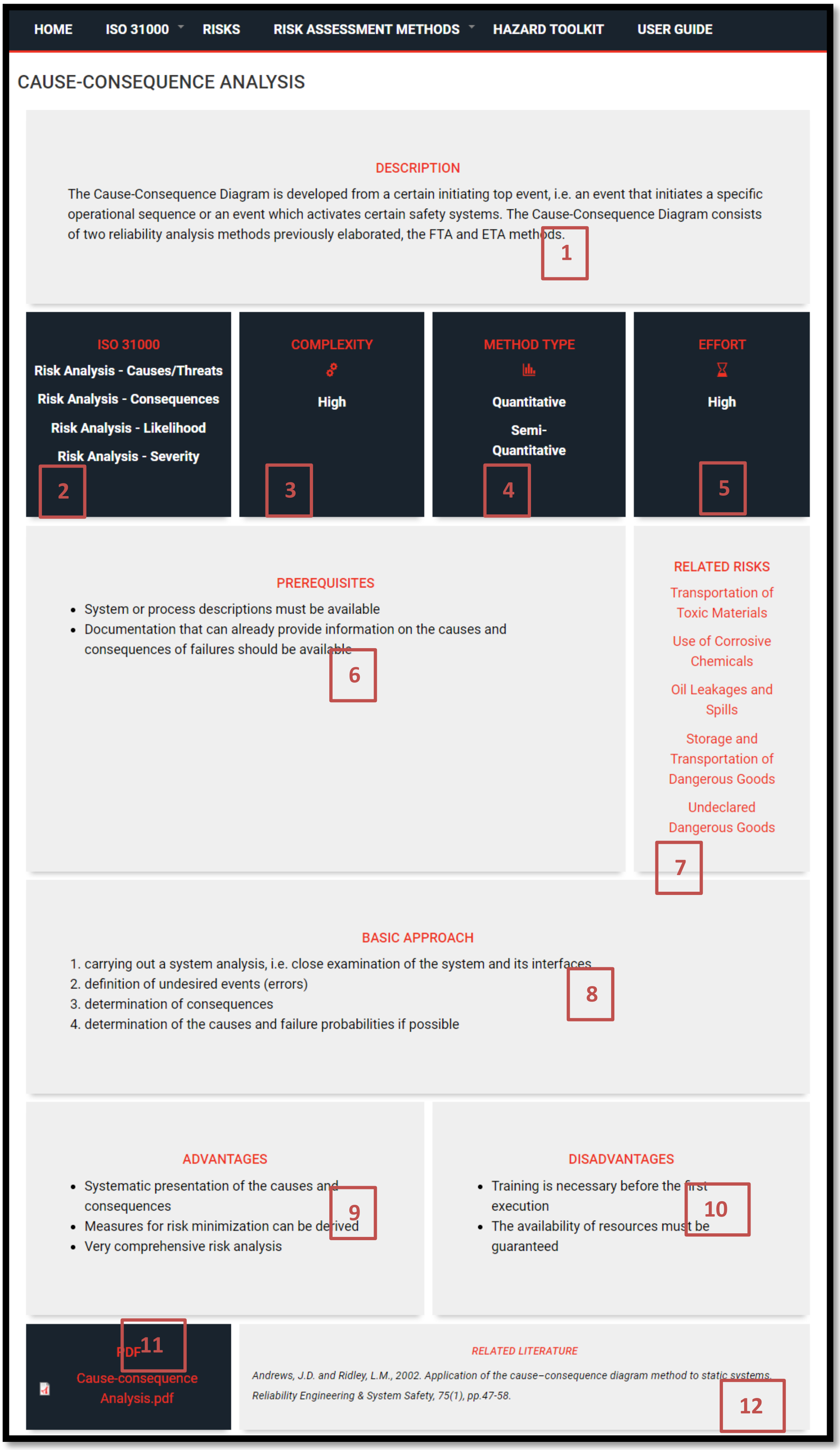

HOME ISO 31000 RISKS RISK ASSESSMENT METHODS HAZARD TOOLKIT USER GUIDE

RISK ANALYSIS METHODS (CAUSES/THREATS)

