NBU, corpus II, room 708 | riskmlab@nbu.bg

R!SK
MANAGEMENT LAB

SEMANTIC FIELD
OF THE RISK MANAGEMENT LABORATORY

TERMS AND DEFINITIONS

The Semantic field of the Risk Management Laboratory is based on BDS ISO 31000:2011, wherein the terms used in the Standard are adapted to the specific objectives and tasks of the Laboratory.

Basic Terms

1. **"Risk"** is the impact of uncertainty on the achievement of objectives. The objectives (expectations) are subject to impacts from events that may cause (un)wanted consequences.
Risk – effect of uncertainty on objectives (2.1) NOTE:

- An effect is a deviation from the expected — positive and/or negative.
- 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).
- Risk is often characterized by reference to potential events (2.17) and consequences (2.18), or a combination of these.
- 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.
- Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood.

2. **"Risk event"** is the occurrence or change of a specific set of circumstances.

Event – occurrence or change of a particular set of circumstances (2.17)

3. **"Risk source"** is any element which has the potential to generate risk either alone or in combination with others.

Risk source – element which alone or in combination has the intrinsic potential to give rise to risk (2.16)

4. **"Consequence"** is an outcome of an event affecting the objectives. We explore every possible consequence of a risk event by trying to express it in qualitative and quantitative terms and trace out the possible chain reactions.

Consequence – outcome of an event affecting objectives (2.18)

5. **"Losses or damages"** are the unwanted consequences.

6. **"Uncertainty"** is used with two meanings in the risk management definition: a) to denote likely (probable) impacts, i.e. ones which may or may not occur; b) to describe incomplete information about the impact.

7. **"Likelihood or plausibility"** is the chance of something happening.

Likelihood – chance of something happening (2.19)

8. **"Insecurity"** is a rational assessment or perception of the existence of risks. Unlike risk level, the insecurity level can not be quantified. Insecurity does not need risk.

Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood. (2.1. Note 5)

9. **"Risk criterion"** is tolerable, acceptable risk; terms of reference against which the magnitude of risk is evaluated.

Risk criteria – terms of reference against which the significance of a risk is evaluated (2.22)

10 **"Risk level"** is the magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood.

Level of risk – magnitude of a risk or combination of risks, expressed in the terms of the combination of consequences and their likelihood (2.23)

11. **"Risk profile"** is a description of any set of risks and may include the risks relevant to the entire organisation, part of the organisation or as may be defined otherwise.

Risk profile – description of any set of risks

12. **"Unwanted insecurity"** is a breach of a risk criterion.

13. **"Wanted insecurity"** is a risk taking for the sake of a certain objective.

14. **"Impact"** is likely causation of consequences.

15. **"Danger" or "Threat"** is an event which can cause unwanted consequences.

16. **"Security"** is a state of compliance with the risk criteria; tolerable risk levels.

17. **"Force majeure, disaster"** is an event the likelihood and consequences of which are unmanageable.

Risk management

18. **"Risk management"** means coordinated activities to direct and control an organisation (country, sector or customer) with regard to risk. It involves undertaking of consistent processes across the organisational framework to help ensure that the risk in an organisation is managed efficiently, effectively and consistently.

Risk management – coordinated activities to direct and control an organization with regard to risk (2.2)

19. **"Organisational risk management framework"** is a set of elements that provide the fundamental organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation; it forms

an integral part of the policy, both strategic and operational, and of the practices across the organisation. The foundations include the policy, objectives, mandate and commitment to manage, while "organisational arrangements" include plans, relationships, accountabilities, resources, processes and activities.

Risk management framework – set of components that provide the foundations for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization (2.3) NOTE:

- The foundations include the policy, objectives, mandate and commitment to manage risk (2.1).
- The organizational arrangements include plans, relationships, accountabilities, resources, processes and activities.
- The risk management framework is embedded within the organization's overall strategic and operational policies and practices.

20. **"Risk management policy"** is statement of the overall intentions and direction of an organisation related to risk management.

Risk management policy – statement of the overall interventions and direction of an organization related to risk management (2.4)
21. **"Risk attitude"** is the approach of an organisation to assess and eventually pursue, retain, take or turn away from risk;

22. **"Risk management plan"** is a programme included in the organisational risk management framework, specifying the approach, management components and resources to be applied to the management of risk; "management components" typically include procedures, practices, assignment of responsibilities, sequence and timing of activities.

Risk management plan – scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk (2.6) NOTE:

- Management components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities.
- The risk management plan can be applied to a particular product, process and project, and part or whole of the organization.

23. **"Risk owner"** is a person (natural or legal) having accountability and authority to manage a risk.

Risk owner – person or entity with the accountability and authority to manage a risk (2.7)
"Risk management process" is the systematic application of management policies, procedures and practices to manage the activities of communicating, consulting, establishing the context, and the activities of identifying, analyzing, evaluating, treating, monitoring and reviewing risk.

24. **"Risk management process"** – systematic application of management policies, pro-

cedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk (2.8)

25. **"Risk context"** means establishing circumstances – defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy. In establishing the context the organisation should be able to choose its response in respect to objectives, impacts, likelihoods and consequences.

