RISK MANAGEMENT

Daniel SORA

Regional Department of Defense Resources Management Studies

Abstract: *One of the most important internal control standards that make up the code on Internal Control, approved by Ministry of Public Finance Order no. 946/2005, is the standard on risk management.*

According to the above mentioned standard, each public entity is required to systematically analyze at least once a year, the risks related to its activities, to develop appropriate plans in order to limit the possible consequences of these risks and to name those responsible for implementing plans. This practice has migrated from the private sector the public sector, so that more and more European Union countries governments have integrated risk management in the public management reforms undertaken in recent years.

Keywords: risk management, consequences, public management

"When I was young, people called me a gambler. As the scale of my operations increased I became known as a speculator. Now I am called a banker. But I have been doing the same thing all the time."

Sir Ernest Cassell — Banker to Edward VII

The entire history of human society is a chronology of exposure to risks of all kinds and human efforts to deal with those risks. From the first emergence of the species *Homo sapiens,* our ancestors practiced risk management in order to survive, not only as individuals but as a species. The survival instinct drove humans to avoid the risks that threatened extinction and strive for security. Our actual physical existence is proof of our ancestors' success in applying risk management strategies.

Although the term *risk management* originated in the 1950s, Henry Fayol recognized its significance earlier[1]. Fayol, a leading management authority, was influenced by growing mass production in the United States, and the existence of giant corporations and their management challenges. In 1916, he structured industrial activities into six functions, including one called *security,* which sounds surprisingly like the concept of risk management:

"The purpose of this function is to safeguard property and persons against theft, fire and flood, to ward off strikes and felonies and broadly all social disturbances or natural disturbances liable to endanger the progress and even the life of the business. It is the master's eye, the watchdog of the one-man business, the police or the army in the case of the state. It is generally speaking all measures conferring security upon the undertaking and requisite peace of mind upon the personnel".

Organizations face a very wide range of risks that can impact the outcome of their operations. The desired overall aim may be stated as a mission or a set of corporate objectives. The events that can impact an organization may inhibit what it is seeking to achieve (hazard risks), enhance that aim (opportunity risks), or create uncertainty about the outcomes (control risks).

1. Risk definition

The Oxford English Dictionary definition of risk is as follows: '*a chance or possibility of danger, loss, injury or other adverse consequences*' and the definition of at risk is 'exposed to danger'. In this context, risk is used to signify negative consequences. However, taking a risk can also result in a positive outcome. A third possibility is that risk is related to uncertainty of outcome.

For the purposes of this discussion, *risk* is defined as "a condition in which there exists an exposure to adversity." In addition, there is an expectation of what the outcome should look like. Therefore, **risk** is defined here as follows: a condition in which there exists a possibility of deviation from a desired outcome that is expected or hoped for.

Potential risks that might occur in the future are not excluded. In addition, we do not limit the range of risk to circumstances in the external environment. Many crises in the economy and the financial services industry happen because of problems within organizations. These often have to do with problems in the human resource area, which belong in the realm of the behavioral sciences.

[1] Henri Fayol, *General and Industrial Management,* New York: Pitman, 1949.

The term *risk* is linked to the possibility of deviation. This means that the possibility of risk can be expressed as a probability, ranging from 0 to 100 percent. Therefore, the probability is neither impossible nor definite.

This definition does not require that the probability be quantified, only that it must exist. The degree of risk may not be measurable, for whatever reason, but the probability of the adverse outcome must be between 0 and 100 percent.

Another key element of the definition is the "deviation from a desired outcome that is expected or hoped for." The definition does not say how such an undesirable deviation is defined. There are many ways of building expectations. By projecting historical data into the future, we build expectations. This pattern of behavior can be observed in our everyday lives. Another way of building expectations is to forecast by using information directed toward the future, not by looking back. The definition of *expectations* is absolutely key in the concept of risk, as it is used to define the benchmark. Any misconception of the expectations will distort the measurement of risk substantially.