METHOD	DESCRIPTION
Cause-consequence Analysis	The Cause-Consequence Diagram is developed from a certain initiating top event, i.e. an event that initiates a specific operational sequence or an event which activates certain safety systems. The Cause-Consequence Diagram consists of two reliability analysis methods previously elaborated, the FTA and ETA methods.
Preliminary Hazard Analysis	The preliminary hazard analysis (PHA) is a semi-quantitative risk analysis methods that is used to identify potential hazards and the corresponding top events (risks). The PHA sheet identifies as well the required measures and follow-up actions to control the hazard sources. The PHA should consider hazardous components, facilities, safety-related equipment, and environmental constraints.
Failure Mode and Effects Analysis	The Failure Mode and Effects Analysis is a cross-industry established method to identify and eliminate potential failures, problems, errors and risks of a system, design or process before adverse consequences reach the internal/external customers. The basic idea of the FMEA is thus the preventive risk identification and error prevention instead of a subsequent correction.
Fault Tree Analysis	The FTA (fault tree analysis) is a scientific method for detailed fault analysis. It serves the systematic identification and documentation of possible causes for errors or misconduct. Found causes are broken down as precisely as possible to get a comprehensive fault analysis.
Checklist	Checklists are a very simple way to identify risks. As a rule, checklists consist of standardized questionnaires that help to systematically record risks. They can contain open or closed questions, whereby closed questions are better suited for the identification of risk potentials, since the evaluation of the answers is simpler and thus leads faster to concrete results. The questions mostly arise with creative techniques. Workshops, brainstorming, etc.

- Page 1
- » next page

When clicking on one of the proposed methods, for example the *Cause-Consequence Analysis*, the corresponding method card is displayed.


HOME
ISO 31000
RISKS
RISK ASSESSMENT METHODS
HAZARD TOOLKIT
USER GUIDE
CAUSE-CONSEQUENCE ANALYSIS
DESCRIPTION
The Cause-Consequence Diagram is developed from a certain initiating top event, i.e. an event that initiates a specific operational sequence or an event which activates certain safety systems. The Cause-Consequence Diagram consists of two reliability analysis methods previously elaborated, the FTA and ETA methods.
1
ISO 31000
Risk Analysis - Causes/Threats
Risk Analysis - Consequences
Risk Analysis - Likelihood
Risk Analysis - Severity
2
COMPLEXITY
High
3
METHOD TYPE
Quantitative
Semi-Quantitative
4
EFFORT
High
5
PREREQUISITES
System or process descriptions must be available
Documentation that can already provide information on the causes and consequences of failures should be available
6
RELATED RISKS
Transportation of Toxic Materials
Use of Corrosive Chemicals
Oil Leakages and Spills
Storage and Transportation of Dangerous Goods
Undeclared Dangerous Goods
7
BASIC APPROACH
1. carrying out a system analysis, i.e. close examination of the system and its interfaces
2. definition of undesired events (errors)
3. determination of consequences
4. determination of the causes and failure probabilities if possible
8
ADVANTAGES
Systematic presentation of the causes and consequences
Measures for risk minimization can be derived
Very comprehensive risk analysis
9
DISADVANTAGES
Training is necessary before the first execution
The availability of resources must be guaranteed
10
PDF
11
Cause-consequence Analysis.pdf
RELATED LITERATURE
Andrews, J.D. and Ridley, L.M., 2002. Application of the cause–consequence diagram method to static systems. Reliability Engineering & System Safety, 75(1), pp.47-58.
12