Establishing the context – defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy (2.9)
26. **"External context"** is the external environment in which the organisation seeks to achieve its objectives: the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether at international, national, regional or local level; factors and trends affecting the objectives of the organisation, and relationships with external stakeholders, their values and perceptions.

External context – external environment in which the organization seeks to achieve its objectives (2.10) NOTE: It 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;
- relationships with, and perceptions and values of external stakeholders

27. **"Internal context"** is the internal environment in which the organization seeks to achieve its objectives. The internal context can include: governance, organisational 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 external stakeholders, their values and perceptions; the organisation's culture; standards, guidelines and models adopted by the organisation, and form and scope of contractual relationships.

Internal context – internal environment in which the organization seeks to achieve its objectives (2.11) NOTE: It 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 preceptions and values of, internal stakeholders;
- the organization's culture;
- standards, guidelines and models adopted by the organization;
- form and extent of contractual relationships

28. **"Risk monitoring"** is checking, supervising, observing threats or determining the status in order to identify change from the performance level required or expected. Monitoring can be applied to an organisational risk management framework, risk management process, risk or control. This is continual monitoring, scanning of context by the organisation and decision makers to manage risk.

Monitoring – continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected (2.28) NOTE: Monitoring can be applied to a risk management framework, risk management process, risk or control

29. **"Risk review"** is an activity undertaken to determine the suitability, adequacy and effectiveness of the explored entity to achieve established objectives. It can be applied to an organisational risk management framework, risk management process, risk or control. Includes systematization and selection of risk context and its drivers.

Review – activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives (2.29) NOTE: Review can be applied to risk management framework, risk management process, risk or control

30. **"Communication and consultation"** is a continual and iterative process that an organisation conducts to provide, share or obtain information and to engage in dialogue with stakeholders regarding the management of risk. This information can relate to the existence, nature, form, likelihood, significance, evaluation, acceptability and treatment of the management of risk. Communication is carried out with the organisation's internal and external stakeholders to obtain inputs, understand their objectives, plan their participation and take their views into account in substantiating the risk criteria. Consultation is a two-way process of substantiated communication between an organisation and its stakeholders on an issue prior to making a decision or determining a direction on that issue. Consultation is: a process which impacts a decision through influence rather than imposition and an input to decision making, not joint decision making.

Communication and consultation – continual and iterative processes that an organization conducts to provide, share or obtain information and to engage in dialogue with stakeholders regarding the management of risk (2.12) NOTE 1: The information can relate to the existence, nature, form, likelihood, significance, evaluation, acceptability and treatment of the management or 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;
- an input to decision making, not joint decision making.

31. **"Stakeholder"** is a person or organisation that can affect, be affected by or perceive themselves to be affected by a decision or activity. A decision maker can also be a stakeholder.

Stakeholder – person or organization that can affect, be affected by or perceive themselves to be affected by a decision or activity (2.13) NOTE: A decision maker can be a stakeholder.

32. **"Risk assessment"** is a set of risk identification, risk analysis and risk evaluation processes.

Risk assessment – overall process of risk identification, risk analysis and risk evaluation (2.14)

33. **"Risk identification"** is a systemic rational process which seeks to establish what can happen as well as how, when, when, why and how likely is this to happen. Identification is a process of finding, recognizing and describing risks, which is comprised of: identification of risk sources, events, their causes and their potential consequences. Risk identification can involve factual data, theoretical analysis, recommendations of experts and other competent persons, taking also into account the stakeholders' needs.

Risk identification – process of finding, recognizing and describing risks (2.15) NOTE 1: Risk identification involves the identification of risk sources, events, their causes and their potential consequences. NOTE 2: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder's needs.

34. **"Risk analysis"** is an embedded process to comprehend the nature of risk and to determine the level of risk; it provides the basis for risk evaluation and decisions about risk treatment; it helps develop understanding of the impact, its consequences and their likelihood of occurrence. Risk analysis involves qualitative and/or quantitative description of the effect of (un)wanted events as well as establishing the reliability of the risk level determination process and of the existing risk controls; it also involves establishing the risk sensitivity of decision makers.

Risk analysis – process to comprehend the nature of risk and to determine the level of risk (2.21) NOTE 1: Risk analysis provides the basis for risk evaluation and decisions about risk treatment. NOTE 2: Risk analysis includes risk estimation.

35. **"Risk evaluation"** is a process of comparing the results of the risk analysis with the risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. Risk evaluation precedes the taking of a decision about risk treatment; it involves risk prediction and prioritization of the application of risk criteria in the case of complex risk profiles.

Risk evaluation – process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable (2.24) NOTE: Risk evaluation assists in the decision about risk treatment.

36. **"Risk treatment"** is a process intended to modify a risk. It may include: avoiding the risk by deciding not to start or continue with the activity that gives rise to risk; taking or increasing risk in order to pursue an opportunity; removing the risk source; changing the likelihood; changing the consequences; sharing the risk with another party or parties

(including contracts and risk financing) and retaining the risk on the basis of an informed decision. Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction". Risk treatment can create new risks or modify existing risks. Iterative risk treatment is a process of improving the existing controls or developing and implementing new controls. It includes assessment and selection of response options, including cost-benefits analysis. It proposes new priorities and proceeds to implementation upon approval of action plan. Once the organisation reaches the risk criterion, it decides whether to continue treating the risk.

