Janusz Zawiła-Niedźwiecki

Operational risk as a problematic triad:

- risk
- resource security
- business continuity

Operational risk management is always integrated, covering the triad, rather than a single issue

print pdf epub mobi

edu-Libri

Operational risk
as a problematic triad:

- risk
- resource security
- business continuity

Janusz Zawiła-Niedźwiecki

Operational risk as a problematic triad:
- risk
- resource security
- business continuity

edu-Libri
Kraków–Legionowo 2014

Editors and correction: edu-Libri

Cover and title page design: GRAFOS

Translated by Robin Gill of Biuro Tłumaczeń Narrator

This book is a synthesis of the findings published in the Polish habilitation paper *Operational risk management in ensuring business continuity*, published in 2013 by the publishing house edu-Libri (www.edu-libri.pl).

Publisher's reviewers:
Prof. Marek Lisiński (Cracow University of Economics)
Prof. Waldemar Tarczyński (University of Szczecin)

Habilitation reviewers:
Prof. Ryszard Borowiecki (Cracow University of Economics)
Prof. Bogdan Nogalski (University of Gdańsk)
Prof. Jan Skalik (Wrocław University of Economics)

Publishing house: edu-Libri s.c.
ul. Zalesie 15, 30-384 Kraków
e-mail: edu-libri@edu-libri.pl

DTP: GRAFOS
Printing and binding: Sowa Sp. z o.o.
Warszawa

ISBN (print) 978-83-63804-42-8
ISBN e-book (PDF) 978-83-63804-43-5
ISBN e-book (epub) 978-83-63804-51-0
ISBN e-book (mobi) 978-83-63804-52-7

Table of contents

Introduction

The impermanence and unreliability of all human products is inherent in engineering and economic practice, and also in every individual's everyday life. We do not truly expect that anything will serve us "forever", but we are annoyed if something fails unexpectedly. Therefore, for the provider of the product or service, raising the level of reliability is a challenge taken up as part of professional business organisation in the broad sense – both academically and commercially.

Providing reliable operation of equipment and technical systems has been known since the dawn of industrial history, or at least since the 19th-century industrial revolution. To this day, science is developing reliability theory, positioned at the juncture of mathematics and the technical sciences. The issue of technical failures, their causes and effects, or the interference they cause, is inherent in engineering behaviour, and extensive experience in both verifying the scientific findings and shaping professional best practice in the design of devices and systems with established reliability, and the drawing up of organisational solutions with predicted failure of the devices used in mind.

At the same time, there is no analogously advanced theory for the efficiency of entities which are business and administrative in nature. Their efficiency is undermined by the impact of operational risks (to a large extent organisational), i.e. the risks to which an organisation is susceptible mainly due to imperfections in internal processes, shortage of employee skills or poor resource management. Over recent years, this issue has been included in the catalogue of risk types in business practice which are identified and measured, and in the face of which appropriate technical and organisational security, and ultimately appropriately estimated financial reserves have been created.

This paper is a summary of the author's achievements and his research on the problematic triad "Operational Risk – Resource Security – Business Continuity", which have regularly been presented in earlier publications, the most important (in logical content order) are shown below.

1. In terms of "operational risk" issues:

- *Uncertainty in management* [2007], VIII International Conference "Financial Management – Risk Management and Value Creation", University of Szczecin, Międzyzdroje April 18-20, "Scientific Papers" No. 455.

- *The concept of operational risk and a classification of types* [2010], "Organisation Review" (Polish original: "Przegląd Organizacji") No. 6.
- *Operational risk and its estimation* [2008] (co-author M. Soczko), [in:] Knosala R. (ed.), *Computer Integrated Management*, Opole University of Technology Publishing House, Opole.
- (Ed.) *Operational Risk Management* [2008], (academic co-editor I. Staniec), C.H. Beck, Warsaw.

2. In terms of "resource security":

- *TSM - Total Security Management. Recommendations for the creation of an Operational Security Policy* [2003], (co-authors: M. Blim, M. Byczkowski) European Network Security Institute, Warsaw.
- *Information Security Aspect of Operational Risk Management* [2009], (co-author M. Byczkowski), "Foundations of Management" No. 2.
- *Security of information systems* [2012], (co-author F. Wołowski), edu-Libri, Kraków.

3. In terms of "Business Continuity":

- *Business continuity and management theory* [2006], "The Economics and Organisation of Enterprises" (Polish original: "Ekonomika i organizacja przedsiębiorstwa") No. 4.
- *Ensuring business continuity in limiting operational risk* [2010], (co-author P. Gołąb), [in:] J. Monkiewicz, Gąsiorkiewicz L. (ed.), *Managing risk in business continuity*, C.H. Beck, Warsaw.
- *Business Continuity* [2010], "Foundations of Management" No. 2.
- *A proposed methodology for managing business continuity* [2003], "Organisation Review" (Polish original: "Przegląd Organizacji") No. 6.
- *An model for evaluating the maturity of business continuity management in an organisation* [2007], "Organisation Review" (Polish original: "Przegląd Organizacji") No. 4.

The issue of **systematically improved business continuity in an organisation** in the management of operational risk is closely linked with other issues in management science. This can be seen when the highlighted wording is conceptually analysed.

- **Continuity** is a positive feature of active conduct similar in meaning to such concepts as: consistency, durability, resistance, or tradition. In other words, consistency is to be understood as a deliberate sequence of successive operations with a set goal and combined in such a way that not only do they not interfere with each other, but also some of the earlier operations serve as preparation for some of the later.
- **Operation** is unambiguously associated with activity.
- **Business continuity** is the evaluation of an activity perceived as consistent and resistant to obstacles. In other words, organisational procedures forming the organisation's ability to respond effectively in the event of disruption.

- **Organisation**, in this sense, is synonymous with an entity which is a system of operations created in society for economic, administrative, non-profit, etc. purposes.
- **Systematic improvement** is the flagship postulate of quality management, and business continuity, as the postulate for efficient activity, is one of a list of specific quality demands on an organisation's operation, in addition, at both the strategic and operative management levels. On both levels, improvement is one of the criteria for the realisation of an objective, closely related to others such as effectiveness, efficiency and productivity.
- **Systematic improvement** is also a basic principle of a learning organisation and knowledge management. This means the ability to analyse and evaluate events in the current practices of the organisation and draw conclusions from them for the future.
- **Provision** is synonymous with a whole range of terms representing a certain type of operation (supply, development, preparation, manipulation, influence), including organisational.
- **Management** is control appropriate to circumstances over the realisation of a specific organisational goal based on the resources at its disposal.
- **Business continuity** refers to the management of operational risk. It is a form of influence over the level of this risk, although not directly, as it does not include efforts to change the causes of that risk or the mechanism of its actualisation, but only efforts to increase resistance to its manifestations. The important turning point is therefore the moment at which business continuity solutions guarantee the organisation's influence over the manifestations of risk, and which takes place after the occurrence of the critical event that is a consequence of the risk.
- **Business continuity** also includes another category of activities aimed at reducing the risk by means of security procedures. They can, like business continuity, rely on reducing the organisation's vulnerability to the impact of risk, but they can also directly intervene in the causes of the risk and its mechanism. In addition, these relationships may appear as do those in the framework of operational risk management, to only include solutions in security (in practice this is frequent, though usually resulting from a lack of foresight) or only in the field of business continuity (in practice very rare, usually occurring when the assessment of economic rationality shows for the omission of providing security solutions), or providing security integrated with continuity (in fact an ever more frequent case, and displaying a mature and economically rational approach to risk management. For these reasons, providing security and ensuring business continuity should be seen as part of operational risk management.
- This wording in full is also axiomatic. Within it lies the effort to ensure smooth, and therefore safe, well-organised, properly targeted, reproducible and efficient operation. In particular, security, and, by its relationship with it, business continuity, too, are fundamental values in the functioning of society and individuals.

The scope of the book includes several issues that intertwine with each other in a specific manner, as shown in Table W.1.

The objectives of table W.1 may also be interpreted as corresponding to the hypotheses that:

- there is a problematic triad Risk – Security – Continuity, and a crucial feature is functional integrity, which should lead to an integrated system of concepts,
- there is a real relationship of complementarity between the provision of business continuity and other types of interaction mitigating operational risk,
- there are criteria which enable the necessary classification of operational risk,
- it is possible to develop the aforementioned principles and methodologies of analysis and design.

The realisation and verification of these hypotheses were served by research which allowed the establishment and improvement of the business continuity model, the methodology of its implementation, and then verification of its applicability in real projects.

The book comprises 6 chapters and summaries.

The first chapter defines the objective and scope of the book, and characterises the major perspectives of the issue of operational risk and business continuity.

The second chapter presents the current state of knowledge and common problems in defining and classifying risk which, although decades of research have been conducted on them, are still not fully resolved. The reason for this is the widespread acceptance, as leading, of the financial prospect in relation to the full spectrum of risk types. Meanwhile, operational risk, as opposed to other types of risk, requires a specific approach, including its analysis in terms of the organisation. The author's scientific contribution is presented as a research problem to develop a universal classification of risk, taking into account:

- the specificity of the structure of the economy as the sum of sectors through the selection of criteria taking into account that specificity,
- The universal features of the organisation,
- the determinants of the nature of the risk.

The third chapter characterises operational risk, indicating that in essence it is a problematic triad: Risk – Security – Business Continuity. The currently dominant approach to capital adequacy, specific to the financial disciplines, is shown and its shortcomings are discussed. The conclusion presents, based on the theory of organisation, proprietary classification of types of operational risk, coherently combined using several criteria related to the process approach to management of the organization, a model-cycle management of the organisation and strict compound vulnerability to the risk of the main types of resources of the organisation and organizing their use.

Table W.1. The objectives of the book and the key issues raised

Main objectives	1. To demonstrate that, in relation to operational risk, it is right to treat it as an inseparable problematic triad Risk - Security - Continuity 2. To develop a systematic methodology for operational risk analysis, in the sense of the aforementioned problematic triad, and leading to an indication – relevant to the threats and vulnerabilities identified and the resulting potential interference – of how to conduct preventive and corrective measures				
Chapter	**Issue**				**Additional objectives corresponding to the issue**
2. Risk	Risk				Indicating the concept of research into the possibility of developing a comprehensive risk classification
3. Operational risk and its classifications		Operational risk as a triad Risk-Safety-Continuity			Developing a comprehensive classification of operational risk
4. The process of operational risk management					Developing principles for systematic risk analysis leading to the determination of critical processes, major threats and relevant vulnerabilities
5. Ensuring safety in the management of operational risk	Prevention		Providing security including solutions providing continuity as a form of additional protection against risk	Ensuring business continuity including the provision of security as a set of solutions pre-empting the need for business continuity solutions	Indicating the relationship of complementarity between the provision of business continuity and other types of interaction mitigating operational risk
6. Ensuring business continuity in managing operational risk.	Therapy (repair work)				Developing procedures for proper handling in the creation of organisational and procedural solutions for business continuity mitigating operational risk.

The fourth chapter presents the classic model of the risk management process, in which a critical element is the identification of risk and its consequence, analysis, assessment, selection of treatment of the risk, and monitoring. The proper discipline of management science is emphasised, not always present in the approach of other disciplines, which is an analytical approach towards the "cause of the risk – the mechanism by which the risk proceeds – the effects of risk" as the only one which fully dissects, describes, and assesses the essence of risk. The author's contribution to the science is a four-layer learning approach in monitoring risks.

The fifth chapter presents the issues of providing security and business continuity in terms of Total Security Management, which sees them as mutually complementary to the potential threat, i.e. in the sense of a preventive action on the part of security assurance solutions, and repair and substitution on the part of provision of business continuity. The author's contribution to the study (emphasising the crucial role of Maciej Byczkowski, a long-term partner in research on this issue) is characterised by the universal security principles and the specific rules related to the organisational approach from the perspective of the protection of particular types of organisational resources.

The sixth chapter contains a formulation of the conclusion of the author's many years of research on the provision of business continuity as a complex of actions whose aim is the impact of the identified risk factors and the response to each, as well as unidentified manifestations of risk, to minimise its impact on the business of the organisation. In the pioneering period (the 1990s) of the crystallisation of views on this issue and the formulation of the first proposals for good practice, the author's research has been directed in the first part to defining the methodology of designing business continuity solutions. The second part consisted of verifying whether the methodological premises are reflected in the preparation of companies that – pressured by the regulations introduced – undertook a systematic process of implementation and maintenance of business continuity solutions, where they included them formally in their structure and organisational practice. At the same time and gradually, the formulated published standards of good practice on this issue were considered. On the basis of the research, a final methodological model, named TSM/BCP (Total Security Management – Business Continuity Planning) was elaborated, and an assessment of its applicability was conducted. The end of the chapter presents the principles of verifying the degree of maturity of managing the provision of business continuity.

The summary contains a review of the author's scientific contribution and the conclusions of this study, and further research issues that arise from the book are indicated. The author is aware that the approach presented of the main issue in this publication sets out new research questions. The principles of business continuity presented aim to improve measures directed towards stabilising the organisation's operation under conditions of uncertainty and associated risks. These organisational changes are often associated with destructive activities, i.e. first a weakening of the existing state takes place, then change, and then it is replaced with a new solution, which in turn should be fixed. The approach presented in this book involves a simplification in relation to reality which is the existence of certain

invariants in the organisation, such as: business objectives, the environment, processes, resources, structure, etc. Interference which appears triggers the organisation's stabilising mechanisms, bringing it to a state close to the initial. Thus, the principles of providing business continuity support the concepts of change management, innovation management, knowledge management, the concepts of agile, learning organisations, and so on. Against this backdrop, questions may be raised – Is the violation of business continuity always a threat to the organisation? How should we treat the introduction of organisational changes which also violate the organisation's business continuity? Can the results obtained in the book be used in change management (to ensure business continuity in the organisation in which the changes are made) and how? These and similar questions are left as a matter for further research. Firstly, the new issue in its basic shape should be set out.

1. Introduction to the issue

In the sphere of economic management and the theory in support of this practice, we may observe a dramatic increase in interest in risk. It is becoming a significant management problem. This fact is not solely caused by the accumulation of existing knowledge and practices and their development. It stems more from the fact that the strong trends of liberalisation and globalisation in the world economy has led to unprecedented intensification of market competition. This automatically increases the risk of failure of individual economic projects and the economic activity as a whole conducted by the organisation[1]. All indications are that the existing strategies for an organisation's activities are not sufficient to minimise risk, and the side effects of these strategies can mean that organisations become victims of unaccounted-for risk, the conflicting expectations of stakeholders and the organised management, both for consumers and groups of monopolistic producers.

In this context, work is ongoing on exploring the contemporary model of the organisation. In an attempt to define it, the idea and the concept of "the enterprise of the future" has been elaborated. This concept is an attempt to respond to the challenges of the progress of civilisation, as well as economic development and technical thought. Evidence of this are:

- firstly – the information revolution that means that the chief capability of any organisation becomes knowledge management,
- secondly – the pressure of the environment on the organisation resulting from variable market demand, expectations of high standards of quality products and services, the rapid development of technologies and techniques, and the evolution of legal requirements.

These are also practical and direct manifestations of globalisation.

A particular consequence of the rise of competition is the search for and implementation of increasingly sophisticated workflow, manufacturing, and services solutions. This in turn exposes the organisations implementing such solutions to a specific type of risk directly associated with organisational operation and availability of internal resources. This risk is called operational. Its importance and impact on

[1] This is the subject of research on theory of risk society, see. [Beck, 1986].

the effectiveness of the organisation will continue to grow, and with them the need for scientific penetration of the nature, sources and manners of manifestation of operational risk and the organisation's ability to respond to such risks.

In addition, a series of dramatic economic and political developments in recent years has shown the world that the mere awareness of specific types of risk is insufficient if you do not apply comprehensive, mature management of them, and this entails both the need to control the feedback in the risk management cycle [Conrow, 2000], and the need for substitute activity in the case of ineffectiveness of this management [Gołąb, 2009]. The most obvious example of this was the issue of the year 2000 (also called Y2K). Firms became aware in the early 1990s that most of the software produced for computer systems relied on an incorrect entry for recording the date in 2000; the Y2K problem mobilised literally the whole world to conduct risk analyses, implement remedial programs, and make emergency plans in case these adjustments were ineffective. The methods and organisational principles of risk analysis, removal of faults, and emergency plans developed at the time are still used and improved to this day. This particular issue, the consequence of a technical simplification (years later to be fateful), probably influenced the theory of risk management, security assurance and guarantee of business continuity and their practical dissemination more strongly than even such dramatic events as the terrorist attack on 11 September 2001.

Other types of conclusion arose as a consequence of the collapse of Barings Bank in 1995 and the power company Enron in 2001. Both events resounded widely throughout the worldwide economy. Both occurred due to the lack of sufficient regulation:

- internal (Barings) – the collapse was caused by the serial fraud of a seemingly insignificant employee,
- systemic (Enron) – there were abuses by top management in collusion with an audit company.

The falls of both companies significantly influenced the foundations of the risk management model. The need was particularly confirmed to expand the monitoring and supervision of feedback in the risk management cycle, including at the level of the national supervisory authorities and regulators. Attention was also paid to the importance for the organisation not only of financial (business) risk, but the rapidly growing importance of operational (organisational) risk [Ebnöther, Vanini, McNeil, Antolinez, 2003].

Finally, natural and technical disasters in recent years, such as the tsunami in several Asian countries, hurricanes in the Caribbean Sea, failures of offshore drilling platforms and nuclear power plants, demonstrated the scarcity of organisational preparation within local communities, authorities and employees of public administration, and entities established to provide assistance. The scale of the aggressiveness of these dangers to a large extent explains the true insufficiency of the reaction, but also indicates the need for a methodical procedure in building response mechanisms. In Poland, it is to such inferences, brought about by the dramatic flooding in Lower Silesia in 1997, that we owe the powerful monitoring system for the upper

Oder, and the principles of cooperation between those services called to assist and the bodies appointed to monitor natural phenomena.

The current state of the approach to threats such as those mentioned above indicates the general importance of the issue of risk in the economy and ongoing business activity. The Polish economist Professor K. Jajuga says: "The importance of risk management has increased in recent years around the world, mainly due to the increase in risk in the economy. The main elements indicating the development of risk management are:

- the emergence of new theoretical solutions in the field of risk analysis and management, which are at the basis of advanced theoretical tools,
- the inclusion by economic operators of risk management in the overall management strategy,
- the rise of the profession of risk manager,
- the introduction of requirements for information about risk management strategy in financial statements,
- the formation of databases enabling risk assessment,
- the creation by professional communities and by supervisors and regulatory bodies of standards and requirements for risk management,
- the emergence of international and national organisations which disseminate knowledge and professional standards in the field of risk management".

Worthy of particular emphasis is the fact that, although the main instances mentioned above relate to financial firms, the nature of the problems, and especially the recommended methods of dealing with them, are organisational in nature and therefore belong to a large extent to the specific discipline of management science, and not just financial science. Very often there is the association of risk with the financial sector and the financial sciences. At the same time, it might be said that it is the financial sector and the financial sciences we have to thank for the advancement in dealing with risk issues, while its natural scope is covered by issues relevant to three disciplines of the field of economics: economics, finance and management sciences, and further a number of other disciplines in the fields of social sciences and technical sciences at least.

With regard to operational risk, this indicates an interesting question, which will be developed in this book, that the financial sciences mainly develop methods for determining the necessary level of capital adequacy (reserves sufficient to compensate for the loss), while the essence of the materialisation of operational risk (the specific mechanism which leads from causes to effects) can be determined, and consequently its level affected, on the basis of action which is the subject of study of other sciences than finance, especially management sciences.

The procedure which directly affects the essence of operational risk and enables us to influence its level is to consciously combine prevention (hedging solutions, made possible by the understanding of its causes) and the practised ability to undertake therapy (solutions enabling continued activity). Both of these issues are the essence of understanding operational risk as the problematic triad

Risk – Security – Continuity, which as a scientific proposition is the author's contribution to the science, and which will be discussed in this book.

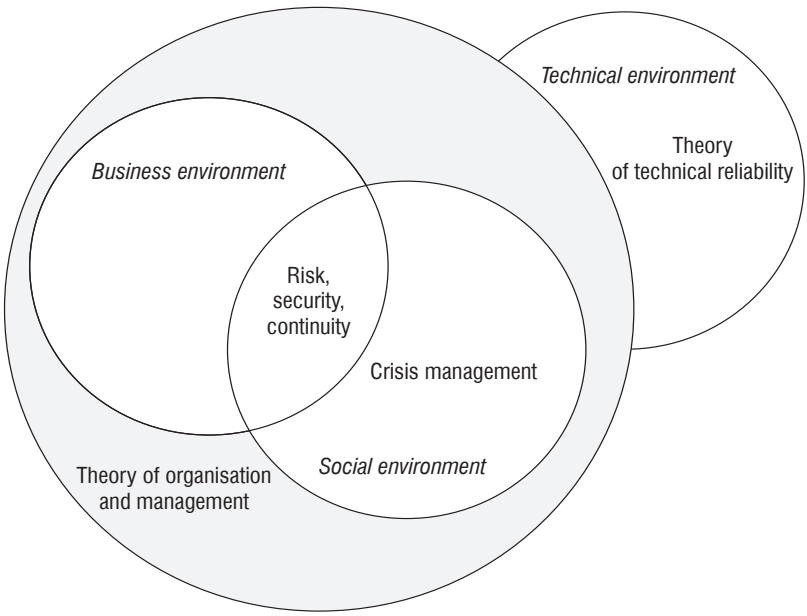

Figure 1.1. Components of risk management, security assurance, and assurance of business continuity (within organisation and management theory) with the theory of technical reliability and crisis management

Particularly important for the expression of the ability to control the level of risk is maintenance of the capability to preserve business continuity. Firstly, this is the postulate for perfection in the system's operation that is every organisation. In this sense, ensuring business continuity is the subject of strategic management; it expresses the overriding objective of organisational efficiency and includes leadership in the area of operational risk management [De Wit, Meyer, 2005]. From the strategic perspective, it remains an issue on the border of the disciplines of economics and management sciences. Secondly, business continuity is understood as organisational behaviour forming the organisation's ability to respond effectively in the event of disruption resulting from the interaction between specific manifestations of threats and the organisation's internal susceptibility, its infrastructure, resources and organisational solutions. In this sense, ensuring business continuity is the subject of operational management and is the last link in the operational risk management chain.

Operational risk has only recently become a separate category of risk. The first widely accepted definition was proposed in 1999 by the British Bankers Association [BBA, ISDA, RMA, 1999], and the most recent, provided by the Basel Committee

in the cyclically amended document *Sound Practices for the Management and Supervision of Operational Risk* [Basel Committee on Banking Supervision 2010], comes from 2004. The primary reason for the frequent updates to *Sound Practices...* is the imprecise separation of risks classified into this category, and continued focus on the clarification of the particular interpretation of this recommendation. This points to its basic problem – the lack of a scientifically structured look at operational risk taking into account the approaches of different fields and disciplines.

From the essence of operational risk, which always accompanies any activity, it flows that it is of interest for all disciplines related to the functioning of the organisation, particularly in economics, finance and management. The levels of this interest, and thus the state of the art in terms of the various disciplines, are different. In these deliberations it has been limited to the field of economics, but it is clear that a number of aspects of the problem of control of risks would be covered by the legal, technical or social sciences. In addition, it must be emphasised that in terms of the operationalisation of risk management, this book focuses on ensuring business continuity.

The most important factor in these considerations is that in these works the financial view of risk assessment dominates. This involves the use of the approach to operational risk stemming from the many years of experience of the Basel Committee (and the economic and scientific communities associated with it) in the assessment of individual risk types, conducted in order to determine the capital adequacy. As a result, a clear gap is perpetuated in knowledge about the possibilities of impacting on operational risk other than the creation of financial reserves. "Others" here entails legal, organisational and technical means.

The author of this book in his papers has emphasised the need for expanding the list of issues concerning operational risk to cover:

- crisis management,
- environmental security,
- process security,
- labour safety,
- occupational risk,
- personal security,
- information security,
- IT security,
- physical security,
- technical security,
- protection of tangible and intangible assets,
- business continuity.

Only such an extended approach will allow the full use of the sciences of organisation and management in order to mitigate risk. More importantly, only such an approach will enable the realisation that it is exactly this type of risk that refers to the phenomena and problems in the field of management, which – although

previously not assigned to operational risk – have long been known and may provide proven organisational and managerial concepts, methods and techniques.

Management is a scientific discipline as strongly associated with practice, as are perhaps only the technical sciences, and this relationship, it is probably no coincidence, lies in the industrial roots of the first concepts of the theory of organisation and then management. Thus it is an applied science, and all its concepts are always verified empirically. This entails a specific pragmatism that must be inherent in these concepts in order for them to be accepted by scientific communities (theorists) and in business environments (practitioners). This pragmatism in the first place requires that the consideration of any conception of those elements that bring it to the realities of practice, which is in fact not fully possible, should at least ensure that the degree of simplification of reality in the theoretical model be as small as possible. In turn, in scientific analytical techniques the point is that the tested reality actually determines all those elements that constitute its true variability, volatility and dynamics. An important challenge for management is the fact that very often the standardised, typical approach, based on statistical regularities does not lead to the expected results, and success is sometimes associated with deviating from the standards and statistics.

