Funded by
the European Union

Transformational Learning Network for Resilience

Enabling Ukrainian higher education to ensure a sustainable and robust reconstruction of (post-war) Ukraine

ZHYTOMYR POLYTECHNIC STATE UNIVERSITY

RISK MANAGEMENT. RISK ASSESSMENT TECHNIQUES

Iryna Patseva,
doctor of technical sciences, professor

Liudmyla Herasymchuk,
candidate of agricultural sciences, associate professor

Content

1. Terms and definitions

Funded by the European Union

Terms and definitions

Risk	Risk management	Risk management framework
• effect of uncertainty	• coordinated activities to direct and control an organization with regard to risk	• set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management processes throughout the organization

Terms and definitions

Risk management plan

- document within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk

Risk management

- coordinated activities to direct and control an organization with regard to risk

Risk management process

- systematic application of management policies, procedures and practices to the tasks of communicating, consulting, establishing the context, identifying, analyzing, evaluating, treating, monitoring and reviewing risk

Terms and definitions

Kisk assessment

- overall process of risk identification, risk analysis and risk evaluation

Risk identification

- process of finding, recognizing and describing risks

Risk description

- A structured statement of risk, usually covering 4 elements: sources (process of finding, recognizing and describing risks), event (occurrence or change of a particular set of circumstances), causes and effects

Терміни

Risk analysis

- process to comprehend the nature of risk and to determine the level of risk

Level of risk

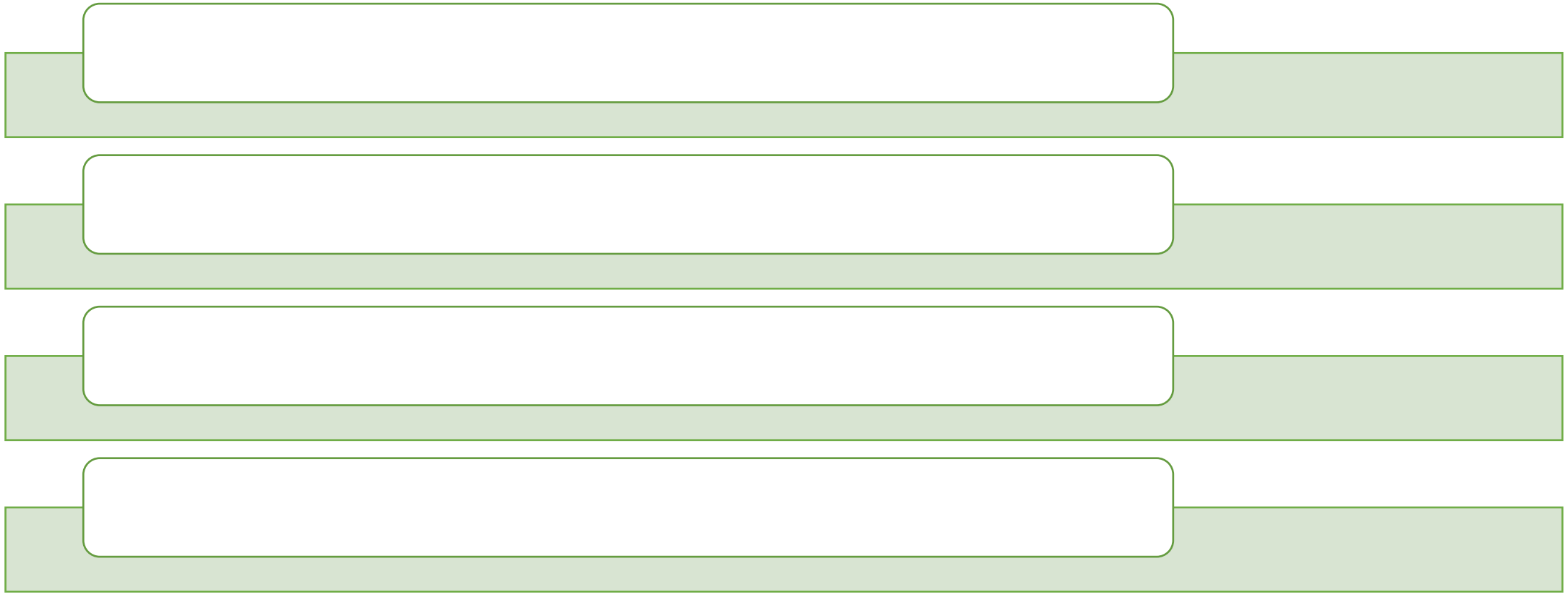
- magnitude of a risk expressed in terms of the combination of consequences and their likelihood

2. Risk assessment concepts

The risk management process aids decision making by taking account of uncertainty and the possibility of future events or circumstances (intended or unintended) and their effects on agreed objectives.

