We've translated ISO 31000 risk management definitions into plain English in order to make them easier to understand*.

Communication and consultation - Consequence - Context - Control - Event

External context - Internal context - Level of risk - Likelihood - Monitoring - Residual risk

Review - Risk - Risk analysis - Risk assessment - Risk attitude - Risk criteria - Risk evaluation

Risk identification - Risk management - Risk management framework - Risk management plan

Risk management policy - Risk management process - Risk owner - Risk profile

Risk source - Risk treatment - Stakeholder

Communication and consultation

Communication and consultation **is a dialogue between an organization and its stakeholders. This dialogue is both continual and iterative. It is a two-way process that involves both sharing and receiving information about the management of risk. However, this is not joint decision making. Once communication and consultation is finished, decisions are made and directions are set by the organization, not by stakeholders. Discussions could be about risks, their nature, form, likelihood, and significance, as well as whether or not risks are acceptable or should be treated, and what treatment options should be considered.**

Consequence

A *consequence* is the outcome of an event and has an effect on objectives. A single event can generate a range of consequences which can have both positive and negative effects on objectives. Initial consequences can also escalate through cascading and cumulative effects.

Context

To establish the *context* means to define the external and internal parameters that organizations must consider when they manage risk.

An organization's *external context* includes its external stakeholders, its local, national, and international environment, as well as any external factors that influence its objectives.

An organization's *internal context* includes its internal stakeholders, its approach to governance, its contractual relationships, and its capabilities, culture, and standards.

Control

A *control* is any measure or action that modifies or regulates risk. *Controls* include any policy, procedure, practice, process, technology, technique, method, or device that modifies or regulates risk. Risk treatments become controls, or modify existing controls, once they are implemented.

Event

An *event* could be one occurrence, several occurrences, or even a nonoccurrence (when something doesn't actually happen that should have happened). It can also be a change in circumstances.

Events always have causes and usually have consequences. Events without consequences are referred to as near-misses, near-hits, close-calls, or incidents.

External context

An organization's *external context* includes all of the external environmental parameters and factors that influence how it manages risk and how it tries to achieve its objectives. It includes its external stakeholders, its local, national, and international environment, as well as key drivers and important trends that influence its objectives. It also includes stakeholder values, perceptions, and relationships, as well as its social, cultural, political, legal, regulatory, technological, economic, natural, and competitive environment.

Internal context

An organization's *internal context* includes all of the internal environmental parameters and factors that influence how it manages risk and tries to achieve objectives. It includes its internal stakeholders, its approach to governance, its contractual relationships, and its capabilities, culture, and standards.

***Governance* includes the organization's structure, policies, objectives, roles, accountabilities, and decision making process, and *capabilities* include its knowledge and human, technological, capital, and systemic resources.**

Level of risk

The *level of risk* is its magnitude. It is estimated by considering and combining consequences and likelihoods. A level of risk can be assigned to a single risk or to a combination of risks.

Common level of risk categories include the following: extreme risk, high risk, moderate risk, and low risk. Of course, you need to define each category so that everyone is using the same terminology in the same way.

Likelihood

***Likelihood* is the chance that something might happen. Likelihood can be defined, determined, or measured objectively or subjectively and can be expressed either qualitatively or quantitatively (using mathematics).**

Monitoring

To *monitor* means to supervise and to continually check and critically observe. It means to determine the current status and to assess whether or not required or expected performance levels are being achieved.

Residual risk

***Residual risk* is the risk left over after you've implemented a risk treatment option. It's the risk remaining after you've reduced the risk, removed the source of the risk, modified the consequences, changed the probabilities, transferred the risk, or retained the risk.**

Review

A *review* is an activity. Review activities are carried out in order to determine whether something is a suitable, adequate, and effective way of achieving established objectives.

In general, ISO 31000 2018 expects you to review your risk management framework and your risk management process. It specifically expects you to review your risk management policy and plans as well as your risks, risk criteria, risk treatments, risk management controls, residual risks, and your risk assessment process.

Risk

According to ISO 31000, *risk* is the *"effect of uncertainty on objectives"* and an *effect* is a positive or negative deviation from what is expected. The following will explain what this means.

ISO 31000 recognizes that all of us operate in an uncertain world. Whenever we try to achieve an objective, there's always the chance that things will not go according to plan. Every step has an element of risk that needs to be managed and every outcome is uncertain. Whenever we try to achieve an objective, we

don't always get the results we expect. Sometimes we get positive results and sometimes we get negative results and occasionally we get both.

The traditional definition of *risk* combines three elements: it starts with a potential event and then combines its probability with its potential severity. A high risk event would have a high likelihood of occurring and a severe impact if it actually occurred.

While ISO 31000 defines *risk* in a new and unusual way, the old and the new definitions are largely compatible. Both definitions talk about the same phenomena but from two different perspectives. ISO thinks of risk in *goal-oriented terms* while the traditional definition thinks of risk in *event-oriented terms*. These two definitions can and do co-exist. They're two different ways of talking about the same phenomena.

ISO provides a conceptual definition of risk while the traditional formulation operationalizes this general definition: it explains how to quantify risk. It argues that the amount or level of risk can be calculated by combining probability and severity.