The perspective of risk (and actually three integrated perspectives: Risk – Security – Business Continuity) in the author's opinion may become the key to the interpretation of contemporary management challenges. The reasons for this position are as follows (and are explained in detail in this book):

- by analysing the risk the reasons for the limited predictability of any action is clarified as fully as possible,
- by setting the course the security most fully indicates the method for improving this predictability,
- ensuring business continuity most fully expresses the human desire for full capability with regard to difficulties in activities undertaken.

In this context, we should look at contemporary management concepts and the place of operational risk, which on the one hand may be an element of the proper approach to a given concept, while on the other it may be the subject of relevant interaction for a given concept. This is generally shown in Table 1.1, which presents the most common current concepts discussed, where we must remember that they do not usually mutually exclude each other, often use the same methods, techniques and management tools, and in a given organisation create current management practice.

It follows from the above, and will be shown more precisely later, that operational risk is always present in the management of organisation whatever the management concept. However, in the opposite sense, i.e. in answer to the question "which of the management concepts is particularly well suited to clarifying the essence of operational risk", we should look towards the process approach, the resource approach and the approach of a learning organisation.

Table 1.1. Modern management concepts in the context of operational risk management

Types of approach	Management Concepts	Examples of typical relationships with operational risk
Focus on the management of the organisation	Pro-market oriented	In particular, the risk of inappropriate decision making.
	Pro-quality and and value oriented	Ensuring security and business continuity in the context of quality assurance. There is also a suggestion that operational risk management is generally part of quality management. The issues of the danger of losing value both financially and organisationally.
	Results and efficiency oriented	Taking account of operational risk in terms of avoiding disruption. The danger of internal overregulation, the issue of preserving the primacy of results over security.
	Process oriented	Identification and analysis of critical processes.
	Project oriented	Project risk management.
	Logistics oriented	Disruption and interruption of the supply chain as a typical challenge in logistics management.
	Oriented towards: • reengineering, • outsourcing, • cloud computing	Security and continuity of services in the context of a radical reorganisation.
	Oriented towards: • social responsibility, • ethics • trust	Irresponsibility as an analogy of danger, and as its cause. The scarcity of social capital as a basis for sustainable development (education and training).
	Oriented towards: • knowledge, • competences, • intellectual capital, talent	Lack of knowledge or lagging behind development.
	Oriented towards early warning	The practical usefulness of prevention of threats.
	Oriented towards deals (in the context of the resource approach)	Risk as opportunity.
	Infonomics oriented	Dependence on information and the efficiency of the processing system.
Focus on organisational changes	Oriented towards radical changes	Risk constitutes a typical context for introducing changes (issues: effectiveness of the change, appropriate procedure, an accurate deadline, etc.
	Oriented towards systematic changes	

Types of approach	Management Concepts	Examples of typical relationships with operational risk
Focus on organisational changes	Oriented towards benchmarking	Inappropriate selection of template, improper adaptation process.
	Oriented towards innovation	In particular, the risk of inappropriate innovation decisions.
Focus on organisational forms	Oriented towards: • a learning organisation, • an intelligent organisation, • a flexible organisation	Lagging behind development, the lack of organisational flexibility.
	oriented towards network organisation	Danger of breaking their inefficiency of ties.
	oriented towards virtual organisation	Dependence on teleinformatics, for example.
Return to traditional management concepts		
Systemically oriented		The selection and interaction of components of the organisation as a system.
Resource oriented		Identification of critical resources, the "minimum acceptable configuration".
Oriented towards time and individual energy		Human-specific susceptibility to the individual conditions of operation.

The process approach is the basis for determining the most the sensitive parts of an organisation's activity viewed as a set of critical processes. An analysis of their sensitivity allows the identification of a set of critical resources, i.e. the most vulnerable, and at the same time the key for the ability to maintain continuity of critical processes.

In recent years, there has been a form of renaissance of the resource approach. Regardless of critical comment with reference to the strategic view of this approach, in the context of risk analysis (in terms of business continuity) it is essential in view of the fact that the organisational disruption of business continuity always consists of a direct loss of resources or loss of control over resources. This sets the mode of the analytical approach in providing security and business continuity.

Another issue is the aspect of organisational culture, which in order to ensure business continuity should rely on continuous improvement, both in terms of risk analysis and response to the symptoms of risk, and therefore should rely on solutions providing security and continuity.

The question of knowledge of the issues of guaranteeing the management of business continuity itself requires further discussion. There are three general scientific perspectives here – economics, finance, and management. From the economic perspective, the primary objective is to ensure business continuity and

financial continuity (capability). This is connected with macro activities (global and regional phenomena) and microeconomic on the level of traders. Ensuring economic continuity should take place by the identification of the degree of uncertainty in the prospects for economic phenomena and selection of activities with an acceptable level of risk. Each perspective is characterised by basic categories and processes between which occur the basic dependencies for determining business continuity (Fig. 1.2). Macro categories dominate, such as inflation, which not only affects the other categories and macroeconomic processes, but also affects operational and financial continuity, and then microeconomic processes. In addition, there are common categories, such as the macro-, operational, and micro- production. All of these require special studies in terms of the problematic triad of risk - security - continuity.

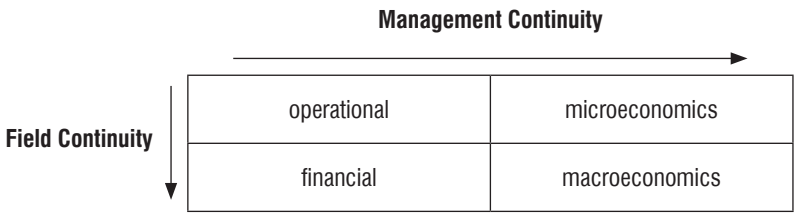

Figure 1.2. Economics and continuity in terms of basic perspectives

Suggested in theoretical considerations and essential in business practice is also the analysis of business continuity from the perspective of accounting (finances). In this perspective, continuity is analysed by studying economic processes on the basis of economic events and the financial accounting system. The crucial issue is to analyse the use of economic data by the company (both organisational and financial performance):

- in macro terms in terms of inflation (including expected inflation), unemployment, economic growth, exchange rate differences;
- in micro terms in terms of competitiveness, innovation, demand and its flexibility, expected innovation, investment processes.

This analysis refers to the distribution in Figure 1.2, as ensuring financial continuity is achieved through the analysis and selection of the manners of proper liquidity management and ensuring operational continuity through the analysis and selection of ways to manage competitiveness, changes in demand and changes in obtaining all three essential factors of production.

In turn, in the study of management, the issue of business continuity as interpreted specifically in this science has thus far only been undertaken residually, despite the fact that the stability of operation and durability of an organisation's procedures and structures are motifs in the theory of organisation from the very beginning. It may be interpreted from the first concepts of F. Taylor, K. Adamiecki or H. Fayol's postulate of safe organisation. Nevertheless, as a practical matter the

challenge only began to be formulated during the IT revolution of the late 1970s and 80s. Then the first institutions achieved a high enough level of business computerisation to begin to notice the dependence of their image in the eyes of customers and their economic performance on the smooth operation of IT systems. This source of the modern perception of the problem of business continuity as uninterrupted service contributed to the development of consultancies in this field, and to the formation of several major centres working on the recommendations of business continuity best practice. The best known are:

- The American Disaster Recovery Institute International (The Institute for Continuity Management), est. 1989,
- The UK Business Continuity Institute, founded in 1994,
- The American Virtual Corporation, established in 1994,
- The Asian Business Continuity Management Institute network, developed since 2005[2].

Their activity consists of commercial consulting, developing their own standards of recommended procedure, training linked to the granting of certificates of qualification, integration of specialists in the field by offering electronic and traditional forms of exchange of experiences and meetings, and publishing guidelines and case-studies for particular areas of business and administration. These communities are also supported by groups of entrepreneurs especially interested in the development of such recommendations. The leaders of these projects are usually also involved in academic teaching related to training in business management.

The second stream of the development of the concept of providing business continuity includes the work of standardisation committees, particularly in Australia and New Zealand, Singapore, the USA and the UK. It is also characteristic that the aspects of business continuity emerge in the course of work on the elaboration of standards of service, security, and crisis management. This is observable in the ISO 20000 series of standards ISO 2700x, ISO 31000, ISO 22301m or ISO 22313. This is similar in the case of the Basel Committee.

From the above review, it can be shown that there is a renewed need to re-emphasise the difference in the perception of risk from the perspective of the scientific disciplines of economics and finance and the discipline of management. In economic and financial terms, the point is primarily to determine the appropriate level of resources necessary to fund the effects of the actualisation of the risk. These resources cannot be too small, but it would also be unreasonable if their level was too high, and so research has focused on methods of as accurate as possible modelling of this level. In terms of management theory, the focus is to a much greater extent on more organisational aspects. Firstly, in terms of preventing the materialisation of the risk, and secondly in planning the organisational response in the event of its materialisation. This means that you need a thorough knowledge of its essence in the sense of the threat mechanism and the context of its

[2] See www.bcm-institute.org, www.drii.org, www.thebci.org, www.virtual-corp.net

occurrence associated with resource and organisational determinants of the activities of a given organisation and its environment. Of course, the two takes – economic and financial, and management – are complementary in the search for the best understanding of the nature of risk and its actualisation and the selection of response. In relation to reaction, the financial approach is, however, static and passive, while organisational solutions for ensuring business continuity are characterised by dynamics and the flexibility to adapt to a particular situation which is a consequence of the materialisation of the event.

Increasing scientific knowledge, especially with regard to the paradoxical delays indicated above in formulating scientific findings regarding the operational and organisational principles of operational risk management in terms of business continuity, inclines to the view that there is a need to give this issue more intensive reflection and research from the perspective of management sciences, which hitherto has virtually not happened. An important question is siting of the issues of the Operational Risk – Security – Business Continuity triad in this discipline, i.e. whether and to what extent it belongs, and to what extent it lies outside. The discussion shows that this triad is an important part of management theory and there is an urgent need to permanently formalise its system of concepts, the rules of conduct within its framework, and the rules for managing it.

2. Risk

2.1. Risk and uncertainty

To date, the concept of risk has been ambiguous because of the multiplicity of interpretations given to it over the years. For a very long time the meaning of this word was associated on the one hand with "uncertainty", and on the other with „accident" and "hazard". Serious attempts to clarify the concept of risk were undertaken during the 19th-century development of a new, in economic and political terms, society. This model, after further evolution, obviously, operates to this day[3], and a socially important role in it is given to institutions which, although known much earlier, have only in the new economic situation reached the status of particular social significance and responsibility, i.e. banks and insurance companies. Today, they are international – like the European Union – and national financial systems, whose stability is the condition of both local and global economic balance. These systems and their significance arise from the social need to manage risk, which is after all the essence of the operations of financial firms. Their approach has also been transposed to other industries, and furthermore the non-financial aspect of risk is beginning to be perceived. Hence the need for continued research and ever more precise definition of risk and isolation of its types.

Given the extent of the issues covered by this concept, current knowledge about risk has become a comprehensive and multi-layered theory. On the one hand it formulates generally accepted and unquestioned basic premises, such as the inseparable connection between risk and activity. On the other, however, it is divided into a number of related trends including among:

- areas of economic activity (banking, insurance, capital market, industry, trade, etc.),
- the perspective of individual social sciences (especially sociology, psychology, economics, finance, and management),

[3] In this study, no efforts were made towards a strictly historical argument. Both the conditions of the modern economy and banking or insurance were available in some countries – for example in the UK – already in the middle of the 18th century. A popular presentation of the development of thinking about risk can be found in [Bernstein, 1996].

- the mechanism for the creation and realisation of risk (the different approaches and classifications of risk in this approach are outlined in section 2.2).

In the history of philosophy, there is also the view that awareness of risk is one of the conditions for the beginning of the modern era in terms of the birth in people of a sense that their future can be shaped by they themselves, and is not just a fate imposed by the supernatural[4], and therefore human free will faces a future that is difficult to foresee, which henceforth it now has to shape alone. This points to the need to properly define an issue that is very similar and often identified with risk, i.e. uncertainty. Risk is, after all, born of uncertainty in action.

The issue of uncertainty has two main perspectives: traditional (deterministic) and modern. In the history of philosophy, the earlier one, uncertainty in human action and prediction of phenomena, especially physical, referred to man's limited knowledge of the world about him. With this approach, it could be stated that uncertainty is the incompleteness or imperfection of human knowledge and the effect of limited human cognitive capacity [Wust, 1937].

Deterministic views, whether in the field of life and physical sciences or abstract philosophy, have ultimately been confounded by the scientific discoveries of the 20th century. The new view of physical phenomena (spacetime theory, wave theories, quantum mechanics, and nuclear physics) changed the concept of uncertainty, henceforth interpreted as relativity and duality of physical phenomena, and the discontinuity of matter and energy. From this perspective, uncertainty is a feature not only of human perception and an expression of its infirmities, but simply a feature of the physical world, quite apart from the quality of human perception. As a philosophical interpretation of this new perspective on nature, in 1926 Heisenberg formulated his uncertainty principle.

Although uncertainty as a philosophical category is non-measurable, in a general sense to some extent it expresses entropy, especially when uncertainty refers to changes in an object subjected to be some organisational action, the results of which are anticipated with a certain probability of materialisation.

Given the approaches of philosophy, physics and the social sciences, it should be emphasised that this uncertainty is understood as:

- an organic feature of reality resulting from the randomness of phenomena, of which even the most stable should only be considered as occurring with extremely high probability, but not with complete certainty,
- a peculiar imperfection associated with incomplete perception by the human observer of elements shaping the phenomenon.

At the same time, due to the fact that reality (nature) is seen through the prism of human activity, uncertainty can be defined as active or passive. Passive uncertainty (objective) is not shaped by the individual; it is a feature of reality. Active uncertainty concerns the human mind.

[4] However, to this day the concept of uncertainty is seen philosophically, also from the theological point of view, which is expressed by the aphorism of St. Augustine - "If you could understand it, it would not be God".

A similar notion is unpredictability; however, this refers to the result of a specific event or very explicit action, while uncertainty expresses the general state of inability to accurately determine a course of action and the probability of each variant of the result.

2.2. Types and classifications of risk

Risk arises when in conditions of uncertainty we undertake a deliberate action, i.e. a string of deliberate acts, and at the same time an ongoing series of decisions, inextricably linked to the nature of the action. Moreover, the emergence of the knowledge of risk, including that we identify in the context of an action and its decisions, affects the further course of action, which now, next to the goals, should be characterised by efforts to reduce, offset or postpone the risk. This creates a kind of loop of behaviours, whose root cause is integral uncertainty.

So far, the concept of risk issues proposed in 1921 by Knight [1957] has not been properly challenged. Nevertheless, we have failed to clarify this concept satisfactorily, and nor have we been to formulate a universal definition of risk. This is primarily because the perception of risk is strongly dependent on the perspective of the affected party. At the same time, these are not all the conditions relativising the perspective of risk. In causal terms of rather than in terms of effect, we can speak of an objective definition of risk, since in this approach the mechanism of its formation is studied and we can accurately describe its characteristics. In contrast, from the perspective of effects, risk is perceived more subjectively, because the same event can give rise to effects with different consequences for different stakeholders, even of similar profile and position.

Initially, research on risk was only conducted in particular segments of the financial market, i.e. in insurance, banking, and the capital market. It was initiated here because the financial market is precisely called upon to deal with risk; it is the business of operators in this market. They accept their various types of risks from their clients (e.g. related to insuring the client, accepting their deposits, granting them loans, etc.) and manage them, grouping them by type (defined in specific financial products), while dispelling their own risk due to the significant number of customers. These entities do business from accepting the risk of others and play an important social role in doing so. At the same time, financial businesses experience risk in running their own business, in which they are no different from other businesses for which risk is only an element which impedes the planning and conduct of business.

On the substance of the issue of risk, for all businesses, and more generally all organisations, the degree of importance of risk in their business is decided upon by further aspects, such as [Beck, 1986]:

- the business planning horizon – the further away it is, the greater the degree of unpredictability associated with risk,
- experience as knowledge of specific forms of risk – the higher, the more possible it is to use statistical analysis tools to determine the risk,

- instability of the environment, understood in many dimensions, from the geographical (e.g. areas particularly vulnerable to natural disasters) via economic, legal, and political,
- The business impact of some types of risks that are often also the source of its other types.

Reflecting on the wording of the definition of risk, we need to be aware that:

- it is heterogeneous,
- it occurs both in of objective and subjective aspects,
- it can be seen in different contexts (intrinsic characteristics, situations of manifestation, types of activities of parties experiencing it),
- it is variable and is affected by many factors (in part dependent and in part independent of the parties experiencing it),
- it is more a process than a state.

This leads to the conclusion that – beyond a single general definition – it is perfectly natural to use a number of detailed definitions. Their diversity results from both through a defining lens, and so its subjective perception, as well as from the specifics of the type of activity, which risk touches and through which it is sometimes created.

Such a general definition is:

The risk R is the product of the probability P of a disruptive event occurring and the size of damages S resulting thereof[5].

$$R = P \cdot S$$

The author's observations, made over the course of years of research on operational risk, lead to the conclusion that in ongoing economic activity there is no need for a universal definition of risk, which various types of risk are determined, both in broad terms, as well as for individual markets or sectors of the economy, as well as in the system: organisation's environment versus its internal arrangement and operation. An example would be credit risk in banking and non-banking commercial relations, in their ideological mechanism the same, but still seen as different with regard to the scale, concentration, dispersion and time horizon.

Searching for a classification of risk useful for projects in the field of business continuity, the author has also concluded that the major difficulty in classifying types of risks is due to the need to take account of the causes of its formation (causal view), the method and process of its actualisation (view from the perspective of vulnerability) and manifestations of its materialisation (effect view). And here we are not even considering so much the subjectivity of the assessment of the realisation of the risk. The main difficulty is constituted by the complicated relationship

[5] Such a definition is proposed by the USA Commission on Insurance Terms, 1966, and also [FERMA, 2003].

between the organisation and its environment, hence the need to assign both causes and effects to the environment or to the organisation (its operations). In the author's view, all of the following combinations are possible (with the proviso that the first two are the most common):

- a cause in the environment, and an effect within the organisation – for example, lowering the profitability of production due to an increase in the value of the national currency,
- both cause and effect within the organisation – for example, the downtime caused by employee error,
- a cause within the organisation, and an effect in the environment – for example, appearance of a product defect during its use by the purchaser,
- both cause and effect in the environment (although of course there is here a mechanism for the impact of the effect of risk on the organisation and its activities) – e.g. depletion of the market as a consequence of geographically distant natural disaster.

Other significant features of the different types of risks that should be taken into account when considering the general classification of the risk are:

- time of occurrence of the cause to the effect,
- the size of potential or actual damage,
- the disorder of the damage (interference) again in several aspects, such as: value of the losses, the time required to restore the original state (if at all possible), the nature of the consequences (physical, geographical, social, organisational, etc.)
- repeatability (the frequency of materialisation) of this type of risk and the damage resulting from it,
- the predictability of the risk (knowledge of statistical regularity of occurrence, the range of possible scenarios of actualisation and the possible consequences).

Well-established and uncontroversial classifications of risk are limited to financial risk, broken down into four market segments and the entities operating there that face such risks and in a similar way take account of them in their management practice. These are: banking, insurance, the capital market, and other economic agents. In banking, the classification introduced by the global recommendations of Basel II has been effective since 2006. In insurance in the European Union the Solvency II Directive will soon apply. In the capital market of the European Union, a set of MiFID directives have been introduced since January 2007, which divide risk in the same way as banking regulations, putting additional emphasis on the risk of speculation in derivatives.

For other entities, i.e. manufacturing, trade and service enterprises, considered to be the separation and definition of market risk, credit risk and liquidity risk are undisputed. Other risks and their classification have not been agreed in a widely accepted model. Probably the consequence of this is that in this case the risk divisions are not determined on the basis of pre-defined criteria for classification.

Particularly interesting is the fact that operational risk, so clearly already highlighted in the case of financial institutions, is still not perceived seriously here.

In many papers, fragmentary classifications are given relating to individual criteria, such as: perspective (internal or external) of assessment by the company, type of activity and membership of the industry/sector/type of market, the need for, or value placed on the risk, type of threat, ability to protect against, time horizon (business planning, the consequences of protection, the impact of dangers, etc.) and many others. Until recently, the state did not interfere with practice, because outside the financial market, where risk is the subject of the business, it was almost a marginal issue in management. Today, however, due to the increasing level of organisational complexity in all social activities, organisations are consciously undertaking to manage business risk and use it in creating and building value. Risk is even becoming one of the central challenges in business management.

The traditional approach was limited to a simplified analysis of the organisation's activities and treated risk as an insignificant issue in management. In the majority of cases, risk management amounted to the preparation of preventive measures against dangers which might cause losses, and the opportunity was not taken to build lasting added value in the organisation. In addition, it did not provide consistent and systematic methods for risk management, which for most organisations is important in the context of the increasingly frequent need to define new and existing types of business risk.

Thus, the need for a comprehensive look at risk as a structured multi-threaded image of issues has become increasingly important. In response, various attempts are ongoing to capture this issue [Nocco, Stultz, 2006; Strzelczak 2003] – covering these is beyond the scope of this book.

2.3. The concept of comprehensive risk classification

In this study, a different, original suggestion towards research will be indicated. It is based on the consideration of two aspects of the analysis of the issue. The first is the logical sequence starting from the causes of critical events, via the mechanism of their actualisation, to the final actualisation, or effects, which are usually damages and losses (see Fig. 2.1). Risk is, in fact, recognised by:

- dangers, which constitute the causal image of the risk
- the interaction of these dangers with vulnerabilities in the business that experiences the risk, which constitutes the essence of the materialisation mechanism of risk,
- the effects of risk materialisation.

It is therefore a combination of a causal approach, a mechanism for actualisation, and an effect approach, with the aim of capturing the dynamics of overlapping critical events which embody a business risk. And these elements should be taken into account when setting a comprehensive classification.

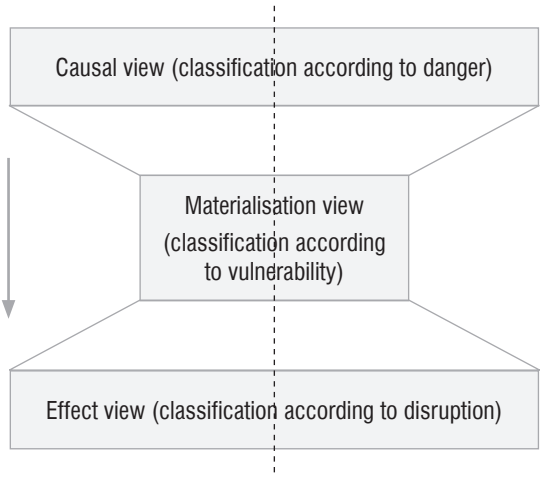

Figure 2.1. Cause and effect model of risk classification

The second aspect of the analysis is to integrate the various divisions of risk with its types, carried out from the perspective of the various areas of social activity and bodies operating in their area. Such divisions should be made separately in terms of causation, and separately in the terms of the effect. Figure 2.2 shows, in the form of a cross section, only the idea of classification, which requires careful examination and clarification. This classification must connect:

The division of risk types specific to industries, sectors and areas of socio-economic activity,

- the division into risk of the body's internal and external risk,
- the division into specific and systemic (systematic)risk
- and it should be open to other, more detailed breakdowns.

For example, consider as a starting point the division of financial risks as categorised by Culp [2002] while of course reviewing the criteria for the division:

- market risk,
- financing risk,
- market liquidity risk,
- credit risk,
- legal risk.

After these considerations, it is also worth defining business risk by adopting a radical division of general risk perceived by the organisation into business and operational risk. Such a division is justified in Chapter 5 as the distinction between the concept of activity (which relates to business risk) and the concept of action (which in turn relates to operational risk, as discussed in Chapter 3). Thus:

Business risk can be defined as the risk of losses due to inappropriate decisions about the selection of clients, form of products and services, or obligations to business partners or as a result of failure or inconsistency in a country's economic system.