Funded by the European Union

Risk management includes the application of logical and systematic methods for

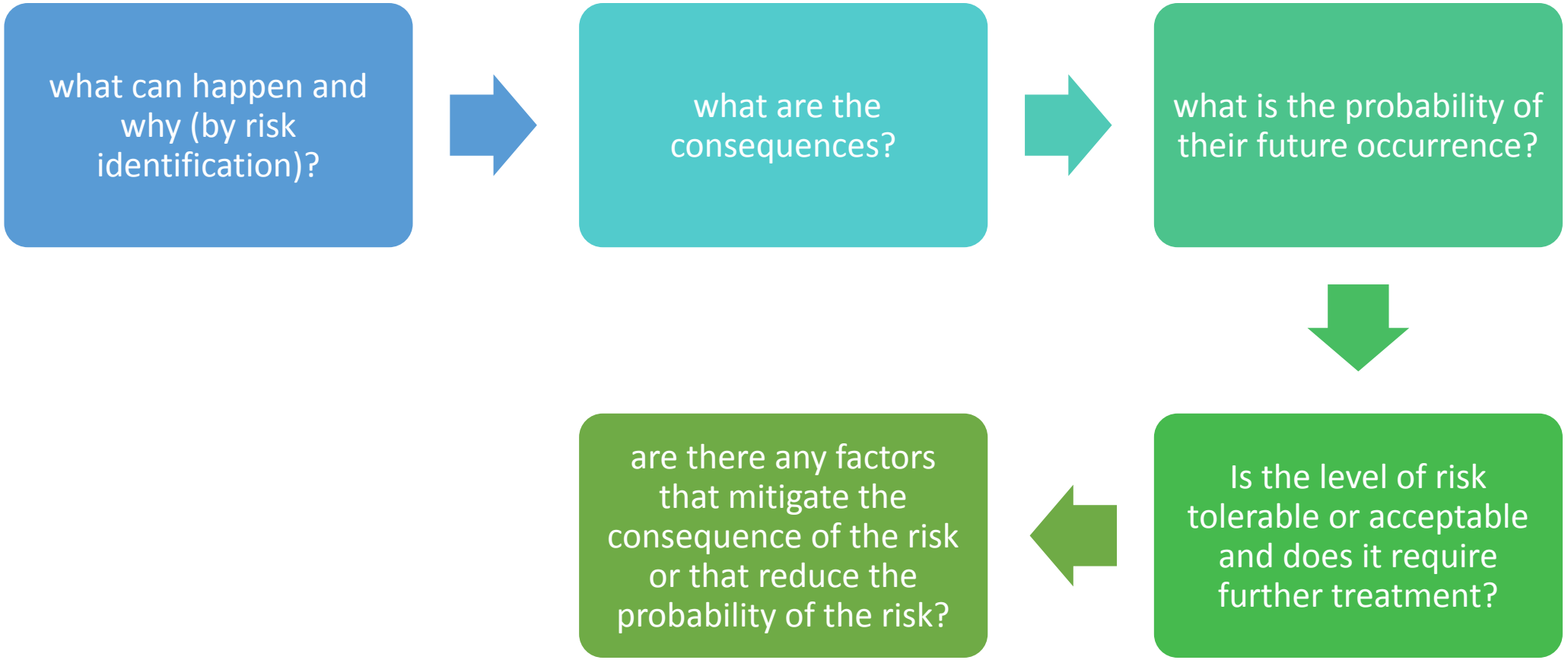


Risk assessment

is that part of risk management which provides a structured process that identifies how objectives may be affected, and analyses the risk in term of consequences and their probabilities before deciding on whether further treatment is required.

Funded by the European Union
TransLearn

Risk assessment attempts to answer the following fundamental questions:



The purpose of risk assessment

is to provide evidence-based information and analysis to make informed decisions on how to treat particular risks and how to select between options.

Some of the principal benefits of performing risk assessment include:

Funded by the European Union

- understanding the risk and its potential impact upon objectives
- providing information for decision makers
- contributing to the understanding of risks, in order to assist in selection of treatment options
- identifying the important contributors to risks and weak links in systems and organizations
- comparing of risks in alternative systems, technologies or approaches
- communicating risks and uncertainties
- assisting with establishing priorities
- contributing towards incident prevention based upon post-incident investigation
- selecting different forms of risk treatment
- meeting regulatory requirements
- providing information that will help evaluate whether the risk should be accepted when compared with pre-defined criteria
- assessing risks for end-of-life disposal

Funded by the European Union
TransLearn

Risk assessment comprises the core elements of the risk management process which are defined in ISO 31000 and contain the following elements:

- communication and consultation
- establishing the context
- risk assessment (comprising risk identification, risk analysis and risk evaluation)
- risk treatment
- monitoring and review

Risk assessment is not a stand-alone activity and should be fully integrated into the other components in the risk management process.

Successful risk assessment is dependent on effective communication and consultation with stakeholders.

Involving stakeholders in the risk management process will assist in:

Funded by the European Union

- developing a communication plan
- defining the context appropriately
- ensuring that the interests of stakeholders are understood and considered
- bringing together different areas of expertise for identifying and analysing risk
- ensuring that different views are appropriately considered in evaluating risks
- ensuring that risks are adequately identified
- securing endorsement and support for a treatment plan

Stakeholders should contribute to the interfacing of the risk assessment process with other management disciplines, including change management, project and programme management, and also financial management.

Establishing the context

defines the basic parameters for managing risk and sets the scope and criteria for the rest of the process. Establishing the context includes considering internal and external parameters relevant to the organization as a whole, as well as the background to the particular risks being assessed.

In establishing the context, the risk assessment objectives, risk criteria, and risk assessment programme are determined and agreed.

For a specific risk assessment, establishing the context should include the definition of the external, internal and risk management context and classification of risk criteria:

Funded by the European Union

1) Establishing the external context involves familiarization with the environment in which the organization and the system operates (slide 21)

2) Establishing the internal context (slide 22)

3) Establishing the context of the risk management process (slide 23)

4) Defining risk criteria (slide 24)

1) Establishing the external context involves familiarization with the environment in which the organization and the system operates including :

cultural, political, legal, regulatory, financial, economic and competitive environment factors, whether international, national, regional or local

key drivers and trends having impact on the objectives of the organization

perceptions and values of external stakeholders

Funded by the European Union

2) Establishing the internal context involves understanding

capabilities of the organization in terms of resources and knowledge	information flows and decision-making processes	internal stakeholders	objectives and the strategies that are in place to achieve them
perceptions, values and culture	policies and processes	standards and reference models adopted by the organization	structures (e.g. governance, roles and accountabilities)

Funded by the European Union

3) Establishing the context of the risk management process includes

- defining accountabilities and responsibilities
- defining the extent of the risk management activities to be carried out, including specific inclusions and exclusions
- defining the extent of the project, process, function or activity in terms of time and location
- defining the relationships between a particular project or activity and other projects or activities of the organization
- defining the risk assessment methodologies
- defining the risk criteria
- defining how risk management performance is evaluated
- identifying and specifying the decisions and actions that have to be made
- identifying scoping or framing studies needed, their extent, objectives and the resources required for such studies

4) Defining risk criteria involves deciding

the nature and types of consequences to be included and how they will be measured	the way in which probabilities are to be expressed	how a level of risk will be determined
the criteria by which it will be decided when a risk needs treatment	the criteria for deciding when a risk is acceptable and/or tolerable	whether and how combinations of risks will be taken into account

Criteria can be based on sources such as

- agreed process objectives
- criteria identified in specifications
- general data sources
- generally accepted industry criteria such as safety integrity levels
- organizational risk appetite
- legal and other requirements for specific equipment or applications

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

Risks can be assessed at an organizational level, at a departmental level, for projects, individual activities or specific risks. Different tools and techniques may be appropriate in different contexts.

