Risk Assessment Frameworks

**What Is ISO/IEC 3101?**

[**ISO 31010**](https://www.iso.org/standard/72140.html)is a risk management standard developed by the International Organization for Standardization (ISO). It provides guidelines on assessing and managing risk in an organization and is intended to be used with other ISO risk management standards, such as ISO 31000. This publication provides a framework for organizations to identify, assess, and manage risk using various risk assessment techniques.

ISO 31010 is designed to be flexible and can be applied to a variety of contexts and industries. The standard is intended to help organizations make informed decisions about risk management and to develop [**risk management strategies**](https://lazarusalliance.com/what-are-the-problems-with-risk-management/) that are tailored to their specific needs and circumstances.

**What Are the Risk Assessment Implementation Guidelines in ISO 31010?**

Before providing the series of techniques that organizations can use for risk assessment, ISO 31010 includes guidelines on how to implement these techniques. Note that this implementation guide is meant to complement [**ISO 31000 guidelines**](https://www.iso.org/iso-31000-risk-management.html) on risk management and incorporate the techniques later defined in this document within that framework.

The general implementation guideline includes the:

* **Assessment Planning:**This process involves preparing the organization for its initial and ongoing risk assessments. These guidelines include defining the scope and purpose of the assessment, understanding the organizational context for assessing risk, including insight and expertise from SMEs within the organization, defining assessment objectives, establishing criteria for measuring risk, and understanding how social and human factors may impact both the assessment and ongoing risk management.
* **Information Management:**Collecting information is a critical part of risk assessment, and the methodologies employed to perform this task must align with the criteria and goals of the organization. Organizations should be able to source information (including determining reliability and category of information sources), analyze data within its historical lifecycle, and establish potential information uncertainties. In addition, the organization should model data and risk models at this point in its assessment process. Modeling data, in this context, means mapping problems, outcomes, and representations of processes into a model that makes the evaluation of inputs and outputs viable.
* **Application of Assessment Techniques:** This guideline guides how to determine sources of risk, identify risks, investigate the effectiveness of existing controls, and analyze the likelihood of risks. This guideline also directs organizations to follow techniques defined in Annex A and B of this document (described in more detail below).
* **Analysis Review:**Organizations should be able to verify and validate results from their risk assessment based on the models and metrics developed in the previous steps. This also includes working on any potential uncertainty that could shape the analysis of those results, such as system variables or unreliable data sources. Finally, organizations should use results to apply to decision-making.
* **Application of Results Towards Decision-Making:**Any decisions about measuring risks and their impact on a system, making determinations about acceptable risks, and selecting between different types of risk based on preferability should be informed by the described risk assessment process.

**What Are the Risk Assessment Techniques Outlined in ISO 31010?**

In line with its breakdown of a risk assessment process, ISO 31010 provides an appendix of specific techniques that an organization can use to follow through on its analysis. Additionally, these techniques are mapped explicitly into the risk assessment process defined in ISO/IEC 31000.

* **Eliciting Insights from Stakeholders and Experts (B1):** This family of techniques focuses on how to gather information from SMEs and other stakeholders in an accurate and effective way. Some techniques defined here include structured brainstorming, gaining a consensus from a group of experts (the Delphi technique), distributed 1-1 brainstorming sessions (Nominal group technique), interviews, and surveys.
* **Identifying Risks (B2):** This family of techniques emphasizes how the organization accurately gathers information on and identifies risks within its systems. These techniques include the use of classification and taxonomies, using Failure Modes and Effects (FMEA) and Failure Modes, Effects, and Criticality (FMCEA) Analysis, using Hazard and Operability (HAZOP) studies, scenario analysis, and Structured What-If Techniques (SWiFT).
* **Determining Sources of Risk (B3):**This family of techniques foregrounds the capacity of an organization to properly understand the causes of risks through the study of risk relationships. These techniques include analyzing intangible risk sources (Cindynic approach) and team-based causal analysis (Ishikawa analysis).
* **Analyzing Controls (B4):**This family of techniques emphasizes the organization's ability to determine if controls are adequate and appropriate for identified risks. This includes bow-tie analysis, Hazard Analysis and Critical Control Points (HACCP), and Layers of Protection Analysis (LOPA).
* **Understanding Consequences (B5):**These techniques help the organization understand the more significant impact of risks depending on the context and history of the system. These techniques include Bayesian analysis, Bayesian Networks and Influence Diagrams, Business Impact Analysis (BIA), Cause-Consequence Analysis (CCA), Event Tree Analysis (ETA), Fault Tree Analysis (FTA), Human Reliability Analysis (HRA), Markov Analysis, Monte Carlo simulation, and Privacy Impact Analysis (PIA).
* **Analyzing Dependencies (B6):**This technique requires that the organization perform causal mapping or use chains of argument or logic showing the relationships between events, controls, and risks. This includes causal mapping and cross-impact analysis.
* **Providing Measure of Risk (B7):** These techniques provide ways to measure risk impact on systems or the wider public. These techniques include toxicological risk assessment, Value at Risk (VaR) assessment, and Conditional VaR.
* **Evaluating Significance of Risk (B8):** This family of techniques defines ways to determine how to treat risk within the organization's context. This includes testing for the principle of "reasonably practicable" for risk toleration, using Frequency-Number (F-N) diagrams and Pareto charts, assessing based on Reliability-Centered, Maintenance (RCM), and using mapping risk indices.
* **Selecting Between Options (B9):**These techniques relate to the organization's capability to make decisions between two more paths for risk management, including decisions regarding acceptable risk and implemented controls. These techniques will include Cost-Benefit Analysis (CBA), decision tree analysis, game theory, and Multi-Criteria Analysis (MCA).
* **Recording and Reporting (B10):** These techniques refer to the organization's ability to record risk information into a database to provide insights into evolving risk potential and evaluation. These techniques will include risk registers, maintaining maintenance documents, and modeling with S-curves.

**Why Is it So Important to Manage Risk Effectively?**

Risk assessment helps organizations understand the potential impact of a cybersecurity breach and the likelihood of that breach occurring. Organizations can develop a plan to prevent, detect, and respond to cybersecurity incidents by identifying potential vulnerabilities and threats.

Additionally, risk assessments can help organizations allocate resources more effectively. Not all risks are created equal, and by assessing and prioritizing risks, organizations can focus their resources on the most critical areas of vulnerability.

Finally, many regulatory frameworks and standards, such as the GDPR and PCI DSS, require organizations to perform risk assessments as part of their compliance efforts. Failure to conduct risk assessments and mitigate identified risks can result in significant financial and reputational damage.

Some of the more general benefits of proper risk assessment include:

* **Prioritize Security Measures:**Risk assessment helps identify potential vulnerabilities and threats and rate them based on organizational priorities. Organizations can focus their resources on the most critical areas of vulnerability by understanding the likelihood and potential impact of a cybersecurity incident.
* **Improve Compliance Efforts:**Many regulatory frameworks and standards require organizations to perform risk assessments as part of their compliance efforts. Risk assessment can also help that organization better understand its security posture if it is optional.
* **Enhance Collaboration:**Risk assessment can help facilitate communication and collaboration between different stakeholders.
* By involving them in the risk assessment process, organizations can ensure everyone is on the same page regarding cybersecurity risks and strategies to mitigate them.