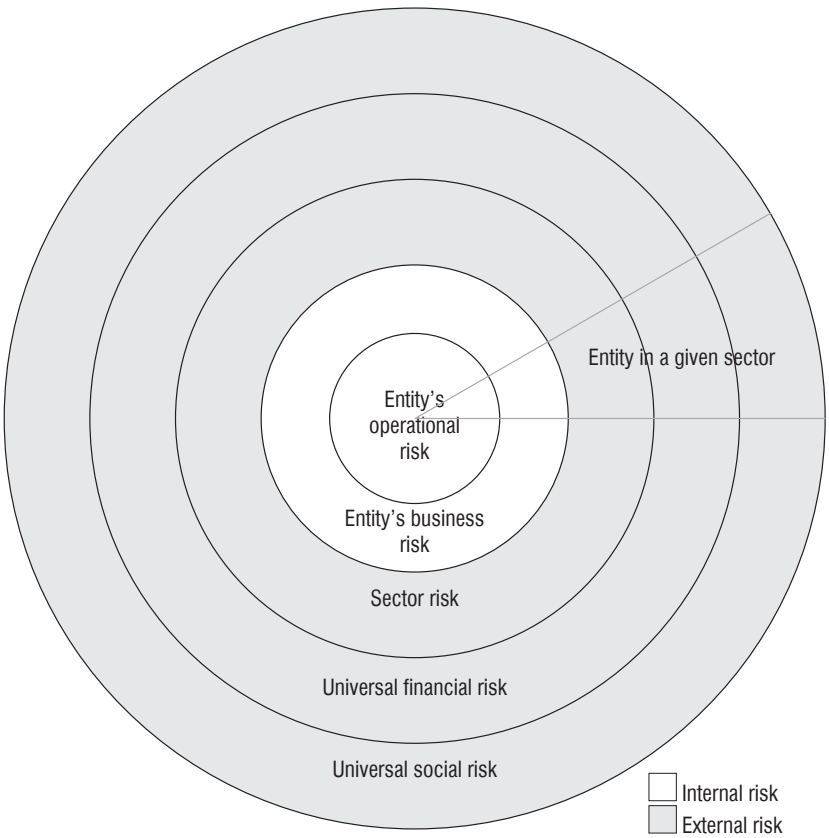

Figure 2.2. Structural model of risk classification

2.4. Risk measurement

First of all, we should note the often unfairly overlooked division of risk metrics into objective metrics, characterised by the risk itself, and subjective metrics related to the relationship of the organisation and, indeed, its decision makers, to risk. In the practice of risk management this is a very important difference, because regardless of the calculation of risk through the use of selected methods for measuring, the risk values finally adopted in the course of decision-making as part of managing them are derived from the subjective response of the decision-makers.

As part of the systematisation of risk metrics, we should include:

- decomposition of risk metrics in the direction of determining the probability of the results of individual events endangered by risk and the value of those results;
- the degree of multi-dimensionality of the risk being considered;
- the need to consider extreme risk (catastrophic in nature and with a huge level of losses).

Risk metrics, from the perspective of the design and nature of a given measure, can be subdivided as follows:

- metrics based on the statistical distribution of a random variable, which is a risk variable (the effect of the risk is subject to analysis, illustrated by the possible values of the risk variable);
- metrics resulting from the dependency of the risk variable on risk factors (what is, in fact, analysed is the cause of the risk as the effect of the risk factor on the risk variable);
- measurement data in the form of classes of risk, and thus the risk variable is not necessarily a random variable, the semantic differential method (only the effect of the risk is analysed) is the most commonly used.

The general approach is characterised by Figure 2.3. This issue is rapidly expanding, especially in the search for analogies with other areas in economics.

It should be stressed, however, that the financial measurement methods with respect to operational risk are mainly for the determination of the capital adequacy for the risk, and thus the level of financial security which the organisation needs to be able to face the consequences of the different types of risks affecting its activities. Except where the risk relates to financial resources, this is not a metric for the risk itself, but only for defining the necessary reserves. Consider this in these examples taken from economic life.

The first example concerns the financial resources and the issue of security. Assume that an organisation is preparing to participate in a tender procedure, counting on a multi-million dollar contract. A condition of participation is to pay the deposit, a few per cent of the value of the potential contract. If we consider the risk of loss of the amount in the deposit (theft, denial of bank guarantee), should the risk should be measured by the amount of the deposit or the amount of the lost contract with an as yet unknown exact value? Is it necessary to make this value precise or is it sufficient to say that it is significant? And as a consequence, special remedial solutions will be necessary to protect against its loss.

The second example relates to non-financial resources and business continuity issues. An organisation is paralysed as a consequence of heavy snowfalls; workers cannot get to the workplace, and components cannot be received and finished products dispatched. The only solution is to engage all available forces in the organisation of human and technical resources to unblock routes of communication. The risk of such an event should obviously be calculated financially, but on the other hand, an assessment is required which will indicate that the decision to mobilise

forces and means is justified. This need not be financial, but simply an indicator, i.e. yes or no.

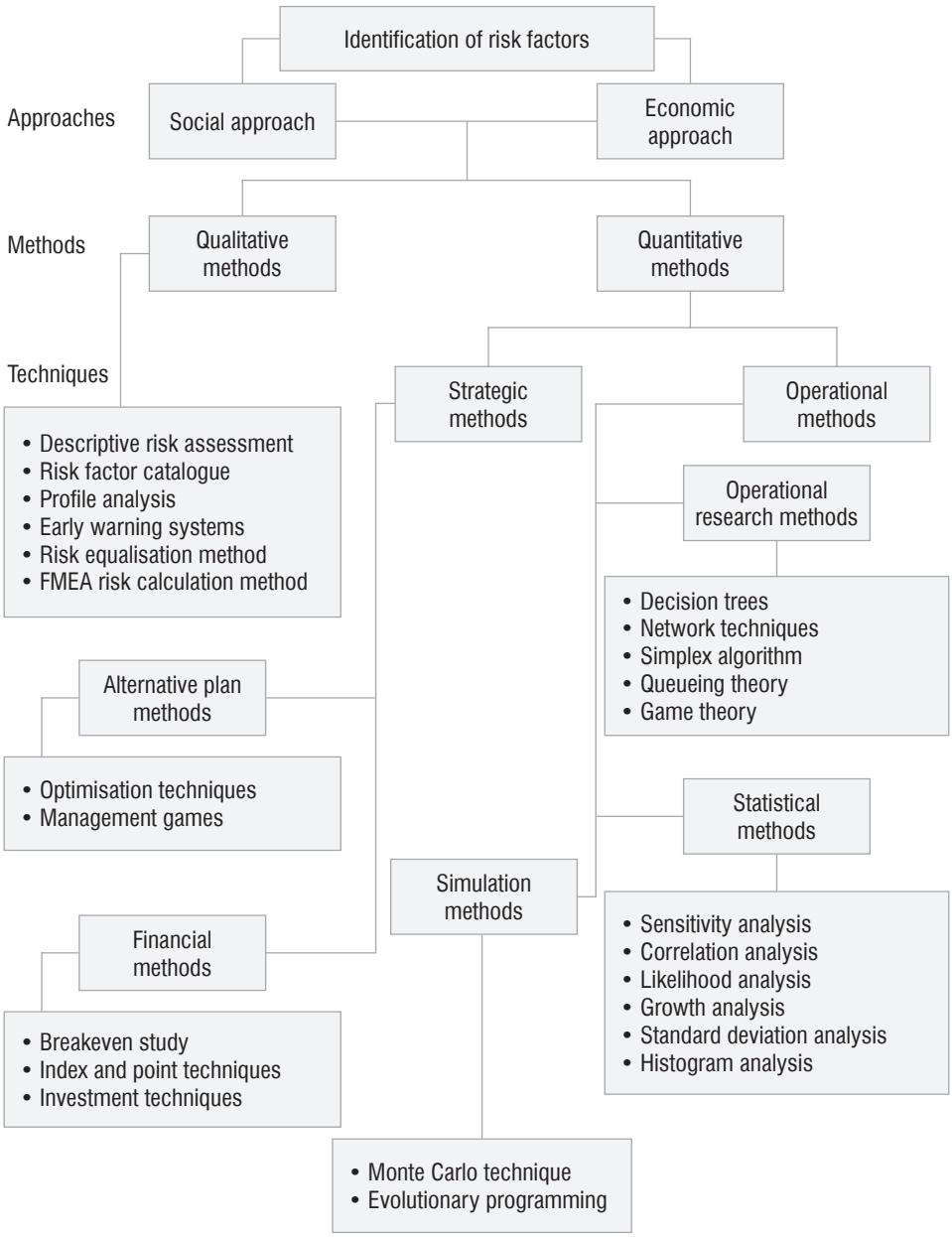

Figure 2.3. Risk measurement - approaches, methods, techniques

This means that in terms of mitigation of operational risk, and thus ensuring organisational security and business continuity, it is necessary to adopt a different way of thinking. This issue is developed in subsection 4.2.

2.5. Risk management

The primary objective of risk management is to improve the financial performance of the company and provide conditions such that it does not incur losses greater than assumed. Management should lead to the situation where the organisation (its management) is aware of the risk and its dimensions, and current activity does not go beyond the risk consciously adopted as acceptable. Influencing the risk must take into account the existence of opportunities and risks, and the ability to cover potential losses, where losses seen as profits lost from not taking certain actions must also be considered.

For a long time, risk has not been systematically analysed outside the financial sector, where for natural reasons it is the leitmotif in the development of insurance, banking and capital markets' products and services. However, the growth of wealth of societies in the second half of the 20th century led to increasingly frequent recourse to insurance products, and at the same time a growing awareness of the possibility of securing business from the basic types of risk. To the end of the 20th century, an integrated approach to enterprise risk management was perpetuated, also closely associated with the analysis of the processes occurring within it, and with the postulate of the security of management, which also included the protection of reputation and business continuity [Strzelczak, 2003].

In terms of the conditions of effective management, it is a detailed analysis and recognition of the nature and extent of the potential risk, as this allows selection of actions in a timely manner for moderating or preventing negative effects. We should aim for the situation where an informed decision can be taken as to the limits of permissible exposure to the risk, in the context of the potential achievement or loss of benefits in business. Hence: risk management strategy is a plan of action for important areas in the organisation, depending on the formulation of objectives and forms of action referred to the anticipated changes in the factors affecting the level of probability of loss of benefits or losses. This should constitute a planned response to risk, formulated on the basis of knowledge about the sources and methods of its materialisation in the form of damage and based on knowledge of how to prevent and measure risk, and valuation of the damage, i.e. its effects.

You can never eliminate risk entirely; you can only seek to minimise it. The risk that remains is called residual risk. As a rule, further minimising of the risk is economically unjustified, i.e. the cost would be greater than the potential loss. However, we should be aware of the likelihood of occurrence of an incident that is an expression of such a minimised risk. The organisation should be aware of the existence of residual risk and the need for an informed decision about accepting it.

Modern risk management refers to a division into the following basic groups of risk: material threats, financial threats, strategic threats and operational threats, and also adopts the following six principles of management.

1. Enterprise risk management should be management of all its modes simultaneously.
2. The risk management process must directly involve the company's top management.
3. General enterprise risk types should be treated as a risk portfolio – which means that it requires an understanding of its individual elements and the relationships between them – and must be managed via the objectives and processes across the organisation [Casual Actuarial Society, 2003].
4. Quantitative methods of measuring risk should be applied.
5. Tools and risk management procedures adopted are common to all types of businesses.
6. Risk is not so much minimised as optimised, and enterprise risk management becomes the decision-making and implementation of activities to achieve an acceptable level of risk.

Specific types of risks emerged at the turn of the 21st century as a result of pathological management in certain corporations: Bank of Credit and Commerce International – 1991; Maxwell Corporation – 1991; Enron – 2001; World Com – 2001; Parmalat – 2003. In response the corporate governance rules were introduced[6], and within them the principles of supervision and monitoring. Three pillars of risk control serve this end:

- ownership discipline (i.e. disciplinary measures which are available to a company's owner),
- market discipline (and thus disciplinary measures against the company available to market participants),
- regulatory discipline (and thus the means public authorities have against the company to enforce the security of specific behaviours).

To properly manage risk, company management must understand that the most important steps are: its identification, analysis, and measurement (or estimate). Until this happens, it is hard to speak specifically about a risk, because you cannot properly take measures or security solutions to limit the risk. In general it can be said that, without knowing the risk, one can only deal with the danger understood primarily as: ignorance, recklessness, and negligence. When due diligence in action is added, we are no longer speaking about a vague danger, but about a risk as the likelihood of a specific effect or as a distribution of likelihoods imagined as a set of consequences. Then you can decide which methods of management to choose (to neutralise it) and build the relevant organisational structure.

[6] E.g. Polish Forum Corporate Governance www.odpowiedzialnybiznes.pl, European Corporate Governance Institute www.ecgi.org

The growing importance of enterprise risk management has meant that since the end of the 20th century public standards of risk management have arisen. These were created as the result of initiatives by a number of institutions that promote best practice in managing varieties of risk. Among them, special attention should be paid to the standard recommended in 2004 by the Committee of Sponsoring Organisations of the Treadway Commmission – known as COSO II – Integrated Enterprise Risk Management [Nocco, Stultz 2006]. COSO II is based on eight elements of integrated risk management, which largely correspond to those previously developed from internal control standards (known as COSO I).

1. Internal environment – risk management policy within the organisation, specifying, inter alia, its tolerance for risk and recognised ethical values.
2. Goal setting – a system of risk management which provides the company leadership with processes for setting goals and verifying compliance with the company's mission and its propensity to/tolerance of risk.
3. Identification of events/threats – establishing the internal and external events that may affect the achievement of planned objectives.
4. Risk assessment – above all, risk analysis, and within this determining the likelihood of its occurrence and the possible scale of impact, which aims to determine ways to affect risk.
5. Response to risk – the basic approaches to risk, such as: avoidance, acquisition, reduction or breakdown, and actions to influence risk according to the established tolerance levels.
6. Control – control policies and procedures for verifying the degree of implementation of risk management programs.
7. Communication – the range of information and forms of communication between employees.
8. Monitoring – a systematic assessment of degree of task realisation to achieve an adequate resistance to risk.

In turn, in its enterprise risk management standard of 2003, the Casualty Actuarial Society of the United States (CAS) defines this management as "the process of assessing, controlling, operating, financing and monitoring risks from all sources for the purpose of increasing short-and long-term organisational values for stakeholders" [Casualty Actuarial Society, 2003]. The CAS model distinguishes 4 types of risk:

- the risk of threats (physical), including the risk of civil liability, property damage, and natural disasters,
- financial risk, including valuation, assets, currency and liquidity risk,
- operational risks, including the risk of customer dissatisfaction, failed product, fraud, loss of reputation,
- strategic risks, including the risk of competition, social trends, and capital availability.

The CAS management process model consists of 7 steps:

1) determining the context of the organisation's activity in terms of risk,

2) risk identification,

3) risk analysis and classification,

4) developing a comprehensive portfolio of risk,

5) assessing (estimating) and prioritising risks,

6) the effect on the risk of adopting appropriate action plans,

7) monitoring and control.

Also in 2003, FERMA (the Federation of European Risk Management Associations) recommended a standard of risk management developed by a group of the UK's largest sector organisations: IRM (The Institute of Risk Management), AIRMIC (The Association of Insurance and Risk Managers) and ALARM (The National Forum for Risk Management in the Public Sector). This Standard uses the terminology adopted by the International Organisation for Standardisation (ISO) in the document "Recommendations of ISO/IEC Guide 73 – Vocabulary – Guidelines for standards". This Standard [FERMA, 2003] distinguishes between internal and external risk factors and divides risk into: financial, strategic, operational and dangers, and the risk management process into 7 stages:

1) determining the company's strategic objectives,

2) risk assessment,

3) risk information,

4) decision to address the risk,

5) affecting the risk,

6) reporting of residual risk,

7) monitoring.

The most difficult of these is risk assessment, which includes its identification, description, and measurement. The Standard attaches great importance to reporting and communication in risk management, as well as to the proper organisation of managing it.

The above principles in relation to operational risk are developed in Chapter 2.

2.6. Risk management maturity level assessment

At the end of these considerations, let us consider the question of the efficiency and maturity of the risk management process. The basis of modern management systems is a process approach. This is based on the belief that the intended action is carried out with proper productivity when it is treated as a process. Ongoing productivity achieved and its improvement are assessed by measuring the process parameters. This must lead to a comprehensive measurement of the effectiveness and productivity of the process. Every process, and thus also the risk management process.

Measuring the effectiveness and productivity of a process is one of the mandatory assessment tools[7] in quality management systems. And risk management, especially as a result of the management of the provision of security and business continuity management, are procedures for the quality assurance of this action.

Measurement and evaluation of the processes are carried out under monitoring and constitute an integral part of them. The basic elements of the assessment are:

- the ability of the process to perform the tasks (including validation of the ability after any significant change in the process or its environment),
- flexibility (as the ability to change),
- effectiveness,
- productivity,
- efficiency and others.

Most important for the overall assessment are the indicators of effectiveness and productivity. Effectiveness and productivity are considered to be detailed categories of a universal praxeological concept – efficiency (things are done well), which is measured as the ratio of parameters delivered to those planned (e.g. yield) of a process and determines the degree of utilisation of resources. Within the context of efficiency, the measurability and accountability of its goals are essential issues. They should primarily be characterised by such features as: precision, measurability, prioritisation, comprehensibility, feasibility, and availability.

Effectiveness (good things are done) – is measured as the ratio of parameters completed to planned of process productivity, and determines the ability to achieve the desired objectives. This is about the ability to select appropriate goals, without which even smooth operation is pointless. Productivity, on the other hand, is the relationship between results achieved and resources used. Effectiveness and productivity can be seen as results of the quality of a process, and this means that the quality of the process as a synonym of the original capacity is primary to effectiveness, productivity, and flexibility. The emphasis recently placed on assessing the flexibility of a process stems from the frequent impacts of the environment, which force an internal change in the organisation.

A schema for assessing the effectiveness and productivity of a process involves [Rummler, Brache, 2000]:

- managing the process objectives,
- managing the process productivity,
- managing the process resources,
- managing at the interface between the activities.

This schema consists of the following phases and steps to determine the measures that allow the assessment process:

[7] Other assessment tools include: internal audit, assessment of user satisfaction, assessment of objectives, and management review.

- phase of determining the requirements and objectives of the process
  - identifying the requirements and sources of process goals,
  - analysis of the essence of these requirements and their transfer to the level of the process,
  - setting objectives for the process;
- phase of designing the metrics and monitoring system
  - establishing the process metrics,
  - defining the responsibilities and tools for measuring and monitoring;
- phase of registering and evaluating the process results
  - registering process parameters,
  - accounting of the process metrics,
  - interpreting the results achieved,
  - deciding on necessary corrective actions.

The metrics for assessing a process apply to activities and the manner of their execution. They are divided using two criteria. According to the position of observation (setting the value of the metric), for:

- external metrics that measure the productivity of the process,
- internal metrics that measure the efficiency of the process.

In turn, by category of data used to construct metrics for:

- metrics of economic productivity, which express the assessed aspect of the process in monetary values,
- operating productivity metrics that reflect the efficiency state of the process and may be quantified.

Metrics serve systematic monitoring, carried on traditionally or using technical tools. Always, however, the limiting aspects of the effectiveness of the evaluation will be:

- the need for anticipatory ideas on the effects of disruption that have not yet happened, and estimating the cost dimension;
- estimating the potential maximum loss suffered as a result of disruption which, although it occurred, its dimensions were limited by the use of solutions providing security and business continuity;
- ongoing interpenetration of routine workflow solutions with solutions aimed at ensuring security and business continuity.

A special form of process measurement is statistical control, whose importance is emphasised by ISO 9001, and which in the past was more often used on processes in industrial plants. Meanwhile, the latest concepts [Armstrong, 2001] suggest that – preserving the condition of proper selection of parameters – using statistical control we can analyse any process. In addition, this is the subject of recommendations promoted in the banking and insurance branches of the financial sector (recommendations of Basel II and EU Directive Solvency II), that induce

organisations to run statistical databases on incidents and to build on that basis internal (i.e. specific to the organisation) management models for different types of risk, including operational risk, with the implication that the following will be assured: quality, security, and business continuity.

Level I Traditional approach	– internal monitoring – internal audit – individual prevention programmes – based on organisational culture and human resource quality
Level II Awareness	– risk definition – risk policy – risk assessment – warning signals – risk management structures – commencement of data gathering about events – economic capital models
Level III Monitoring	– vision and goals of operational risk management – comprehensive risk indicators – risk limits – reporting – engagement of operating personnel – training
Level IV Quantification	– database of operational damages – measurable quantitative goals – prediction models – economic capital including risk – active risk committee
Level V Integration	– integrated set of management and operational tools – risk analysis integrated with management of the entire company – correlation of risk indicators and operational losses – assignment of risk (insurance) linked to analysis of the level of risk and capital – remuneration of managers dependent on company results corrected for the value of the risk

Figure 2.4. Levels of risk management maturity

Source: [BBA, ISDA, RMA, 1999].

The assessment carried out on the basis of metrics is to lead to arrangements for the further improvement of the process. This should be done using a process maturity test, for example, according to Armstrong's model [2001], which introduces a five-step scale for maturity level:

- preliminary – the results of the process are characterised by volatility,
- repeatable – the process achieves reproducible results,
- defined – the process is efficient and effective, consistent with the criteria,
- directed – the process is highly efficient and effective,
- optimised – the results achieved are of the highest quality.

Similarly, the maturity of comprehensive risk management can be assessed. An example of such an evaluation model is shown in Figure 2.4.

The use of this type of model is based on an initial assessment of the level currently achieved and the development of a plan (and its controlled implementation) for improving risk management in order to achieve the next levels, which is verified by periodic assessments of compliance with the model. Especially emphasised should be the need to include risk management rules (including security rules) in the shaping of the organisational culture and the need for full involvement of all employees in the organisation (not just those participating in the risk management structures).

3. Operational risk and its classifications

3.1. The problematic triad "Risk – Security – Business Continuity"

Operational risk in terms of providing business continuity is related to the question of the time horizon over which the planned action is considered and the accompanying risks and associated threats. This is significant because of the question – on the basis of which scientific discipline is the nature of the risk and providing security and business continuity being considered? This should be carried out differently if you are look from a distant time horizon – then it is a question of the scope of the discipline of economics, for which in the context of business continuity such issues as the following are important: the economic cycle, growth (development) and its saturation and possible achievement of the growth boundary (e.g. the hypothesis that the economic model of the European Union is perhaps coming to the end of its development).

On the other hand, if you take a short time horizon, it is a question of the scope of the discipline of management science, and operational risk is considered the risk of insufficient effectiveness of operation from the perspective of the operational (ongoing) goal of this action. And it is just such an approach that is the subject of this book. In this approach, operational risk is the possibility of failure of technical expectations, productivity or qualifications, as well as intentional criminal damage. It is therefore about how internal organisational processes are sufficiently effective, including resistance to disruption, as to enable the organisation to meet its objectives. There is no automatic synergy between the two areas, namely the business and the operational activities of the organisation. We can, in fact, imagine a situation where a company, after designing an attractive product and finding the appropriate category of recipients, is not able to meet the challenge of producing or delivering this product to customers as a result of ineffective (in any aspect) organisation of production, sales or logistics in the broad sense. This may be a purely organisational problem, but might also be a lack of qualifications in personnel, shortage of funds, etc.

The logical consequence of awareness, identification and assessment of risk is the search for security and remedial solutions. In particular, it is worth emphasising the synergistic relationship between the issues of security provision and business continuity. From the perspective of tasks assigned to ensuring business continuity, all actions aimed at security are preventive. On the other hand, from the perspective of safety and security, business continuity solutions are a remedial reaction to the ineffective protection. This is illustrated in Figure 3.1.

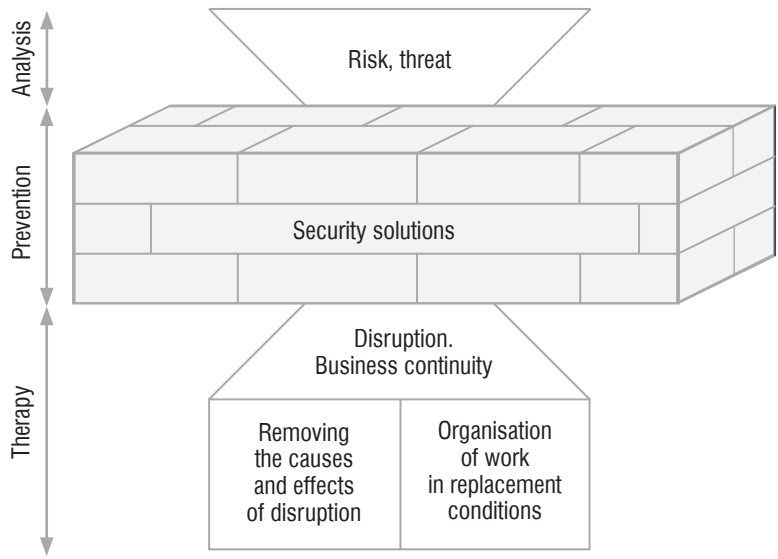

Figure 3.1. Relationships between the tasks of providing security and business continuity

An integrated perspective on operational risk, security and business continuity may be the key to integrating modern management concepts, because, as pointed out in the introduction:

- analysing the risk explains the reasons for the limited predictability of a given activity,
- determining security methods shows how to increase this predictability,
- ensuring business continuity reflects the desire for full capability with regard to difficulties in activities undertaken.
- the triad Risk – Security – Business Continuity entails the management of risks involving the rational spread of emphasis between prevention against threats to the organisation's activities and the planned response to the presence of disruption.

In fact, using the concept of operational risk management includes the control of the triad of issues Risk – Security – Continuity.