Funded by the European Union
TransLearn

Risk assessment provides an understanding of risks, their causes, consequences and their probabilities. This provides input to decisions about:

- whether an activity should be undertaken
- how to maximize opportunities
- whether risks need to be treated
- choosing between options with different risks
- prioritizing risk treatment options
- the most appropriate selection of risk treatment strategies that will bring adverse risks to a tolerable level

Having completed a risk assessment, risk treatment involves selecting and agreeing to one or more relevant options for changing the probability of occurrence, the effect of risks, or both, and implementing these options.

This is followed by a cyclical process of reassessing the new level of risk, with a view to determining its tolerability against the criteria previously set, in order to decide whether further treatment is required.

Funded by the European Union

As part of the risk management process, risks and controls should be monitored and reviewed on a regular basis to verify that

- assumptions about risks remain valid
- assumptions on which the risk assessment is based, including the external and internal context, remain valid
- expected results are being achieved
- results of risk assessment are in line with actual experience
- risk assessment techniques are being properly applied
- risk treatments are effective

3. Risk assessment process

3.1 Overview

3.2 Risk identification

3.3 Risk analysis

3.4 Risk evaluation

3.5 Documentation

3.6 Monitoring and reviewing risk assessment

3.7 Application of risk assessment during life cycle phases

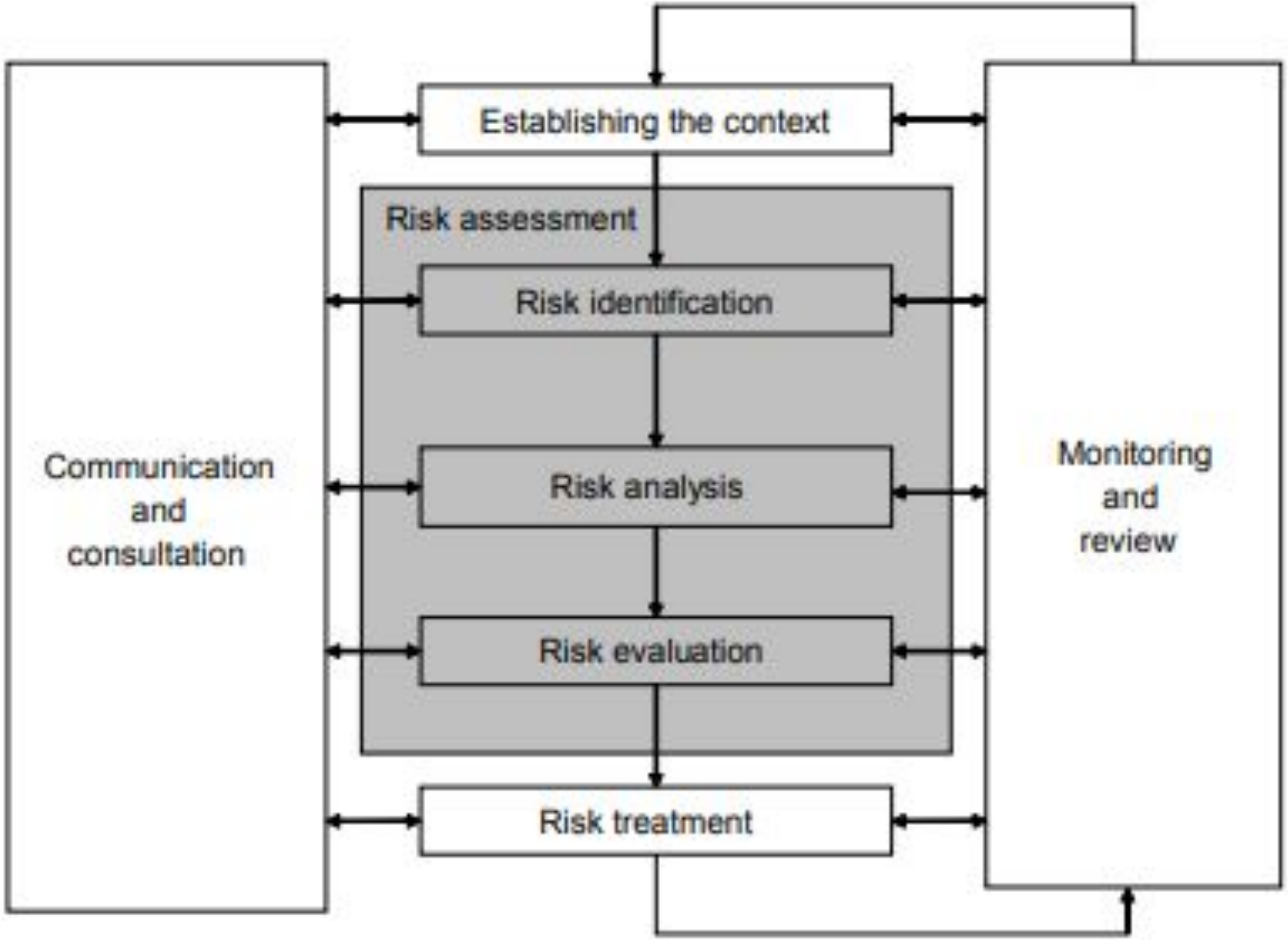
Overview

Risk assessment provides decision-makers and responsible parties with an improved understanding of risks that could affect achievement of objectives, and the adequacy and effectiveness of controls already in place. This provides a basis for decisions about the most appropriate approach to be used to treat the risks. The output of risk assessment is an input to the decision-making processes of the organization.