Risk treatment – process to modify risk (2.25) NOTE 1: It can include:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to risk;
- taking or increasing risk in order to pursue an opportunity;
- removing the risk source;
- changing the likelihood;
- changing the consequences;
- 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.

37. **"Risk management iterations"** are carried out, on one side, between monitoring during the context establishment process, communications/consultations and risk evaluation, and on the other side – between risk evaluation and risk treatment after each treatment action until a preferred and efficient plan providing the greatest benefit at the lowest cost is found.

38. **"Control"** is a measure that has the potential to modify the risk. Controls include any process, policy, device, practice, or other actions which modify risk.

Control – measure that is modifying risk (2.26) 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.

39. **"Residual risk"** is the risk remaining after risk treatment. Residual risk can contain unidentified risk. Residual risk can also be known as "retained risk".
Residual risk – risk remaining after the risk treatment (2.27) NOTE 1: Residual risk can contain unidentified risk. NOTE 2: Residual risk can also be known as "retained risk".

Risk types

40. **"Political risk"** in proper sense is an impact (radical reform, riot, coup, civil war, revolt and terrorism) that can lead to (un)wanted change within political institutions.

41. **"Political risk to"** is a political change or political uncertainty that can cause outbreak of bankruptcy, impaired quality of life, loss of income, employment and asset value.

42. **"Economic risk"** is an impact that can render an investment unprofitable or lead to bankruptcy. Depending on the economic sector or operation concerned, the economic risk can be: financial, i.e. systemic or relating to credit, refinancing, impairment of collateral, concentration of doubtful receivables, interest or exchange rates, stock/commodity exchanges, liquidity or markets; organisational, i.e. relating to operations, legal matters, reputation, change of commodity, labour or asset prices, payments and profits.

43. **"Risk to national security"** is a threat to individuals, society or institutions.

44. **"National security infringement"** is a threat from a human factor.

Crisis

45. **"Crisis"** is a systemic breach of risk criteria, materialized risks leading to major damage and secondary risks.

46. **"Political crisis"** is a breach of political risk criteria that blocks or suspends the functioning of key political institutions or leads to their destruction.

47. **"Economic crisis"** is a systemic breach of economic risk criteria, pervasive bankruptcy.

48. **"Crisis management"** is response to the breach of risk criteria, controlling the risk in tolerable limits and addressing the consequences of the occurred unwanted events.

National security

49. **"National security"** is compliance, organised and assured by the State, with risk criteria in respect to individuals' life, property, rights and freedoms, their institutions and environment, the national borders, territorial integrity and independence of the country.

50. **"National security assurance"** is management of risk and crises in the areas identified in the definition above.

51. **"National security rules"** are those that govern relations within society, guarantee the security of individuals and institutions in the country on the basis of the Constitution; they establish a system of interaction between government bodies and citizens and their organisations; determine the modus operandi and supervision of the national security system.

Risk and Crisis Research Laboratory

52. **"The Mission of the Laboratory"** is applied research on security and insecurity in the country and critical evaluation of how authorities manage the risks to citizens, society and public institutions.

Documents of the Laboratory

Inbound

53. Risk Indication Protocol

54. Protocol Summary

Internal

55. **"Risk file"** is chronologically collated information regarding a certain risk, starting from its emergence or from the beginning of the observations on that risk up to the last indication of the risk and its management.

56. **"Risk indication"** is information on the emergence of new or evolution of known risk; on likely adverse impacts on the expectations of citizens, society and public institutions.

57. **"Crisis file"** is chronologically collated information regarding breached risk criteria, their concatenated consequences, new risks and damages.

58. **"Laboratory analysis"** is evaluation and prediction of risks or crises, identification of their owner and the effect of the owner's management or response.

59. **"Laboratory research"** is laboratory analysis and provision of recommendations on risk/crisis treatment; laboratory research is undertaken when deemed appropriate or when commissioned by a client.

Outbound

60. **"Risk Report"** is a document presenting analysis and research undertaken by the Laboratory.

61**."Political Constellation Report"** is periodic laboratory analysis of the balance among parliamentary and potential parliamentary parties (coalitions) and their positioning vis-à-vis government as a major source of political (in)security. The report includes a dynamic matrix of political actors' relations with key economic and media actors. The latter are examined from the perspective of: (a) concentration and change of ownership; (b) publishers' links with and dependencies on economic and political actors; (c) propensity to corruptive on-demand coverage.

62. **"Institutional Trust Report"** is periodic laboratory analysis of polls on the trust in political institutions as a major source of political (in)security.

63. **"Energy Sector Crisis Report"** is laboratory analysis of the energy sector.

64. **"Demographic Risks Report"** is laboratory analysis of the demographic state of the nation and the secondary risks to the labour market, the social and pension system, the health status of the population and the education system.