3.2. The existing approach towards operational risk

The issue of operational risk was taken up in the 90s of the twentieth century by the Basel Committee in the preparation of comprehensive recommendations on good risk management practices in banking. The momentum with which these recommendations have been introduced in entities on the financial market (such as Basel II and the Solvency Directive), and the precedence of the work of the Basel Committee over other studies on this issue, has resulted in the absorption of the Basel Committee's definition and classification in the scientific field. It should be critically stressed that this classification was developed as a summary of banking practice and in the scientific sense has methodological flaws.

This definition, from the point of view of the science of organisation and management, needs assessment of:

- the differences between the concept of "operational" and the potential concept of "operative",
- the catalogue of issues (and its clear boundaries) that comprises operational risk.

Operational risk should be seen as an issue related to the efficiency of an organisation. For this reason, in order to assess the definition proposed by the Basel Committee, we should appeal to the classical management scheme (Fig. 3.2).

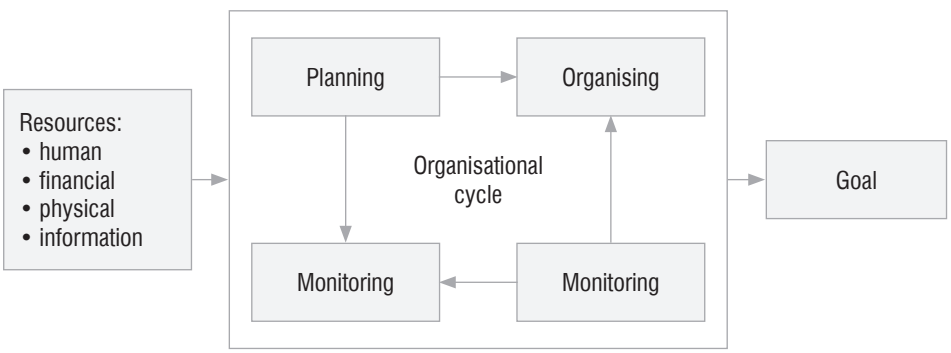

Figure 3.2. A conceptual model of management

While the economic risks associated with the functioning of the organisational cycle are addressed to the goal of the organiation's activities, operational risk concerns how resources are used in the organisational cycle to achieve the objective, and is therefore subject to the requirements imposed by the management of economic risk.

Considering the alternative use of the terms "operational" or "operative" we can actually refer to operationalism as a direction in the methodology of science,

according to which scientific terms and concepts have empirical sense when they can be defined by the description of the operation defining their use. The adjective "operating" is thus to mean "relating to the operation", i.e. actions to perform a specific task in the way of logical and planned transformation (of resources) conducted within the organisation. In turn, the adjective "operative" in its very root, signifying vigorous, efficient and effective action, is attributed to all ongoing activities in an organisation, making it a broader concept than term "operating", in particular in the relationship with the environment. At this point, it is worth returning to the consideration of the difference between activity and action (see chap. 5). Both action and operability are specifically associated with the handling of resources, while activity and operationality are related to the comprehensive functioning of the organisation. In conclusion, it must be assumed that the term "operational risk" is framed and interpreted in the Basel Committee documents in accordance with the methodology of management science, which does not mean full acceptance of abovementioned definition.

With regard to the problems listed in the Basel Committee's definition of operational risk we should refer to the appropriate analytical approaches for operational management, i.e. the process approach and the interaction of an organisation with the environment. In this context, we should evaluate not only the definition, but the classification of categories of events (7 categories) and event types within each category, which are its source of interpretation or generalisation. This classification unfortunately mixes manifestations of risk in terms of causal and effect relationship, and therefore does not meet the basic requirements of scientific classification, i.e. clarity and consistency of criteria. Therefore, in the rest of this book, an original classification of the types of operational risk is proposed.

In the literature analysing and describing risk there are different risk classifications, but the issue of operational risk itself is considered rather marginally, hence the few attempts to classify this type of risk. This is not accompanied by a methodological outlining of the limits of the issue, nor a methodical formulation of the criteria for classification.

Interesting contributing work worth mentioning is C. Pritchard's book [2001]. It is an example of how operational risk issues are viewed in many areas of the professional literature. They are devoted to other leading problems (in Pritchard, management of IT projects), for which risk is an important factor in success or failure. From the perspective of such issues as projects in Pritchard, the issue of risk is then presented specifically and incompletely. The term "risk" does not even bear the adjective "operational", and that this is the subject can only be learned from the description of the manifestations of the risks that are considered. To a greater extent than on manifestations of risk, and therefore, indirectly, its types, such works are focused on clarifying the process of managing the basic problem area (in Pritchard – design), and only in the second step to add elements of risk management to the process.

3.3. Proposed perspective according to organisation theory

As a consequence of the defects in the Basel classification, we can also see the defects in the definition. The risk factors articulated suggest intentions, which in the light of the theories of organisation and management should be recognised as follows:

- certain internal and external events are possible which disrupt an organisation's activity, i.e. impair the operation of processes,
- processes are to a certain degree and extent susceptible to disruptive events,
- certain resources are critical for the maintenance of processes,
- an organisation may bear legal responsibility for the consequences of disrupted processes or resources.

It should also be stressed that as a result of the classification of the Basel Committee category of events, features of these resources may lie at the foundation of disruptive events. This applies especially to the specificity of human resources, and the complexity of IT systems and the dependence of many processes on these resources and systems.

A new definition should take these elements into account, i.e. the importance of certain processes (maybe not all, but certainly the critical ones) with the recognition of the vulnerability of the resources needed to carry out these processes, either in the context of external and internal threats to effectively reduce or stop the execution of certain processes, or result in property damage and legal responsibility for such events and their effects. The proposition for a more precise definition (kept similar to the existing) reads:

> Operational risk is the risk of material and reputational loss and legal liability resulting from inadequate or failed processes and their essential resources (personnel, material, IT and financial), and the disruption emerging as a result of the impact of internal and external threats.

As a consequence of such a definition and in relation to the considerations of the Basel classification, there is an evident need to make a systematic classification of risk. The author's proposal is presented in tables[8] 3.1 and 3.2. The proposed classification criteria refer to three elements of risk manifestation:

- the character of the individual processes implemented in the organisation,
- the types of threats that may disrupt those processes,

[8] The classification given in Tables 3.1 and 3.2 is the author's major contribution to the science, in addition to establishing the BCM rules against the backdrop of the principles of operational risk management.

- vulnerability to threat: the organisation of processes and the different types of resources necessary for carrying out these processes[9].

The issue of the processes included in the classic division of basic, auxiliary and management processes [Dahlgaard, Kristensen, Kanji, 2004]. At the same time, processes in general are treated as a representation of the internal factors of an organisation, supplementing them with a category of external factors related to the organisation's impact on the business environment.

In this arrangement, the threats – as manifestations of risk – potentially act on the organisation as a whole (and are then recognised as factors acting from the outside, i.e. from the environment) or on specific categories of processes (primary, auxiliary, management).

With regard to the impact of the environment on the whole organisation and in relation to fundamental processes, taking account of threats and vulnerabilities, comprehensive risk types have been indicated. Of course, when considering the situation of a particular organisation, some of these risk types may not exist, either because of the trivial importance of the threat or because of immunity to it. For example, a software company running a data service centre (outsourcing service) cannot be exposed to the risk of power failure due to its having a spare source in the form of an electric generator driven by liquid fuel.

However, in relation to auxiliary processes and resources, it has been assumed that these processes rely on resource sharing by the organisational units conducting the basic processes. Similarly, it has been assumed that management processes are based on a specific value added to the resource which is the internal organisation of the company, and so to the organisational structure and the ordered relationships between units at different levels and their positions.

The issue of an organisation's vulnerability to risks in relation to auxiliary and and management processes referrs to the postulated attributes of the ideal system: effectiveness, productivity, rationality, safety, and repeatability.

The different types of operational risks identified in Table 3.1 are further characterised in Table 3.2 in the description system:

- the nature of the causes of a given type of risk,
- the mechanism by which it actualises,
- The type of effects that such a risk causes,
- typical examples of the effects.

The description is designed to be helpful in targeting research on different types of operational risk and practical identification of the areas and disciplines which can help to manage it.

[9] Detailed characteristics of the materialisation of risk in the form of process disruppion as interactions between threats and an organisation's vulnerabilities are discussed in Chapter 5

Table 3.1. The author's proposal for the classification of types of operational risk

		VULNERABILITY						
		Operational efficiency						
THREATS	**Environment**	Risk of natural disaster						
		Risk of terrorism						
		Risk of external functional interference in the work environment (e.g. lack of access to the premises)						
	Basic Processes	Risk of disrupting the physical environment (e.g. too high a temperature)						
		Risk of internal functional disturbance of the work environment (e.g. strike, accident)						
		Risk of technical disruption of the work environment (e.g. air conditioning failure)						
		Risk of IT disruption of the work environment (e.g. computer failure)						
	Auxiliary Processes	**Areas of risk materialisation (As an expression of security resources and organizing)**	**Postulates of the ideal organisation (as an expression of organisational goals)**					
				Effective	**Efficient (organisationally optimum)**	**Rational (cost optimal)**	**Safe**	**Repeatable**
			Personnel Resources	Risk of lack of competence	Risk of lack of reserve personnel	Risk of staff turnover	Risk of relativism of interpretation	Risk of routine (ossification)
							Risk of ill will	
			Material resources	Risk of lack of functionality	Risk of lack of material reserves		Risk of side effects	Risk of wear
			Financial resources	Risk of inappropriate spending	Risk of overspending		Risk of exhaustion of funds	
			Information Resources	Risk of lack of full content	Risk of lagging behind development		Risk of unavailability	Risk of distortion
	Management processes		**Organisation**	Risk of incident (failure)	Risk of a lack of organisational capacity		Risk primacy of security over effectiveness	Risk of absences

Table 3.2. Characteristics of types of operational risk

Causes	Materialisation mechanism	Effects	Examples
Risk of natural disasters			
Natural	Described by the natural sciences	From natural (changes in the environment), through social, to focused on individual entities or locations	• earthquake • flood • hurricane • extensive fire • torrential rain, hail, snow
Risk of terrorism			
Social and psychological	Described by the social sciences	From social to focused on individual entities or locations	• assault, kidnapping • blackmail
Risk of external functional interference in the work environment			
External to the organisation, and often unknown to the organisation	Without direct connection to the normal activities of the organisation, but cutting it off from external links	Non-destructive limitation of normal activities	• lack of access to the premises
Risk of internal functional disturbance of the work environment			
Negligence in relations and working conditions	Breaking of internal relations (between the units or stations) determining processes in the organisation	Non-destructive limiting the of the capability for full implementation of the normal functions of the organisation	• strike • employee accident
Risk of disrupting the physical environment			
Scarcity of safeguards against factors impacting on the working environment	Exceeding the tolerance limits	Limitation on normal operation for workers or equipment with special requirements	• Too high a temperature because of the weather • Too high a temperature due to technical failure
Risk of disrupting the technical environment			
Wear or hidden defect	Progressive deterioration of quality parameters or a sudden excess	Limitation on normal operation	• equipment failure
Risk of disrupting the IT environment			
Similarly as above, concerns specific cases of technical risk associated with IT systems			• computer failure

Causes	Materialisation mechanism	Effects	Examples
Risk of lack of competence			
Poor selection of employees for tasks or worker lags behind professional challenges	Unprofessional assessment of premises for action or decision-making	Misleading actions or decisions about the legal, physical, financial, or reputational effects	• unknowingly incorrect or hasty action by an employee
Risk of lack of reserve personnel			
Improper planning of tasks and resources	Gradual or sudden exhaustion of necessary personnel	Inability to fully perform tasks	• unexpected absence • inability to perform all tasks
Risk of staff turnover			
Inadequate working conditions, inadequate assessment of the situation on the labour market	Employees searching for another place of employment	Inability to ensure the quality, dimension or efficiency of work conducted	• unexpected resignation • changes in personnel more frequent than the period required to master the tasks in the workplace
Risk of relativism of interpretation			
Lack of clear communication, or lack of information	Actions initiated from position that is objectively relevant, but run in an inappropriate direction or manner	Activities inadequate to objective circumstances	• unknowingly incorrect or hasty execution of a command
Risk of employee ill-will			
Ethically wrong choice of appropriate workers for jobs	Utilisation of the jobs or insufficient protection / control over actions contrary to the interests of the employer	Loss of property or reputation in the employer's business	• deliberately incorrect activity by an employee • misappropriation of entrusted funds
Risk of routine (ossification)			
Long-term performance of the same tasks or activities	Gradual shaping of reflex action	Reflex action in a situation that requires a special procedure	• driver driving "by heart" in spite of changes in traffic rules
Risk of lack of functionality			
Boundaries of the functionality of the organisation	Inability to perform a new task, apparently similar to previous	Inability to carry out a task	• acceptance of an order which at some stage of execution cannot be continued

Causes	Materialisation mechanism	Effects	Examples
Risk of lack of material reserves			
Improper planning of tasks and resources	Lack of resources already detected during the execution of a task	Inability to carry out a task	• unexpected lack of components in production
Risk of side effects			
Insufficient knowledge of the context of the task	Activity causes additional and not necessarily immediately evident adverse effects	Material or reputational losses and liability for the losses of third parties	• unexpected deleterious effect of planned activities
Risk of wear			
Limited durability of individual resources	Consumption of resources leading to exceeding the tolerance limits	Inability to carry out a task	• loss of parameters in the manufacturing device
Risk of inappropriate spending			
Insufficient competence	Incorrect assessment of decision-making evidence	Losses as a result of wrong decisions	• misguided investment
Risk of overspending			
Insufficient competence	Incorrect assessment of decision-making evidence	Excessive level of expenditure	• error in trade negotiations
Risk of exhaustion of funds			
Improper planning of financial tasks and resources	In the course of operation financial resources are depleted without being able to properly replenish them quickly	Loss of liquidity	• Inability to purchase
Risk of lack of full content			
Lack of competence or lack of access to appropriate sources of information	No information in the course of action taken requiring such information	Inability to carry out a task	• Incomplete design documentation
Risk of lagging behind development			
Lack of competence or deficiencies in the update of information	No information in the course of action taken requiring such information	Inability to carry out the task or performance under conditions of incomplete information	• Investment project in an area that has just been designated for other purposes

Causes	Materialisation mechanism	Effects	Examples
Risk of unavailability of information			
Lack of access to appropriate sources of information	No information in the course of action taken requiring such information	Inability to carry out the task or performance under conditions of incomplete information	• Unavailability of information from market competitors
Risk of distortion of information			
Lack of sufficient competence	Incorrect interpretation of information	Bad or limited-quality performance	• Economic Forecasts
Risk of incident (failure)			
Vulnerabilities in organising activities or resources of the organisation	Interaction between threats and proper operation with vulnerability	Inability to maintain current organisational operation	• Failure of the production line
Risk of a lack of organisational capacity			
Lack of sufficient competence in the field of organisation and management	Improper planning of tasks and resources	Inability or limited ability to carry out the task	• Disruption in a complex project
Risk primacy of security over effectiveness			
Excessive literalness in the interpretation of rules and best practice	More and more careful adherence to formal rules leading to limitation, and even paralysis of the action	Inefficient operation	• "Work to rule"
Risk of absences			
Improper organisation of activities (including inappropriate resources)	Activity is unstable, imprecisely organised, uses uncertain resources	Results do not achieve the expected quality parameters	• Defective product

4. The process of operational risk management

By analysing its operations, you can specify what an organisation does. "Operations are the activities which comprise all the activities directly related to the production of a product, which can be tangible goods or services" [Waters, 2001, p 20]. Operations are arranged in the processes. A process in terms of a logical organisation sequence of consecutive steps, or parallel, which leads to meet the customer's expectations, both internally and externally, by providing them with a product, service, consistent with its documentation requirements.

Operational management focuses on the manner in which an operation is performed. "It is the function of management responsible for all activities directly relating to the manufacture of a product: for the collection of the various initial components and processing them into the planned final products" [Waters, 2002, p 32].

It should be emphasised that the common notion – operative management – is something else. This refers to the term "operative", which means vigorous, effective and efficient action. Operative management refers to ongoing activity and therefore includes not only operationally transforming the resources into products/services, but also the development of other aspects of the organisation.

4.1. Risk management organisation

Operational risk management is directly related to the functioning of the organisation and the processes comprising its activities. Manifestations of this risk are an ongoing subject in management, regardless of the awareness of this on the part of executives. In the case of an organisation's established processes, it may even be found that managing operational risk is one of the main tasks of management, as the management in this case is mostly dealing with exceptions/deviations from the planned actions or incidents. Accordingly, operational risk management, more than in the case of other risk groups, is integrated with the management mechanism. Therefore a serious dilemma arises in respect of this – whether and how much operational risk management should be excluded from general management and made an autonomous process. This has been the subject of numerous studies by

the author. In particular, analysis of the practices of the financial sector (in terms of operational risk serving as a close analogy to other economic sectors), where there is a presrciption requiring that dedicated risk management be separated in a framework for determining capital adequacy in terms of risk, this indicates that operational risk management is carried out in two streams. The first – general – is difficult to separate from the observational aspect of ongoing management. Within its framework, issues and problems are solved that are the consequences of materialising risks. Management activities are routine reactions, analyses of the situation, evaluations and decisions. However, they are more effective, the more powerful is the second stream of operational risk management. It is autonomous in character and associated only with this type of risk, based on the task structures (time dedicated), it operates intervally (periodic work). The first stream compared to the second relies more on intuitive and situational actions. The second is focused on in-depth analysis and the development of solutions precisely relating to the risk. It is most beneficial when the first stream derives from the second. Further considerations apply to the second trend.

Risk management covers:

- the establishment of a dedicated task force or organisational structure with specific tasks and competencies,
- definition of the applicable rules for carrying out risk issues, based on the general recommendations (e.g. industry-wide like Basel II) or internal experiences of a given issue,
- a set of methods and measures to control the impact of risk factors on the functioning of the organisation and used for this purpose in making rational decisions.

In terms of the institutionalisation of the risk management function, it is important to define the role of employees and management. All levels of the organisation, i.e. employees, managers, directors, management board and supervisory board, should have responsibilities associated with the risk management system. In this way, the base may be prepared to allow the active participation of the organisation's employers and management in operational risk reduction. These conditions are shown in Figure 4.1.

The division of responsibilities between the different levels, organisational units and employees is as follows. The Supervisory Board and the Management Board should:

- know about the most important types of risk to which the organisation is exposed,
- know the potential consequences of deviations from the assumed indicators for the value of the company,
- ensure an adequate level of awareness within the organisation,
- know the extent to which the organisation is prepared for crisis
- be aware of the importance of trust in the pressure groups for the organisation,

- comply with the principles of communicating with the environment,
- receive information about whether the risk management process is functioning properly,
- present a clear risk management strategy, including the concept of operations and the division of duties.

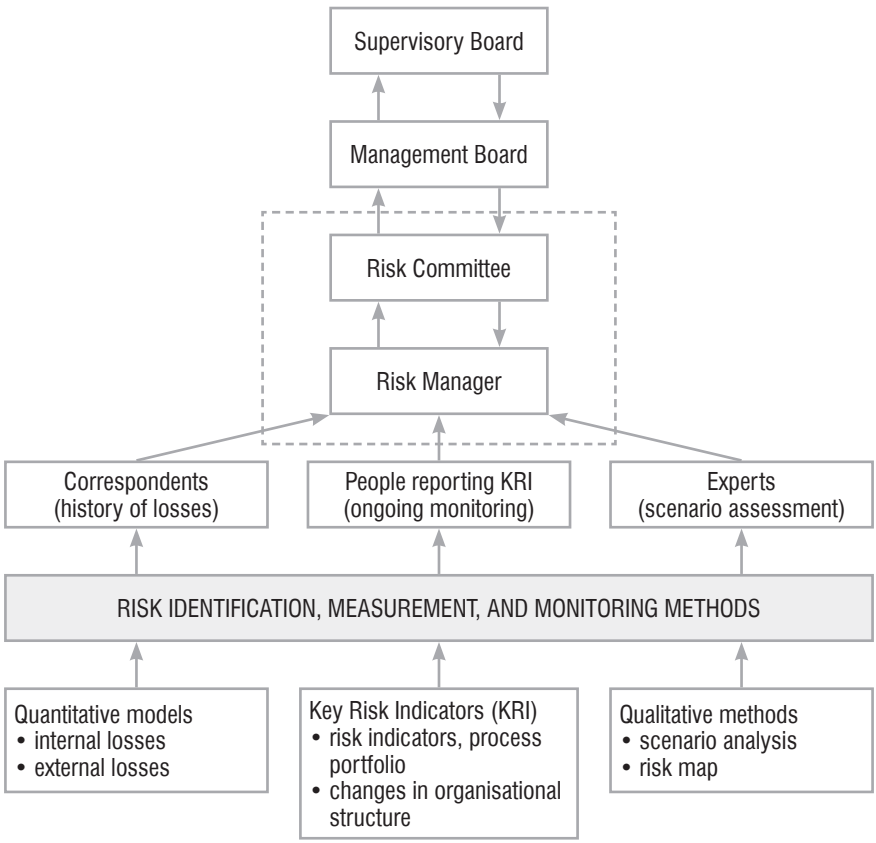

Figure 4.1. The risk management system

Organisational units should:

- be aware of the threaets that exist in the business, and for which they are responsible, and their potential effects on other areas of the business, as well as the potential consequences events in other areas may have for their own activities;
- have indicators that will enable constant examination of the key economic and financial results and progress towards the goals, and to identify issues that require intervention;

- to have systems that indicate deviations from the budget assumptions or forecasts often enough to be able to take appropriate action,
- systematically and promptly inform top management of any new risks or improper functioning of the measures applied.

Employees should:

- understand their responsibility for a given risk type,
- know how they can contribute to the continuous improvement of the risk management process,
- understand that risk management is primarily awareness of the threats,
- systematically and promptly inform top management of any new risks or improper functioning of the measures applied.

The condition for the effectiveness of risk management is the use of a process approach (Fig. 4.2) and its full integration with all management processes and support of risk analysis from interdisciplinary knowledge of its causes, mechanisms and consequences [Conrow, 2000]. Additional verification of the correctness and effectiveness of the identification of risk factors, determining the level of risk and neutralising it, and finally its management, is provided by an interim audit, in principle compatible with any conventional rules of improving the organisation's internal control, and within the risk management model constituting a form of control feedback which enables a spiral process of improvement.

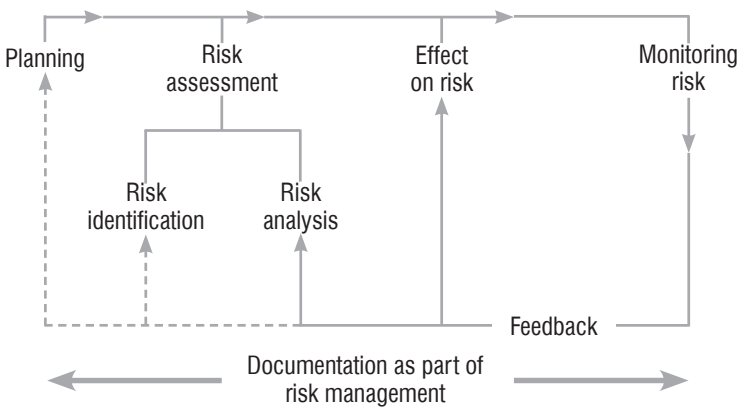

Figure 4.2. A functional model of risk management

Source: [Conrow, 2000].

In practice, individual risk management activities are interwoven, and it should be remembered that this process is not separate from other management processes, but strongly integrated with them. With this in mind, risk management can be divided into stages and steps, which is also needed to ensure the functioning of the risk management process on a spiral of improvement [Loader, 2006, pp. 123-125].

Stage I – Risk assessment:

- risk identification,
- risk analysis,
- estimation of risk,
- prioritisation of risks.

Stage II – Active approach to risk (also referred to as affecting risk or manipulation of risk):

- elimination of (avoiding) risk
- risk reduction (including prevention),
- risk segmentation,
- risk division,
- risk transfer,
- risk financing,
- (in some cases) risk toleration.

Stage III – Risk Monitoring

- social approach focused on threats to humans,
- economic approach focused on the efficiency of the organisation,
- systematic inspection,
- risk control.

4.2. Risk identification, analysis, and assessment

In risk management, the most important aspect is accurate and complete identification of the types of risks faced by the organisation and its activities. Then comes careful analysis, and estimation. The desired situation is to have statistics with adequate credibility, describing the distribution of the occurrence of disruptive phenomena. In a situation where there are no such statistics, there remains estimation of the risk factors. It should be emphasised here that a body with high organisational culture, regardless of the requirements of supervisors, from its own beliefs collects and analyses statistical data concerning the organisation of work and its conditions of operation. This is also a specific element of the organisation's knowledge management.