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation. The manner in which this process is applied is dependent not only on the context of the risk management process but also on the methods and techniques used to carry out the risk assessment.

Funded by the European Union

Contribution of risk assessment to the risk management process



Risk identification is the process of finding, recognizing and recording risks.

Risk identification

The purpose of risk identification is to identify what might happen or what situations might exist that might affect the achievement of the objectives of the system or organization. Once a risk is identified, the organization should identify any existing controls such as design features, people, processes and systems.

The risk identification process includes identifying the causes and source of the risk (hazard in the context of physical harm), events, situations or circumstances which could have a material impact upon objectives and the nature of that impact.

Risk identification methods can include:

evidence based methods, examples of which are check-lists and reviews of historical data

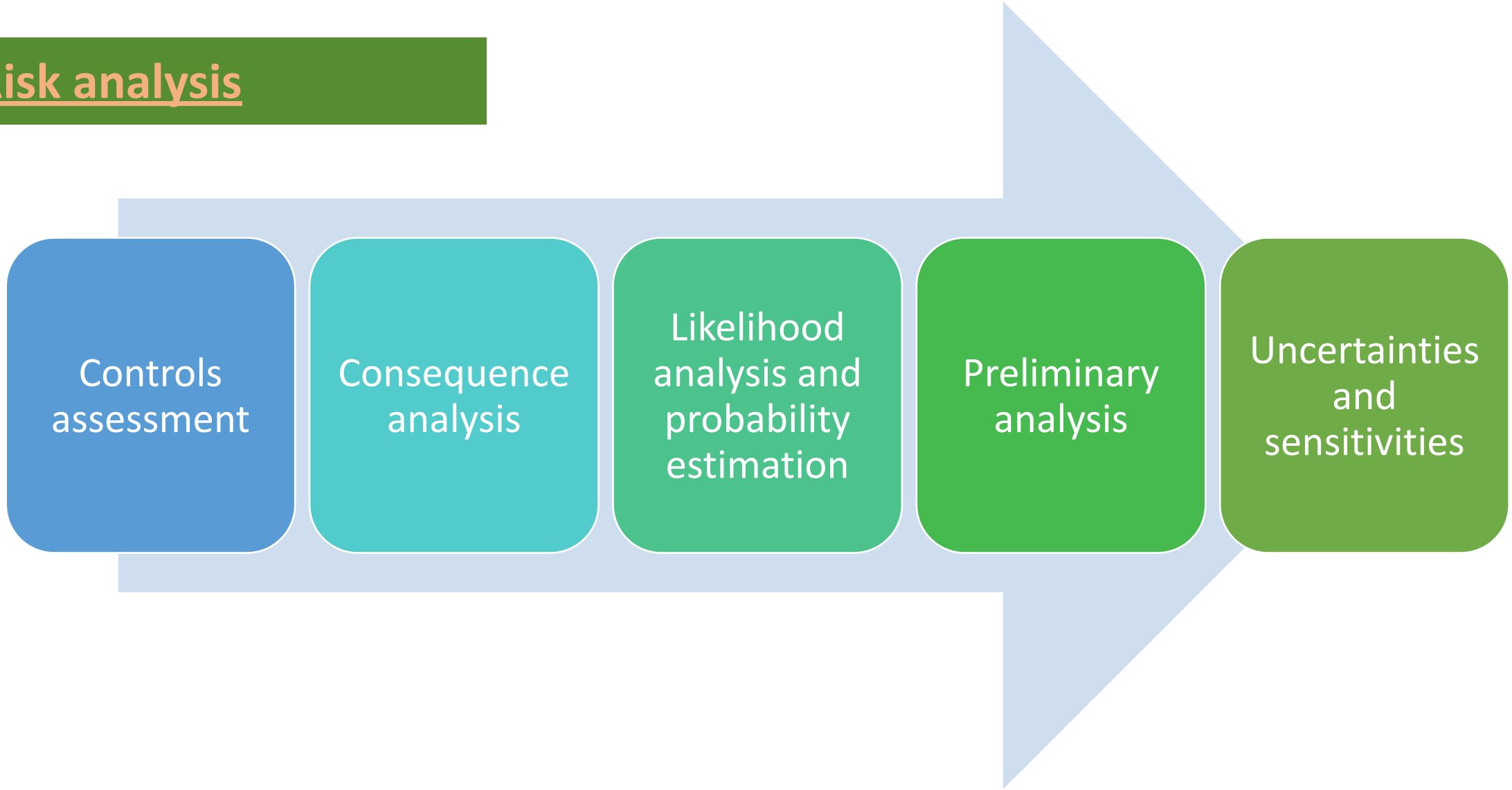
systematic team approaches where a team of experts follow a systematic process to identify risks by means of a structured set of prompts or questions

inductive reasoning techniques such as HAZOP

Various supporting techniques can be used to improve accuracy and completeness in risk identification, including brainstorming, and Delphi methodology.

Irrespective of the actual techniques employed, it is important that due recognition is given to human and organizational factors when identifying risk. Hence, deviations of human and organizational factors from the expected should be included in the risk identification process as well as "hardware" or "software" events.

Risk analysis



Risk analysis is about developing an understanding of the risk. It provides an input to risk assessment and to decisions about whether risks need to be treated and about the most appropriate treatment strategies and methods.

Risk analysis consists of determining the consequences and their probabilities for identified risk events, taking into account the presence (or not) and the effectiveness of any existing controls. The consequences and their probabilities are then combined to determine a level of risk.

Risk analysis involves consideration of the causes and sources of risk, their consequences and the probability that those consequences can occur. Factors that affect consequences and probability should be identified. An event can have multiple consequences and can affect multiple objectives. Existing risk controls and their effectiveness should be taken into account. More than one technique may be required for complex applications.

Risk analysis normally includes an estimation of the range of potential consequences that might arise from an event, situation or circumstance, and their associated probabilities, in order to measure the level of risk. However in some instances, such as where the consequences are likely to be insignificant, or the probability is expected to be extremely low, a single parameter estimate may be sufficient for a decision to be made

In some circumstances, a consequence can occur as a result of a range of different events or conditions, or where the specific event is not identified. In this case, the focus of risk assessment is on analysing the importance and vulnerability of components of the system with a view to defining treatments which relate to levels of protection or recovery strategies.

