The Risk Assessment Process

Risk assessment techniques

https://www.iso.org/standard/72140.html

- supporting standard of the ISO 31000 framework
- focuses on the risk assessment step
- not specific to information security
Introduction

– description of a selection of techniques mostly originated in the technical domain, that can be used in a wide range of settings and in different sectors.
– techniques have evolved over time and continue to evolve, and many can be used in a broad range of situations outside their original application.
– techniques can be adapted, combined and applied in new ways or extended to satisfy current and future needs.

Scope

– to provide guidance on the selection and application of techniques for assessing risk in a wide range of situations.

Main uses of the described risk assessment techniques: situations between the two following extremes

– known situations: established rules and procedures and previous assessments of risk can be used.
– novel, complex or challenging situations, with high uncertainty, little experience, and little information on which to base assessment: conventional techniques of analysis might not be useful or meaningful, and multiple techniques might be used.
How to select and apply one or more specific techniques

– choice tailored to the context and use, to provide information of the type and form needed by the stakeholders

– qualitative vs quantitative: choice based on the output of most use to stakeholders and the availability and reliability of data (quantitative techniques require high quality data)

– main criteria:
  • purpose of the assessment
  • stakeholders' needs
  • legal, regulatory and contractual requirements
  • operating environment and scenario
  • importance of decisions
  • available information
  • complexity of the situation
  • available expertise
## IEC/ISO 31010:2019 Risk assessment techniques

Characteristics of the techniques relevant to the above criteria, to be used for selecting which technique(s) to use

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application</strong></td>
<td>How the technique is used in risk assessment</td>
<td>Elicit views, identify, analyse cause, analyse controls, etc.</td>
</tr>
<tr>
<td><strong>Scope</strong></td>
<td>Applies to risk at organizational level, departmental or project level or individual processes or equipment level</td>
<td>organization, project/department, equipment/process</td>
</tr>
<tr>
<td><strong>Time horizon</strong></td>
<td>Looks at short-, medium- or long-term risk or is applicable to any time horizon</td>
<td>Short, medium, long, any</td>
</tr>
<tr>
<td><strong>Decision level</strong></td>
<td>Applies to risk at a strategic, tactical or operational level</td>
<td>Strategic, tactical, operational</td>
</tr>
<tr>
<td><strong>Starting info/data</strong></td>
<td>Level of starting information/data needed</td>
<td>High, medium, low</td>
</tr>
<tr>
<td><strong>Specialist expertise</strong></td>
<td>Level of expertise required for correct use</td>
<td>Low: intuitive or 1–2 days' training</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Moderate: training course &gt; 2 days</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High: significant training/specialist expertise</td>
</tr>
<tr>
<td><strong>Qualitative – quantitative</strong></td>
<td>Whether the method is qualitative, semi-quantitative or quantitative</td>
<td>quantitative, qualitative, semi-quantitative, either qualitatively or quantitatively</td>
</tr>
<tr>
<td><strong>Effort to apply</strong></td>
<td>Time and cost required to apply technique</td>
<td>high, medium, low</td>
</tr>
</tbody>
</table>
Categorization of the 41 selected techniques

- B1: eliciting views from stakeholders and experts
- B2: identifying risk
- B3: determining sources, causes and drivers of risk
- B4: analysing existing controls
- B5: understanding consequences and likelihood
- B6: analysing dependencies and interactions
- B7: providing measures of risk
- B8: evaluating the significance of risk
- B9: selecting between options
- **B10: recording and reporting**
B1. Eliciting views from stakeholders and experts

Main approaches: individual (interview, survey, etc.), group (brainstorming, etc.)
Pros: providing for a breadth of expertise, stakeholder involvement
Cons: subjectivity, biased views

Representative techniques
• brainstorming: stimulating and encourage a group of people to develop ideas related to one of more topics of any nature
• Delphi technique: gaining consensus of opinion on a particular topic from a group of experts by collecting and collating judgments through sequential questionnaires – first experts express their opinions individually, independently and anonymously, then they have access to each other views as the process progresses
• interviews: structured or semi-structured discussion with individuals
• surveys: engaging more people than interviews, with more restricted questions (typically through questionnaires)
B2. Identifying risk

Main kinds of techniques: evidence based (literature reviews, analysis of historical data, etc.), empirical methods, perception surveys, encouraging imaginative thinking about the future (e.g., scenario analysis), checklists or taxonomies

Representative techniques

- **Checklists, classifications and taxonomies** (e.g., NIST SP 800-30 taxonomies of threat sources and of vulnerability predisposing conditions)
- **Failure modes and effects analysis (FMEA)**: (i) subdividing hardware, systems, processes or procedures into elements, (ii) considering the ways in which each element might fail, the failure causes and effects
- **Hazard and operability (HAZOP) studies**: a structured and systematic examination of a planned or existing process, procedure or system to identify potential deviations from the design intent, and examining their possible causes and consequences
- **Scenario analysis**: developing models of how the future might turn out
Main kinds of techniques: causal analysis, bow tie analysis (included also in category B4).
Often a hierarchy of causes exists.