Many definitions of risk include the term *adverse deviation* to express the negative dimension of the expected or hoped-for outcome. We do not agree with this limitation, which implies that risk exists only with adverse deviations, which must be negative and thus are linked to losses. Such a restriction would implicitly exclude any positive connotations from the concept of risk. We believe that risk has two sides, which both have to be included in the definition, and that risk itself has no dimension, negative or positive.

2. Degree of risk

Risk itself does not say anything about the dimension of measurement. How can we express that a certain event or condition carries more or less risk than another? Most definitions link the degree of risk with the likelihood of occurrence. We intuitively consider events with a higher likelihood of occurrence to be riskier than those with a lower likelihood. This intuitive perception fits well with our definition of the term risk. Most definitions regard a higher likelihood of loss to be riskier than a lower likelihood.

If risk is defined as the possibility of a deviation from a desired outcome that is expected or hoped for, the degree of risk is expressed by the likelihood of deviation from the desired outcome.

The expected value of a loss or profit in a given situation is the likelihood of the deviation multiplied by the amount of the potential loss or profit. If the money at risk is $100 and the likelihood of a loss is 10 percent, the expected value of the loss is $10. If the money at risk is $50 and the likelihood of a loss is 20 percent, the expected value of the loss is still $10. The same calculation applies to a profit situation. This separation of

likelihood and value impact is very important, but we do not always consider this when we talk about more or less risk.

Frequently, persons who sit on supervisory committees (e.g., board members and trustees of endowment institutions and other organizations) have to make decisions with long-ranging financial impact but have inadequate backgrounds and training to do so. Organizational structures and processes are rarely set up to support risk management, as these structures are usually adopted from the operational areas.

Banks and other regulated financial institutions have been forced by government regulations and industry self-regulating bodies to develop the culture, infrastructure, and organizational processes and structures for adequate risk management. Risk management has become a non-delegable part of top management's function and thus a non-delegable responsibility and liability. Driven by law, the financial sector has developed over the past years strategies, culture, and considerable technical and management know-how relating to risk management, which represents a competitive advantage against the manufacturing and insurance sectors.

3. Risk management

Risk management is basically a scientific approach to the problem of managing the pure risks faced by individuals and institutions. The concept of risk management evolved from corporate insurance management and has as its focal point the possibility of accidental losses to the assets and income of the organization.

Risk is everywhere and derives directly from unpredictability. The process of identifying, assessing and managing risks brings any business full circle back to its strategic objectives: for it will be clear that not everything can be controlled. The local consequences of events on a global scale, such as terrorism, pandemics and credit crunches, are likely to be unpredictable. However, they can also include the creation of new and valuable opportunities.

Those who carry the responsibility for risk management (among whom the insurance case is only one example) are called *risk managers.* The term *risk management* is a recent creation, but the actual practice of risk management is as old as civilization itself.

Definition of **risk management:** In a broad sense, the process of protecting one's person or organization intact in terms of assets and income. In the narrow sense, it is the managerial function of business, using a scientific approach to dealing with risk. As such, it is based on a distinct philosophy and follows a well-defined sequence of steps.

4. Types of risks

Risks can be classified according to the nature of the attributes of the risk, such as timescale for impact, and the nature of the impact and/or likely magnitude of the risk. They can also be classified according to the timescale of impact after the event occurs. The source of the risk can also be used as the basis of classification. In this case, a risk may be classified according to its origin, such as counterparty or credit risk.

A further way of classifying risks is to consider the nature of the impact. Some risks can cause detriment to the finances of the organization, whereas others will have an impact on the activities or the infrastructure. Further, risks may have an impact on the reputation of the organization or on its status and the way it is perceived in the marketplace.

Individual organizations will decide on the risk classification system that suits them best, depending on the nature of the organization and its activities. Also, many risk management standards and frameworks suggest a specific risk classification system. If the organization adopts one of these standards, then it will tend to follow the classification system recommended.

