



Bashynska Iryna, Ph.D. (Economics), Associate Professor, Department of Accounting, Analysis and Audit of ONPU
The author of more than 120 publications, including 3 copyright certificates, 10 monographs, 30 articles (including 2 Scopus), 53 tutorial manuals.
Courses: Risk Management, Safety Theory of Social Systems, Models and Methods of Decision Making in Analysis and Auditing, Training Course: Project Management.
Scientific specialization: Innovative activity of industrial enterprises; Risk Management, Problems of Ensuring Economic Security; Practical application of marketing in the activities of enterprises.



Fillypova Svitlana, DEcon, Professor, Full member of the Academy of Economic Sciences of Ukraine, Director of the Institute of Business, Economics and Information Technologies ONPU, scientific advisor of the Consulting and Training Center "Polytech-Consult" of the Odessa National Polytechnic University, Chairman of the Dissertation Council D 41.052.10 in the Odessa National Polytechnic University.
Was awarded the Honorary Awards of the Ministry of Education and Science of Ukraine "Excellence in Education" and "For Scientific Achievements".
Author of more than 300 scientific and methodological works, including 40 monographs, 9 copyright certificates, 19 textbooks, among them - 9 with with MES stamp.
Courses: Management Analysis, Organization of Accounting, Basics of Research a Patenting of Intellectual Property, Management Consulting.
Scientific specialization: Methodology and Mechanisms of Innovation Transformation of the Industrial Sector of the Economy of Ukraine.

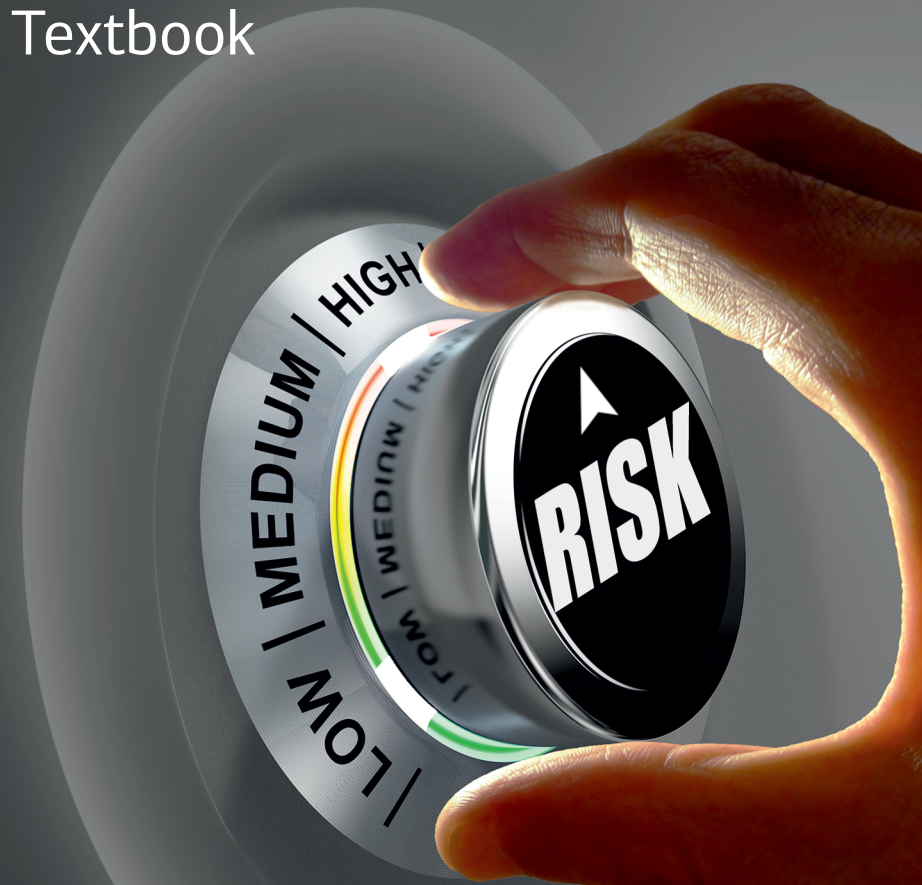
Risk management. Lecture course.

Bashynska I., Fillypova S.

BASHYNSKA IRYNA
FILLYPOVA SVITLANA

RISK MANAGEMENT. LECTURE COURSE.

Textbook





Ministry of Education and Science of Ukraine
Odessa National Polytechnic University
Institute of Business, Economics and
Information Technology
Department of Accounting, Analysis and Audit

BASHYNSKA IRYNA, FILLYPOVA SVITLANA

**RISK MANAGEMENT.
LECTURE COURSE.**

Textbook

Odessa

2017

TABLE OF CONTENTS

INTRODUCTION.....	5
TOPIC 1. Risk (General review)	7
TOPIC 2. Risk Management.....	16
TOPIC 3. Subject, object and necessity of studying economic risk.....	20
TOPIC 4. Classification of risks and the general scheme of the sequence of their assessment	23
TOPIC 5. Business Risks	28
TOPIC 6. Political and Country Risks	33
TOPIC 7. Marketing Risks	37
TOPIC 8. Financial Risks	41
TOPIC 9. Banking Risks	47
TOPIC 10. Risks in the Personnel Management System	50
TOPIC 11. Environmental Risks	58
TOPIC 12. Comprehensive Assessment of Risks	61
TOPIC 13. Enterprise Risk Management Program.....	65

TOPIC 14. Risk Management Culture	69
References	77
Annex 1. Glossary	82
Annex 2. ISO 31000:2009	86

INTRODUCTION

The only alternative to risk management is crisis management – and crisis management is much more expensive, time consuming and embarrassing.

JAMES LAM,
Enterprise Risk Management, Wiley
Finance © 2003

Unbalance, uncertainty, multicriteria are typical signs of a market economy that is always accompanied by risks. Entrepreneurship and risk are organically interconnected phenomena in a market economy.

Lots of works of domestic and foreign scientists are devoted to the study of the nature of risk and risk management: Aven Terje, Barton Tomas L., Blackman Andrew, Crawley John, Crockford Neil, Donets L.I., Goldstein G. Y., Guts A. N., Grabovyi P.G., Luk'yanova V.V., Matviychuk A.V., Palianytsia V., Petrova S.N., Seuring P.S., Shenkir Uiliam G., Stefanich D., Uoker Pol L., Yawar S.A.

In most works of these scientists, some aspects of the essence of economic risks, their analysis, identification and management are investigated. The purpose of course of lectures on risk management is to analyze the achievements of scientists and to raise basic awareness of risk management concepts and mechanisms, to enable participants to identify and manage risks in their own units and to strengthen project management through adequate forward planning of potential risks.

As a result of studying the textbook students of economic specialties will have the opportunity:

- to understand that economic processes develop mainly in conditions of uncertainty, conflict, multicriteria, and the impossibility of real economic forecasting, necessary for making rational decisions;
- develop the skills to independently carry out a qualitative analysis, identification of risk;
- carry out appropriate calculations using modern computers and corresponding software and methodical complexes;
- to assess the degree of risk by certain quantitative indicators that are consistent with the goals and system of the hypotheses adopted;
- to control, model and take into account the risk, to manage it, using the appropriate methods that are in the arsenal of economic risk.

The course of lectures is of interest to students of economic specialties, as well as teachers – in the preparation of lecture and practical classes, the development of options for individual and control assignments, as well as all those who are interested in identification, analysis and risk assessment.