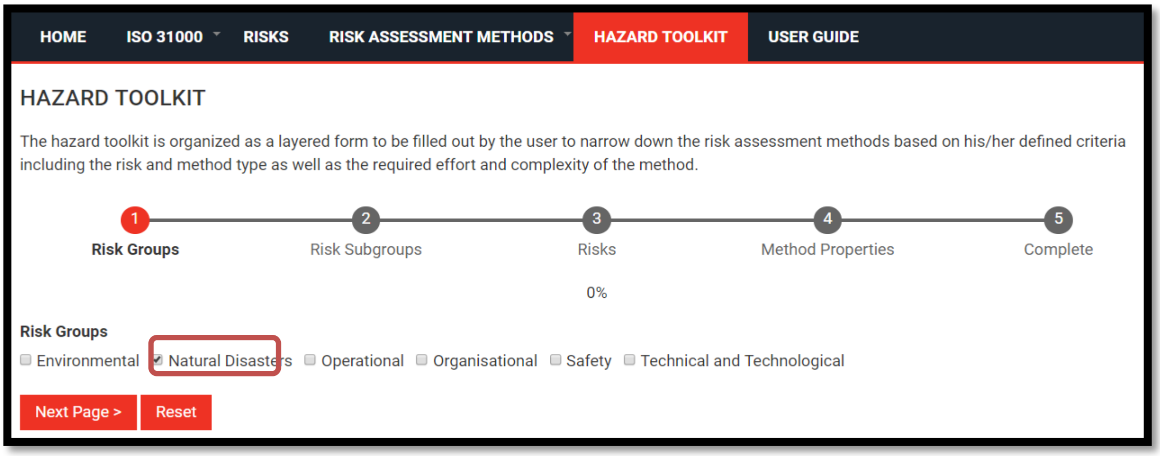
The method card contains all-important information about the risk assessment method including:

1. A short description
2. The ISO 31000 step(s) the method is adequate for
3. Complexity
4. Method type
5. Effort
6. Prerequisites
7. Related (linked) risks
8. The basic approach to follow
9. Advantages of using the method
10. Disadvantages of using the method
11. Useful attachments: Method card in pdf format, etc.
12. Related literature sources

5 HAZARD Toolkit

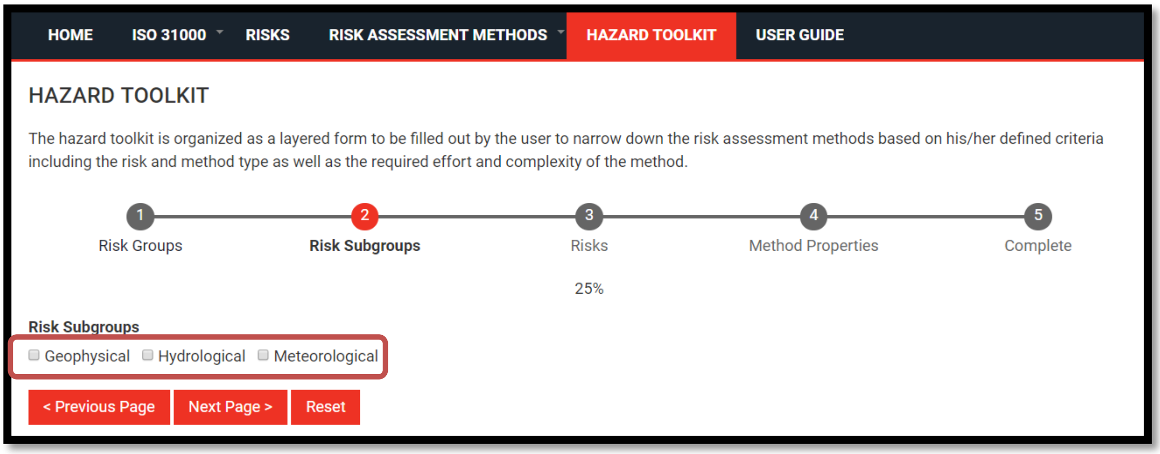
The first step of the HAZARD Toolkit permits the user to choose from the list of uppermost elements of the risk hierarchy. In other words, the user may choose which groups of risks he/she is interested in from the following list:

- Environmental
- Natural Disasters
- Operational
- Organisational
- Safety
- Technical and Technological

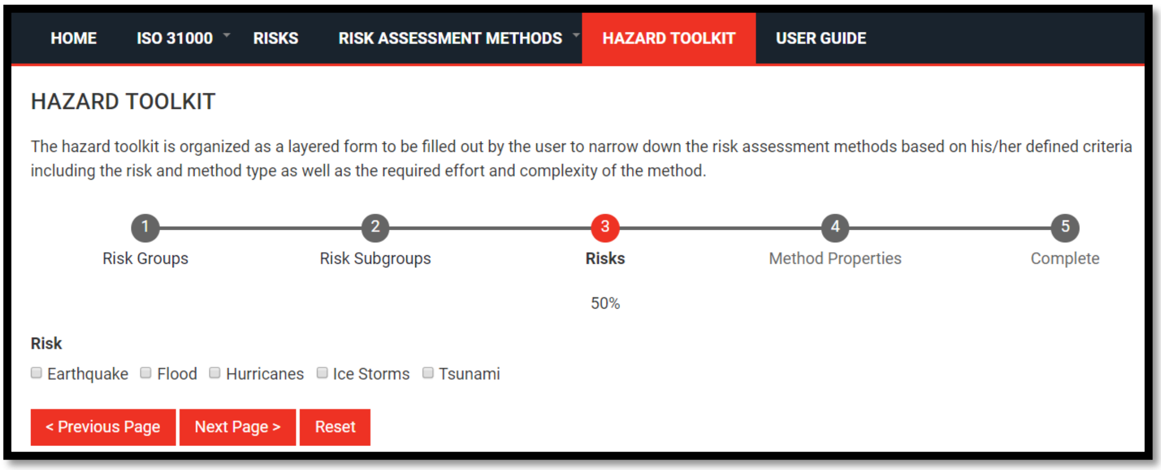


In the next step (after clicking on *Next Page*), the user is prompted to choose from the subgroups of risks based on his/her choice in the previous step, in order to further reduce the search area.

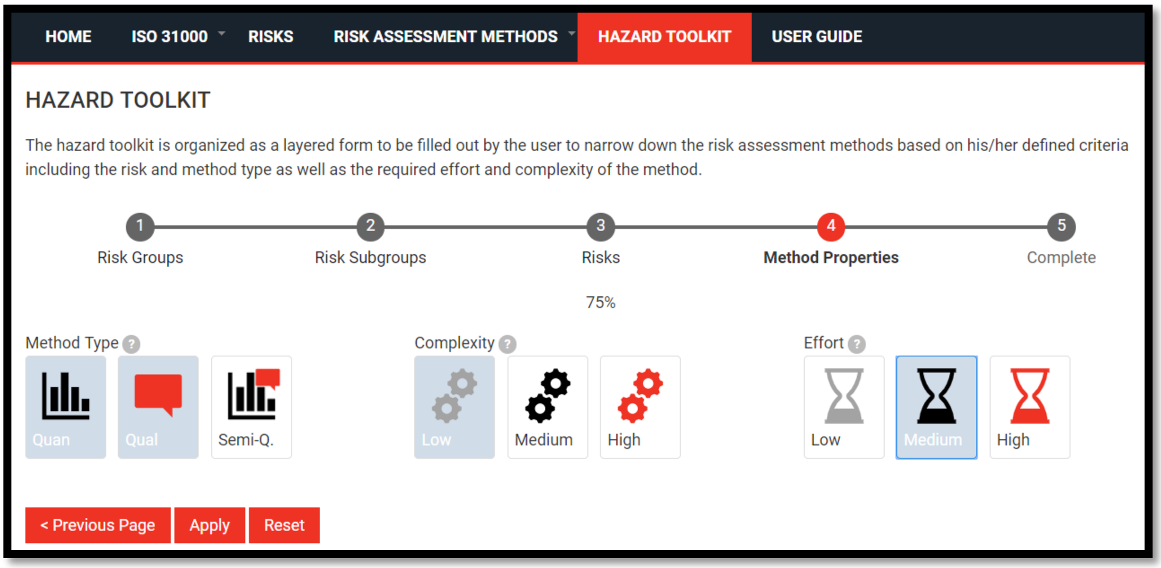
For example, if the user chose *Natural Disasters* in the previous step, then the corresponding subgroups *Metrological*, *Hydrological* and *Geophysical* will appear in the Risk Subgroup Step as shown below:



After choosing the risk subgroups on the *Risk Subgroup* page and clicking on *Next Page*, a new page opens displaying the concrete/specific risks belonging to the previously chosen subgroups. These risks describe situational hazards that may occur in practice in a harbour setting. The user may again choose one or multiple risks that they would like to assess.



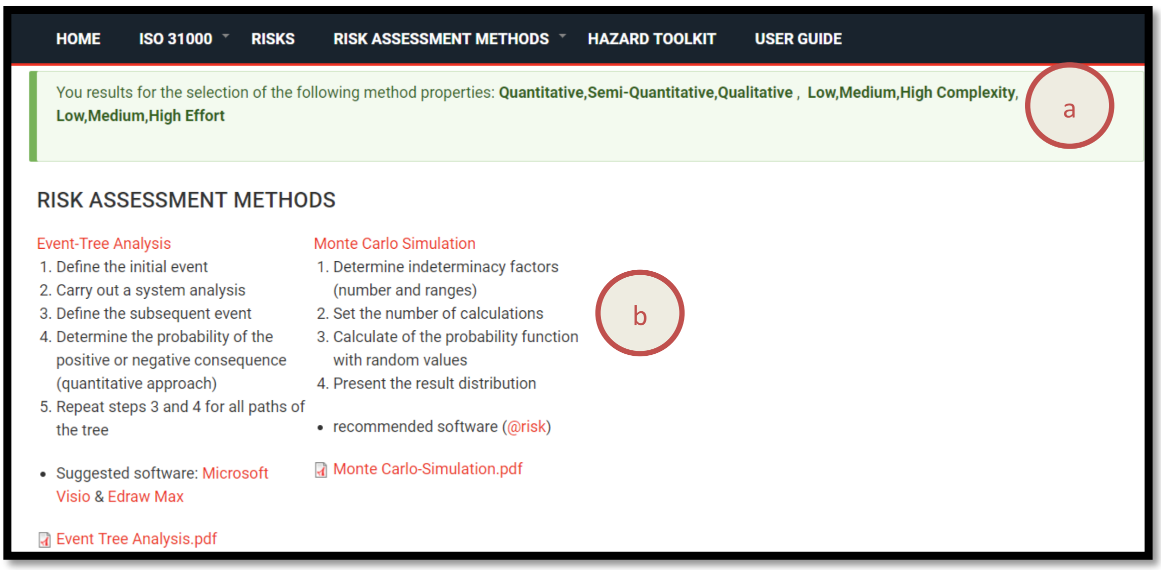
The last step of the HAZARD Toolkit is a menu page offering the possibility to determine the properties of the risk assessment methods that are relevant for the user. Here, it is possible to choose the method type, the effort and the desired complexity. For both effort and complexity, a simple scale with the values high, medium and low, is used. It is possible to choose more than one value per property. For the method type, one can choose between quantitative, qualitative and semi-quantitative methods. Here again more than one value can be selected.



Once the user has made her/his choice of the desired method properties, the user can then proceed and click on *Apply* to access the output of the Toolkit. An example hereof is given in the following figure.

The message in the green box in a gives a reminder for the user, which method properties have been chosen.