In broad terms, the analysis of operational risk is initiated from a strategic assessment of the susceptibility of the most significant business activities, known as critical, to threats. This assessment is referred to as the BIA (Business Impact Analysis) [Charters, 2011], and begins by identifying key processes and their particularly critical elements and factors that may adversely affect that criticality. For each critical business process, a BIA provides mainly the following information:

- the amount of potential financial losses presented cumulatively over a time interval (it is assumed that the organisation should know the estimated

value, determined mainly on the basis of past experience, the losses incurred on the basis of lost benefits for every hour of downtime, plus additionally a divided threshold for periods of abrupt increase in these losses);

- the level of potential losses uncountable over a uniform scale for all processes (it is assumed that the organisation should strive to evaluate the branding losses and estimate their value on the basis of lost profits in the long term);
- the maximum allowable duration of interruption of a process – in other words, the time after which the process must be restarted for the established acceptable level of quality (it is assumed that the organisation's decision-makers, through study, should specify this requirement in relation to the then draft business continuity solutions, keeping in mind that this also implies a certain level of spending on these solutions);
- the minimum functional level of process restoration – in other words, an acceptable established level of quality to resume the process after a failure (this is not synonymous with the restoration of the original level of quality);
- the time after which the process must be restarted at its established acceptable level (it is assumed in this case that the organisation's decision-makers, through study, should specify this requirement in relation to the then draft business continuity solutions, keeping in mind that this also implies a certain level of spending on these solutions);
- the specification of the resources necessary to maintain the efficiency of critical processes, called the Minimum Acceptable Configuration.

In the context where the organisation's management approves the findings of the BIA, we can proceed to the analysis of risk much more effectively oriented towards business areas already identified as crucial for the organisation. This analysis is based primarily on the identification of risk types, and more and more there is talk of the identification of the types of threats, assuming that a threat is a manifestation of a risk specific to certain conditions of the organsation's activity. The purpose of this identification is to use a number of methods and techniques, such as checklists, interaction diagrams, process and systems mapping, and records of incidents and events, expert assessments, and creative and scenario methods.

Risk analysis should lead to the most precise possible definition of the nature of the identified risk types, and an indication of the types of threats that are the expression of risks in the specific terms of the organisation. In particular, the description of the nature of the threat/risk should refer to their causes (sources), the mechanism of materialisation (including the organisation's vulnerability) and the effects (Figure 2.1 and the accompanying description).

At this point it is worth looking back to the point at which section 2.4. finished. The point is that the vast majority of types of operational risk (see Tab. 3.1 and 3.2) are non-financial in nature.In such cases, the methods of analysis, and in particular the methods of risk measurement involving financial estimates, are of limited use. Above all, they do not serve as a direct measurement of risk, and only the determination of capital adequacy as the level of funding that the organisation should

have to bear the financial consequences of the actualisation of risks. Therefore, the methods that are suitable for analysing operational risk are mainly qualitative (descriptive and qualificative). This is because the nature of these risk types is multifaceted and each lead it to a common denominator, popularly speaking, that is, the search for one metric of assessment, and this is either impossible or leads to far-reaching simplification. This is an important argument for the use of qualitative methods, descriptive in the analytical phase and qualificative in the estimate phase. In this situation, consideration should be given to the value of those qualitative methods, which often are treated as being of "inferior quality" to quantitative methods. Recently there has been an effective argument indicating that these allegations are unfounded. The author of this work agrees with this view, relying on arguments related to the teleological interpretation of the methodological approach in the analysis of operational risk. The fact is that, of course, it is important to know the size of the corresponding financial reserves to meet the potential negative consequences of risk materialisation, but this is only of passive relevance. Active confrontation of the risk requires preparing solutions against its impact, on policies limiting its intensity, and on activities providing the ability to rapidly remove the effects of risk materialisation. For the preparation of such solutions and actions, first a description of the essential elements of the phenomena that make up the risk formation and risk materialisation is needed. Then, however, in relation to risk assessment, it is necessary to identify the individual eligibility rules for the threats, and the established ranges for qualifacative ratings: point (such as 0-1-2-3 or 1-3-5-9), percentage, or semantic (e.g. large-medium-small or destructive-non-destructive). This does not mean rejecting *a priori* quantitative assessment methods, such as statistical methods, which promote the recording of incidents (breaches of normal activity) and use of the data contained within this register from the moment the threshold set by the statistical reliability is crossed [*Help-desk*, 2007]. Qualificative ratings allow you to determine the kind of assumed risk approach that should be applied to the risk according to its assigned interval assessment. In practice, management usually provides sufficient reasons for the decision as to the selection of security solutions and corrective actions. Typical types of methods of analysis and qualitative evaluation are presented in Table 4.1. They all have the basic drawback of limited quantitative estimation; in practice, however, with regard to operational risks the benefits outweigh these drawbacks.

An example of the estimation method specially developed for operational risk is TSM-ORA (Total Security Management – Operational Risk Assessement)[10]. The first steps for analysis in this method are:

- defining the system boundaries within which the resources are to be found (it is assumed that the analysis does not necessarily apply to the entire organisation, but then you must indicate which organisational units and which processes are to be included),

[10] This method was developed in 2004 at the Technical University of Warsaw (with the leading participation of the author of this work) at the request of UNIDO as part of its project for support the management with material facilities in the Polish police force.

- describing the environment – both physical and legal and organisational – in which the system works (in particular, it examines how the level of efficiency of the processes is required and where the metrics of that efficiency come from),
- defining the assets to be indicated by the analysis process, which are the assets that determine the smooth running of processes (business continuity violations come directly from the unavailability of resources or their services for the process).

Table 4.1. Types of qualitative methods in risk analysis

Types of methods	Usefulness
Descriptive risk assessment	If there is no well-established practice of analysing risk, then using this method can make a systematic description and try to develop a basic opinion as to the seriousness of the risks/threats (e.g. large-medium-small).
Risk factor catalogue	If the type of risk/threat is well described as to its nature, it is possible to for the organisation to prepare a template identifying the individual characteristics of the risk /threat and assigning them an interval evaluation. The more these characteristics are examined, however, the harder it is to determine the total or resultant value of such an assessment.
Profile analysis	A risk profile of the organisation is prepared, which is a list of analysis sections (characteristics of the organisation), and an assessment of the degree of risk in relation to individual sections (features) is conducted.
Early warning systems	These examine the critical factors for a given risk/threat and determine the thresholds of vulnerability which can be regarded as warning signals, or examine the characteristic symptoms of the materialising threat.
Risk equalisation (mostly loss compensation)	The different types of risks/threats are studied in order to identify those that should be affected to reduce their level to the specified acceptable levels.
Risk assessment adapted from FMEA	Explores the causal relationships of the actualisation of risks/threats and identifies the key factor in the criticality applying the traditional use of this method in quality analysis.

This analysis comprises a determination of the objectives and functions of the system of action, which should ensure the availability of assets; then the determination of the processes performed by the system, and pursuing its objectives, and finally identifying the resources (including intangible assets) that make this possible. Assets should be assessed in terms of characterising their validity in the light of the objectives of the system. The values of the evaluation should be based on the cost of obtaining and maintaining the assets.

The next step is to identify threats. This analysis depends on determining which of them actually relate to the system being analysed and the probability with which they may occur. This probability may depend on the type and value of the assets of the system of action, subject to individual threats. The evaluation of

this susceptibility of such resources can be accomplished in two ways. The first is to develop a list of weaknesses in the system, i.e. its vulnerabilities that could be exploited by potential threats, and then an estimate of their ease of use. This technique is difficult to the extent that the weaknesses in the system of operation only usually come to light when disruption is experienced. A sufficiently reliable assessment is therefore possible in this case only on the basis of statistics of incidents which in practice have rarely taken place. The second method is to start from the identified threats and assess how vulnerable individual assets are to them. When it comes to interaction between threats and the system, as a result of a vulnerability, we are talking about disruption. The crown of the risk analysis process is to develop a map of the potential disruptions, which is formed by a combination of the analysis and evaluation of two factors: the probability with which a disruption may occur, and the impact it will have on the system of operation.

It is also interesting, and possible to use on the basis of analogy, to use risk analysis for technical systems, such as event tree analysis, fault tree analysis, and threat exploration and operational readiness studies.

4.3. Influencing and monitoring risk

Influencing the level of risk, aimed at limiting it, and consisting mainly of introducing security solutions must maintain business rationality. Therefore, except in cases of solutions strictly required by the law, we are looking for a compromise between expected losses, associated with the effects of the materialisation of the risk, and expenditure on security solutions. The remaining unprotected scope of risk is called residual.

Even residual risk justifies the development of business continuity plans. Furthermore, the unreliability of the introduced security solutions needs to be considered. This is the second significant reason to prepare business continuity plans.

For these reasons, the relationship between security solutions and the business continuity solutions supporting them is derived from the business assessment of the situation by the organisation's decision-makers. Additional rationality for such an assessment is based on the fact that a risk is also an opportunity and taking it provides competitive business opportunities.

The consequence of risk analysis is to conduct work on providing security and business continuity that can be achieved by looking for solutions that affect the manifestations of risk. These issues, which constitute Phase II of the risk management process [Loader, 2006], are discussed in Chapters 4 and 5.

Operational risk management is carried out by the adoption of various criteria for assessing the materialisation of its purpose – from minimising the risk of the assumed effect on activities to maximising the effect at a given level of risk. This is accompanied by planning/accounting of management activities, effect and monitoring of risk, both in the direct sense and by providing the resources necessary to

act on the risk. As part of the planning, all these activities should be budgeted, reported, evaluated and improved.

Managing them requires appropriate knowledge of all the aspects of the identified risks, such as: their causes, mechanisms, and symptoms of actualisation, the possible location of disruptions, their potential scale, observation techniques, etc. Due to the fact that operational risk is primarily concerned with the unavailability of resources, and these are of every possible kind, the monitoring of the individual elements of the description of risks, threats and potential disruptions is very extensive, requiring different methods and techniques relevant to the specific resources recognised as critical or the specifics of how they are used. As described in relation to the methods of measuring operational risk, there is also the issue of what is to be subject to monitoring, and this usually features some resource or characteristic way of using it. This feature is usually a physical or technical (material resources), psycho- or sociological or skill-based (personnel resources), technical and cognitivist (IT resources), organisational (how to use the resources), and very rarely economic and financial (financial resources). With regard to the principles of monitoring so prepared and corresponding to the resources, procedures are laid down for extraordinary notification of a risk actualisation based on the assumed signals/parameters: acceptability, early warning and emergency, and procedures for adherence to business continuity.

In addition to an organisation's operational risk management, what is important is not only the risk of a single critical event, but the overall risk map consisting of all possible critical events. This allows you to determine the overall risk, particularly the risk of probable events, the domino effect (risk accumulation) or particularly severe risk events. Therefore, risk monitoring should be carried out comprehensively and continually improved, which means that this is an issue typical of knowledge management. Management of risks is largely derived from the accumulation of knowledge in the sense of the ability to collect information, selecting that which is important, and drawing conclusions from it (signals) in order to take appropriate preventive and remedial action. This hides entire complexes of issues that are associated with separate sets of competencies (know-how), which in turn should be appropriately associated. This book has already mentioned as an example the flooding of the Oder – since the event in 1997 the monitoring system in that area has been expanded. It has been improved both in terms of information gathering techniques and methods of analysing them, but also in the efficiency of the services which should react by bringing aid.

In this broad context, it is difficult to give specific guidance as to methods of monitoring. They must be matched to a specific problem according to the rules and disciplines of a given scientific discipline and the specific occupations and characteristics of the economic sectors involved in it. However, it is worth showing a general model for building such a monitoring system based on knowledge and skills management.

There are several approaches to knowledge management, their authors and supporters attempt to create the belief that a rigorously uniform approach is possi-

ble to such management, indicating one of these approaches. In opposition to this, the author, on the basis of practical experience, is convinced of the possibility and the need for simultaneous use of several approaches, combined on the basis of the layers seen by analogy with the 7-layer OSI model of network services in ICT [ISO 7498-1]. This construction of an integrated knowledge management system allows relatively separably – i.e. in a coordinated manner but in different orders, at different times and by separate groups of people – solution of organisational, process, resource, or personnel policy issues. Building a layered integrated approach (Tab. 4.2) moves from the organisational layer to the layer of intellect (the imaginary sequence of layers must be interpreted from the bottom of the table to the header). In each of them, a different classical approach to knowledge management should dominate.

Table 4.2. Layers and formal approaches in integrated knowledge management

Imagined layer	Prevailing approach
Intellectual layer (socialising knowledge, the relationships of people and the interpretation of content)	Behavioral approach
Content layer (areas of knowledge, from overt to covert knowledge)	Resource approach
Operating layer (knowledge disclosure, collecting, codifying, sharing and management)	Process approach
Organisational layer (strategy, structure, audit)	System approach

The organisational layer defines issues of organisational structure dedicated to knowledge management – so formally separate (dedicated organisational units) and task forces (working groups, task, ad hoc, temporary, implementation, etc. forces), or completely informal groups – and the roles (dependencies), the powers and responsibilities for purposes in this layer designated to knowledge management goals. Primarily, features of the system approach are used here, particularly the definition of principles: creation, codification and transfer of knowledge, which are used to determine the goals of knowledge management.

The operational layer determines the structure and the implementation of the knowledge management process. Primarily, characteristics of the process approach are used here, because this is the way to implement the principle of continuous improvement, and capture the element of the dynamics of phenomena characteristic of modern management. In addition, this approach assumes that knowledge management is measurable. This is achieved by the decomposition of a management

process into three related spirals of improvement (collection, codification and sharing), each more homogeneous in terms of the nature of action. Their task is to gather knowledge according to need, formulating knowledge in a user-friendly form, relevant from the organisational point of view and the operational use of knowledge already accumulated. The convention of spirals of improvement provides an ongoing compromise between needs and capabilities.

The content layer defines the resources of explicit knowledge and certain kinds of clues pointing to hidden knowledge. Here, we primarily use characteristics of the resource approach, which is considered to be the most traditional in knowledge management, but its main value is related to the fact that it corresponds directly to the tasks determined at the level of strategic management. In this approach, knowledge is considered to be the company's most important resource. Thus, it is seen as: key competencies, key skills, the ability to solve problems in teams, the ability to acquire knowledge from the environment, the implementation of new tools, experimentation, etc.

The intellect layer mainly uses the behavioral approach, which serves to socialise knowledge, i.e. operating, provoking, stimulating and supporting knowledge transfer, as pure knowledge is created in people's minds and develops in relationships between them.

Practical differences in knowledge management between different areas of knowledge show up with an intensity increasing with the order of the layers, especially at the level of the layer of intellect, which in some areas of knowledge need not appear. At the level of the organisational layer, a joint task organisational structure of knowledge management is constructed across the enterprise and the relationships in force within it. At the process level a mechanism is built of three spirals of improvement. The level of content in the case of certain areas of knowledge might in fact be the last. This applies for example to strictly technical knowledge in which the use of knowledge is often based on the use of professional knowledge in a very instantiated form. The intellect layer takes on importance, where operational activities are naturally variable, difficult to standardise, based on the mechanisms of accumulation of individual experience/skill that requires difficult synthesis, also difficult to describe in general, and even more difficult to codify.

5. Ensuring security in the management of operational risk

Security. This term, like risk, is not unambiguous. In the context of risk management, security is a particular social and subjective state, limited to a single organisation or sector of related organisations. It is a social good in terms of human needs, human values and human rights. From a societal perspective, proper to crisis management[11], it is seen primarily as a value.

According to Maslow's classic study [1954], a sense of security is the second basic human need. Therefore, it is true that "the objective of crisis management is not only the fastest return to normal. The essence of this type of management is to force the organisation to be aware of its moral and social responsibility to internal and external stakeholders, to society, and even to the world" [Mitroff, Pearson, 1993].

Ensuring security is the prevention of threats, as it comprises solutions, whose primary goal is to prevent critical situations by perceiving threat factors, monitoring characteristic and typical symptoms of their activation, and preventing their interaction with the organisation's system of action and its environment. If these measures fail and there is a disruption of organisational activity, it comes time for planned and organised remedial activity, which should provide an acceptable ability to maintain business continuity.

5.1. Security in terms of resources

In the practice of operational risk management, a significant influence is maintained by the strong association of this risk with the organisation's resources. Their deficiency, too little availability or poor quality are, in practice, organisational activity perceived as a threat, whereas the certainty of these resources at an appropriate

[11] It should be noted that in this work security is referred to as a risk as seen from the perspective of a single organisation. There is, in parallel, perception of risk and security from a social perspective, which is defined by the concept of crisis management.

level and of an appropriate quality is seen as a sign of security. The intuitive perception is that security is associated with a type of resource, and this is often reflected within the organisation – operational risk management is divided into two categories, namely classical and modern areas of ancillary management in the organisation. The first category comprises: physical and technical protection and personnel security. These issues have long been studied by the organisation theory. For these areas it is fully justified to speak of recommended best practices. With this, the perspective on physical and technical security is marked by specifics of the industry in which a given entity operates, while personnel security, as the effect of a personnel policy, is a universal issue, similar in any organisation, and, therefore, uniquely supported theoretically and by an equally rich literature. The second category comprises: information and IT system security, and ensuring business continuity. In this case, due to the new issues, there are different views at the question, and consequently different concepts of threat analysis and search for solutions.

It is worth noting that, with the establishment of the principles of systematic management of operational risk, equally established are the terms "resource security management", "operational security management", and over the full scope "total security management" (TSM).

Ensuring security implies solutions whose primary goal is to prevent situations by perceiving threat factors, monitoring characteristic and typical symptoms of their actualisation, and preventing their interaction with the organisation's system of action and its environment. If these measures fail and there is a disruption of organisational activity, the time comes for planned and organised remedial activity, which should provide acceptable business continuity.

Influencing operational risks, i.e. the organisation's responsiveness to an identified risk, may rely on affecting its causes, its materialisation mechanism, or its effects. Such action takes place in the context of the essence of the risk itself and the capability to act on it, and in the context of the organisation's ability to undertake such an act, whether this be in terms of disposal of the relevant measures/tools, or the appropriate skills. Such a situation is generally positively dynamic, i.e. achieving better and better cognition of the risk and the practice of impacting on it by an organisation's experience, which enhances the effectiveness of risk mitigation. Of course, this applies only to the types of risks with sources within the reach of the organisation's impact, and with an intensity and scale of impact commensurate with the organisation's capacity to respond.

The impact on critical events as manifestations of risk may relate to the causes of these events (prevention as *ex-ante* procedures) or to their effects (*ex-post* therapy). Contrary to appearances, this does not assume an automatic superiority of preventive over corrective action. The evaluation and selection of actions are made based on economic criteria – sometimes the rational approach to a risk is to repair its effects, and not to prevent them. The first type of interaction is defined as the provision of operational security, the second of providing business continuity. The impacts of both types are based on risk analysis, its causes and consequences, but also on an analysis of the essence of the organisation's activities, associated with

a given manifestation of risk. Risk appears via phenomena of a specific character, whose effect on an organisation is possible only when such a phenomenon strikes at a vulnerability of the organisation relating to one or more of the processes it has implemented, or in the sense of the organisational shortcomings of such a process, or weakness in the selection of resources used by the process. In practice, every critical event (the materialisation of the risk) is an infringement of a resource (or loss of control over a resource) conditioning the implementation of the process. Risk analysis therefore depends on the identification and assessment:

- of processes that determine the performance of an organisation's tasks,
- of the set of disruptive phenomena, and the probabilities of their occurrence,
- of the vulnerability of resources, measured in terms of the potential impact of a disruptive phenomenon on the activities of the organisation.

The practical influence on operational risk and ensuring security in terms of TSM depends on the design and implementation of solutions relevant to the basic themes presented in Table 5.1.

Table 5.1. Themes affecting operational risk in integrated management for securing the security of an organisation

Total Security Management (TSM)			
Business continuity management	Information security management	Physical and technical security management	Personnel security management
1) Which processes are we protecting? 2) What disruptions do we anticipate?	1) What information do we protect? 2) Against what are we protecting it?	1) What sites do we protect? 2) What are we concerned about?	1) What kind of people do we need? 2) What do we require of them?
3) How do we protect resources and processes?			
For example, DRII, TSM/BCP methodology	For example, TISM methodology	Industry best practices	Industry best practices

Ensuring the security of the organisation, especially in terms of TSM, is recognised for particular types of resources. Therefore, we talk about personnel security, physical and technical security, financial security and of information and IT security. It is easy to see that the individual categories are closely related, and also partly overlap. And so we speak, for example, of personnel security, of personal data security, of the physical security of financials, etc.

Ensuring physical and technical security derives from the following key points:

- the need to circumscribe the precise location of the boundaries of the organisation and the zones of execution of various functions and services to clients, and by employees of the organisation and for their benefit;
- the need to imagine and define potential threats and possible scenarios of their materialisation as disruption of the organisation's normal operation;

- the need to organise processes for performing the organisation's functions, providing physical security and matching and applying security solutions, including technical.

The use of best practice within this subject depends on developing:

- a division (classification) of protection zones,
- rules for the selection of security solutions,
- rules of security for each zone,
- rules to authorise access
- rules to monitor protection,
- principles of selection and verification of security personnel.

However, ensuring personnel security derives from the following key points:

- the need to select and hire employees with a high level of morale and responsibility (the "rule of righteousness");
- the requirement of adequacy of employee professional skills to the tasks performed and the potential ability to adapt to changing requirements, which may be derived from the entity's organisational and business development or the competitive development of the market (the "rule of expertise");
- the need both for personnel selection and organisation of work, which from the two parties cocreates the atmosphere and conditions for the identification of the professional success of an employee with the success of the employer (the "rule of loyalty").

The use of best practice within this subject depends on developing:

- a Code of Ethics for employees,
- principles of selection and verification of personnel,
- arrangements made for joining the organisation and departing from it,
- rules for determining individual and team roles and workstation design,
- principles of delegation,
- principles of remuneration and motivation,
- principles of personnel review,
- rules for determining individual career paths,
- principles of promotion,
- principles of systematic employee training,
- rules for protecting the confidentiality of the company, customers, etc.

In turn, ensuring information security derives from the following key points:

- ensuring that information is made available only to authorised persons (the "rule of confidentiality");
- ensuring the complete accuracy and completeness of information and the methods for processing it (the "rule of integrity");
- ensuring that authorised persons have access to information and associated assets only when it is needed (the "rule of availability").

Three levels of substantive information security management have been defined:

- information security policy – definition of security requirements at the level of the entire organisation, and for all groups of information and all the systems and solutions for the processing of that information (including storing and transporting);
- information group – detailing safety requirements for groups of information, isolated primarily as an autonomous class of information for specific issues processed in a specific functionality (such as financial information, personnel information, customer information, etc.), but also sometimes covered by separate general legal provisions, for example, classified information, information on personal data;
- a processing system – meeting the safety requirements by traditional systems, but mostly IT, which process certain groups of information for certain categories of users.

Regarding the strictly IT solutions, it is necessary to ensure the protection of information in three basic criteria[12]:

- information security,
- security of service provision,
- authenticity and accountability of data and entities.

The first criterion consists of the following components:

- *confidentiality* – information is available only to those persons who are entitled to it;
- *integrity* – ensuring the accuracy and completeness of the information, and the methods and means of processing it;
- *availability* – ensuring that authorised users have access to information and associated resources whenever required.

The second criterion consists of the following components:

- *reliability of systems* – the system can be absolutely relied upon, it is user-friendly and resistant to random operator errors (*foolproof*);
- *integrity of systems* – the accuracy of the system and methods and ways of processing information it uses;
- *availability* – ensuring that authorised users have guaranteed access to the system and its resources.

The third criterion consists of the following components:

- *data indisputable* – the data stored in the system and made available through it are certain, and can be relied upon;

[12] Standards: ISO 12207, ISO 13355, ISO 15408, ISO 27001-6 series and the ITIL principles of best practice.

- *indisputable subjects* – the accuracy of identification of the system user and confirmation of authorisation to use the information it contains;
- *settlement accounts of subjects* – ensuring that permitted (authorised) users are not able to deny the fact of their access to the system and the documented use of its resources.

In designing security solutions, the following general principles are applied relating to the specific types of resources which are used by the organisation in its activities, including primarily to the people as the main source of danger and threat object:

- *rule of authorised access* – each employee has been trained in the principles of safety and security and meets the criteria for admission to employment and information (business secrets);
- *rule of necessary privileges* – every employee has the right of access to work and information, limited to that which is necessary to perform the tasks entrusted to him;
- *rule of necessary knowledge* – every employee knows about the work that is accessible to him, at least as far as it is necessary for the performance of his duties;
- *rule of necessary services* – the organisation provides only those services required by the customer;
- *rule of security measures* – each security mechanism must be secured by another (similar), and in special cases an additional (third) independent security measure may be used;
- *rule of collective awareness* – all employees are aware of the need to protect the resources of the organisation and actively participate in this process;
- *rule of individual responsibility* – specific individuals bear responsibility for the security of the individual elements;
- *rule of necessary presence* – only authorised persons have the right to be in certain places;
- *rule of constant readiness* – the organisation is prepared for all threats; it is unacceptable to temporarily disable security mechanisms;
- *rule of weakest link* – the security level is determined by the weakest (least secure) element;
- *rule of completeness* – the security is only effective when used in a comprehensive approach, addressing all levels and units in the work process in the broad sense;
- *rule of evolution* – each organisation must constantly adapt its internal mechanisms to changing external conditions;
- *rule of suitability* – mechanisms used must be appropriate to the situation;
- *rule of acceptable balance* – remedial measures taken may not exceed the level of acceptance (especially recommended here are metrics of cost for inputs, outputs, and potential losses).