References

1. Amir E. Khandani; Andrew W. Lo (2007). "What Happened To The Quants In August 2007?"
2. Another record profit for Exxon. BBC News. 31 July 2008.
3. Antunes Ricardo; Gonzalez, Vicente (3 March 2015). "A Production Model for Construction: A Theoretical Framework". *Buildings*. 5 (1): 209–228. doi:10.3390/buildings5010209.
4. Aven T, Krohn B.S. (2014). A new perspective on how to understand, assess and manage risk and the unforeseen. *ReliabEngSystSafe* 2014;121:1–10.
5. Aven T. (2013) On the meaning of the black swan concept in a risk context. *SafeSci* 2013;57:44–51.
6. Aven Terje (2014). Implications of black swans to the foundations and practice of risk assessment and management / *Reliability Engineering and System Safety* 134 (2015), 83-91
7. Barton, Tomas L., Shenkir, Uiliam G., Uoker, Pol L. (2008), *Risk-menedzhment [Risk management. Practice of leading companies]*, Vilyams, Moscow, Russia, 208 p.
8. Bashynska I. (2014) Informing staff and company management about threats and risks of information security // *Problems of social and economic development of business: Collection of scientific articles*. Vol. 2 – Publishing house "BREEZE", Montreal, Canada, 2014. – 400 p. – P. 256-258. – Available at: http://conf.at.ua/28.11.2014_Vol.2.pdf. [accessed 01.11.17]
9. Bashynska I.O. (2015) Using the method of expert evaluation in economic calculations. // *Aktual'ni Problemy Ekonomiky=Actual Problems in Economics*, 7 (169), 408-412

10. Bashynska I.O. (2016) Using SMM by industrial enterprises // Aktual'ni Problemy Ekonomiky= Actual Problems in Economics, 12 (186), 360-369
11. Belles-Sampera Jaume, Guillen Montserrat, Santolino Miguel (2017). Risk Quantification and Allocation Methods for Practitioners. Publisher: Amsterdam University Press.
12. Blackman Andrew (2014). The Main Types of Business Risk. Available at: <https://business.tutsplus.com/tutorials/the-main-types-of-business-risk--cms-22693> [accessed 01.11.17]
13. Bremmer Ian (2007). "How to Calculate Political Risk," Inc. Magazine, April 2007, p. 101
14. Business Risks. Archived from the original on 2012-11-03. Business Risks [accessed 01.11.17]
15. Committee Draft of ISO 31000 Risk management (PDF). International Organization for Standardization. 2007-06-15.
16. Crawley John (2011). "U.S. airline shares up as oil price slides". Reuters.
17. DIS 31000 (2009). Risk management – Principles and guidelines on implementation. International Organization for Standardization.
18. Donets, L.I. (2006), Ekonomichni ryzyky ta metody yikh vymiriuvania [Economic risks and methods of measurement], tutorial, TSNL, Kyiv, Ukraine, 312 p.
19. Eurasia Group and PricewaterhouseCoopers, "Integrating Political Risk Into Enterprise Risk Management"
20. Flyvbjerg Bent & Budzier Alexander (2011). "Why Your IT Project May Be Riskier Than You Think". Harvard Business Review. 89 (9): 601–603.

21. Grabovyi, P.G., Petrova, S.N. etc. (1994) Riski v sovremenom biznese [Risks is in the modern business], tutorial, Alians, Moscow, Russia, 200 p.
22. Hsiu-Jung Tsai; Ming-Chi Chen (2010). "The Impacts of Extreme Events of Dynamic Interactions on Interest Rate, Real House Price and Stock Markets" (PDF). *International Research Journal of Finance & Economics* (35): 187.
23. Hubbard Douglas (2009). *The Failure of Risk Management: Why It's Broken and How to Fix It*. John Wiley & Sons. p. 46.
24. Influencing types of business risk. Influencing factors types in Business Risk. [accessed 01.11.17]
25. Investopedia, definition. Business Risks, Investopedia [accessed 01.11.17]
26. ISO/IEC Guide 73:2009 (2009). *Risk management – Vocabulary*. International Organization for Standardization.
27. Jolly Adam (2003). *Managing Business Risk: A Practical Guide to Protecting Your Business*. Kogan Page Limited. pp. 6–7.
28. Kennedy C. (1988). "Political Risk Management: A Portfolio Planning Model". *Business Horizons*. 31: 21.
29. Kevin W., Knight A.M. ISO 31000:2009; ISO/IEC 31010 & ISO Guide 73:2009 Available at: http://www.inmetro.gov.br/download/wac/painel_1/7th_inter_conf_brazil_2012_may_2012_presentation.pdf [accessed 01.11.17]
30. Krueger Norris and Peter R. Dickson (1994). "How believing in ourselves increases risk taking: perceived self-efficacy and opportunity recognition". *Decision Sciences* 25, no. 3 (1994): 385-400.
31. Landsburg Steven (3 March 2003). "Is your life worth \$10 million?". *Everyday Economics*. Slate. Retrieved 17 March 2008.

32. Matthee H. (2011). Political risk analysis. In B. Badie, D. Berg-Schlosser, & L. Morlino (Eds.), *International encyclopedia of political science*. (pp. 2011-2014). Thousand Oaks, CA: SAGE Publications, Inc.
33. Matviychuk, A.V. (2005), *Analiz i upravlinia ekonomichnym ryzykom* [Analiz and management economic risk], tutorial, TSNL, Kyiv, Ukraine, 224 p.
34. Miles D. Anthony (2011). *Risk Factors and Business Models: Understanding the Five Forces of Entrepreneurial Risk and the Causes of Business Failure*. dissertation.com. p. 1.
35. Mulry Meg, Wong-Fupuy Carlos, Irwin Stephen. (2017) *Evaluating Country Risk*. October 13, 2017. Published by A.M. Best Rating Services, Inc. Available at: <http://www3.ambest.com/ambv/ratingmethodology/OpenPDF.aspx?rc=197697> [accessed 01.11.17]
36. Official site of the Interregional Recruiting Company Navigator. [Electronic resource] – Available at: <http://xn--80aafey1amqq.xn--j1amh/> [accessed 01.11.17]
37. Shtefanych, D., Palianytsia, V. (1999), *Upravlinia pidpriemnetskym ryzykom* [Management an enterprise risk], tutorial, *Ekonomichna dumka*, Ternopil, Ukraine, 214 p.
38. Smithells R. W., Newman C.GH. (1992). Recognition of thalidomide defects. *JMedGenet* 1992; 29:217–23.
39. Sokolova AA, Martynchik O.A. (2010). Methodological recommendations for conducting seminars and practical classes on the course "RISKOLOGY" for students of economic specialties. *Zhytomyr National Agroecological University*, 48 p.
40. Sottilotta, C.E. (2013) *Political Risk: Concepts, Definitions, Challenges*, LUISS School of Government Working Paper Series SOG-WP6/2013 ISSN|2282-4189. Available at:

http://sog.luiss.it/sites/sog.luiss.it/files/SOG%20Working%20Papers%20Sottilotta%20ISSN_0.pdf [accessed 01.11.17]

41. Systematic approach to the prophylactics of personnel security of enterprise / I. O. Bashynska, K. V. Biziukova // *Ekonomika: realiyi chasu. Naukovyy zhurnal.* – 2016. – № 5 (27). – С. 104-111. – Available at: <http://economics.opu.ua/files/archive/2016/n5.html> [accessed 01.11.17]
42. Taleb N. N. (2007) *The blackswan: the impact of the highly improbable.* London: Penguin; 2007.
43. Walker P.H., Seuring P.S., Sarkis P.J., Klassen P.R. (2014). Sustainable operations management: recent trends and future directions. *International Journal of Operations & Production Management* 34 (5).
44. William Leiss (2017). *Black Holes of Risk: Collected Papers on Risk Management, 1995-2017, Volume I: The Ubiquity of Risk*, Nov 2017 Kindle Direct Publishing
45. Yawar S.A., Seuring P.S. (2015). Management of social issues in supply chains: a literature review exploring social issues, actions and performance outcomes *Journal of Business Ethics*, 1-23.