The actual output is given in b. Here a list of one or more risk assessment methods is given, which are filtered following the criteria the user entered throughout the Toolkit steps. For each method, only the steps of its basic approach are laid out, to avoid overloading the user with unnecessary information. The complete method card can still be accessed by clicking on the method title, which is defined as a hyperlink.



8 CONCLUSION OF THE HAZARD SEAPORT RISK ASSESSMENT TOOLBOX

The HAZARD Seaport Risk Assessment Toolbox has been compiled to help stakeholders at seaports to better identify, analyse and evaluate the risks in their operational environment.

While it has been constructed especially with the Baltic Sea Region ports in mind, the generic structure and contents of the Toolbox make it applicable to a wider range of seaports and their stakeholders also beyond the European Union.

This guideline serves as a basis to guide stakeholders on how to use the Toolbox itself. The interview study conducted at major BSR seaports revealed that there is no standard implemented process for risk assessment. Therefore, a standard process for risk assessment according to ISO 31000:2018 was selected to enable a clear understanding of the principles, framework as well as the phases of risk assessment process.

The online HAZARD Toolbox is based on the requirements defined by the stakeholders represented by authorities, port operators and rescue services. These requirements include for example the development of a guideline to perform risk analysis, identifying threats and hazards, simulation solutions and the provision of a proactive risk management approach.

The principles, framework and process of ISO 31000 with the associated risk assessment methods and risks would enable stakeholders to perform risk assessment according to their scope, context and requirements. Several methods for risk assessment provide a comprehensive identification of possible threats and hazard sources that could trigger a top event (risk). Simulation methods are integrated into the Toolbox to enable an accurate quantitative analysis of spills and leakages associated with oil and hazardous materials.

A various set of quantitative, qualitative, semi-quantitative as well as hybrid methods are provided to align the complexity and effort of the chosen methods with the resources and time constraints of the user. The detailed description of each method can be viewed, as a method card, in the online Toolbox.

The Toolbox is accompanied with clear guideline and user manual to provide clear steps to identify, analyse and evaluate risks that could occur at seaports. The Toolbox is structured to be dynamic so that additional methods, risks and other content can be added. Additional workshops and exercises will be carried out to improve and expand the current content of the Toolbox.

REFERENCES

Andrews, J. D., Ridley, L. M. (2002): Application of the cause–consequence diagram method to static systems, *Reliability Engineering & System Safety*, 75(1), pp. 47–58.

Belamarić, G., Kurtela, Ž., Bošnjak, R. (2016): Simulation method-based oil spill pollution risk analysis for the port of šibenik, *Transactions on maritime science*, 5(2), pp. 141–154.

Birkmann, J. (2011): First- and second-order adaptation to natural hazards and extreme events in the context of climate change, *Natural Hazards*, 58(2), pp. 811–840.

Hamka, M. (2017): Safety risks assessment on container terminal using hazard identification and risk assessment and fault tree analysis methods, *Procedia engineering*, 194(1), pp. 307–314.

Hogganvik, I. and Stølen, K., (2006): A graphical approach to risk identification, motivated by empirical investigations, *International Conference on Model Driven Engineering Languages and Systems*, pp. 574-588, Springer, Berlin, Heidelberg.

International Organization for Standardization (2018), ISO 31000: 2018, Risk management–Guidelines.

John, A., Paraskevadakis, D., Bury, A., Yang, Z., Riahi, R., Wang, J. (2014): An integrated fuzzy risk assessment for seaport operations, *Safety Science*, 68(1), pp. 180–194.

John, A, Yang, Z, Riahi, R, Wang, J. (2016): A risk assessment approach to improve the resilience of a seaport system using Bayesian networks, *Ocean Engineering*, 111(1), pp. 136–147.

Kaundinya, I. Nisancioglu, S, Kammerer, H, Oliva, R. (2016): All-hazard Guide for Transport Infrastructure, Transportation Research Procedia, 14(1), pp. 1325–1334.