5.2. Business continuity as security

Business continuity, as a requirement of the organisation conceived as a system of action[13], is as a basic postulate analogous to the idea, with a long and broadly described tradition, of the requirement of reliability of technical systems as products of human creativity and action. Like reliability, defined as the degree of an object's ability to fulfil its requirements, it is crucial to assess the quality of the system or technical product, just as in the evaluation of the effectiveness and quality of the system of (the organisation's) activities, an important component of this evaluation is the ability of the organisation to maintain continuous operation. This type of expectation is primarily due to the attitude of the organisation to the client in the broader sense as a recipient of the effect of the action (product or service), and consists of an equally broadly understood organisational culture.

The risk experienced by an organisation is a direct consequence of the actions carried out, whose necessity and sense result from a conscious decision on the need for and direction of such action. The uncertainty that constantly surrounds you does not mean that you take risks. For this to happen, there must be a need for action. This is what is risky. Threats, as a form of manifestation of risk, are examined in terms of their potential impact on the organisation and are potential phenomena, toward which are geared: observation of evidence of disruptions and preventive actions carried out in order to prevent the interaction between the risk and the system of the organisation (its vulnerabilities). In practical terms, the risk lies in the fact that the decision taken and the action which is its consequence may face particular difficulties and obstacles relevant to the overall uncertainty in the area and environment of the organisation, and are perceived as a threat in anticipation. So the threat:

- is a form of actualisation of the risk,
- has an objectively measurable form and specific characteristics,
- has a source and a cause,
- is characterised by a specific mechanism of materialisation,
- impacts on the organisation's system of operation in a way that is subjectively measurable from the perspective of that organisation, and the degree of impact is dependent on the susceptibility of the organisation's system of operation and its environment.

In turn, these disruptions (materialisations of threats) are the actual object of activities referred to more broadly as business continuity policy. When a given threat affects the organisation's system of operation or its environment, and the system becomes vulnerable to these effects, we are dealing with disruption that:

- is due to the interaction between the risk and the system of operation or the environment of that system,

[13] System of operation – the set of elements that contribute to the occurrence of a specific effect (outcome) and between which there is an interaction organised with regard to the effect, even in situations with the disruptive influence of the environment.

- results in significant changes in the operation of the organisation,
- is not evaluated objectively, and subjectively is evaluated from the perspective of a given system of operation.

Therefore, the procedure for ensuring business continuity is similar to that which serves to protect against threats. They differ in the relation of time and nature of impact in terms of the threat, which are intended to be combatted by security and are to be reduced as a result of conduct ensuring business continuity. Both complement each other to ensure that the organisation has the expected resistance to various circumstances and violations of normal activity.

5.3. Management maturity assessment as a security provision

Meeting the aforementioned principles of information security is the basis for assessing the degree of maturity of the security management, a model of which was proposed by the IT auditors' association ISACA (see Figure 5.1).

Degree 0 No awareness	– no defined security requirements – security treated as an issue for individual users
Degree I Beginning	– awareness of a need – management considers it a problem for IT services (e.g. access rights, antivirus protection)
Degree II Intuitive	– attempts to create security – no uniform approach – results dependent on the engagment of interested parties
Degree III Defined	– defined principles (including a Security Policy) throughout the organisation – security procedures and maintained and communicated – no monitoring of application
Degree IV Managed	– uniform approach for all units and all solutions – business perspective applies – application monitoring mechanism in place
Degree V Optimised	– conscious risk management – compatibility between security strategy and business strategy – provision of security as a process (knowledge, improvement)

Figure 5.1. Maturity levels of information security management

Source: ISACA - Information Security Audit and Control Association

6. Ensuring business continuity in managing operational risk

Activity. For further arguments, it is important to emphasise the difference between activity and action. This is because of the focus on action understood as only part of the activity. It is assumed that each organisation runs activity, which consists of individual actions. The inspiration for this distinction is the process view, by which the organisation's activity takes the form of processes which implement subsequent operations. Activity corresponds to the generality of processes in the organisation [Waters, 2002]. Action, however, corresponds to the manipulation layer of activity (handling), corresponding to the transformations of resources within primary and secondary processes. We should also distinguish between the concept of "operational" activity, relating to the operation, and the concept of "operative" activity, being the current one.

Organisational dysfunctionality, which this book deals with, can be explained as follows. If there is a failure of a device, a system (e.g. IT), human error, accident in the workplace, then we are talking about the dysfunction of the action itself or its direct conditions, which is seen in terms of business continuity. If, however, the following consequences of an action occur: lack of profitability of the organisation, insufficient level of sales of its products, the lack of liquidity, then this is a dysfunction of the organisation that goes beyond performance and beyond the area of operational risk analysis, procedures for safe operation or providing business continuity, even though it may result in discontinuation of operation.

Action can be understood in narrow and broad senses. The narrower sense comes from the praxeological theory of organisation – according to this it is a deliberate, conscious and arbitrary human behaviour, and so it is bound directly to human activity. In the general theory of organisation, the role of the human factor is not, however, perceived as dominant. Thus, in a broader sense operation is the interaction occurring between two or more objects. Such an object is both the organisation itself and its individual components. From this perspective, action belongs to the ontological category "relationships", which means that the concept is not definable, but can only be explained by exemplification. Operation is characterised by:

- reality, as it is based on a specific (specified physically, temporally and spatially) transfer of matter, energy and information,
- productivity, as it brings certain effects in the form of changes (or preventing changes) within the interacting entities as parties to the relationship or in their environment,
- objectivity, as it uses natural (laws of nature) or social regularities,
- autonomy, as it is based on an ontic foundation (it refers to real things),
- independence, it does not necessarily have to co-exist with interacting entities,
- dependence on resources.

Action depends on the execution of an operation, but is limited to the layer of manipulating resources and relationships, whereas the previously discussed activity includes in addition elements of management, including the assessment (evaluation) of the results of actions.

Business continuity. Ensuring business continuity is a therapy against disruptions. Business continuity refers to those operations included among primary and secondary processes, which means it focuses down on action, and skips business issues that go beyond the level of manipulation of resources that make up the broader conceptual category – i.e. activity. It can be assumed that speaking of business continuity we are limiting ourselves to the purely organisational aspect of activity.

Business continuity should be considered as one of the postulates of the perfect ideal system [Nadler, 1967], which the organisation should be. Practical attempts to implement various postulates of perfection, of course, can be and usually are to some degree mutual contradictions, for example, a typical operation to ensure the continuous operation of an IT system is to increase the redundancy of communication, or introduce additional security measures, and this is incompatible with the demands of optimal organisation and optimal operating expenses. The postulate regarding the perfect continuous operations of the system, that is its business continuity, is in practice unattainable, but can be used for marking out rational operation of the system in the forecasting approach for design or reengineering [Hammer, Champy, 1993].

6.1. Model provision of business continuity

In general, business continuity is the ability of organisations to respond to disruptions in the conditions of normal operation, so that, where possible, it can quickly restore normal conditions, and where this is not possible, transfer to a scheduled substitute method to perform tasks. Business continuity can thus be seen both in the context of the organisation's tasks and the processes for the implementation of these tasks, as well as in the context of the factors that may disrupt with these processes through the organisation's vulnerability, representing its susceptibility to disruption.

Providing business continuity includes:

- a mechanism by which the organisation can respond to disruptions (partly based on homeostasis[14], and so spontaneous reaction by components of the organisation, and in part by systematically developing learned response capabilities),
- the process of developing the aforementioned mechanism of responsiveness to disruption (as a support process – within the meaning of process analysis – the core business of the organisation),
- on ongoing capacity management process ensuring business continuity and its continual improvement.

The mechanism to respond to disruptions includes:

- an organisational structure dedicated to the task of providing continuity, supplementing the overall organisational structure,
- formal regulations defining the relationships within the organisational structure that relate to providing continuity,
- perpetuated practice (possibly written) for proceeding in situations where a response is required to a fault that has been identified.

It should be particularly emphasised that the response to the disruption, in terms of ensuring business continuity, must be understood not only as a direct action against the disruptions, but also as a preventive activity, related to the analysis of the threats and vulnerabilities, and with an exploration of methods and solutions for preventing the occurrence of disruptions. In this sense, efforts towards business continuity and security are intertwined. From the point of view of business continuity, security solutions provide prevention against threats, while from the point of view of security solutions, business continuity provides additional security for when the nominal security solutions fail.

Therefore, whenever we are talking about:

- business continuity – it means the aspirational status of the organisation's resistance to disruption,
- ensuring business continuity – it means a string of planned actions, aiming to prevent disruption or removing the causes and consequences of the occurrence of disruption, or the introduction of alternative operating conditions until the effects of the disruption can be removed,
- managing provision of business continuity – this means the process of management, involving in particular setting objectives, planning and monitoring the development of solutions for ensuring continuity, as well as the evaluation of the actions and reasoning in relation to the potential and possible disruptions, in order to preserve the organisation's business continuity.

Provision of business continuity derives from the following premises:

[14] Homeostasis – the ability of a cybernetic system to self-regulate retaining a constant balance.

- the need to make assumptions about the priority functions and processes for which ensuring business continuity is of the utmost importance for the organisation;
- the need to estimate the potential losses that may arise as a result of disruptions and the necessary expenditures for preventive and remedial solutions;
- the need to predict the potential disruption to normal operation and the need to develop scenarios for alternative and remedial actions.

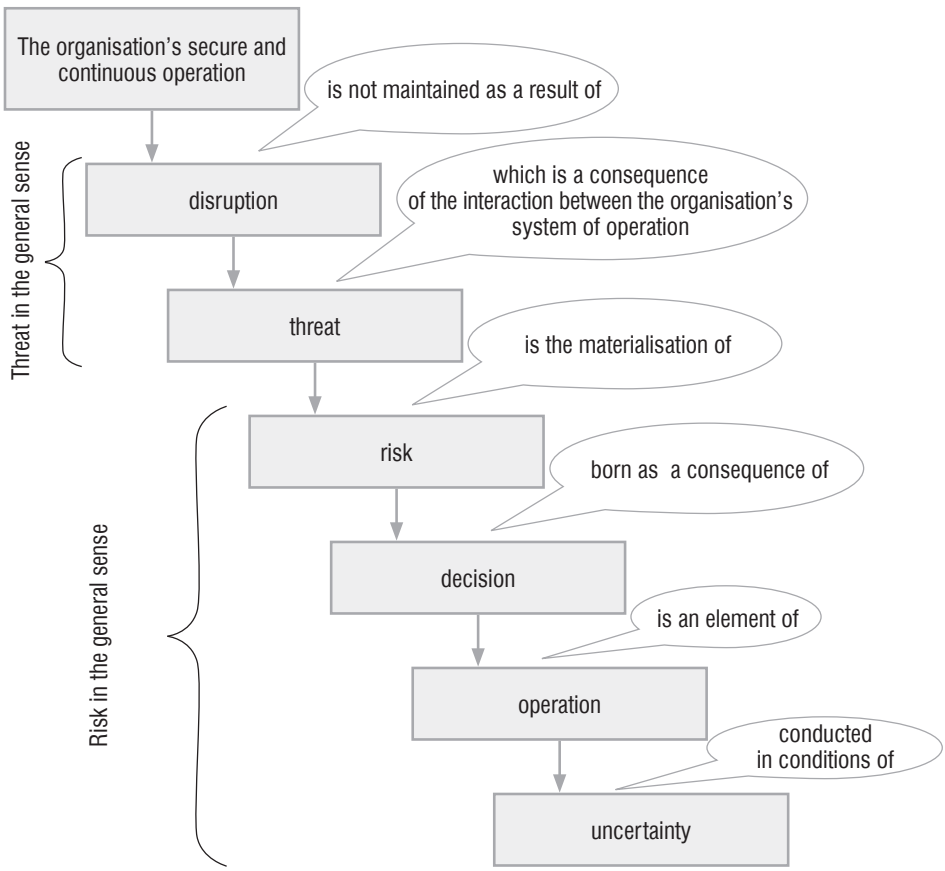

Figure 6.1. The logical mechanism for violating the proper operation of the organisation

Crucial elements of business continuity management provision are:

- an understanding of the risk facing the organisation, measured by its probability and its consequences, including identifying and prioritising critical business processes;
- an understanding of the impact that downtime can have on business activity (it is important to find a feasible solution for both smaller and major incidents that could threaten the existence of the organisation);

- formulating and describing the business continuity strategy consistent with business objectives and priorities;
- formulating and describing plans to ensure business continuity consistent with the adopted strategy;
- regular testing and updating of the approved plans and processes;
- ensuring that the management of the provision of business continuity is incorporated in organisational processes and structure;
- consideration of the purchase of appropriate insurance, which may constitute part of the business continuity process.

From the organisational perspective, the issues of managing the provision of business continuity coincide with quality management, security management, environmental management, financial management, and this type of business processes within the organisation. Consideration of the integration of the management of these issues, also in the sense of common organisational structures of management, is rational, and, indirectly, is also recommended by ISO 22301, ISO 22313, the ISO 900x series, the ISO 1400x series, the ISO 2700x series, and ISO 31000. It follows that:

- as part of the organisation's business, we must be aware of the possibility of disruptions that prevent the normal continuation of that business;
- regardless of the nature of the causes of these events, in formal or in business terms of the perceived obligation of due diligence in carrying out its tasks, the organisation should strive to continue its operations;
- endeavours to continue business during the occurrence of disruption should be based on a previously developed, consistently perfected and tested business continuity plan, sometimes called a contingency plan;
- ensuring business continuity includes the prediction of scenarios of potential disruption and separable design of:
- solutions to prevent the threats themselves,
- solutions for dealing as soon as possible with the consequences of disruptions,
- solutions for continuing limited operations in critical conditions;
- the approach to business continuity should be rational, that is, calculated to ensure a balance between the expected degree of certainty in maintaining business continuity and the costs of so maintaining it; it is therefore also necessary to assume the gradual surrender of successive elements of normal activity appropriate to the dimension of the critical situation identified (it does not always make sense, especially in economic terms, to make persistent efforts to maintain business continuity);
- the continuity plan should be flexible enough to allow adaptation to disruptions deviating from the expectations underlying the original plan;
- it is necessary to define the essence of the process of the organisation as the minimum activities that must be maintained with business continuity plans; the inability to continue such minimum activities is the basis for the

decision to abandon the use of the continuity plan and focus purely on removing the effects of disruption;

- in the preparation of the plan, business, legal and organisational aspects must be considered first and foremost, as these decide on the necessary scope of solutions;
- business analysis may concern the issue of the company's prestige, and certainly a kind of balance sheet of risk and the financial resources allocated to its limitation; it is reasonable to treat the continuity plan as a long-term project in which the goals will be achieved gradually by successive approximations (versions of the business continuity plan);
- legal analysis is especially important when formulating the assumptions of the continuity plan, as it allows to define the scope of the company's liability for various areas of its operations, identify sensitive points, and select non-technical forms of security;
- organisational analysis allows the designation of resources, in particular the appropriate staff to operate the continuity plan in critical conditions, providing them with adequate material, financial and information resources, and the scope of decision-making autonomy relevant to such a situation, in day-to-day conditions enable them to prepare for such a difficult role;
- none of the elements of this analysis, and also the design of technical solutions, is a closed stage; improvement of the continuity plan depends on constant renewal of the analysis and design of alternatives with respect to changes in the organisation's business, development of the continuity plan, and conclusions after the materialisation of an actual disruption.

Systematic procedure for disruptions is to determine:

- Which disruptions (threats in interaction with the system of operation) are subject to remediation, i.e. are covered by the preventive arrangements or procedures to ensure continuity;
- which technical infrastructure facilities are protected against threats,
- which business processes are protected against threats,
- which information flows are protected from threats,
- who is responsible for restoring business continuity in the event of disruption.

Managing the organisation's activity in accordance with the ISO 2700x and ISO22301 standards, you must create solutions that effectively preserve continuity. Such solutions may constitute the ability to start up a mechanism against the disturbance in order to restore the organisation's state before the emergence of the disruption (homeostasis). The effectiveness of solutions to anticipate disruption and their relevance to actual events should be placed above the minimum threshold of acceptance by decision-makers, who usually carry out the assessment based on two criteria:

- the prestige of the organisation and its degree of challenge as a result of the suspension or restriction of activities,

- the relationship between cost of security solutions and the cost of potential losses and restoration of the actions harmed by the disruption.

A rationally conceived homeostasis system leads to a conscious temporary reduction of the quality of action to a level previously set in the light of such determinants as:

- the loss of a dissatisfied or injured client,
- benchmarking against competitors and best market practices,
- robust standards of cooperation with partners and customers – SLA[15].

Reducing the operational quality should not last longer than the time needed to eliminate the causes and effects of the disruption, and the sometimes the former can resolve spontaneously, if such is the nature of the disruption.

The perception of disruption as a violation of business continuity is based on two essential factors in assessing their significance:

- the likelihood or incidence of disruption,
- the impact (malicious or not) of disruption on business continuity.

The assessment criteria are not measures, since they correspond to the nature of the phenomenon of each disruption individually. Assessment should be individual and made from the point of view of a given organisation.

A model process for ensuring business continuity consists of actions in three areas of design, leading to the formation of:

- an organisational structure established to ensure business continuity (or, more broadly risk, security and continuity),
- a spiral mechanism of organising activities to achieve the planning purpose,
- forms of consolidation of knowledge on the problem and solutions.

The spiral organising cycle, viewed wholly classically as the Deming cycle (PDCA), is to analyse the factors critical to designing solutions and their gradual improvement. The analysis includes:

- identification of business processes in order to identify their most important elements,
- risk identification leading to the identification of threats and ways in which they may manifest,
- identifying vulnerabilities as critical resources or features of their situation, where the organisation is particularly strongly exposed to danger.

This analysis is used to specify the possible disruptions, as well to assess their significance. From this moment begins the planning phase for scenarios as remedial solutions (in the sense of the procedural concept) and as documentation of a solution. Planning includes typical activities in the organisational microcycle: idea, execution,

[15] SLA – Service Level Agreement – a realistic and precise determination by the parties of the parameters of the services they provide, including acceptable levels of unavailability of these services, as not altering the terms of, for example, a service agreement. See [Hiles, 1993].

monitoring, use (often only as a test). The resulting scenario should be systematically improved in the context of practical experience (used for critical events) and the evolution of knowledge about the problem (periodic inspections using the line and staff method).

Consolidation of knowledge takes place in the direct organisational context, which includes training activities, tests and staff meetings inspired by the Crisis Committee and individual organisational units, and in the context of integrated documentation. Of great importance for the efficient collection and consolidation of knowledge (also in the sense of independence from absenteeism and turnover of staff involved in work on business continuity) is the introduction of comprehensive principles of documentation and its internal editing. This documentation is for use in responding to the occurrence of a critical situation, when there is often no time to think about interpretation of the notes. Knowledge consolidation is in fact the act of perpetuating the experience and its ensuing appropriate working practices. The basic intention is to prepare a long-term programme of building capacity to maintain continuous operation together with the estimated costs of such capacity in relation to the estimated potential consequences (losses as a result of) disruptions.

In view of the finding that only two factors determine the assessment of disruption (the size of its impact and its incidence), in this case their superposition leads to the identification of four general approaches to threats response (Figure 6.2). The model approach to threat/disruption response can take place in four ways, known as approaches to response. The assignment of individual cases of threats to individual methods of model response is not only individual and subjective, but also temporary. It is advisable to periodically, as frequent as possible verify such an assessment, taking into account the development of the organisation and its system of action, and the increase in knowledge of the impact of specific threats and the likelihood of their occurrence in the form of disruptions. The allocation to each category should take into account economic and prestige criteria. The evaluation metrics are determined by the semantic differential method. Addressing the response to threats (and consequently dealing with disruptions) is a synthetic view of organisational approaches to the problem. It is based on the adoption of the four general approaches to threats and disruptions, and on determining the way (method, rules, responsibility) to develop specific solutions, edited in the form of policies to deal with disruptions. It also clarifies the organisational structure, which is entrusted with the administration of this problem.

Toleration means accepting temporary inconveniences. Monitoring means that the knowledge of the disruption is sufficient to trigger the compensation mechanism on the basis of organisational homeostasis. Prevention means investment and technical measures to prevent the negative effects of disruption. Business continuity planning is a set of scenarios for threats expected to materialise and the activities planned for such events.

The approach of tolerating disruption refers to proceeding with disruptions which are external to the organisation, and only secondarily affect it, especially non-invasive, and chiefly non-destructive. An example: a transportation company

which deals with the press distribution – if there is a disruption involving the occurrence of intense fog, the natural solution is to wait until the intensity of the fog reduces, and the subsequent distribution of the newspapers. The organisation's "Tolerance Policy" (rules of conduct) should define the basic rules for accepting the ensuing disruption, examining the conditions for its persistence, confirmation of its end, and return to routine functioning. The policy document should be accompanied by procedures detailing the necessary activities for organisational units in the case of disruptions which qualify as relevant to this policy. Examples of rules – despite the fact that the organisation's reaction to disruption may in extreme cases rely on the suspension of fulfilling its statutory functions, it may be appropriate to inform trading partners or the general public of this, directing employees to do remedial work which are intractable to the disruption, starting off solutions tracking the intensity of the disruption. In contrast, when the problem is resolved, it should be verified that it is possible to restart suspended operations/functions.

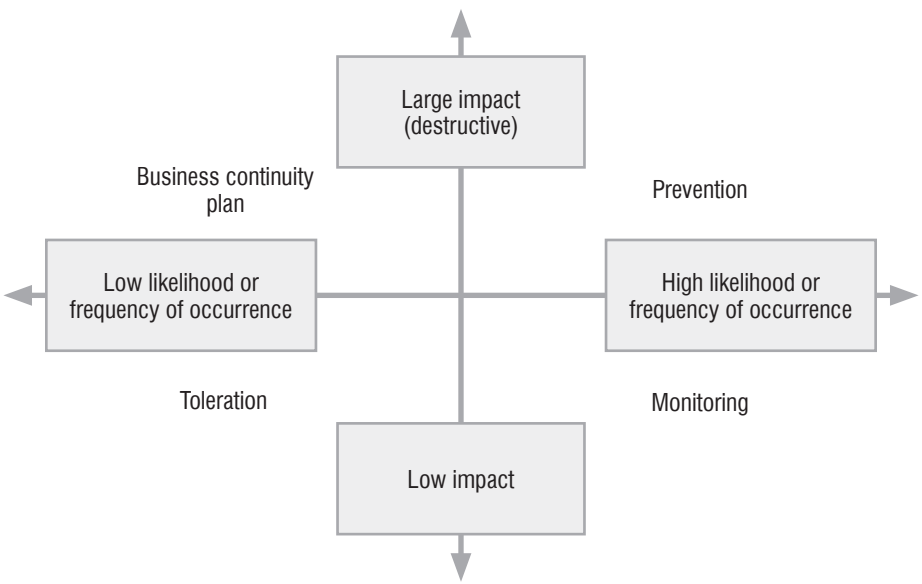

Figure 6.2. Model procedure for threats

The monitoring approach relates to the conduct with disruptions that are trivial in nature, although frequent (by which we must assume an incidentally greater impact due to the accumulation of events in a short time), but clearly non-destructive. This approach leads to the obligation to follow detailed solutions for organisational moves and even meticulous internal regulation of internal reaction to all typical disruptions. The essence is a negligible or zero increase in cost due to response solutions, which are mainly of an organisational nature. An example: employee sickness absence – providing an adequate response to this disruption requires the introduction, at least in relation to sensitive jobs, of an obligation to notify the employer as soon as possible and the development of principles for

organising replacements. The "Monitoring Policy" (code of conduct) adopted in organisations should define the basic rules for the organisation's response to disruptions, where the awareness of their existence in conjunction with the existing procedures of behaviour should be adequate to start up the the organisation's disruption compensation mechanisms. The policy document should be accompanied by procedures detailing the necessary activities for organisational units in the case of disruptions which qualify as relevant to this policy.

The prevention approach refers to the handling of significant disruptions, which are destructive and potentially occur frequently. The natural consequences of this prevention approach are investment and risk mitigation solutions. The "Prevention Policy" (rules of conduct) adopted in organisations should specify plans for the organisation of preventive measures, which in relation to particular essential elements of the organisation, especially the vulnerable elements of the technical infrastructure, to overcome the destructive effects of the disruption. Typical activities undertaken for this purpose are: the creation of backup and redundant solutions which are multiplied compared to average needs. The policy document should be accompanied by analyses precisely defining the degree and extent of sensitivity of existing solutions, plans for risk mitigation solutions, procedures/instructions detailing the organisation and operation of ongoing teams, and specialist teams to combat specific threats (fire, hacker attack, failure of computer systems). Examples – a backup computer centre, mirrored lines of communication carried along physically different paths and/or using different transmission media, including shifts for special intervention teams with the appropriate skills.