Annex 1. Glossary

GENERAL TERMS

Acceptable Risk	That level of risk (likelihood of occurrence and consequence of impact) for any activity or situation that is sufficiently low that society (or an organization within society that is managing the risk) is comfortable with it. Society (and an individual organization) does not generally consider expenditure in further reducing such risks justifiable.
Accidental threat	An unplanned threat caused by a human being.
Action plans	Written or verbal plans that reflect the overall incident goal (control objectives) and incident strategy, objectives for the designated operational period, specific tactical actions and assignments, and supporting information for the designated operational period. They provide designated personnel with knowledge of the objectives to be achieved and the strategy and steps to be used for achievement, hence improving coordination across different levels of government and intrastate jurisdictional borders. Actions plans not only provide direction, but also provide a metric for measuring achievement of objectives and overall system performance.
Calamity risk	The risk that a single event of major magnitude leads to a significant deviation in actual claims from the total expected claims.
Catastrophe risk	The risk that a single event, or series of events, of major magnitude, usually over a short period (often 72 hours), leads to a significant deviation in actual claims from the total expected claims. ¹
Claims risk	An underwriting risk. A change in value caused by ultimate costs for full contractual obligations (claims without administration costs) varying from those assumed when these obligations were estimated.
Credit risk	The risk of a change in value due to actual credit losses deviating from expected credit losses due to the failure to meet contractual debt obligations.
Disaster risk	The likelihood over a specified time period of severe alterations in the normal functioning of a community or a society due to hazardous physical events interacting with vulnerable social conditions, leading to widespread adverse human, material, economic, or environmental effects that require immediate emergency response to

	satisfy critical human needs and that may require external support for recovery.
Disaster risk management (DRM)	Processes for designing, implementing, and evaluating strategies, policies, and measures to improve the understanding of disaster risk, foster disaster risk reduction and transfer, and promote continuous improvement in disaster preparedness, response, and recovery practices, with the explicit purpose of increasing human security, well-being, quality of life, and sustainable development.
Disaster risk reduction (DRR)	Denotes both a policy goal or objective, and the strategic and instrumental measures employed for anticipating future disaster risk; reducing existing exposure, hazard, or vulnerability; and improving resilience.
Diversification	Reduction in risks among assets and/or obligations of an institution by accumulating risks that are not fully correlated in an aggregated risk position, e.g. the aggregated amount of risks within a product portfolio or at a company level is smaller compared to the simple addition of the individual risks.
Expense risk	The risk of a change in value caused by the fact that the timing and/or the amount of expenses incurred differs from those expected, e.g. assumed for pricing basis
Hazard	The potential occurrence of a natural or human-induced physical event that may cause loss of life, injury, or other health impacts, as well as damage and loss to property, infrastructure, livelihoods, service provision, and environmental resources
Hazard identification	The process of finding, listing and characterising hazards.
Hazard record	The document in which identified hazards, their related measures, their origin and the reference to the organisation which has to manage them are recorded and referenced.
Likelihood	A probabilistic estimate of the occurrence of a single event or of an outcome, for example, a climate parameter, observed trend, or projected change lying in a given range. Likelihood may be based on statistical or modeling analyses, elicitation of expert views, or other quantitative analyses.
Local disaster risk management (LDRM)	The process in which local actors (citizens, communities, government, non-profit organizations, institutions, and businesses) engage in and have ownership of the identification, analysis, evaluation, monitoring, and

	treatment of disaster risk and disasters, through measures that reduce or anticipate hazard, exposure, or vulnerability; transfer risk; improve disaster response and recovery; and promote an overall increase in capacities. LDRM normally requires coordination with and support from external actors at the regional, national, or international levels. Community-based disaster risk management is a subset of LDRM where community members and organizations are in the center of decisionmaking.
Natural hazard	A threat attributable to forces of nature.
Predictability	The extent to which future states of a system may be predicted based on knowledge of current and past states of the system.
Reference system	A system proven in use to have an acceptable safety level and against which the acceptability of the risks from a system under assessment can be evaluated by comparison.
Residual risk	A risk that remains after security controls have been selected, approved and implemented.
Risk acceptance criteria	The terms of reference by which the acceptability of a specific risk is assessed; these criteria are used to determine that the level of a risk is sufficiently low that it is not necessary to take any immediate action to reduce it further.
Risk acceptance principle	The rules used in order to arrive at the conclusion whether or not the risk related to one or more specific hazards is acceptable.
Risk Analysis	A process consisting of three components: risk assessment, risk management and risk communication. Systematic use of all available information to identify hazards and to estimate the risk.
Risk Assessment	A scientifically based process consisting of the following steps: hazard identification, hazard characterization, exposure assessment, and risk characterization.
Risk Characterization	The qualitative and/or quantitative estimation, including attendant uncertainties, of the probability of occurrence and severity of known or potential adverse health effects in a given population based on hazard identification, hazard characterization and exposure assessment.
Risk Communication	The interactive exchange of information and opinions concerning risks among risk assessors, risk managers, consumers and other interested parties.
Risk estimation	The process used to produce a measure of the level of risks being analysed, consisting of the following steps:

	estimation of frequency, consequence analysis and their integration.
Risk evaluation	A procedure based on the risk analysis to determine whether an acceptable level of risk has been achieved.
Risk level	The degree of risk.
Risk management	The systematic application of management policies, procedures and practices to the tasks of analysing, evaluating and controlling risks.
Risk margin	A generic term, representing the value of the deviation risk of the actual outcome compared with the best estimate, expressed in terms of a defined risk measure
Systematic risk	Any risk inherent to the entire market or entire market segment which cannot be mitigated through diversification.
Tail-Value-at-Risk	A coherent risk measure. For a given confidence level $1-\alpha$ it measures the average losses over the defined threshold (typically set as the VaR for a given quantile), i.e. the conditioned mean value, given that the loss exceeds the $1-\alpha$ percentile.
Threat agent	An identifiable organization, individual or type of individual posing deliberate threats, or a specific kind of accidental threats or natural hazard.
Threat event	An actual incident in which a threat agent exploits a vulnerability with potentially adverse effects on an IT asset of value.
Value-at-Risk	Value-at-risk is a quantile of a distribution and used as a (non-coherent) risk measure.
Vulnerability	The propensity or predisposition to be adversely affected.
Exposure	The condition of being subjected to a hazard or source of risk.
Forecast	Statement or statistical estimate of the occurrence of a future event. This term is used with different meanings in different disciplines, as well as “prediction”.

Annex 2. ISO 31000:2009

(Fragment)

Introduction

Organizations of all types and sizes face internal and external factors and influences that make it uncertain whether and when they will achieve their objectives. The effect this uncertainty has on an organization's objectives is "risk".

All activities of an organization involve risk. Organizations manage risk by identifying it, analysing it and then evaluating whether the risk should be modified by risk treatment in order to satisfy their risk criteria. Throughout this process, they communicate and consult with stakeholders and monitor and review the risk and the controls that are modifying the risk in order to ensure that no further risk treatment is required. This International Standard describes this systematic and logical process in detail.

While all organizations manage risk to some degree, this International Standard establishes a number of principles that need to be satisfied to make risk management effective. This International Standard recommends that organizations develop, implement and continuously improve a framework whose purpose is to integrate the process for managing risk into the organization's overall governance, strategy and planning, management, reporting processes, policies, values and culture.

Risk management can be applied to an entire organization, at its many areas and levels, at any time, as well as to specific functions, projects and activities.