Kwesi-Buor, J., Menachof, D.A. and Talas, R., (2016): Scenario analysis and disaster preparedness for port and maritime logistics risk management, Accident Analysis & Prevention.

Laine, V., Goerlandt, F., Baldauf, M., Mehdi, R., Beşikçi, E., Koldenhof, Y. (2018): OpenRisk Guideline. Methods for Maritime Risk Assessement on Accidental Spills.

Liungman, O. and Mattsson, J., (2011): Scientific Documentation of Seatrack Web; physical processes, algorithms and references, online available at: https://stw-helcom.smhi.se.

Mokhtari, K., Ren, J., Roberts, C., Wang, J. (2011): Application of a generic bow-tie based risk analysis framework on risk management of sea ports and offshore terminals, *Journal of hazardous materials*, 192 (2), pp. 465–475.

Na, U., Shinozuka, M. (2009): Simulation-based seismic loss estimation of seaport transportation system, *Reliability Engineering & System Safety*, 94 (3), pp. 722–731

Nagi, A., Schröder, M., Kersten, W. (2018): Cooperative Risk Management in Seaports: A Theoretical Framework, *Proceedings of the 30th Annual NOFOMA Conference*, pp. 401 – 416, Kolding, Denmark.

National Fire Protection Association, 2017. NFPA 704, Standard System for the Identification of the Hazards of Materials for Emergency Response. National Fire Protection Association.

Pasman, H. J., Rogers, W. J., Mannan, M. S. (2017): Risk assessment: What is it worth? Shall we just do away with it, or can it do a better job?, *Safety Science*, 99(1), pp. 140–155.

Polatidis, N, Pavlidis, M, Mouratidis, H. (2018): Cyber-attack path discovery in a dynamic supply chain maritime risk management system, *Computer Standards & Interfaces*, 56(1), pp. 74–82.

Rausand, M., (2005), Preliminary hazard analysis, Norwegian University of Science and Technology.

Schmidt, J, Matcham, I, Reese, S, King, A, Bell, R, Henderson, R.,. . . Heron, D. (2011): Quantitative multi-risk analysis for natural hazards: A framework for multi-risk modelling, *Natural Hazards*, *58*(3), pp. 1169–1192.

Sen, A., (2000), The discipline of cost-benefit analysis. The Journal of Legal Studies, 29(2), pp. 931-952.

Stamatis, D.H., (2003): Failure mode and effect analysis: FMEA from theory to execution, ASQ Quality press.

Yang, Z. L, Bonsall, S., Wang, J. (2010): Facilitating uncertainty treatment in the risk assessment of container supply chains, *Journal of Marine Engineering & Technology*, *9*(2), pp. 23–36.

HAZARD Project has 14 full Partners and a total budget of 4.3 million euros. It is executed from spring 2016 till spring 2019 and is part-funded by EU's Baltic Sea Region Interreg programme.

HAZARD aims at mitigating the effects of major accidents and emergencies in major multimodal seaports in the Baltic Sea Region, all handling large volumes of cargo and/or passengers.

Port facilities are often located close to residential areas, thus potentially exposing a large number of people to the consequences of accidents. The HAZARD project deals with these concerns by bringing together Rescue Services, other authorities, logistics operators and established knowledge partners.

HAZARD enables better preparedness, coordination and communication, more efficient actions to reduce damages and loss of life in emergencies, and handling of post-emergency situations by making a number of improvements.

These include harmonization and implementation of safety and security standards and regulations, communication between key actors, the use of risk analysis methods and adoption of new technologies.

See more at: http://blogit.utu.fi/hazard/

EU STRATEGY FOR THE BALTIC SEA REGION FLAGSHIP
Interreg Baltic Sea Region
EUROPEAN UNION EUROPEAN REGIONAL DEVELOPMENT FUND
HAZARD