Representative technique: Ishikawa analysis (fishbone) method
A team approach to identify possible causes of any desirable or undesirable event, effect, issue or situation. The possible contributory factors are organized into broad categories to cover human, technical and organizational causes. The information is depicted in a fishbone (also called Ishikawa) diagram

example of fishbone diagram
(source: IEC 31010:2018)

http://pralab.diee.unica.it
Main goal: checking whether controls are appropriate and adequate. Any causal analysis technique can be used as a basis for checking that each cause is controlled.

Representative technique: Bow tie analysis

- Graphical depiction of pathways from independent causes of an event to its consequences, usually drawn by a team in a workshop scenario
- It shows the controls that modify the likelihood of the event and those that modify the consequences if the event occurs
- Useful to display and communicate information about risks in situations where an event has a range of possible causes and consequences
B4. Analysing existing controls

example of *bow-tie* diagram (source: IEC 31010:2018)

http://pralab.diee.unica.it
Main kind of approaches:

• exploring **consequences**: **experimentation**, research into **past events** (e.g., epidemiological studies), **modelling** (e.g., mathematical or engineering models and logic methods), **imaginative thinking** (e.g., scenario analysis)

• estimating **likelihood**: **extrapolation** from relevant historical data (if any), **synthesis** from data about failure or success rates of system components, probabilistic **simulation**
Representative techniques

- **Bayesian analysis** (see below)
- **Bayesian networks**: graphical models of the conditional dependencies between random variables
- **Business impact analysis**: analyses how incidents and events could affect an organization's operations, and identifies and quantifies the capabilities that would be needed to manage it
- **Event tree analysis** (see below)
- **Fault tree analysis** (see below)
- **Privacy impact analysis / data protection impact analysis**: analyse how incidents and events could affect a person's privacy and identify and quantify the capabilities that would be needed to manage it. The latter helps organizations comply with the requirements of the data protection regulators (e.g. **European Union General Data Protection Regulation**, GDPR) and demonstrate that appropriate measures have been taken to ensure compliance.
**B5. Understanding consequences and likelihood**

**Bayesian analysis:** given **mutually exclusive** hypotheses $H_1, \ldots, H_n$ with **prior** probabilities (**subjective** experts' beliefs) $P(H_i)$, their **posterior** probabilities based on newly available data $D$ can be computed by **Bayes' formula**:

$$P(H_i|D) = P(H_i) \frac{P(D|H_i)}{\sum_{j=1}^{n} P(H_j)P(D|H_j)}$$

**Limitations:**
- posterior probabilities heavily depend on the choice of the prior
- solving complex problems can involve high computational costs and be labour intensive
B5. Understanding consequences and likelihood

**Event tree analysis:** qualitative, graphical technique that represents the mutually exclusive sequences of events that could arise following an initiating event according to whether the various systems designed to change the consequences function or not ("forward" logic). The tree can be quantified to provide the conditional probabilities of the different possible outcomes, assuming independent controls.

**Strengths:**
- identifying events that might otherwise not be foreseen
- useful to improve control efficiency

**Limitations:**
- some important initiating events or event sequences may be missed
- only success and failure states of a system are considered, but not, e.g., partially operating controls
- overlooking dependencies along possible paths may lead to optimistic estimates of the likelihood of particular consequences
- difficult to build from scratch for complex systems

http://pralab.diee.unica.it
An example of event tree analysis (source: IEC 31010:2009): modelling the consequences of an explosion (initiating event) in a process plant.

Systems in place to mitigate outcomes:
- sprinkler system
- fire alarm

<table>
<thead>
<tr>
<th>Initiating event</th>
<th>Start of a fire</th>
<th>Sprinkler system works</th>
<th>Fire alarm is activated</th>
<th>Outcome</th>
<th>Frequency (per year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explosion</td>
<td></td>
<td></td>
<td>Yes 0.99</td>
<td>Controlled fire with alarm 7.9 × 10⁻³</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>No 0.001</td>
<td>Controlled fire with no alarm 7.9 × 10⁻⁶</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yes 0.8</td>
<td></td>
<td>Yes 0.999</td>
<td>Uncontrolled fire with alarm 8.0 × 10⁻⁵</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>No 0.01</td>
<td>Uncontrolled fire with no alarm 8.0 × 10⁻⁸</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>No fire               2.0 × 10⁻³</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
In the previous event tree