Although the practice of risk management has been developed over time and within many sectors in order to meet diverse needs, the adoption of consistent processes within a comprehensive framework can help to ensure that risk is managed effectively, efficiently and coherently across an organization. The generic approach described in this International Standard provides the principles and guidelines for managing any form of risk in a systematic, transparent and credible manner and within any scope and context.

Each specific sector or application of risk management brings with it individual needs, audiences, perceptions and criteria. Therefore, a key feature of this International Standard is the inclusion of "establishing the context" as an activity at the start of this generic risk management process. Establishing the context will capture the objectives of the organization, the environment in which it pursues those objectives, its stakeholders and the diversity of risk criteria – all of which will help reveal and assess the nature and complexity of its risks.

The relationship between the principles for managing risk, the framework in which it occurs and the risk management process described in this International Standard are shown in Figure 1.

When implemented and maintained in accordance with this International Standard, the management of risk enables an organization to, for example:

- increase the likelihood of achieving objectives;
- encourage proactive management;
- be aware of the need to identify and treat risk throughout the organization;
- improve the identification of opportunities and threats;
- comply with relevant legal and regulatory requirements and international norms;
- improve mandatory and voluntary reporting;
- improve governance;
- improve stakeholder confidence and trust;
- establish a reliable basis for decision making and planning;
- improve controls;
- effectively allocate and use resources for risk treatment;
- improve operational effectiveness and efficiency;
- enhance health and safety performance, as well as environmental protection;
- improve loss prevention and incident management;

- minimize losses;
- improve organizational learning; and
- improve organizational resilience.

This International Standard is intended to meet the needs of a wide range of stakeholders, including:

- those responsible for developing risk management policy within their organization;
- those accountable for ensuring that risk is effectively managed within the organization as a whole or within a specific area, project or activity;
- those who need to evaluate an organization's effectiveness in managing risk; and
- developers of standards, guides, procedures and codes of practice that, in whole or in part, set out how risk is to be managed within the specific context of these documents.

The current management practices and processes of many organizations include components of risk management, and many organizations have already adopted a formal risk management process for particular types of risk or circumstances. In such cases, an organization can decide to carry out a critical review of its existing practices and processes in the light of this International Standard.

In this International Standard, the expressions “risk management” and “managing risk” are both used. In general terms, “risk management” refers to the architecture (principles, framework and process) for managing risks effectively, while “managing risk” refers to applying that architecture to particular risks.

Risk management — Principles and guidelines

1 Scope

This International Standard provides principles and generic guidelines on risk management.

This International Standard can be used by any public, private or community enterprise, association, group or individual. Therefore, this International Standard is not specific to any industry or sector.

NOTE For convenience, all the different users of this International Standard are referred to by the general term “organization”.

This International Standard can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.

This International Standard can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.

Although this International Standard provides generic guidelines, it is not intended to promote uniformity of risk management across organizations. The design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices employed.

It is intended that this International Standard be utilized to harmonize risk management processes in existing and future standards. It provides a common approach in support of standards dealing with specific risks and/or sectors, and does not replace those standards.

This International Standard is not intended for the purpose of certification.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1 risk

effect of uncertainty on objectives

NOTE 1 An effect is a deviation from the expected — positive and/or negative.

NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).

NOTE 3 Risk is often characterized by reference to potential **events** (2.17) and **consequences** (2.18), or a combination of these.

NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated **likelihood** (2.19) of occurrence.

NOTE 5 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood.

[ISO Guide 73:2009, definition 1.1]

2.2 risk management

coordinated activities to direct and control an organization with regard to **risk** (2.1)

[ISO Guide 73:2009, definition 2.1]

2.3 risk management framework

set of components that provide the foundations and organizational arrangements for designing, implementing,

monitoring (2.28), reviewing and continually improving **risk management** (2.2) throughout the organization

NOTE 1 The foundations include the policy, objectives, mandate and commitment to manage **risk** (2.1).

NOTE 2 The organizational arrangements include plans, relationships, accountabilities, resources, processes and activities.

NOTE 3 The risk management framework is embedded within the organization's overall strategic and operational policies and practices.

[ISO Guide 73:2009, definition 2.1.1]

2.4 risk management policy

statement of the overall intentions and direction of an organization related to **risk management** (2.2)

[ISO Guide 73:2009, definition 2.1.2]

2.5 risk attitude

organization's approach to assess and eventually pursue, retain, take or turn away from **risk** (2.1)

[ISO Guide 73:2009, definition 3.7.1.1]

2.6 risk management plan

scheme within the **risk management framework** (2.3) specifying the approach, the management components and resources to be applied to the management of **risk** (2.1)

NOTE 1 Management components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities.

NOTE 2 The risk management plan can be applied to a particular product, process and project, and part or whole of the organization.

[ISO Guide 73:2009, definition 2.1.3]

2.7 risk owner

person or entity with the accountability and authority to manage a **risk** (2.1)

[ISO Guide 73:2009, definition 3.5.1.5]

2.8 risk management process

systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, **monitoring** (2.28) and reviewing **risk** (2.1)

[ISO Guide 73:2009, definition 3.1]

2.9 establishing the context

defining the external and internal parameters to be taken into account when managing risk, and setting the scope and **risk criteria** (2.22) for the **risk management policy** (2.4)

[ISO Guide 73:2009, definition 3.3.1]

2.10 external context

external environment in which the organization seeks to achieve its objectives

NOTE External context can include:

- the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
- key drivers and trends having impact on the objectives of the organization; and

- relationships with, and perceptions and values of external stakeholders (2.13).
- [ISO Guide 73:2009, definition 3.3.1.1]

2.11 internal context

internal environment in which the organization seeks to achieve its objectives

NOTE Internal context can include:

- governance, organizational structure, roles and accountabilities;
- policies, objectives, and the strategies that are in place to achieve them;
- the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- information systems, information flows and decision-making processes (both formal and informal);
- relationships with, and perceptions and values of, internal stakeholders;
- the organization's culture;
- standards, guidelines and models adopted by the organization; and
- form and extent of contractual relationships.

[ISO Guide 73:2009, definition 3.3.1.2]

2.12 communication and consultation

continual and iterative processes that an organization conducts to provide, share or obtain information and to engage in dialogue with **stakeholders** (2.13) regarding the management of **risk** (2.1)

NOTE 1 The information can relate to the existence, nature, form, **likelihood** (2.19), significance, evaluation, acceptability and treatment of the management of risk.

NOTE 2 Consultation is a two-way process of informed communication between an organization and its stakeholders on an issue prior to making a decision or determining a direction on that issue. Consultation is:

- a process which impacts on a decision through influence rather than power; and
- an input to decision making, not joint decision making.

[ISO Guide 73:2009, definition 3.2.1]

2.13 stakeholder

person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

NOTE A decision maker can be a stakeholder.

[ISO Guide 73:2009, definition 3.2.1.1]

2.14 risk assessment

overall process of **risk identification** (2.15), **risk analysis** (2.21) and **risk evaluation** (2.24)

[ISO Guide 73:2009, definition 3.4.1]

2.15 risk identification

process of finding, recognizing and describing **risks** (2.1)

NOTE 1 Risk identification involves the identification of **risk sources** (2.16), **events** (2.17), their causes and their potential **consequences** (2.18).

NOTE 2 Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and

stakeholder's (2.13) needs.

[ISO Guide 73:2009, definition 3.5.1]

2.16 risk source

element which alone or in combination has the intrinsic potential to give rise to **risk** (2.1)

NOTE A risk source can be tangible or intangible.

[ISO Guide 73:2009, definition 3.5.1.2]

2.17 event

occurrence or change of a particular set of circumstances

NOTE 1 An event can be one or more occurrences, and can have several causes. NOTE 2

An event can consist of something not happening.