The planning approach known as business continuity planning refers to the handling of significant disruptions, destructive, but rare, which economically justify the decision to abandon the prevention approach and consciously take risks. An example: the Stock Exchange – world statistics say that the suspension of trading due to malfunctions in the computer system occurs no more often than once every few years, and lasts no longer than one day, so it is reasonable to rely on a scenario of replacement operation, which such a rarely occurring serious failure is dealt with. The "Business Continuity Planning Policy" (rules of conduct) adopted in organisations should specify plans for the actions necessary in the event of materialisation of risks in the form of a specific disruption. The plans should include organisational arrangements for the conduct of the policy itself, and scenarios for disruptions and their anticipated responses, in order to ensure the continuation of the organisation's primary business activity at least. In addition, the business continuity planning policy should define rules for responding *ad hoc* to events which, unfortunately, were not predicted in the scenarios (either in general or in terms of scale). The business continuity planning policy document should be accompanied by procedures/instructions detailing the organisation of the departments responsible for business continuity plans, the basic rules of communication in emergency conditions, rules for responding to common threats, scenarios covering predicted extensive disruption and response to them, and rules for including the experience in combatting the distortions which have taken place recently in the new version of contingency plans. In practice, these plans are divided into two classes. The first

class are DRP (disaster recovery plans), which relate to proceedings in the case of obvious technical failures (including IT failures) and the associated losses in the current availability of technical infrastructure. DRP define the procedure for repairing or replacing the component of the technical infrastructure. The second class are proper BCP (business continuity plans) that determine how, in the case of a serious disruption of business activities, to ensure the substitution conditions for those activities and how to organise a course to restore the *status quo ante*. BCPs use DRPs, which are carried out spontaneously in the case of technical failure or are implemented within the BCP plans in the event of serious disruption to business activity, if technical failure is part of that disruption.

6.2. Organising business continuity

The basic idea of assigning competences to departments responsible for the daily management of the preparation of policies to address the problems of disruption and the organisation of crisis management activated in the event of emergency is shown in Figure 6.3.

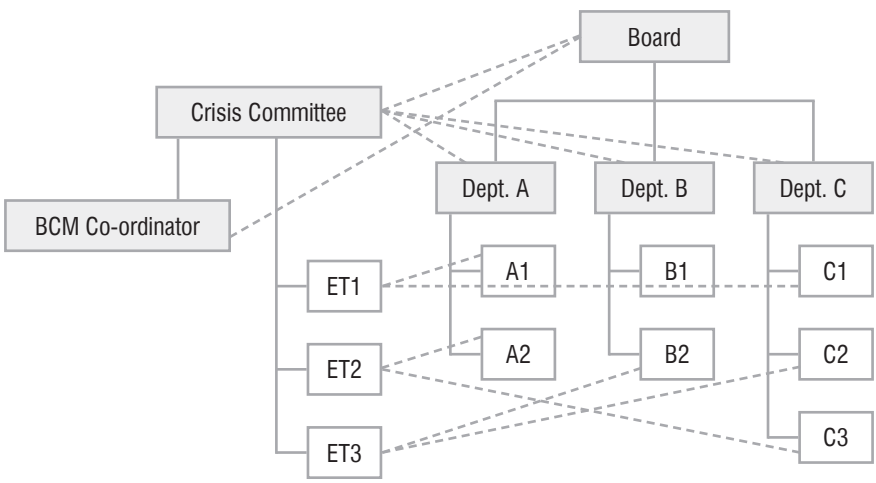

Figure 6.3. Business continuity management

The BCM Coordinator (also known as the Anti-Crisis Team) is a unit or operational staff role[16] permanently set in the organisation, established to coordinate the organisation's preparations for conscious and planned coping with disruption of business activity, including the development of documentation of emergency

[16] A unit is an organisational unit formally functioning in the organisational structure. Role means a complex of additional tasks assigned to a position or organisational unit, which broaden the scope of existing tasks for the position/unit.

scenarios, complete procedures regarding the implementation of routine or emergency business processes, and instructions. In between the meetings of the Crisis Committee, it coordinates the ongoing implementation of the tasks imposed by the Committee on the individual organisational units, is responsible for maintaining and distributing the current BCP documentation (plans, scenarios), and is responsible for organising training and testing. In the event of an emergency, it supports the actions Crisis Committee.

The Crisis Committee (also called the Crisis Staff) is the executing body, which meets periodically, regularly as part of the planned work on the development of capacity for effective business continuity, or *ad hoc* basis in cases of emergency. Its function is to order (and settle on the implementation of) individual organisational units' specific tasks in the framework of the gradual preparation of BCM solutions and BCP and DRP documentation, and the acquisition of skills for dealing with crisis situations. It should prepare itself to lead recovery from the crisis, if such occurs. It should have a strong authority from the organisation's management (preferably it will include one of the members of that management). In many, especially smaller, organisations, the role of the committee is played by the Board of Directors. After the occurrence of a serious disruption, the committee becomes the crisis headquarters, with major powers of everyday management, as the seriousness of the event may require the rapid adoption of non-standard actions associated with periodic changes in business practices, subordination and tasks of organisational units and employees, and fast-track decision-making and special investments.

Emergency Teams are the task forces needed in each field or selected unit, subordinated to the Crisis Committee, acting locally on a similar basis to the central committee. Also, if necessary, at the headquarters these task forces will operate in units of key importance in the event of a crisis in the administration or IT departments. It is also desirable to appoint Emergency Teams beforehand in the major organisational units, especially departments responsible for IT (offices, departments, centres) or local units of special importance. Appropriate training for the members of these Teams is also essential.

The basic assumptions of business continuity and their implementation in a given organisation are described in a special document "Business Continuity Policy", as described further. The starting point for this policy is to recognise the threats and critical components of the technical infrastructure of the organisation distinguished by analysis of the organisation's business processes and their position in the infrastructure plan. The imposition of these elements leads to the determination of maps of potential disruptions, which must be resolved before or after they occur. For this purpose implementation documents are created for business continuity policy and special procedures.

6.3. The analysis and planning procedure

Implementation of business continuity management policy faces the typical barriers for exceptional management (disruptions are a kind of exception in the routine course of work in the organisation). More important barriers are:

- lack of awareness of the needs of the process approach,
- lack of risk management in the organisation,
- lack of integration of risk management, security and continuity,
- lack of support from the top management for risk, security and continuity management,
- lack of experience in this type of project,
- treatment of the issue of business continuity as a typical problem to be solved by a one-time project to develop an emergency plan, and not the establishment of a process of continuous improvement of skills to deal with incidents;
- hastily addressing the issue without prior selection of methods for solving the problem and the methods for executing the project,
- underestimation of the importance of documentation and its regular updating.

In taking account of these barriers, the basis for the implementation of policies for dealing with disruption is the appropriate plan that arises in the process of analysis and design activities, among which stand out in particular:

- analysis of the processes in the organisation,
- identification of stakeholders,
- analysis of the threats to the organisation (like BIA or risk analysis),
- analysis of the susceptibility of the organisations to to disruption (likw BIA or risk analysis),
- mapping of disruptions,
- development of regulations, procedures, instructions,
- implementation of approaches to prevent disruption,
- implementation of approaches to business continuity planning,
- implementation of approaches to monitoring disruption,
- implementation of approaches to tolerating disruption,
- implementation of the adopted procedure for disruptions,
- testing business continuity plans.

This may be organised as shown in Figure 6.4. Some of these activities constitute a cycle which, repeated periodically in a spiral of improvement, enables the organisation to maintain and develop business continuity solutions.

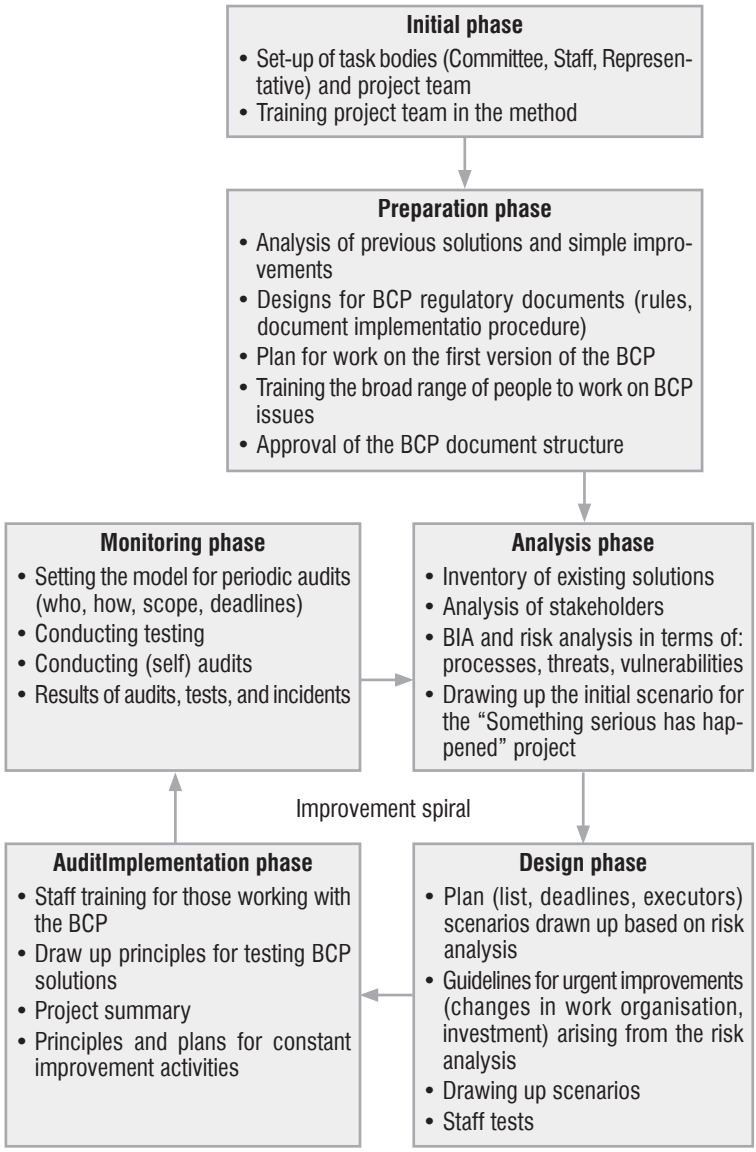

Figure 6.4. Planning using TSM-BCP methods

Analysis of threats to the organisation

Risk analysis is carried out using the standard list of threats (see Table 6.1). At the beginning threats which are irrelevant to a given organisation should be deleted, and possibly others, specific to the organisation, should be added. Then there should be an assessment of whether the threat is external or internal from the point of view of the organisation. The question is whether the threat within the organisation

materialises in its proper form and constitutes a problem for the organisation, for example, is a hurricane a properly identified threat, or should it be damage to the building. This is closely related to dividing risk into of causal and effect relationships, where causal means finding solutions closer to security and monitoring, whereas effect means finding solutions closer to business continuity. External threats cause internal consequences for business continuity, and it is the latter we seek to determine. It may therefore be necessary for successive iterations (verifications) of assessment in order to exclude certain external threats as unlikely or replace them with more clearly defined internal threats. Causal threats should be included in the security policy and covered by monitoring and prevention.

In the next step, we assess whether the threat is direct or indirect. It is necessary to determine whether the disruption does indeed affect the organisation, or is it affected by a subordinate factor, for example, whether a street demonstration is itself the disruption, or is it rather the *de facto* lack of access to the premises caused by the demonstration. And in this case causal threats indicate the need for monitoring and prevention in the context of security policy.

At the end, a revised final list of risks is prepared, classifying causal threats in terms of security policy, but effect threats in terms of developing plans for ensuring business continuity.

Table 6.1. Standard list of threats[17].

Threats
Natural disasters • earthquake • environmental contamination • flood • hurricane • lightning strike • other
Terrorism • blackmail • attack • other
Physical disruptions • no access to buildings • building damage • too low/high atmospheric temperature • too high atmospheric humidity • fire • flood • other

[17] Other suggestions for the lists of threats can be found in the following standards: ISO 27005:2009 and ISO/IEC TR 13335-3:1998.

Threats
Functional disruptions • strike • sabotage • unavailability of workers • accident • other
Technical disruptions • exhaustion of materials • lack of power • air conditioning malfunction • other
IT disruptions Technical infrastructure: • server emergency • workstation emergency • peripherals emergency • network emergency • cable emergency • no connection to external networks • other Software: • licence expiry • unauthorised deletion • malfunction • other Harmful software: • viruses • other Data: • data loss or destruction • unauthorised data access • unauthorised data copying • unauthorised data modification • other
Other disruptions • lack of human resources • lack of financial resources • lack of material resources • lack of external services • other

Analysis of the organisation's susceptibility to disruption

This analysis[18] is carried out using the standard list of critical resources (see tab. 6.2). Firstly, verify and clarify the classification of categories of resources in a manner appropriate to the specific situation of a given organisation. Then identify all the resources that each in location of organisational units (headquarters + field and auxiliary locations), in the light of process analysis and routes of information flow, may affect the continuity of business processes and information processing. As conventional facilities with a particular impact on the conditions of business activity, we must take into account external services, including those universals such as: supply of water, gas, electricity, telephone communications, and specific, such as: cooperation, supply of materials, maintenance services.

As a result of the analysis, a revised list of critical facilities is prepared separately for each location, and there is an analysis of their vulnerability to operational risk.

Table 6.2. Sample list of critical resources (facilities)

Categories	Example
A. Buildings	Company's own building
B. Technical and industrial buildings	Production hall, boiler room, computer centre
C. Office centres	Office space rented in a different building
D. External technical equipment	External free standing electricity generator
E. Internal technical equipment	Internal air conditioning or generator
F. IT infrastructure	IT equipment
G. External telecom equipment	Satellite dish on the roof
H. External services	Telecommunications
I. Logical facilities/virtual solutions	Non-material obligations
J. Key employees	Licenced investment consultant in a financial company
X. Other	

[18] The vulnerability of an organisation to a given threat results from its ongoing organisation, assessed in terms of the importance of business processes and the possibility of a negative impact of individual threats on these processes.

Mapping of disruptions

At this stage the mapping of interference for individual resources takes place, although more often for locations and technical and logical[19] facilities potentially affected by specific threats (factors: process – facility – threat, the idea of a three-dimensional map of disruptions is shown in Figure 6.5). It is very useful to classify operational risk as presented in Table 3.1. Each of the types of operational risk presented serves to look at the possible disruptions from the particular perspective of the specific risk.

The map is used to finally verify which threats may be the most severe and which facilities are most sensitive in the business perspective. The importance of a potential disruption should be assessed and verified through the prism of maintaining process stability.

The disruption map is the most comprehensive analytical document. Thorough preparation allows for a comprehensive solution to the problem of providing business continuity. However, do not be afraid that this analysis leads to the development of scenarios for each identified potential disruption. Each scenario describes the remedial actions associated with a threat group treated together due to common causes or effects.

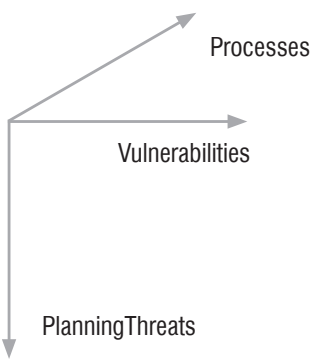

Figure 6.5. Factors affecting disruption

Individual positions on the disruption map are assigned to one of the models of proceeding with disruption according to the classification shown in Figure 6.2.

Development of regulations, procedures, instructions

Processes and the activities that make them up need to keep their repeatability, exactly as they were designed and adopted as appropriate. To obtain this organisational

[19] Logical objects are elements of computer software, IT systems, or parts thereof.

stability of action, the principle of documenting good practice should be applied. The main types of documents used are rules, procedures and instructions.

Comprehensive coverage of the whole of the organisation's activities by a set of procedures depends on determining the issues, processes and sub-areas to be explored and regulated. This is done by extracting the basic criteria for the selection of issues and possible superposition of some of them. The criteria are: for example: organisational (functional) structure, process structure, types of resources, subsystems of the IT system, business continuity, security, correctness of operation.

It is necessary to archive all subsequent versions of the individual procedures. This need is a consequence of, for example, the requirements of the audit, where each questionable situation (problem) assessed in the past should be applicable to the regulatory standards then.

Implementation of an approach to prevent disruption

This approach mainly includes investment activities, and, prior to the realisation of the investment, activities towards an approach to business continuity planning. The disruption map presents a specific list of the organisation's vulnerabilities (in terms of business continuity issues). Many of these weaknesses can be reduced or eliminated by technical investments. Their implementation, however, is significantly hampered by the need for extensive research on the scope of a given investment and the final effectiveness of the new technical solution, which should be to fully remove the organisation's vulnerability to the disruption under consideration. The ultimate rationality of the proposed solution is reviewed in the light of the budgetary capabilities of the organisation, the payback period, and economic criteria. Typical investments are:

- duplication of equipment,
- duplication of computer centres (building a backup centre)
- multiplication of lines of communication,
- multiplication of access points to the network of public services,
- backup power supplies,
- physical, power and logical separation of servers or IT control centre environments,
- despite the specialisation of servers maintaining the potential to reduce work to a smaller number of them,
- asynchrony of data security,
- specialist shifts.

The investment plan adopted by the decision makers for technical solutions is a key document upon which are based the actions constituting this approach.

Implementation of the approach to business continuity planning

These activities are divided as in Table 6.3.

Table 6.3. Division of labour in response to disruption

Organisational unit	Prior to occurrence of disruption	After the occurrence of disruption
BCM Co-ordinator and all organisational units	Drawing up a business continuity plan	Analysis and improvement of the business continuity plan
Crisis Committee (Crisis Staff)	Testing of the business continuity plan	Ensuring business continuity, removing the causes and effects of the disruption

The culmination of the business continuity plans are the situational scenarios. These are divided into:

- external scenarios that describe possible versions of the development of events in the future over which the organisation has no control,
- internal scenarios that are based on causal reasoning, linking choice of action with goal, and certain results are preferred by the organisation in accordance with its hierarchy of objectives [van der Heijden, 1996].

In developing scenarios, especially during the first creation of a business continuity plan, there should be a very strict course of top-down reasoning, reaching to the base of knowledge about the organisation and its objectives. The successive steps of this reasoning (some may be ignored) are:

- goal setting (even the organisation's mission),
- determining the essence of the organisation's activities (basic processes) based on process analysis,
- determine the boundary restriction for activity in the case of disruption (as to the scope and critical functions and the minimum acceptable quality of action), including Business Impact Analysis,
- assessment of threats and the resulting disruption (verification of the disruption map),
- assessment of the ongoing capacity of the organisation to respond *ad hoc* to disruption,
- adoption of organisational solutions to confront the calculated disruption (appointment of a BCM coordinator and Crisis Committee, and the development of appropriate regulations, rights and responsibilities),
- development of disruption scenarios and response activities for them,
- testing the situations described in the scenarios,
- verification of the specific procedure based on tests or conclusions from the existence of disruption.

Situational scenarios organising prognoses, specific, precise thinking and action, enable the simulation and testing of the emergency plans prepared. At the same time, it should be borne in mind that the scenarios for responding to disruptions do not guarantee the full effectiveness of the prognoses either in terms of disruption, or as to the course of emergency situations, or as to the appropriateness of the plans to the actual events, and they therefore require a flexible margin for unforeseen factors/events.

Implementation of the approach to monitoring disruption

This mainly covers activity of an organisational nature, and only then regulatory. Key to it is the monitoring of the extent of disruption, and whether in relation to this the routine compensation mechanism is sufficient. Developing policy solutions relies primarily on formal confirmation of organisational solutions compensating for disruption, and therefore transcribing, analysing, and possibly improving or expanding upon existing practice, and considering what solutions are needed in shaping the organisational structure, the responsibilities of individual units, regulations, procedures and instructions. Monitoring disruption should be regulated by procedures/instructions to make it possible to evaluate and decide when the degree of disruption exceeds the limit of coverage by monitoring and, therefore, the business continuity (plan) approach must apply.

Implementation of the approach to tolerating disruption

This mainly covers activity of a legal nature, and only then regulatory. Basically, it does not require a substantial response to the disruption, but it is necessary to regulate a number of issues. For example, how to determine the measurement of the intensity of disruption must be decided, and who, how, and on what basis determines the organisation's planned response to the disruption and, by analogy, decides to discontinue this action and return to routine performance of tasks. The organisation's activity, in its nature tolerating disruption, involves a slight modification or a temporary interruption of routine work, when it is usually required to notify employees, customers, suppliers, etc. - it should provide an appropriate situational scenario. Furthermore, it is important that business responsibility towards partners (customers, employees and service providers) be defined and limited in accordance with the policy formulated.

Implementation of the adopted procedure for disruptions

The implementation of a policy for dealing with disruption comprises three strands of activity:

- establishment of the formal organisational structures,

- definition of the principles for monitoring threats and responding to disruption, investment plans and models of accident scenarios,
- development of regulations, procedures and instructions, and detailed scenarios for conduct in the event of disruption.

6.4. Business continuity maturity model

Business continuity management is still a young concept in management theory, although patterns are already sought for assessing the relevance of management in this regard. A good example is the BCMM[20] method (Table 6.4).

Table 6.4. Business Continuity Maturity assessment method

Maturity level of business continuity		Basic range			Advanced range		
		Approval of senior management	Professional support	Management	General participation	Planning activities	Joint action
Level 1	Intuitive	No	No	No	No	No	No
Level 2	Supported	Marginal	Partial	No	No	No	No
Level 3	Centrally managed	Partial	Yes	Partial	No	No	No
Level 4	Aware	Yes	Yes	Yes	Yes	No	No
Level 5	Improved	Yes	Yes	Yes	Yes	Yes	No
Level 6	Integrated	Yes	Yes	Yes	Yes	Yes	Yes

Source: Virtual Corporation.

The idea of the method is that the company (organisation) gradually attains higher maturity levels, introducing permanently fixed organisational structures, defining the roles of the participants, and the principles and action plan. At the same time, it is possible to lose an already reached level of maturity in situations where the organisation suffers profound technological, organisational, or environmental changes. The maturity levels are:

- Level 1 BCP is not perceived by top management as a significant and requiring central management. It is dealt with by individual organisational units according to their own assessment and to the extent that they consider to be correct.
- Level 2. The strategic importance of BCP is recognised by one of the organisational units. Within an organisation, or amongs its supporting consultants,

[20] BCMM – Business Continuity Maturity Model, this method was developed by Virtual Corporation, Inc. See www.virtual-corp.net

there is a specialist who can support work on BCP. Top management knows that it is a serious problem, but still does not give it the appropriate priority.

- Level 3. Those organisational units most interested in BCP conduct joint activities concerning the programme, but there is not a company-wide BCP. Top management is aware of the actions taken, and supports them, but is not yet capable of establishing structures, tasks and a BCP.
- Level 4. Top management is aware of the strategic importance of managing the BCP. A permanent office is established for managing BCP issues. There is work on integrated solutions, shared throughout the company. Critical processes are identified, and plans are developed to protect them. They are tested and routinely updated.
- Level 5. All organisational units have tested BCPs positively, including rules to make changes in the plans. Top management also participate in the tests. A several year development programme for BCP solutions has been drawn up.
- Level. 6 All organisational units received high marks in BCP preparation. The interaction between units is tested. Any actual changes to business processes are concurrently tracked and adapted in the BCPs.

Summary

Every business organisation is formed with a view to a specific utility. These expectations in the first place are related to the results of the organisation's activity, but it is equally important that the activity itself is smooth, and as a consequence reasonable costwise. The intention is therefore to create an effective and efficient organisation. In practice, however, its activity is impeded in the execution of business tasks. These are partly due to the risk that accompanies numerous competing players in the market, and refers to the organisation's products (services), its customers, and its relationships with them. At the same time, some obstacles affect the internal governance of the organisation and are a derivative of operational risk. The organisation must be able to cope with these hurdles.

A special category of organised response to operational risk is ensuring business continuity. This issue can be seen from a technical perspective, as well as business and social. In each perspective, the mechanism for the breach in business continuity remains the same. Its primary cause is the state of uncertainty which characterises our reality. Thus, every action the organisation takes, and its associated decisions, bear a risk, manifested as certain threats. These, when they strike a susceptibility in the organisation's operating rules or structure transform into specific disruptions that lead to perturbation of the organisation's activity and to specific damage. The whole constitutes a sequence of consequences of the risk in operation.

An organisation's logical response to disruption is to build a mechanism of homeostasis, based on the monitoring of threats, neutralising them, and when that fails, to restore the state before the disruption, and until then to provide forms of substitute operation. This conduct is the expression of a rational response to the inevitable risk, which should take into account the integration of security as prevention against threats and ensuring business continuity as a therapy against disruption (see Figure S.1).