– the probability of each outcome can then be computed, *conditioned* to all the events in the path from the root, e.g.:

\[ P(\text{Controlled fire with alarm}) = P(\text{Fire alarm active} = \text{Yes} | \text{Spr. system works} = \text{Yes}, \text{Fire} = \text{Yes, Explosion}) \]

– this probability is usually difficult to estimate, due to lack of statistics about the *sequence* of events of interest

– a conditional independence assumption is then made, e.g.:

\[ P(\text{Controlled fire with alarm}) \approx P(\text{Fire alarm active} = \text{Yes}|\text{Fire} = \text{Yes}) \times P(\text{Spr. system works} = \text{Yes}|\text{Fire} = \text{Yes}) \times P(\text{Fire} = \text{Yes}|\text{Explosion}) = 0.999 \times 0.99 \times 0.8 \times 0.01 = 7.9 \times 10^{-3} \]
On each branch of the tree the **conditional probability** of the corresponding event is reported (when available):

1. \( P(\text{Start of a fire}|\text{Explosion}) \) (e.g., expert knowledge)
2. \( P(\text{Spr. sys. works}|\text{Fire}=\text{Yes}) \) (component **reliability**)
3. \( P(\text{Fire alarm works}|\text{Fire}=\text{Yes}) \) (component **reliability**)

<table>
<thead>
<tr>
<th>Event</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explosion</td>
<td>0.02 per year</td>
</tr>
<tr>
<td>Start of a fire</td>
<td>0.99</td>
</tr>
<tr>
<td>Sprinkler system works</td>
<td>Yes: 0.999, No: 0.001</td>
</tr>
<tr>
<td>Fire alarm is activated</td>
<td>Yes: 0.999, No: 0.001</td>
</tr>
<tr>
<td>Outcome</td>
<td>Frequency (per year)</td>
</tr>
<tr>
<td>Controlled fire with alarm</td>
<td>7.9 ( \times ) 10^{-3}</td>
</tr>
<tr>
<td>Controlled fire with no alarm</td>
<td>7.9 ( \times ) 10^{-6}</td>
</tr>
<tr>
<td>Uncontrolled fire with alarm</td>
<td>8.0 ( \times ) 10^{-5}</td>
</tr>
<tr>
<td>Uncontrolled fire with no alarm</td>
<td>8.0 ( \times ) 10^{-8}</td>
</tr>
<tr>
<td>No fire</td>
<td>2.0 ( \times ) 10^{-3}</td>
</tr>
</tbody>
</table>
Fault tree analysis: identifying and analysing factors that contribute to a specified undesired event ("top event"), which is analysed starting from its immediate and necessary causes (e.g., hardware or software failures, human errors) whose logical relationship is represented by, e.g., AND and OR gates ("backward" logic).

The occurrence of the top event is modelled as a Boolean equation, which is graphically represented as a tree diagram.

Main strengths:
- highly systematic, but at the same time flexible approach
- allows identifying simple failure pathways in a complex system

Main limitations:
- time interdependencies are not addressed
- only with binary states (success/failure) are considered
- fault trees can get very large for large scale systems
B5. Understanding consequences and likelihood

Fault tree analysis: an example

A security system in a hospital is powered by a generator. If the generator fails, a switching system switches over to a battery. The top event of interest is that the security system fails through lack of power.

Most important events

– the generator fails
– the switch fails
– the battery fails

How does the top event occur?

– if the generator fails and the back-up system (switch + battery) fails
– the back-up system can fail if either the switch fails or the battery fails
B5. Understanding consequences and likelihood

Fault tree analysis: an example

- **Top event**: System power failure
- **Basic events**:
  - Generator fails
  - Switch fails
  - Battery fails

- **Gates**:
  - AND gate
  - OR gate

http://pralab.diee.unica.it
B5. Understanding consequences and likelihood

Fault tree analysis: an example

• Every node of the tree can be seen as a Boolean variable
• A fault tree can then be considered as an expression in Boolean logic
• For the fault tree on the left:
  \[ T = G \cdot (S + B) \]
B5. Understanding consequences and likelihood

Fault tree analysis: an example

**Cut sets**: collections of basic events whose *simultaneous* occurrence leads to the occurrence of the top event:
- \( \{S, G, B\}, \{G, B\}, \{S, G\} \)

**Minimal cut sets**:
- \( \{G, B\}, \{S, G\} \)

Minimal cut sets can then be used to compute (estimate) the probability of the top event:

\[
P(T) = P((G \land B) \lor (S \land G))
\]
B.14 Fault tree analysis (FTA)

B.14.1 Overview
FTA is a technique for identifying and analysing factors that can contribute to a specified undesired event (called the “top event”). Causal factors are deductively identified, organized in a logical manner and represented pictorially in a tree diagram which depicts causal factors and their logical relationship to the top event.

The factors identified in the tree can be events that are associated with component hardware failures, human errors or any other pertinent events which lead to the undesired event.