NOTE 3 An event can sometimes be referred to as an "incident" or "accident".

NOTE 4 An event without **consequences** (2.18) can also be referred to as a “near miss”, “incident”, “near hit” or “close call”.

[ISO Guide 73:2009, definition 3.5.1.3]

2.18 consequence

outcome of an **event** (2.17) affecting objectives

NOTE 1 An event can lead to a range of consequences.

NOTE 2 A consequence can be certain or uncertain and can have positive or negative effects on objectives. NOTE 3 Consequences can be expressed qualitatively or quantitatively.

NOTE 4 Initial consequences can escalate through knock-on effects.

[ISO Guide 73:2009, definition 3.6.1.3]

2.19 likelihood

chance of something happening

NOTE 1 In risk management terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

NOTE 2 The English term “likelihood” does not have a direct equivalent in some languages; instead, the equivalent of the term “probability” is often used. However, in English, “probability” is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, “likelihood” is used with the intent that it should have the same broad interpretation as the term “probability” has in many languages other than English.

[ISO Guide 73:2009, definition 3.6.1.1]

2.20 risk profile

description of any set of **risks** (2.1)

NOTE The set of risks can contain those that relate to the whole organization, part of the organization, or as otherwise defined.

[ISO Guide 73:2009, definition 3.8.2.5]

2.21 risk analysis

process to comprehend the nature of **risk** (2.1) and to determine the **level of risk** (2.23)

NOTE 1 Risk analysis provides the basis for **risk evaluation** (2.24) and decisions about **risk treatment** (2.25). NOTE 2 Risk analysis includes risk estimation.

[ISO Guide 73:2009, definition 3.6.1]

2.22 risk criteria

terms of reference against which the significance of a **risk** (2.1) is evaluated

NOTE 1 Risk criteria are based on organizational objectives, and **external** (2.10) and **internal context** (2.11). NOTE 2 Risk criteria can be derived from standards, laws, policies and other requirements.

[ISO Guide 73:2009, definition 3.3.1.3]

2.23 level of risk

magnitude of a **risk** (2.1) or combination of risks, expressed in terms of the combination of **consequences**

(2.18) and their **likelihood** (2.19)

[ISO Guide 73:2009, definition 3.6.1.8]

2.24 risk evaluation

process of comparing the results of **risk analysis** (2.21) with **risk criteria** (2.22) to determine whether the **risk**

(2.1) and/or its magnitude is acceptable or tolerable

NOTE Risk evaluation assists in the decision about **risk treatment** (2.25).

[ISO Guide 73:2009, definition 3.7.1]

2.25 risk treatment

process to modify **risk** (2.1)

NOTE 1 Risk treatment can involve:

avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; changing the **likelihood** (2.19);

changing the **consequences** (2.18);
sharing the risk with another party or parties (including contracts and risk financing); and
retaining the risk by informed decision.

NOTE 2 Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”.

NOTE 3 Risk treatment can create new risks or modify existing risks.

[ISO Guide 73:2009, definition 3.8.1]

2.26 control

measure that is modifying **risk** (2.1)

NOTE 1 Controls include any process, policy, device, practice, or other actions which modify risk. NOTE 2 Controls may not always exert the intended or assumed modifying effect.

[ISO Guide 73:2009, definition 3.8.1.1]

2.27 residual risk

risk (2.1) remaining after **risk treatment** (2.25)

NOTE 1 Residual risk can contain unidentified risk.

NOTE 2 Residual risk can also be known as “retained risk”.

[ISO Guide 73:2009, definition 3.8.1.6]

2.28 monitoring

continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected

NOTE Monitoring can be applied to a **risk management framework** (2.3), **risk management process** (2.8), **risk**

(2.1) or **control** (2.26). [ISO Guide 73:2009, definition 3.8.2.1]

2.29 review

activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives

NOTE Review can be applied to a **risk management framework** (2.3), **risk management process** (2.8), **risk** (2.1) or **control** (2.26).

[ISO Guide 73:2009, definition 3.8.2.2]

3. Principles

For risk management to be effective, an organization should at all levels comply with the principles below.

a) Risk management creates and protects value.

Risk management contributes to the demonstrable achievement of objectives and improvement of performance in, for example, human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance and reputation.

b) Risk management is an integral part of all organizational processes.

Risk management is not a stand-alone activity that is separate from the main activities and processes of the organization. Risk management is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning and all project and change management processes.

c) Risk management is part of decision making.

Risk management helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action.

d) Risk management explicitly addresses uncertainty.

Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.

e) Risk management is systematic, structured and timely.

A systematic, timely and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results.

f) Risk management is based on the best available information.

The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgement. However,

decision makers should inform themselves of, and should take into account, any limitations of the data or modelling used or the possibility of divergence among experts.

g) Risk management is tailored.

Risk management is aligned with the organization's external and internal context and risk profile.

h) Risk management takes human and cultural factors into account.

Risk management recognizes the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the organization's objectives.

i) Risk management is transparent and inclusive.

Appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels of the organization, ensures that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria.

j) Risk management is dynamic, iterative and responsive to change.

Risk management continually senses and responds to change. As external and internal events occur, context and knowledge change, monitoring and review of risks take place, new risks emerge, some change, and others disappear.

k) Risk management facilitates continual improvement of the organization.

Organizations should develop and implement strategies to improve their risk management maturity alongside all other aspects of their organization.

Annex A provides further advice for organizations wishing to manage risk more effectively.

4 Framework

4.1 General

The success of risk management will depend on the effectiveness of the management framework providing the foundations and arrangements that will embed it throughout the organization at all levels. The framework assists in managing risks effectively through the application of the risk management process (see Clause 5) at varying levels and within specific contexts of the organization. The framework ensures that information about risk derived from the risk management process is adequately reported and used as a basis for decision making and accountability at all relevant organizational levels.

This clause describes the necessary components of the framework for managing risk and the way in which they interrelate in an iterative manner, as shown in Figure 2.

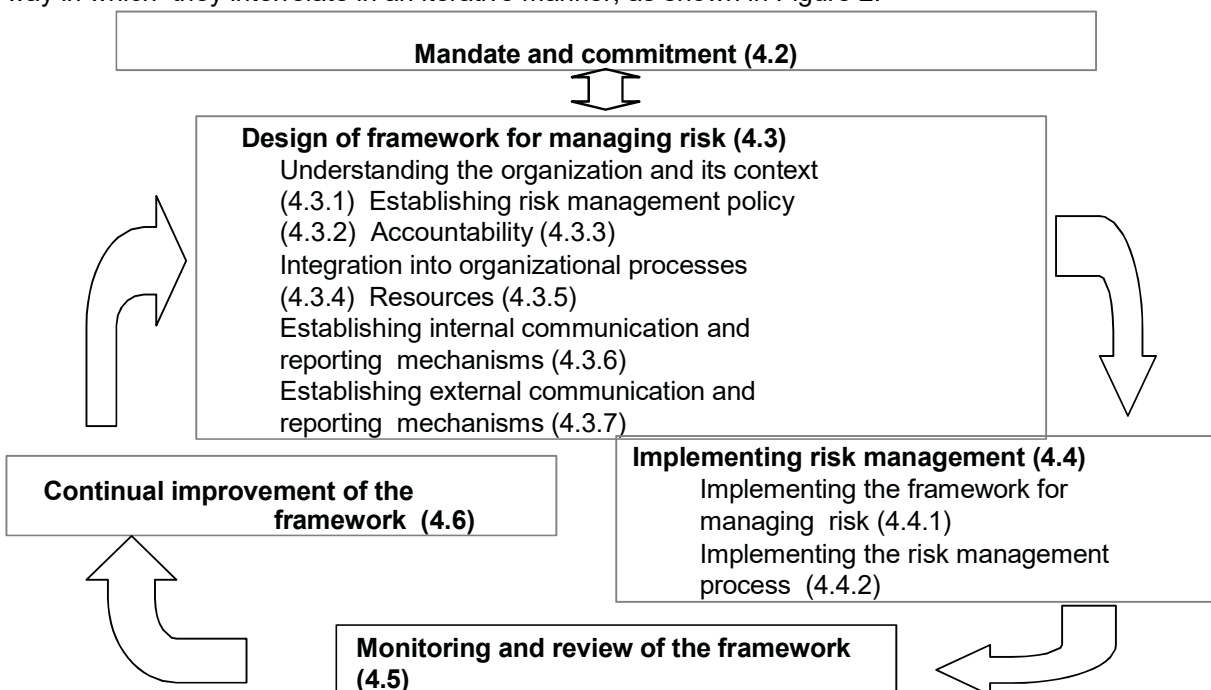


Figure 2 — Relationship between the components of the framework for managing risk