Methods used in analysing risks can be qualitative, semi-quantitative or quantitative. The degree of detail required will depend upon the particular application, the availability of reliable data and the decision-making needs of the organization. Some methods and the degree of detail of the analysis may be prescribed by legislation.

Qualitative assessment defines consequence, probability and level of risk by significance levels such as “high”, “medium” and “low”, may combine consequence and probability, and evaluates the resultant level of risk against qualitative criteria.

Semi-quantitative methods use numerical rating scales for consequence and probability and combine them to produce a level of risk using a formula. Scales may be linear or logarithmic, or have some other relationship; formulae used can also vary.

Quantitative analysis estimates practical values for consequences and their probabilities, and produces values of the level of risk in specific units defined when developing the context. Full quantitative analysis may not always be possible or desirable due to insufficient information about the system or activity being analysed, lack of data, influence of human factors, etc. Or because the effort of quantitative analysis is not warranted or required. In such circumstances, a comparative semi-quantitative or qualitative ranking of risks by specialists, knowledgeable in their respective field, may still be effective.

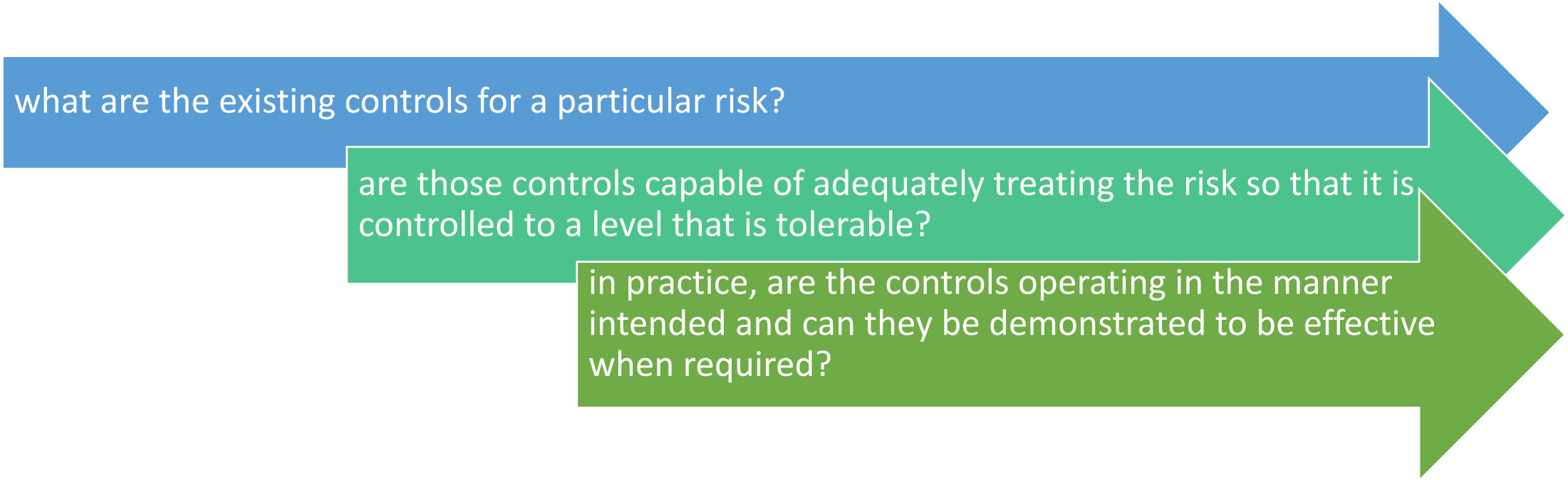
In cases where the analysis is qualitative, there should be a clear explanation of all the terms employed and the basis for all criteria should be recorded.

Even where full quantification has been carried out, it needs to be recognized that the levels of risk calculated are estimates. Care should be taken to ensure that they are not attributed a level of accuracy and precision inconsistent with the accuracy of the data and methods employed.

Levels of risk should be expressed in the most suitable terms for that type of risk and in a form that aids risk evaluation. In some instances, the magnitude of a risk can be expressed as a probability distribution over a range of consequences.

Controls assessmen

The level of risk will depend on the adequacy and effectiveness of existing controls. Questions to be addressed include:



These questions can only be answered with confidence if there are proper documentation and assurance processes in place.

The level of effectiveness for a particular control, or suite of related controls, may be expressed qualitatively, semi-quantitatively or quantitatively. In most cases, a high level of accuracy is not warranted. However, it may be valuable to express and record a measure of risk control effectiveness so that judgments can be made on whether effort is best expended in improving a control or providing a different risk treatment.

Consequence analysis

Consequence analysis determines the nature and type of impact which could occur assuming that a particular event situation or circumstance has occurred. An event may have a range of impacts of different magnitudes, and affect a range of different objectives and different stakeholders. The types of consequence to be analysed and the stakeholders affected will have been decided when the context was established.

Consequence analysis can vary from a simple description of outcomes to detailed quantitative modelling or vulnerability analysis.

Impacts may have a low consequence but high probability, or a high consequence and low probability, or some intermediate outcome. In some cases, it is appropriate to focus on risks with potentially very large outcomes, as these are often of greatest concern to managers. In other cases, it may be important to analyse both high and low consequence risks separately. For example, a frequent but low-impact (or chronic) problem may have large cumulative or long-term effects. In addition, the treatment actions for dealing with these two distinct kinds of risks are often quite different, so it is useful to analyse them separately.