The risk classification system that is selected should be fully relevant to the organization concerned. There is no universal classification system that fulfils the requirements of all organizations. It is likely that each risk will need to be classified in several ways in order to clearly understand its potential impact.

Risk may have positive or negative outcomes or may simply result in uncertainty. Therefore, risks may be considered to be related to an opportunity or a loss or the presence of uncertainty for an organization. Every risk has its own characteristics that require particular management or analysis. Risks can be divided into three categories:

- hazard (or pure) risks;
- control (or uncertainty) risks;
- opportunity (or speculative) risks.

There are certain risk events that can only result in negative outcomes. These risks are ***hazard risks*** or pure risks, and these may be thought of as operational or insurable risks. In general, organizations will have a tolerance of hazard risks and these need to be managed within the levels of tolerance of the organization. A good example of a hazard risk faced by many organizations is that of theft.

The application of risk management tools and techniques to the management of hazard risks is the best and longest-established branch of risk management. Hazard risks are associated with a source of potential harm or a situation with the potential to undermine objectives in a negative way. Hazard risks are the most common risks associated with organizational risk management, including occupational health and safety programmes.

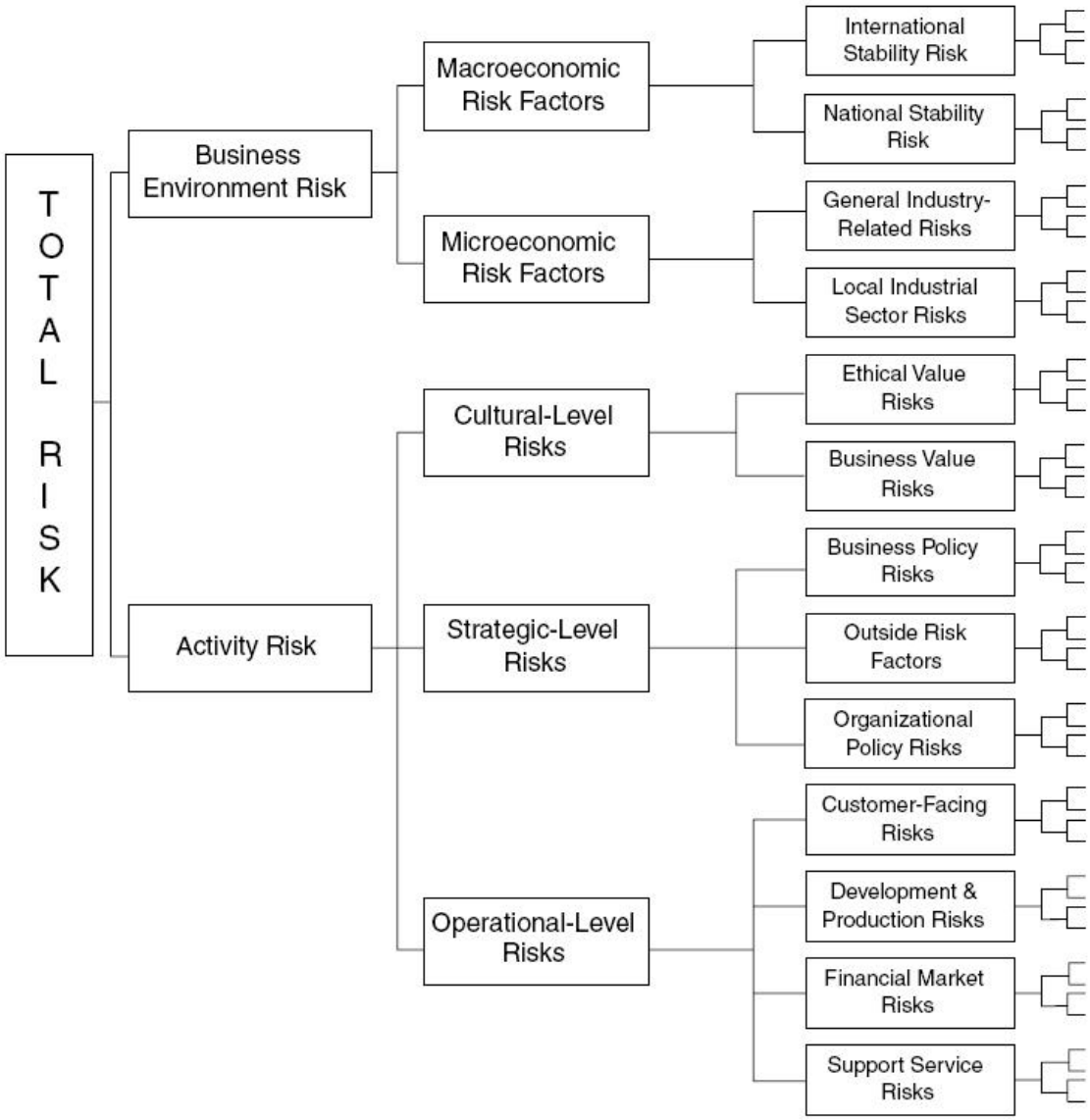

Fig.1 Risk Reference Matrix

There are certain risks that give rise to uncertainty about the outcome of a situation. These can be described as ***control risks*** and are frequently associated with *project management*. In these circumstances, it is known that the events will occur, but the precise consequences of those events are difficult to predict and control. Therefore, the approach is based on minimizing the potential consequences of these events. In general, organizations will have an aversion to control risks. Uncertainties can be associated with the benefits that the project produces, as well as uncertainty about the delivery of the project on *time*, within *budget* and to *specification*. The management of control risks will often be undertaken in order to ensure that the outcome from the business activities falls within the desired range.

At the same time, organizations deliberately take risks, especially marketplace or commercial risks, in order to achieve a positive return. These

can be considered as ***opportunity or speculative risks***, and an organization will have a specific appetite for investment in such risks.