This framework is not intended to prescribe a management system, but rather to assist the organization to integrate risk management into its overall management system. Therefore, organizations should adapt the components of the framework to their specific needs.

If an organization's existing management practices and processes include components of risk management or if the organization has already adopted a formal risk management process for particular types of risk or situations, then these should be critically reviewed and assessed against this International Standard, including the attributes contained in Annex A, in order to determine their adequacy and effectiveness.

4.2 Mandate and commitment

The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organization, as well as strategic and rigorous planning to achieve commitment at all levels. Management should:

- define and endorse the risk management policy;
- ensure that the organization's culture and risk management policy are aligned;
- determine risk management performance indicators that align with performance indicators of the organization;
- align risk management objectives with the objectives and strategies of the organization;
- ensure legal and regulatory compliance;
- assign accountabilities and responsibilities at appropriate levels within the organization;
- ensure that the necessary resources are allocated to risk management;
- communicate the benefits of risk management to all stakeholders; and
- ensure that the framework for managing risk continues to remain appropriate.

4.3 Design of framework for managing risk

4.3.1 Understanding of the organization and its context

Before starting the design and implementation of the framework for managing risk, it is important to evaluate and understand both the external and internal context of the organization, since these can significantly influence the design of the framework.

Evaluating the organization's external context may include, but is not limited to:

- a) the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
- b) key drivers and trends having impact on the objectives of the organization; and
- c) relationships with, and perceptions and values of, external stakeholders.

Evaluating the organization's internal context may include, but is not limited to:

- governance, organizational structure, roles and accountabilities;
- policies, objectives, and the strategies that are in place to achieve them;
- capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- information systems, information flows and decision making processes (both formal and informal);
- relationships with, and perceptions and values of, internal stakeholders;
- the organization's culture; standards, guidelines and models adopted by the organization; and
- the form and extent of contractual relationships.

4.3.2 Establishing risk management policy

The risk management policy should clearly state the organization's objectives for, and commitment to, risk management and typically addresses the following:

- □ the organization's rationale for managing risk;
- links between the organization's objectives and policies and the risk management policy;
- accountabilities and responsibilities for managing risk;
- the way in which conflicting interests are dealt with;
- commitment to review and improve the risk management policy and framework periodically and in response to an event or change in circumstances.

The risk management policy should be communicated appropriately.

4.3.3 Accountability

The organization should ensure that there is accountability, authority and appropriate competence for managing risk, including implementing and maintaining the risk management process and ensuring the adequacy, effectiveness and efficiency of any controls. This can be facilitated by:

- identifying risk owners that have the accountability and authority to manage risks;
- identifying who is accountable for the development, implementation and maintenance of the framework for managing risk;
- identifying other responsibilities of people at all levels in the organization for the risk management process;
- establishing performance measurement and external and/or internal reporting and escalation processes; and
- ensuring appropriate levels of recognition.

4.3.4 Integration into organizational processes

Risk management should be embedded in all the organization's practices and processes in a way that it is relevant, effective and efficient. The risk management process should become part of, and not separate from, those organizational processes. In particular, risk management should be embedded into the policy development, business and strategic planning and review, and change management processes.

There should be an organization-wide risk management plan to ensure that the risk management policy is implemented and that risk management is embedded in all of the organization's practices and processes. The risk management plan can be integrated into other organizational plans, such as a strategic plan.

4.3.5 Resources

The organization should allocate appropriate resources for risk management. Consideration should be given to the following:

- people, skills, experience and competence;
- resources needed for each step of the risk management process;
- the organization's processes, methods and tools to be used for managing risk;
- documented processes and procedures;
- information and knowledge management systems; and
- training programmes.

4.3.6 Establishing internal communication and reporting mechanisms

The organization should establish internal communication and reporting mechanisms in order to support and encourage accountability and ownership of risk. These mechanisms should ensure that:

- key components of the risk management framework, and any subsequent modifications, are communicated appropriately;
- there is adequate internal reporting on the framework, its effectiveness and the outcomes;
- relevant information derived from the application of risk management is available at appropriate levels and times; and
- there are processes for consultation with internal stakeholders.

These mechanisms should, where appropriate, include processes to consolidate risk information from a variety of sources, and may need to consider the sensitivity of the information.

4.3.7 Establishing external communication and reporting mechanisms

The organization should develop and implement a plan as to how it will communicate with external stakeholders. This should involve:

- engaging appropriate external stakeholders and ensuring an effective exchange of information;
- external reporting to comply with legal, regulatory, and governance requirements;
- providing feedback and reporting on communication and consultation;
- using communication to build confidence in the organization; and
- communicating with stakeholders in the event of a crisis or contingency.

These mechanisms should, where appropriate, include processes to consolidate risk information from a variety of sources, and may need to consider the sensitivity of the information.

4.4 Implementing risk management

4.4.1 Implementing the framework for managing risk

In implementing the organization's framework for managing risk, the organization should:

- define the appropriate timing and strategy for implementing the framework;
- apply the risk management policy and process to the organizational processes;
- comply with legal and regulatory requirements;
- ensure that decision making, including the development and setting of objectives, is aligned with the outcomes of risk management processes;
- hold information and training sessions; and
- communicate and consult with stakeholders to ensure that its risk management framework remains appropriate.

4.4.2 Implementing the risk management process

Risk management should be implemented by ensuring that the risk management process outlined in Clause 5 is applied through a risk management plan at all relevant levels and functions of the organization as part of its practices and processes.

4.5 Monitoring and review of the framework

In order to ensure that risk management is effective and continues to support organizational performance, the organization should:

- measure risk management performance against indicators, which are periodically reviewed for appropriateness;
- periodically measure progress against, and deviation from, the risk management plan;
- periodically review whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal context;
- report on risk, progress with the risk management plan and how well the risk management policy is being followed; and
- review the effectiveness of the risk management framework.

4.6 Continual improvement of the framework

Based on results of monitoring and reviews, decisions should be made on how the risk management framework, policy and plan can be improved. These decisions should lead to improvements in the organization's management of risk and its risk management culture.

5 Process

5.1 General

- The risk management process should be
- an integral part of management,
- embedded in the culture and practices, and
- tailored to the business processes of the organization.

It comprises the activities described in 5.2 to 5.6. The risk management process is shown in Figure 3.

5.2 Communication and consultation

Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process.

Therefore, plans for communication and consultation should be developed at an early stage. These should address issues relating to the risk itself, its causes, its consequences (if known), and the measures being taken to treat it. Effective external and internal communication and consultation should take place to ensure that those accountable for implementing the risk management process and stakeholders understand the basis on which decisions are made, and the reasons why particular actions are required.