Consequence analysis can involve

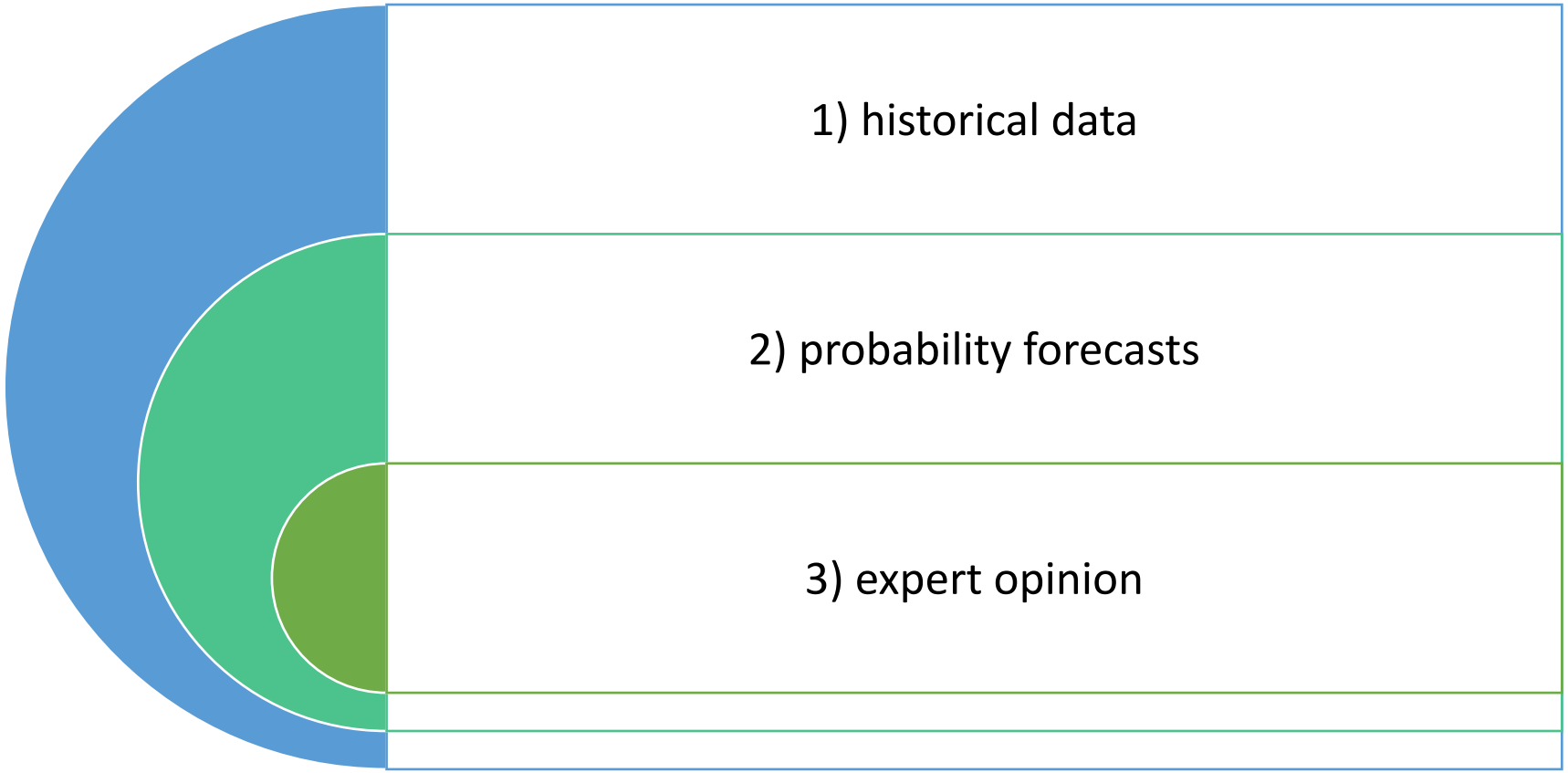
taking into consideration existing controls to treat the consequences, together with all relevant contributory factors that have an effect on the consequences

relating the consequences of the risk to the original objectives

considering both immediate consequences and those that may arise after a certain time has elapsed, if this is consistent with the scope of the assessment

considering secondary consequences, such as those impacting upon associated systems, activities, equipment or organizations

Three general approaches are commonly employed to estimate probability; they may be used individually or jointly:



1) historical data

The use of relevant historical data to identify events or situations which have occurred in the past and hence be able to extrapolate the probability of their occurrence in the future. The data used should be relevant to the type of system, facility, organization or activity being considered and also to the operational standards of the organization involved. If historically there is a very low frequency of occurrence, then any estimate of probability will be very uncertain. This applies especially for zero occurrences, when one cannot assume the event, situation or circumstance will not occur in the future.

2) probability forecasts

Probability forecasts using predictive techniques such as fault tree analysis and event tree analysis. When historical data are unavailable or inadequate, it is necessary to derive probability by analysis of the system, activity, equipment or organization and its associated failure or success states. Numerical data for equipment, humans, organizations and systems from operational experience, or published data sources are then combined to produce an estimate of the probability of the top event. When using predictive techniques, it is important to ensure that due allowance has been made in the analysis for the possibility of common mode failures involving the coincidental failure of a number of different parts or components within the system arising from the same cause. Simulation techniques may be required to generate probability of equipment and structural failures due to ageing and other degradation processes, by calculating the effects of uncertainties.

3) expert opinion

Expert opinion can be used in a systematic and structured process to estimate probability. Expert judgements should draw upon all relevant available information including historical, system-specific, organizational-specific, experimental, design, etc. There are a number of formal methods for eliciting expert judgement which provide an aid to the formulation of appropriate questions. The methods available include the Delphi approach, paired comparisons, category rating and absolute probability judgements.

Preliminary analysis

Risks may be screened in order to identify the most significant risks, or to exclude less significant or minor risks from further analysis. The purpose is to ensure that resources will be focussed on the most important risks. Care should be taken not to screen out low risks which occur frequently and have a significant cumulative effect

Screening should be based on criteria defined in the context.

The initial assumptions and results should be documented.