Failed automatic start up of emergency generator

No start up signal

- Fault in sending signal
  - Broken conductor
  - Fault in circuit A
  - Fault in circuit B

- Fault in transmission of signal
- Fault in reception of signal

Diesel generator fault

- Missing fuel
- Mechanical fault in generator

Symbols
- And gate – fault occurs if all of input events true
- Or gate – fault occurs if any of input events is true
- Base events – further analysis not useful
- Events not analysed further at this time
- Events which are further analysed
- Event analysed at point A on a different page

B.14.2 Use
A fault tree may be used qualitatively to identify potential causes and pathways to a failure (the top event) or quantitatively to calculate the probability of the top event, given knowledge of the probabilities of causal events.

It may be used at the design stage of a system to identify potential causes of failure and hence to select between different design options. It may be used at the operating phase to identify how major failures can occur and the relative importance of different pathways to the head event. A fault tree may also be used to analyse a failure which has occurred to display diagrammatically how different events came together to cause the failure.

B.14.3 Inputs
For qualitative analysis, an understanding of the system and the causes of failure is required, as well as a technical understanding of how the system can fail. Detailed diagrams are useful to aid the analysis.

For quantitative analysis, data on failure rates or the probability of being in a failed state for all basic events in the fault tree are required.

Example of fault tree
(source: IEC 31010:2018)
B7. Providing measures of risk

Main feature: techniques strongly depend on the specific application.

Representative technique: Value at risk
Widely used in the financial sector to provide an indicator of the amount of possible loss in a portfolio of financial assets over a specific time period within a given confidence level.
Main kinds of techniques:
• deciding whether a particular risk is tolerable or acceptable
• indicating the relative significance of a risk or ranking risks in a priority order

Representative technique: Risk indices
A qualitative or semi-quantitative approach to rank and compare risks, by providing a measure of risk derived using a scoring approach and ordinal scales. Some examples:
• Disease risk index: estimating an individual's risk of contracting a particular disease by combining scores for various known risk factors identified in epidemiological studies, taking into account the strength of association between the risk factor and the disease
• Bush fire hazard ratings compare fire risk on different days taking account of predicted conditions such as humidity, wind strength, the dryness of the landscape and the fuel load
• Lenders calculate the credit risks for customers using indices that represent components of their financial stability
Goal: helping decision makers decide between options involving multiple risks, where trade-offs have to be made, providing a logical basis to justify reasons for a decision

Main applications
• decisions on expected financial loss or gain
• allowing different criteria to be weighted and trade-offs made
• exploring the possible consequences of different options
• modelling decision problems
Representative techniques

- **Cost/benefit analysis**: weighs the total expected costs of options in monetary terms against their total expected benefits, to choose the most effective or profitable option. It can be qualitative or quantitative, or a combination of both approaches. It can be applied at any level of an organization.

- **Decision tree analysis**: models the possible pathways from an initial decision that must be made (e.g., whether to proceed with Project A or Project B) to a range of subsequent events and further decisions. These are represented in tree format. The probability of the events can be estimated together with the expected value or utility of the final outcome of each pathway.
Representative techniques (cont.)

- **Game theory**: mathematical model of the consequences of different possible decisions given a number of possible future situations that can be determined by different decision makers or players (e.g., competitors, technologies), taking into account their pay-offs, to compute the optimal strategy of each player.

- **Multi-criteria analysis**: using a range of criteria to transparently assess and compare the overall performance of a set of options, usually to produce an order of preference. The analysis involves the development of a matrix of options and criteria which are ranked and aggregated to provide an overall score for each option.
Main reporting technique about risk magnitude: consequence/likelihood matrix (risk matrix or heat map)

- customized scales for consequence and likelihood need to be defined
- scales can be qualitative, semi-quantitative or quantitative
- colours in the heat map indicate the magnitude of risk
- additional information can be included (e.g., decision rules such as the level of management attention or the urgency of response)
- design should enable risk prioritization
- commonly used as a screening tool when many risks have been identified, e.g., to define which risks need to be referred to a higher level of management
- risks with potentially high consequences are often of greatest concern to decision makers even when the likelihood is very low
example of *risk matrix* as a heat map (source: IEC 31010:2018)
**B10. Recording and reporting**

**Strengths and limitations** of the risk matrix

**Strengths**

- relatively easy to use
- provides a rapid ranking of risks into different significance levels
- provides a clear visual display of the relevant significance of risk
- allows comparing risks with different types of consequences

**Limitations**

- good expertise is required to design a valid matrix
- defining meaningful scales can be difficult
- involves a high degree of subjectivity
- risks cannot be directly aggregated (e.g., is a set of many low-level risks equivalent to a medium risk?)
- combining or comparing the level of risk for different categories of consequences is difficult

http://pralab.diee.unica.it