A consultative team approach may:

- help establish the context appropriately;
- ensure that the interests of stakeholders are understood and considered;
- help ensure that risks are adequately identified;
- bring different areas of expertise together for analyzing risks;
- ensure that different views are appropriately considered when defining risk criteria and in evaluating risks;
- secure endorsement and support for a treatment plan;
- enhance appropriate change management during the risk management process; and

- develop an appropriate external and internal communication and consultation plan.

Communication and consultation with stakeholders is important as they make judgements about risk based on their perceptions of risk. These perceptions can vary due to differences in values, needs, assumptions, concepts and concerns of stakeholders. As their views can have a significant impact on the decisions made, the stakeholders' perceptions should be identified, recorded, and taken into account in the decision making process.

Communication and consultation should facilitate truthful, relevant, accurate and understandable exchanges of information, taking into account confidential and personal integrity aspects.

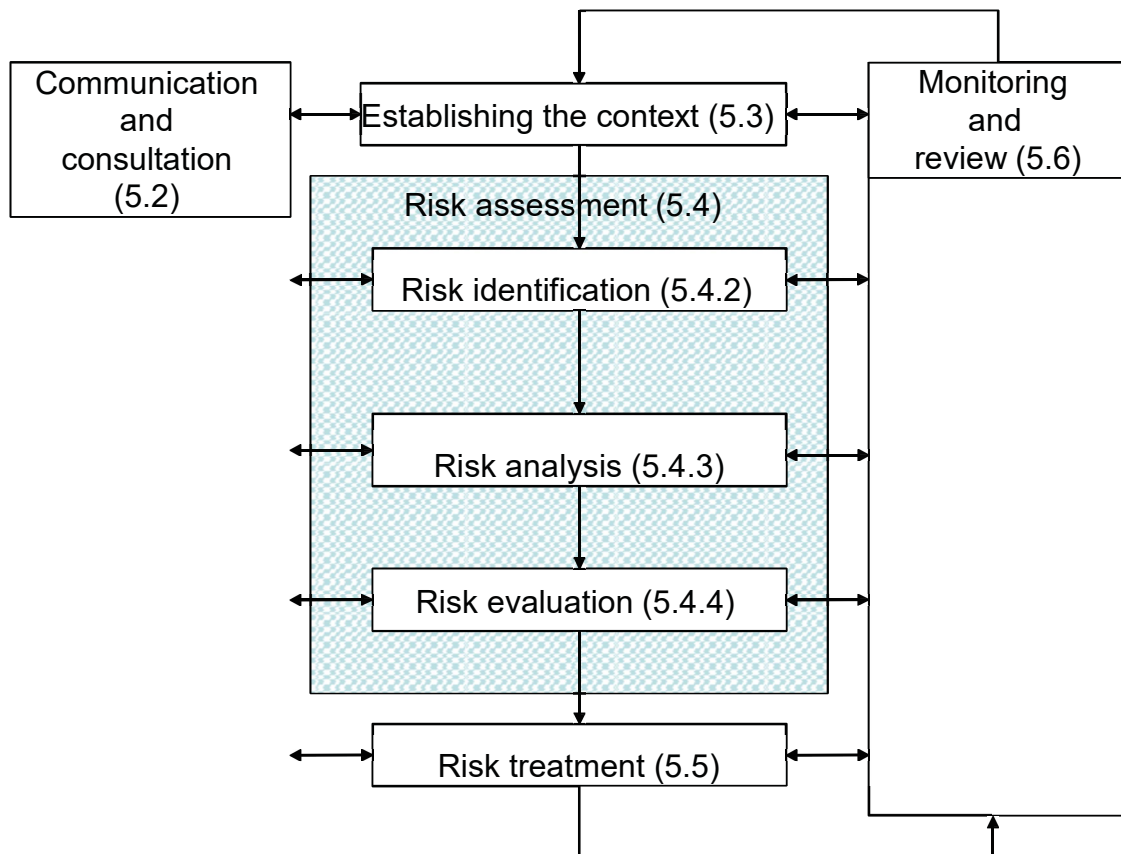


Figure 3 — Risk management process

5.3 Establishing the context

5.3.1 General

By establishing the context, the organization articulates its objectives, defines the external and internal parameters to be taken into account when managing risk, and sets the scope and risk criteria for the remaining process. While many of these parameters are similar to those considered in the design of the risk management framework (see 4.3.1), when establishing the context for the risk management process, they need to be considered in greater detail and particularly how they relate to the scope of the particular risk management process.

5.3.2 Establishing the external context

The external context is the external environment in which the organization seeks to achieve its objectives.

Understanding the external context is important in order to ensure that the objectives and concerns of external stakeholders are considered when developing risk criteria. It is based on the organization-wide context, but with specific details of legal and regulatory requirements, stakeholder perceptions and other aspects of risks specific to the scope of the risk management process.

The external context can include, but is not limited to:

- the social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
- key drivers and trends having impact on the objectives of the organization; and
- relationships with, perceptions and values of external stakeholders.

5.3.3 Establishing the internal context

The internal context is the internal environment in which the organization seeks to achieve its objectives.

The risk management process should be aligned with the organization's culture, processes, structure and strategy. Internal context is anything within the organization that can influence the way in which an organization will manage risk. It should be established because:

- a) risk management takes place in the context of the objectives of the organization;
- b) objectives and criteria of a particular project, process or activity should be considered in the light of objectives of the organization as a whole; and
- c) some organizations fail to recognize opportunities to achieve their strategic, project or business objectives, and this affects ongoing organizational commitment, credibility, trust and value.

It is necessary to understand the internal context. This can include, but is not limited to:

- governance, organizational structure, roles and accountabilities;
- policies, objectives, and the strategies that are in place to achieve them;
- capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- the relationships with and perceptions and values of internal stakeholders;
- the organization's culture; information systems, information flows and decision making processes (both formal and informal);
- standards, guidelines and models adopted by the organization; and
- form and extent of contractual relationships.

5.3.4 Establishing the context of the risk management process

The objectives, strategies, scope and parameters of the activities of the organization, or those parts of the organization where the risk management process is being applied, should be established. The management of risk should be undertaken with full consideration of the need to justify the resources used in carrying out risk management. The resources required, responsibilities and authorities, and the records to be kept should also be specified.

The context of the risk management process will vary according to the needs of an organization. It can involve, but is not limited to:

- defining the goals and objectives of the risk management activities;
- defining responsibilities for and within the risk management process;
- defining the scope, as well as the depth and breadth of the risk management activities to be carried out, including specific inclusions and exclusions;
- defining the activity, process, function, project, product, service or asset in terms of time and location;
- defining the relationships between a particular project, process or activity and other projects, processes or activities of the organization;
- defining the risk assessment methodologies;
- defining the way performance and effectiveness is evaluated in the management of risk;
- identifying and specifying the decisions that have to be made; and
- identifying, scoping or framing studies needed, their extent and objectives, and the resources required for such studies.

Attention to these and other relevant factors should help ensure that the risk management approach adopted is appropriate to the circumstances, to the organization and to the risks affecting the achievement of its objectives.

5.3.5 Defining risk criteria

The organization should define criteria to be used to evaluate the significance of risk. The criteria should reflect the organization's values, objectives and resources. Some criteria can be imposed by, or derived from, legal and regulatory requirements and other requirements to which the organization

subscribes. Risk criteria should be consistent with the organization's risk management policy (see 4.3.2), be defined at the beginning of any risk management process and be continually reviewed.