The preliminary analysis determines one or more of the following courses of action:

decide to treat risks without further assessment

set aside insignificant risks which would not justify treatment

proceed with more detailed risk assessment

Uncertainties and sensitivities

There are often considerable uncertainties associated with the analysis of risk. An understanding of uncertainties is necessary to interpret and communicate risk analysis results effectively. The analysis of uncertainties associated with data, methods and models used to identify and analyse risk plays an important part in their application. Uncertainty analysis involves the determination of the variation or imprecision in the results, resulting from the collective variation in the parameters and assumptions used to define the results. An area closely related to uncertainty analysis is sensitivity analysis.

Sensitivity analysis involves the determination of the size and significance of the magnitude of risk to changes in individual input parameters. It is used to identify those data which need to be accurate, and those which are less sensitive and hence have less effect upon overall accuracy.

The completeness and accuracy of the risk analysis should be stated as fully as possible. Sources of uncertainty should be identified where possible and should address both data and model/method uncertainties. Parameters to which the analysis is sensitive and the degree of sensitivity should be stated.

Risk evaluation

Risk evaluation involves comparing estimated levels of risk with risk criteria defined when the context was established, in order to determine the significance of the level and type of risk.

Risk evaluation uses the understanding of risk obtained during risk analysis to make decisions about future actions. Ethical, legal, financial and other considerations, including perceptions of risk, are also inputs to the decision.

Decisions may include:

- whether a risk needs treatment
- priorities for treatment
- whether an activity should be undertaken
- which of a number of paths should be followed

The nature of the decisions that need to be made and the criteria which will be used to make those decisions were decided when establishing the context but they need to be revisited in more detail at this stage now that more is known about the particular risks identified.

The simplest framework for defining risk criteria is a single level which divides risks that need treatment from those which do not. This gives attractively simple results but does not reflect the uncertainties involved both in estimating risks and in defining the boundary between those that need treatment and those that do not.

The decision about whether and how to treat the risk may depend on the costs and benefits of taking the risk and the costs and benefits of implementing improved controls.

Funded by the European Union
TransLearn

A common approach is to divide risks into three bands:

an upper band

- where the level of risk is regarded as intolerable whatever benefits the activity may bring, and risk treatment is essential whatever its cost

a middle band (or 'grey' area)

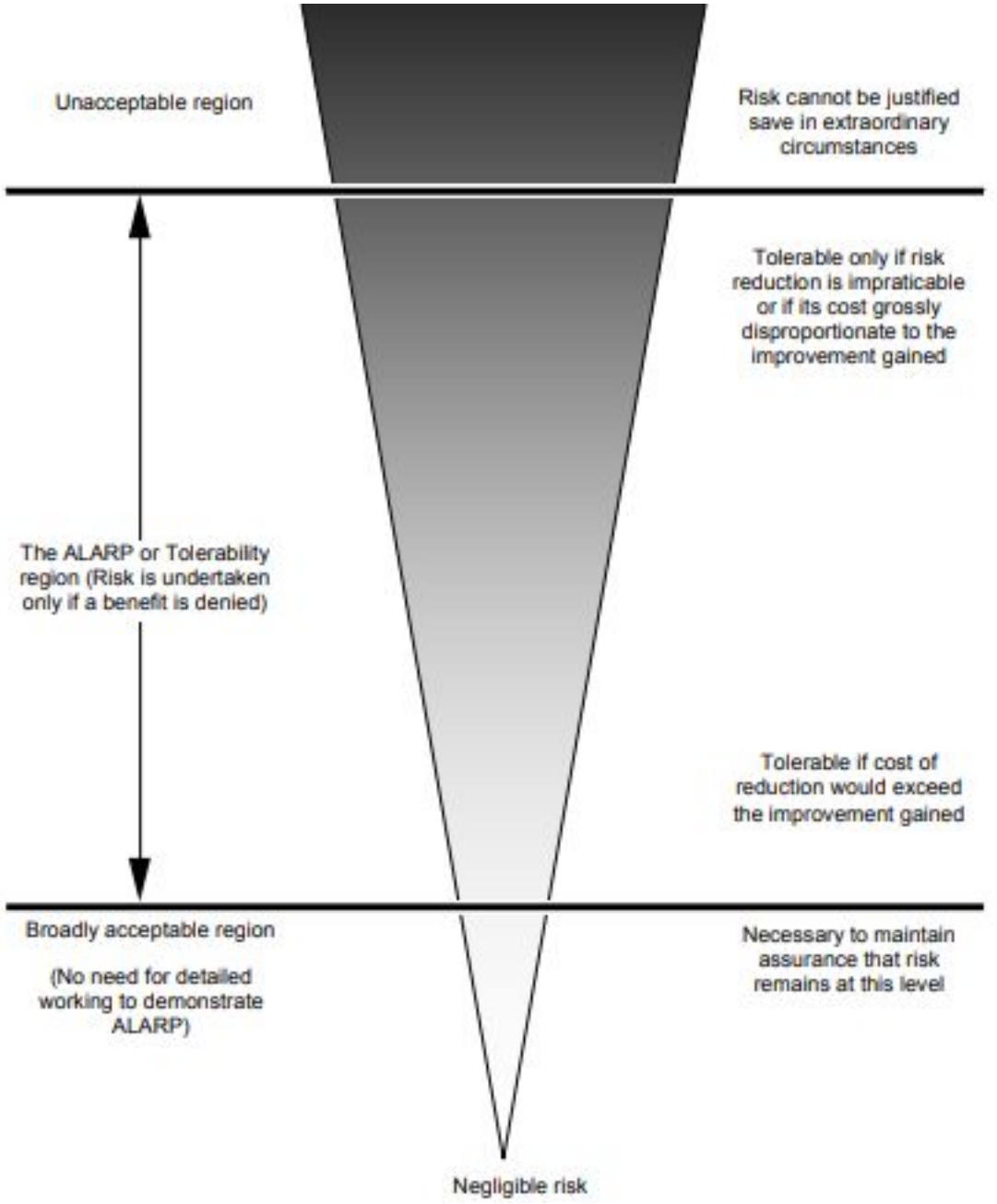
- where costs and benefits, are taken into account and opportunities balanced against potential consequences

a lower band

- where the level of risk is regarded as negligible, or so small that no risk treatment measures are needed

The ‘as low as reasonably practicable’ or ALARP criteria system used in safety applications follows this approach, where, in the middle band, there is a sliding scale for low risks where costs and benefits can be directly compared, whereas for high risks the potential for harm must be reduced, until the cost of further reduction is entirely disproportionate to the safety benefit gained.