A detailed examination of this mechanism was the subject of the author's research, the results of which enabled the creation of this text. The author's original contribution includes:

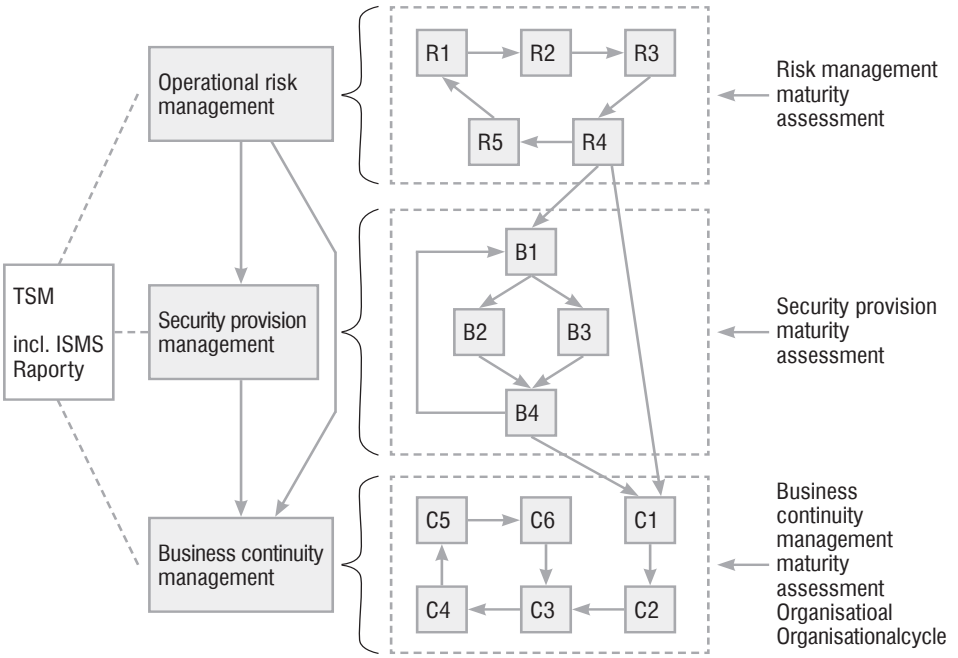

Figure S.1. Integrated management of operational risk, security, and business continuity

Legend for Figure S.1

TSM – *total security management*		
ISMS – *information security management system* [ISO 27001:2007].		
Description in this column on the basis of fig. 3.1		Description in this column on the basis of fig. 6.4.
R1 – risk identification	B1 – needs and solutions analysis	C1 – initial task recognition
R2 – risk analysis and assessment	B2 – defining internal standards	C2 – project preparation
R3 – risk monitoring	B3 – auditing standards observance	C3 – needs and solutions analysis
R4 – risk manipulation	B4 – observance of attempts to infringe security, return to analysis	C4 – solution design
R5 – planned improvement		C5 – implementation of solutions
		C6 – monitoring, after which return to the analysis phase

Proposing an approach leading to a comprehensive classification capturing the stages of risk actualisation and the characteristics of individual sectors of the economy and social activities (Chapter 2). Thus, a research direction was indicated on integrated risk management. The preparation of such a classification is still an open question.

Indication of the problematic triad "Operational Risk – Security – Business Continuity" as a pragmatic recognition of the essence of the managerial challenges associated with the variability of the business environment, particularly deriving from increasing globalisation and increasing market competition (Chapter 1 and Section 3.1).

- Proposing a definition of operational risk, modified in relation to the most commonly found version by the Basel Committee (Section 3.3).
- Proposing a classification of types of operational risk based on criteria specific to the theory of organisations (Section 3.3).
- Presentation of the advantages of the qualitative analysis of risks and qualificative estimation of operational risk, as complementary to the estimation of capital adequacy (Section 4.2). The quality perspective is simpler, and at the same time quite sufficient in the context of systematically developing organisational solutions, to protect against manifestations of risk.
- Proposing monitoring risk a four-level learning approach, bedded in the latest concepts of knowledge management.
- Proposing and practical verification of an original method of analysis of risk/threats based on the following:
  - identifying, analysing and assessing risk/threat on the basis of an original use of various categories of risk classification (described in Section 3.3) as the respective perspectives of assessment;
  - selecting security solutions for different categories of risk/threat on generally accepted principles;
  - verifying the completeness of security on the basis of an originally selected set of principles for providing resource security (described in Section 5.1);
  - designing business continuity solutions using the original method described in Section 6.3. Risk intensity criteria are used, i.e. the strength of its impact and frequency of interaction (Fig. 6.2). The resulting four general attitudes threats express economically viable reactions, from prevention through monitoring, to the planning of emergency scenarios.

Conclusions

1. Operational risk management, defined as the triad of "Operational Risk – Security – Business Continuity", is a quintessential management issue including the very essence of effectiveness, efficiency and productivity of organisational operations (Chapter 1 and Section 3.1).

2. Business continuity management is a part of management science with a target role and value analogous to the importance of reliability theory in the field of technical sciences, already well established in the history of science (Figure 1.1).
3. From a social perspective business continuity management, referenced to a single organisation, supplements the theory of crisis management assigned to a regional or national level (introduction to Chapter 5).
4. Business continuity management is simultaneously counteracting operational risk. It therefore remains in a relationship with other areas of such countermeasures, i.e. management of security provision and quality management (Figure S.2). Since operational risk is an expression of an organisation's imperfection, business continuity management is one of the ways of improving the organisation and in this sense is part of the broader understanding of quality management.

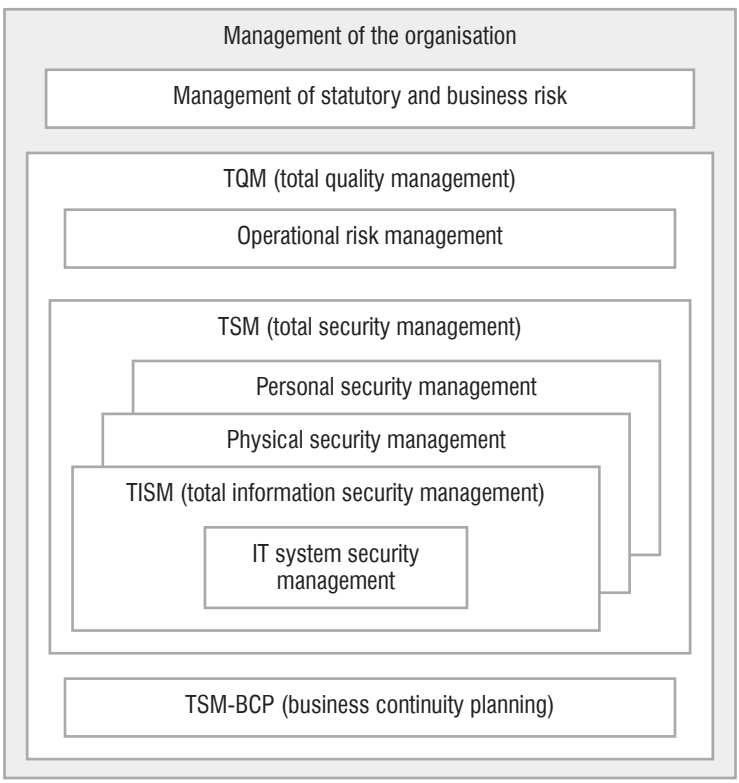

Figure S.2. The relationships between Total Security Management and Total Quality Management

5. Risk is associated with every deliberate action by an organisation, and arises from the general uncertainty that accompanies every human activity (Section 2.1). Risk is manifested in threats, not all of which are relevant to a particular organisation. Determining which of them are of importance is based on an analysis of the processes and susceptibilities of the organisation as a system of operation and its resources (Section 6.1 and 6.3). This analysis serves the development of maps of potential disruption, which allows limiting the activities carried out within the framework of business continuity management to predictable events (disruptions of known character and intensity, occurring in identified places and situations).
6. The model response to the possibility of disruption boils down to four manners of response, called: tolerating, monitoring, prevention and planning (Figure 6.2).
7. Business continuity management is a process that requires the assignment of a dedicated organisational structure, an identification of the operating principles, roles and responsibilities, and the allocation of resources (Figure 6.3).
8. Business continuity management requires continuous improvement, due to the internal variability of the organisation, its processes and resources, and the volatility of the external environment and its impact on the organisation. An important element of this improvement is the systematic gathering of organised knowledge about the phenomena of threats, about disruption that has occurred, and in this context the evaluation of solutions used so far and available for future remedial action. Similarly important is the exercise (testing) of the organisation's efficiency in solving critical situations via simulating the appearance of disruption (Section 6.1).
9. Organisational procedure to ensure business continuity refers to the following issues that should be included or ensured (Section 6.1 and 6.3):
   - when a given threat affects the organisation's system of operation or its environment, and the system becomes vulnerable to this, we are dealing with disruption that:
     - is due to the interaction between the risk and the system of operation or the environment of that system,
     - results in significant changes in the operation of the organisation,
     - is not evaluated objectively, and subjectively is evaluated from the perspective of a given system of operation.
   - as part of the organisation's business, we must be aware of the possibility of disruptions that prevent the normal continuation of that business;
   - regardless of the nature of the causes of these events, in formal or in business terms of the perceived obligation of due diligence in carrying out its tasks, the organisation should strive to continue even limited operations;

- such effort should be based on a previously developed, consistently improved and tested business continuity plan, also sometimes called (but in a narrower sense) a contingency plan, i.e. a plan to remove dysfunctionality;
- ensuring business continuity includes the prediction of scenarios of potential disruption and separable design of:
  - solutions to prevent the threats themselves (mainly to ensure safety),
  - solutions for dealing as soon as possible with the consequences of disruptions,
  - solutions for continuing limited operations in critical conditions;
- the approach to business continuity should be rational, that is, calculated to ensure a balance between the expected degree of certainty in maintaining business continuity and the costs of so maintaining it; it is therefore also necessary to assume the gradual surrender of successive elements of normal activity appropriate to the dimension of the critical situation identified (it does not always make sense, especially in economic terms, to make persistent efforts to maintain business continuity).
- the continuity plan should be flexible enough to allow adaptation to disruptions deviating from the expectations underlying the original plan;
- it is necessary to define the process essence of of the organisation's operation as the minimum activities that must be maintained; the inability to continue such minimum activities is the basis for the decision to abandon the use of substitute solutions and focus purely on removing the effects of disruption;
- in the preparation of the continuity plan, business, legal and organisational aspects must be considered first and foremost, as these decide on the necessary scope of technical solutions;
- business analysis may concern the issue of the company's prestige, and certainly a kind of balance sheet of risk and the financial resources allocated to its limitation; it is reasonable to treat the continuity plan as a process of continual improvement, in which the goals will be achieved gradually by successive approximations (versions of the business continuity plan engaging graduated expenditures from period to period);
- legal analysis is especially important when formulating the assumptions of the continuity plan, as it allows to define the scope of the company's liability for various areas of its operations, identify sensitive points, and select non-technical forms of security;
- organisational analysis allows the designation of the appropriate staff to operate the continuity plan in critical conditions, providing them with the scope of decision-making autonomy relevant to such a situation, in day-to-day conditions enabling them to prepare for such a difficult role;

- none of the elements of this analysis, and also the design of technical solutions, is a closed stage; improvement of the continuity plan depends on constant renewal of the analysis and design of solutions with respect to changes in the organisation's business, development of the continuity plan, and conclusions after the materialisation of an actual disruption.

10. In accordance with the ISO 2700x and ISO22301 standards, you must create solutions that effectively preserve continuity (Section 6.3). By analogy with living organisms, such solutions are intended to provide a capacity for homeostasis i.e. a trait of the organisation that consists of initiating its own internal mechanism for the prevention of disruption in order to restore the state before the emergence of the disruption. The effectiveness of solutions to anticipate disruption and their relevance to actual events should be placed above the minimum threshold of acceptance by decision-makers, who usually carry out the assessment based on two criteria:
    - the prestige of the organisation and its degree of challenge as a result of the suspension or restriction of activities,
    - the relationship between cost of security solutions and the cost of potential losses and restoration of the actions harmed by the disruption.
11. A rationally conceived system homeostasis leads to a conscious temporary reduction (limited to the time of occurrence of the disruptive factor or the effects of disruption) of the quality of action to a level previously set in the light of such determinants as:
    - the loss of a dissatisfied or injured client,
    - benchmarking against competitors and best market practices,
    - robust standards of cooperation with partners and customers – SLA (Service Level Agreement).
12. Systematic procedure for disruptions is to determine:
    - Which disruption (threats in interaction with the system of operation) are subject to remediation, i.e. are covered by the preventive arrangements or procedures to ensure continuity;
    - which technical infrastructure facilities are protected against threats,
    - which business processes are protected against threats,
    - which information flows are protected against threats,
    - who is responsible for restoring business continuity in the event of disruption.
13. Reducing the operational quality should not last longer than the time needed to eliminate the causes and effects of the disruption, and the sometimes the former can resolve spontaneously, if such is the nature of the disruption.

Issues for further research

Uncertainty – the definition of the synthesis of the concept inherent in various academic disciplines. The concept of uncertainty is differently formulated in such disciplines as philosophy, physics, astronomy, economics, and management. It would be useful to examine these interpretations and the temptation to formulate a synthetic approach.

Comprehensive classification of risk, in the form of proposals towards research described in Section 2.3.

Identification of risk (threats) in crisis management. At the moment, this issue constitutes a gap in the theory of crisis management in the sense of an absence of methodological approaches to this problem. It is also of great practical importance due to current European Union law obliging all levels of government to systematically carry out such identification.

Ensuring business continuity in terms of strategic management. Business continuity is seen in two perspectives. The operational perspective is described in this book. However, in the strategic perspective, business continuity is a postulate of the quality and efficiency of an organisation's operation and its management in the aspect closer to the discipline of economics than of management. This issue has so far been seen only intuitively.

Ensuring business continuity from the market perspective. Violations of business continuity in a single organisation can entail consequences beyond its operation, reaching other market participants, and sections of society. The fear of such consequences can lead to cooperation between competitors (see the concept of co-opetition).

Ensuring business continuity from the financial perspective. The issue of business continuity is related to a company's financial activities in several respects, such as:

- protection against excessive losses,
- costs of continuity solutions,
- ensuring company financial liquidity as an activity that provides business continuity.

Relationships between business continuity and crisis management. Crisis management (as indicated in Chapter 5) is developing as an autonomous field of knowledge and practice. Meanwhile, the relationships between these two issues are even intuitively obvious, because they really differ only in scale of social impact, and a synergy can easily be imagined in cases of disasters affecting a single organisation and the wider social community simultaneously.

Relationships between business continuity and organisational management in a crisis. An organisation that finds itself in a crisis of any given nature, is more susceptible to the effects of threats, including those not directly related to the crisis occurring. It can be assumed that the needs of such an organisation in terms of business continuity are clearly larger than average.

Relationships between business continuity and reliability theory. Reliability theory has been developed over a hundred years, and it relates to the technical creations of humankind. Due to a certain range of parallels between the principles of operation of technical devices and organisations, as well as human creations, we can assume the suitability of the findings of reliability theory for the theory of operational risk management, security assurance theory, and the theory of business continuity.

Ensuring business continuity in relation to the concept of an organisation characterised by a high level of change. How do we reconcile ensuring business continuity with the necessity for continuous changes in an organisation in response to a changing environment? These organisational changes are associated with destructive actions: first a weakening of the existing state, its change, and then its replacement with a new solution, which in turn should be fixed. How do we adapt these to the concept of change management, innovation management, agile and learning organisations, and finally to knowledge management?

Bibliography

Andersen B. [1995], *Benchmarking*, [in:] Rolstadas A. (red.), *Performance Management*, Chapman & Hall, London.

Armstrong C.S. [2001], *Engineering and Product Development Management. The Holistic Approoach*, Cambridge University Press, Cambridge.

Basel Committee on Banking Supervision [2010], *Sound Practices for the Management and Supervision of Operational Risk – consultative document*, Bank for International Settlements, Basel.

BBA, ISDA, RMA [1999], *Operational Risk: The Next Frontier*, British Bankers' Association, Philadelphia.

Beck U. [1986], *Risikogesellschaft – Auf dem Weg in eine andere Moderne*, Frankfurt a.M.

Bernstein, P.L. [1996], *Against The Gods: The Remarkable Story of Risk,* John Wiley & Sons, New York.

Business Continuity Institute [2004], *Business Continuity Management: Good Practice Guidelines*.

Byczkowski M., Zawiła-Niedźwiecki J. [2009], *Information Security Aspect of Operational Risk Management* „Foundations of Management" nr 2.

Can J. [1995], *Taxonomy-based Risk Identification*, Carnegie Mellon University, Pittsburgh.

Casual Actuarial Society [2003], *Overview of Enterprise Risk Management*, Enterprise Risk Management Committee.

Charters I. [2011], *A Practical Approach to BIA*, British Standards Institution, London.

Conrow E.H. [2000], *Effective Risk Management. Some Keys to Success*, American Institute of Aeronautics and Astronautics Inc., Reston.

Cruz M. (red.) [2004], *Operational Risk Modelling and Analysis. Theory and Practice*, Incisive Media, Londyn.

Culp C.L. [2002], *The Art of Risk Management: Alternative Risk Transfer, Capital Structure and the Convergence of Insurance and Capital Market*, New York.

Dahlgaard J.J., Kristensen K., Kanji G.K. [1998], *Fundamentals of TQM*, Stanley Thornes Ltd, Chichester.

Dixit A.K., Nalebuff B.J. [2008], *The art of strategy: a game theorist's guide to success in business & life*, WW Norton & Company

Döbeli B., Leippold M., Vanini P. [2003], *From Operational Risk to Operational Excellence*, Risk Waters Group, London.

Drucker P.F. [1999], *Management Challenges for 21st Century*, Harper Business, New York.

Ebnöther S., Vanini P., McNeil A., Antolinez P. [2003], *Operational Risk: A Practitioners Point of View*, „Journal of Risk" nr 5.

FERMA [2003], *Risk management standard*.

Gołąb P. [2009], *Business Continuity Management*, [in:] Monkiewicz, J. Gąsiorkiewicz L. (red.), *Risk Management. Concept-Models-Issues*, Elipsa, Warszawa.

Greenwood D.J., Levin M. [1998], *Introduction to Action Research*, Sage Publications, London.

Hammer M., Champy J. [1993], *Reengineering the Corporation. A Manifesto for Business Revolution*, Harper Business Books, New York.

van der Heijden K. [1996], *Scenarios: the Art of Strategic Conversation*, Wiley, Chichester.

Help-desk [2007], OGC, London.

Hiles A. [1993], *Service Level Agreements: Measuring Cost and Quality in Service Relationships*, Chapman & Hall, London.

Knight F. H. [1957], *Risk, uncertainty and profit*, New York.

Koontz H., Weihrich H. [2007], *Essentials of Management*, McGraw-Hill Publishing.

Loader D. [2006], *Operations Risk Managing a Key Component of Operational Risk*, Oxford.

Maslow A.H. [1954], *Motivation and personality*, Harper, New York.

Mitroff I.I., Pearson C.M. [1993], *Crisis management*, Jossey-Bass, San Francisco.

Morgan G. [2006], *Images of Organization*, Sage Publications, London.

Nadler G. [1967], *Work Systems Design. The Ideals Concept,* Irwin, Homewood.

Nocco B.W., Stultz R.M. [2006], *Enterprise Risk Management. Theory and Practice*, Ohio State University.

Perry C., Riege A., Brown L. [2004], *Scientific Paradigms in Marketing Research about Networks*, [in:] R. Buber, J. Godner, L. Richards (red.), *Applying Qualitative Methods to Marketing Management Research*, Palgrave Macmilian, New York.

Pritchard C. [2001], *Risk Management Concepts and Guidance*, ESI International.

Probst G., Raub S., Romhardt K. [1999], *Managing Knowledge*, Wiley, London.

Quinn J.B., Mintzberg H., James R.M. [1993], *The Strategy Process, Contexts and Cases*, Prentince-Hall International Inc, Rijswijk.

Reason P., Bradbury H. (red.) [2001], *Handbook of Action Research Participative Inquiry and Practice*, Sage Publications, London.

Reilly F.K., Brown K.C. [2008], *Investment Analysis and Portfolio Management*, South-Western College Pub.

Rummler G.A., Brache A.P. [2000], *Improving Performance*, Jossey-Bass, San Francisco.

Schwartz T., McCarthy C. [2007], *Manage Your Energy, Not Your Time*, „Harvard Business Review" no 10/2007.

Senge P.M. [1990], *The Fifth Discipline: The art and practice of the learning organization*, Doubleday, New York.

Stoner J.A., Wankel C. [1986], *Management*, Pretince-Hall, Englewood-Cliffs.

Strzelczak S. [2003], *Business Planning and Risk Management*, [in:] S. Strzelczak (red.), *Economic and Managerial Developments in Asia and Europe. Comparative Studies*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa.

Tharenou P., Donohue R., Cooper B. [2007], *Management Research Methods*, Cambridge University, Cambridge.

Vaughan E.J. [1997], *Risk Management*, John Wiley & Sons Inc., New York.

Waters D. [2002], *Operations Management. Producting Goods and Services*, Financial Times and Pretince Hall.

De Wit B., Meyer R. [2005], *Strategy Synthesis*, Cengage Learning EMEA.

Wust P. [1937], *Ungewissheit und Wagnis*, Köselverlag + Pustet Verlag, Munchen.

Zawiła-Niedźwiecki J. [2009], *Operational risk and the security of an organization,* [in:] J. Monkiewicz, L. Gąsiorkiewicz (red.), *Risk Management. Concepts, models, issues*, Dom Wydawniczy Elipsa, Warszawa.

Zawiła-Niedźwiecki J. [2010], *Business Continuity*, „Foundations of Management" no 2

Websites authoritative on business continuity matters

www.bcm-institute.org (Business Continuity Management Institute)

www.continuitycentral.com

www.davislogic.com (Davis Logic Inc. – Business Continuity Management Information and Resources)

www.drii.org (DRII The Institute for Continuity Management)

www.drj.com (Disaster Recovery Journal)

www.globalcontinuity.com

www.gloria-mundi.org (*Operational risk*)

www.itil-itsm-world.com (Information Technology Infrastructure Library - Information Technology Security Management)
www.mit.edu/security (Massachusetts Institute of Technology)
www.thebci.org (Business Continuity Institute)
www.virtual-corp.net (Virtual Corporation Inc – BCMM – Business Continuity Maturity Model)

Standards

Standard BS 25777:2008 *Information and Communication Technology Continuity Management*.
Standard BS 25999-1:2006 *Business Continuity Management – Code of practice*.
Standard BS 25999-2:2007 *Business Continuity Management – Specification*.
Guide to Business Continuity Management, British Standards Institution 2003.
Standard PN-EN/ISO 9000:2006 *Systemy zarządzania jakością. Podstawy i terminologia*.
Standard PN-EN/ISO 9001:2001 *Systemy zarządzania jakością. Wymagania*.
Standard ISO 12207:1995 *Information technology – Software life cycle processes*.
Standard ISO 15408-1:1999 *Information technology – Security techniques – Evaluation criteria for IT security*.
Standard ISO/IEC 20000-1:2005 (standard BS-15000-1:2002) *IT Service Management. Specification for Service Management*.
Standard ISO/IEC 20000-2:2005 (standard BS-15000-2:2003) *IT Service Management. Code of practice for Service Management*.
Standard ISO 22301:2012 *Societal security - Business continuity management systems – Requirements*.
Standard ISO 22313:2012 *Societal security - Business continuity management systems – Guidance.*

Janusz Zawiła-Niedźwiecki – scientist, educator and business management practicioner

In the past:

- CIO at the Warsaw Stock Exchange, board member and managing director of Powszechny Zakład Ubezpieczeń, Project Manager of the Location Platform (Polish part of the E112 rescue system). Winner of the "Lider Informatyki" Award (as CIO of the Warsaw Stock Exchange) from Computerworld magazine in 1998 and 1999.

Currently:

- business consultant, chairman of the Prof. K. Bartel Foundation, member of the Scientific Council of the Inspector General for Personal Data Protection, Vice-President of the Scientific Committee of the Warsaw Stock Exchange, member of the Banking Technology Forum of the Polish Banks Association in the working groups "Business continuity", "Cloud" and "Mobile Services", member of Programme Council of the IT Leader Club Polska Foundation, Secretary of the Board of the Warsaw Branch of the Polish Economic Society.
- academic and educator at the Faculty of Management of the Warsaw University of Technology, member of the Polish Accreditation Committee; guest lecturer at the University of Warsaw, the Collegium Civitas at the Polish Academy of Sciences, Warsaw Medical University, and the University of Economics in Wrocław; winner of Minister of Privatisation and Rector of Warsaw University of Technology awards; author of over 200 publications, including editor of the monographs: "Operational Risk Management" (2008) and "Business Informatics" (2010, Economic Publishers Award 2011), author of the books: "Security of information systems" (2012, Rector of Warsaw University of Technology Award in 2013) and "Operational risk management in business continuity" (2013).

More – www.januszzawilaniedzwiecki.com