When defining risk criteria, factors to be considered should include the following:

- the nature and types of causes and consequences that can occur and how they will be measured;
- how likelihood will be defined the timeframe(s) of the likelihood and/or consequence(s);
- how the level of risk is to be determined;
- the views of stakeholders;
- the level at which risk becomes acceptable or tolerable; and
- whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.

5.4 Risk assessment

5.4.1 General

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

NOTE ISO/IEC 31010 provides guidance on risk assessment techniques.

5.4.2 Risk identification

The organization should identify sources of risk, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences. The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. It is important to identify the risks associated with not pursuing an opportunity. Comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis.

Identification should include risks whether or not their source is under the control of the organization, even though the risk source or cause may not be evident. Risk identification should include examination of the knock-on effects of particular consequences, including cascade and cumulative effects. It should also consider a wide range of consequences even if the risk source or cause may not be evident. As well as identifying what might happen, it is necessary to consider possible causes and scenarios that show what consequences can occur. All significant causes and consequences should be considered.

The organization should apply risk identification tools and techniques that are suited to its objectives and capabilities, and to the risks faced. Relevant and up-to-date information is important in identifying risks. This should include appropriate background information where possible. People with appropriate knowledge should be involved in identifying risks.

5.4.3 Risk analysis

Risk analysis involves developing an understanding of the risk. Risk analysis provides an input to risk evaluation and to decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods. Risk analysis can also provide an input into making decisions where choices must be made and the options involve different types and levels of risk.

Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur. Factors that affect consequences and likelihood should be identified. Risk is analyzed by determining consequences and their likelihood, and other attributes of the risk. An event can have multiple consequences and can affect multiple objectives. Existing controls and their effectiveness and efficiency should also be taken into account.

The way in which consequences and likelihood are expressed and the way in which they are combined to determine a level of risk should reflect the type of risk, the information available and the purpose for which the risk assessment output is to be used. These should all be consistent with the risk criteria. It is also important to consider the interdependence of different risks and their sources.

The confidence in determination of the level of risk and its sensitivity to preconditions and assumptions should be considered in the analysis, and communicated effectively to decision makers and, as appropriate, other stakeholders. Factors such as divergence of opinion among experts, uncertainty, availability, quality, quantity and ongoing relevance of information, or limitations on modelling should be stated and can be highlighted.

Risk analysis can be undertaken with varying degrees of detail, depending on the risk, the purpose of the analysis, and the information, data and resources available. Analysis can be qualitative, semi-quantitative or quantitative, or a combination of these, depending on the circumstances.

Consequences and their likelihood can be determined by modelling the outcomes of an event or set of events, or by extrapolation from experimental studies or from available data. Consequences can be expressed in terms of tangible and intangible impacts. In some cases, more than one numerical value or descriptor is required to specify consequences and their likelihood for different times, places, groups or situations.

5.4.4 Risk evaluation

The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation.

Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered.

Decisions should take account of the wider context of the risk and include consideration of the tolerance of the risks borne by parties other than the organization that benefits from the risk. Decisions should be made in accordance with legal, regulatory and other requirements.

In some circumstances, the risk evaluation can lead to a decision to undertake further analysis. The risk evaluation can also lead to a decision not to treat the risk in any way other than maintaining existing controls. This decision will be influenced by the organization's risk attitude and the risk criteria that have been established.

5.5 Risk treatment

5.5.1 General

Risk treatment involves selecting one or more options for modifying risks, and implementing those options. Once implemented, treatments provide or modify the controls.

Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. The options can include the following:

- a) avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- b) taking or increasing the risk in order to pursue an opportunity;
- c) removing the risk source;
- d) changing the likelihood;
- e) changing the consequences;
- f) sharing the risk with another party or parties (including contracts and risk financing); and
- g) retaining the risk by informed decision.

5.5.2 Selection of risk treatment options

Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived, with regard to legal, regulatory, and other requirements such as social responsibility and the protection of the natural environment. Decisions should also take into account risks which can warrant risk treatment that is not justifiable on economic grounds, e.g. severe (high negative consequence) but rare (low likelihood) risks.

A number of treatment options can be considered and applied either individually or in combination. The organization can normally benefit from the adoption of a combination of treatment options.

When selecting risk treatment options, the organization should consider the values and perceptions of stakeholders and the most appropriate ways to communicate with them. Where risk treatment options can impact on risk elsewhere in the organization or with stakeholders, these should be involved in the decision. Though equally effective, some risk treatments can be more acceptable to some stakeholders than to others.

The treatment plan should clearly identify the priority order in which individual risk treatments should be implemented.

Risk treatment itself can introduce risks. A significant risk can be the failure or ineffectiveness of the risk treatment measures. Monitoring needs to be an integral part of the risk treatment plan to give assurance that the measures remain effective.

Risk treatment can also introduce secondary risks that need to be assessed, treated, monitored and reviewed. These secondary risks should be incorporated into the same treatment plan as the original risk and not treated as a new risk. The link between the two risks should be identified and maintained.

5.5.3 Preparing and implementing risk treatment plans

The purpose of risk treatment plans is to document how the chosen treatment options will be implemented. The information provided in treatment plans should include:

- the reasons for selection of treatment options, including expected benefits to be gained;
- those who are accountable for approving the plan and those responsible for implementing the plan;
- proposed actions;
- resource requirements including contingencies;
- performance measures and constraints;
- reporting and monitoring requirements; and
- timing and schedule.

Treatment plans should be integrated with the management processes of the organization and discussed with appropriate stakeholders.

Decision makers and other stakeholders should be aware of the nature and extent of the residual risk after risk treatment. The residual risk should be documented and subjected to monitoring, review and, where appropriate, further treatment.

5.6 Monitoring and review

Both monitoring and review should be a planned part of the risk management process and involve regular checking or surveillance. It can be periodic or *ad hoc*.

Responsibilities for monitoring and review should be clearly defined.

The organization's monitoring and review processes should encompass all aspects of the risk management process for the purposes of:

- ensuring that controls are effective and efficient in both design and operation;
- obtaining further information to improve risk assessment;
- analyzing and learning lessons from events (including near-misses), changes, trends, successes and failures;
- detecting changes in the external and internal context, including changes to risk criteria and the risk itself which can require revision of risk treatments and priorities; and
- identifying emerging risks.

Progress in implementing risk treatment plans provides a performance measure. The results can be incorporated into the organization's overall performance management, measurement and external and internal reporting activities.

The results of monitoring and review should be recorded and externally and internally reported as appropriate, and should also be used as an input to the review of the risk management framework (see 4.5).

5.7 Recording the risk management process

Risk management activities should be traceable. In the risk management process, records provide the foundation for improvement in methods and tools, as well as in the overall process.

Decisions concerning the creation of records should take into account:

- the organization's needs for continuous learning;
- benefits of re-using information for management purposes;
- costs and efforts involved in creating and maintaining records;
- legal, regulatory and operational needs for records;
- method of access, ease of retrievability and storage media;
- retention period; and
- sensitivity of information.

BASHYNSKA IRYNA OLEKSANDRIVNA
FILLYPOVA SVITLANA VALERIIVNA

RISK MANAGEMENT.
LECTURE COURSE.

Textbook

in author's edition

Формат 60x84/16. Папір офсетний.
Друк цифровий. Підписано до друку 25.10.2017 р.
Наклад 500. Умовн. друк. арк. 5,93

Видавництво «Діса плюс»
Тел. (057) 768-03-15

Свідоцтво про внесення суб'єкта видавничої справи до
Державного реєстру видавців, виготівників та розповсюджувачів
видавничої продукції:
серія ДК № 4047 від 15.04.2011 р.

Надруковано в друкарні ТОВ «ПромАрт»
61023, м. Харків, вул. Весніна, 12.
тел. (057) 717-28-80 e-mail: promart_order@ukr.net