The ALARP concept



Funded by the European Union

Documentation

The risk assessment process should be documented together with the results of the assessment. Risks should be expressed in understandable terms, and the units in which the level of risk is expressed should be clear.

The extent of the report will depend on the objectives and scope of the assessment.

Funded by the European Union
TransLearn

The documentation can include:

- objectives and scope
- description of relevant parts of the system and their functions
- a summary of the external and internal context of the organization and how it relates to the situation, system or circumstances being assessed
- risk criteria applied and their justification
- limitations, assumptions and justification of hypotheses
- assessment methodology
- risk identification results
- data, assumptions and their sources and validation
- risk analysis results and their evaluation
- sensitivity and uncertainty analysis
- critical assumptions and other factors which need to be monitored
- discussion of results
- conclusions and recommendations
- references

If the risk assessment supports a continuing risk management process, it should be performed and documented in such a way that it can be maintained throughout the life cycle of the system, organization, equipment or activity. The assessment should be updated as significant new information becomes available and the context changes, in accordance with the needs of the management process.

Monitoring and reviewing risk assessment

The risk assessment process will highlight context and other factors that might be expected to vary over time and which could change or invalidate the risk assessment. These factors should be specifically identified for on-going monitoring and review, so that the risk assessment can be updated when necessary.

Data to be monitored in order to refine the risk assessment should also be identified and collected. The effectiveness of controls should also be monitored and documented in order to provide data for use in risk analysis. Accountabilities for creation and reviewing the evidence and documentation should be defined.

Application of risk assessment during life cycle phases

Many activities, projects and products can be considered to have a life cycle starting from initial concept and definition through realization to a final completion which might include decommissioning and disposal of hardware.

Risk assessment can be applied at all stages of the life cycle and is usually applied many times with different levels of detail to assist in the decisions that need to be made at each phase.

Life cycles phases have different requirements and need different techniques For example, during the concept and definition phase, when an opportunity is identified, risk assessment may be used to decide whether to proceed or not.

Where several options are available risk assessment can be used to evaluate alternative concepts to help decide which provides the best balance of positive and negative risks.

Funded by the European Union

During the design and development phase, risk assessment contributes to

- ensuring that system risks are tolerable
- the design refinement process
- cost effectiveness studies
- identifying risks impacting upon subsequent life-cycle phases

As the activity proceeds, risk assessment can be used to provide information to assist in developing procedures for normal and emergency conditions.

4. Selection of risk assessment techniques

Risk assessment may be undertaken in varying degrees of depth and detail and using one or many methods ranging from simple to complex. The form of assessment and its output should be consistent with the risk criteria developed as part of establishing the context.

The reasons for the choice of techniques should be given, with regard to relevance and suitability. When integrating the results from different studies, the techniques used and outputs should be comparable.

In general terms, suitable techniques should exhibit the following characteristics:

it should be justifiable and appropriate to the situation or organization under consideration

it should provide results in a form which enhances understanding of the nature of the risk and how it can be treated

it should be capable of use in a manner that is traceable, repeatable and verifiable

Funded by the European Union

Once the decision has been made to perform a risk assessment and the objectives and scope have been defined, the techniques should be selected, based on applicable factors such as:

- the objectives of the study. The objectives of the risk assessment will have a direct earing on the techniques used. For example, if a comparative study between different options is being undertaken, it may be acceptable to use less detailed consequence models for parts of the system not affected by the difference
- the needs of decision-makers. In some cases a high level of detail is needed to make a good decision, in others a more general understanding is sufficient
- the type and range of risks being analysed
- the potential magnitude of the consequences. The decision on the depth to which risk assessment is carried out should reflect the initial perception of consequences (although this may have to be modified once a preliminary evaluation has been completed);)
- the degree of expertise, human and other resources needed. A simple method, well done, may provide better results than a more sophisticated procedure poorly done, so long as it meets the objectives and scope of the assessment. Ordinarily, the effort put into the assessment should be consistent with the potential level of risk being analysed
- the availability of information and data. Some techniques require more information and data than others
- the need for modification/updating of the risk assessment. The assessment may need to be modified/updated in future and some techniques are more amendable than others in this regard
- any regulatory and contractual requirements.

Various factors influence the selection of an approach to risk assessment such as the availability of resources, the nature and degree of uncertainty in the data and information available, and the complexity of the application.

Resources and capabilities which may affect the choice of risk assessment techniques include:

the skills experience capacity and capability of the risk assessment team

constraints on time and other resources within the organization

the budget available if external resources are required

The nature and degree of uncertainty requires an understanding of the quality, quantity and integrity of information available concerning the risk under consideration. This includes the extent to which sufficient information about the risk, its sources and causes, and its consequences to the achievement of objectives is available. Uncertainty can stem from poor data quality or the lack of essential and reliable data. To illustrate, data collection methods may change, the way organizations use such methods may change or the organization may not have an effective collection method in place at all, for collecting data about the identified risk.

Uncertainty can also be inherent in the external and internal context of the organization. Available data do not always provide a reliable basis for the prediction of the future. For unique types of risks, historical data may not be available or there may be different interpretations of available data by different stakeholders. Those undertaking risk assessment need to understand the type and nature of the uncertainty and appreciate the implications for the reliability of the risk assessment results. These should always be communicated to decision-makers.

Risks can be complex in themselves, as, for example, in complex systems which need to have their risks assessed across the system rather than treating each component separately and ignoring interactions. In other cases, treating a single risk can have implications elsewhere and can impact on other activities. Consequential impacts and risk dependencies need to be understood to ensure that in managing one risk, an intolerable situation is not created elsewhere. Understanding the complexity of a single risk or of a portfolio of risks of an organization is crucial for the selection of the appropriate method or techniques for risk assessment.