There are two main aspects associated with opportunity risks. There are risks/dangers associated with taking an opportunity, but there are also risks associated with not taking the opportunity. Opportunity risks may not be visible or physically apparent, and they are often financial in nature. Although opportunity risks are taken with the intention of having a positive outcome, this is not guaranteed. Opportunity risks for small businesses include moving a business to a new location, acquiring new property, expanding a business and diversifying into new products.

Risk management provides a framework for organizations to deal with and to react to uncertainty. Whilst it acknowledges that nothing in life is certain, the modern practice of risk management is a systematic and comprehensive approach, drawing on transferable tools and techniques. These basic principles are sector-independent and should improve business resilience, increase predictability and contribute to improved returns.

5. Risk description

In order to fully understand a risk, a detailed description is necessary so that a common understanding of the risk can be identified and ownership/responsibilities may be clearly understood.

The next example provides information on the range of information that must be recorded to fully understand a risk. The list of information presented is most applicable to hazard risks and the list will need to be modified to provide a full description of control or opportunity risks.

So that the correct range of information can be collected about each risk, the distinction between hazard, control and opportunity risks needs to be clearly understood.

Example of ***risk description***:

- Name or title of risk
- Statement of risk, including scope of risk and details of possible events and dependencies
- Nature of risk, including details of the risk classification and timescale of potential impact
- Stakeholders in the risk, both internal and external
- Risk attitude, appetite, tolerance or limits for the risk
- Likelihood and magnitude of event and consequences should the risk materialize at current/residual level
- Control standard required or target level of risk
- Incident and loss experience
- Existing control mechanisms and activities
- Responsibility for developing risk strategy and policy
- Potential for risk improvement and level of confidence in existing controls

- Risk improvement recommendations and deadlines for implementation
- Responsibility for implementing improvements
- Responsibility for auditing risk compliance

6. Attitudes towards risk

Different organizations will have different attitudes to risk. Some organizations may be considered to be risk averse, whilst other organizations will be risk aggressive. To some extent, the attitude of the organization to risk will depend on the sector and the nature and maturity of the marketplace within which it operates, as well as the attitude of the individual board members.