Risk analysis

***Risk analysis* is a process that is used to understand the nature, sources, and causes of the risks that you have identified and to estimate the level of risk. It is also used to study impacts and consequences and to examine the controls that currently exist. How detailed your risk analysis ought to be will depend upon the risk, the purpose of the analysis, the information you have, and the resources available.**

Risk assessment

***Risk assessment* is a process that is made up of three separate processes: risk identification, risk analysis, and risk evaluation.**

***Risk identification* is a process that is used to find, recognize, and describe the risks that could affect the achievement of objectives.**

***Risk analysis* is a process that is used to understand the nature, sources, and causes of the risks that you have identified and to estimate the level of risk. It is also used to study impacts and consequences and to examine the controls that exist.**

***Risk evaluation* is a process that is used to compare risk analysis results with risk criteria in order to determine whether or not a specified level of risk is acceptable or tolerable.**

Risk attitude

An organization's *risk attitude* defines its general approach to risk. An organization's risk attitude (and its risk criteria) influence how risks are assessed and addressed. An organization's attitude towards risk affects whether or not risks are taken, tolerated, retained, shared, reduced, or avoided, and whether or not treatments are implemented or postponed.

Risk criteria

Risk criteria **are terms of reference and are used to evaluate the significance or importance of your organization's risks. They are used to determine whether a specified level of risk is acceptable or tolerable. Risk criteria should reflect your organization's values, policies, and objectives, should be based on its external and internal context, should consider the views of stakeholders, and should be derived from standards, laws, policies, and other requirements.**

Risk evaluation

Risk evaluation **is a process that is used to compare risk analysis results with risk criteria in order to determine whether or not a specified level of risk is acceptable or tolerable.**

Risk identification

Risk identification **is a process that involves finding, recognizing, and describing the risks that could influence the achievement of objectives. It is used to identify possible sources of risk in addition to the events and circumstances that could influence the achievement of objectives. It also includes the identification of possible causes and potential consequences. You can use historical data, theoretical analysis, informed opinions, expert advice, and stakeholder input to identify your organization's risks.**

Risk management

Risk management **refers to a coordinated set of activities and methods that is used to direct an organization and to control the many risks that can affect its ability to achieve objectives.**

The term *risk management* also refers to the programme that is used to manage risk. This programme includes risk management principles, a risk management framework, and a risk management process.

Risk management framework

According to ISO 31000, a *risk management framework* is a set of components that support and sustain risk management throughout an organization. There are two types of *components*: foundations and arrangements.

Foundations **include your risk management policy, objectives, mandate, and commitment. And *arrangements* include the plans, relationships, accountabilities, resources, processes, and activities you use to manage your organization's risk.**

Risk management plan

An organization's *risk management plan* describes how it intends to manage risk. It describes the management components, the approach, and the resources that are used to manage risk. Typical management components include procedures, practices, responsibilities, and activities (including their sequence and timing). Risk management plans can be applied to products, processes, and projects, or to an entire organization or to any part of it.

Risk management policy

A *policy statement* defines a general commitment, direction, or intention. A *risk management policy statement* expresses an organization's commitment to risk management and clarifies its general direction or intention.

Risk management process

According to ISO 31000, a *risk management process* systematically applies management policies, procedures, and practices to a set of activities intended to establish the context, communicate and consult with stakeholders, and identify, analyze, evaluate, treat, monitor, record, report, and review risk.

Risk owner

A *risk owner* is a person or entity that has been given the authority to manage a particular risk and is accountable for doing so.

Risk profile

A *risk profile* is a written description of a set of risks. A risk profile can include the risks that the entire organization must manage or only those that a particular function or part of the organization must address.

Risk source

A *risk source* has the intrinsic potential to give rise to risk. A *risk source* is where a risk originates. It's where it comes from. Potential sources of risk include at least the following: commercial relationships and obligations, legal expectations and liabilities, economic shifts and circumstances, technological innovations and upheavals, political changes and trends, natural events and forces, human frailties and tendencies, and management shortcomings and excesses. All of these things could generate a risk that must be managed.

Risk treatment

***Risk treatment* is a risk modification process. It involves selecting and implementing one or more treatment options. Once a treatment has been**

implemented, it becomes a control or it modifies existing controls.

You have many treatment options. You can avoid the risk, you can reduce the risk, you can remove the source of the risk, you can modify the consequences, you can change the probabilities, you can share the risk with others, you can simply retain the risk, or you can even increase the risk in order to pursue an opportunity.

Stakeholder

A *stakeholder* is a person or an organization that can affect or be affected by a decision or an activity. Stakeholders also include those who have the perception that a decision or an activity can affect them. ISO 31000 2018 distinguishes between external and internal stakeholders.

MORE ISO 31000 PAGES

Introduction to ISO 31000 2018
Outline of ISO 31000 2018 Standard
Overview of ISO 31000 2018 Standard
Overview of Old ISO 31000 2009 Standard
ISO 31000 2018 Translated into Plain English
ISO 31000 2009 Translated into Plain English
ISO 31000 2018 Risk Management Audit Tool
ISO 31000 2018 Risk Management Checklist

RELATED RESOURCES

ISO 19011 Internal Auditing Guide
ISO 9001 Quality Management Guide
ISO 9004 Quality Management Guide
ISO IEC 20000 Service Management Guide
AS9100 Aerospace Quality Management Guide
ISO 90003 Software Quality Management Guide
ISO 27001 Information Security Management Guide
ISO 22301 Business Continuity Management Guide
ISO 28000 Supply Chain Security Management Guide
ISO 13485 Medical Device Quality Management Guide

Home Page | Our Library | A to Z Index | Our Customers
How to Order | Our Products | Our Prices | Our Guarantee

Praxiom Research Group Limited help@praxiom.com 780-461-4514

Updated on August 7, 2018. First published on August 7, 2018.

Praxiom Research Group Limited