Risks cannot be considered outside the context that gave rise to the risks. It may appear that an organization is being risk aggressive, when in fact, the board has decided that there is an opportunity that should not be missed. However, the fact that the opportunity is high risk may not have been fully considered.

One of the major contributions from successful risk management is to ensure that strategic decisions that appear to be high risk are actually taken with all of the information available. Improvement in the robustness of decision-making processes is one of the key benefits of risk management.

7. Risk management activities

Risk management is a process that can be divided into several stages, described as identifying, analyzing, evaluating, treating, monitoring and reviewing risk. This provides a clear distinction between the risk management process and the framework that supports this process. Descriptions of the risk management process together with the risk management framework are required in order to produce a comprehensive risk management standard.

There are a number of options when responding to hazard risks. These are often represented as the 4Ts of hazard risk management, and these risk response options are:

- tolerate;
- treat;
- transfer;
- terminate.

8. Risk likelihood and magnitude

Risk likelihood and magnitude are best demonstrated using a risk map, sometimes referred to as a ***risk matrix***. Risk maps can be produced in many formats. Whatever format is used for a risk map, it is a very valuable tool for the risk management practitioner. The basic style of risk map plots the likelihood of an event against the magnitude or impact should the event materialize.

Figure 2 is an illustration of a simple risk matrix, sometimes referred to as a heat map. This is a commonly used method of illustrating risk likelihood and the magnitude (or severity) of the event should the risk materialize. The use of the risk matrix to illustrate risk likelihood and magnitude is a fundamentally important risk management tool. The risk matrix can be used to plot the nature of individual risks, so that the organization can decide whether the risk is acceptable and within the risk appetite and/or risk capacity of the organization.

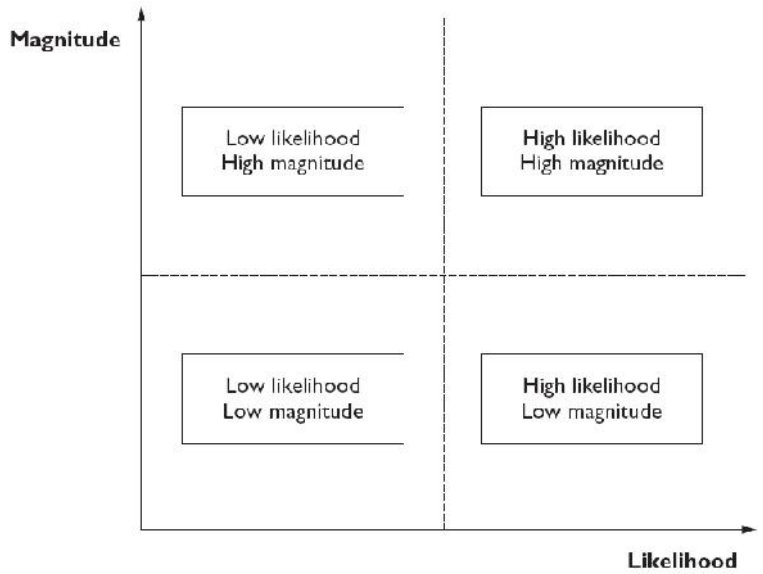

Fig.2 Risk likelihood and magnitude

The horizontal axis is used to represent likelihood. The term likelihood is used rather than frequency, because the word frequency implies that events will definitely occur and the map is registering how often these events take place. Likelihood is a broader word that includes frequency, but also refers to the chances of an unlikely event happening. However, in risk management literature, the word probability will often be used to describe the likelihood of a risk materializing.

The vertical axis is used to indicate magnitude. The word magnitude is used rather than severity, so that the same style of risk map can be used to illustrate hazard, control and opportunity risks. Severity implies that the event is undesirable and is, therefore, related to hazard risks.

However, the more important consideration for risk managers is not the magnitude of the event, but the impact or consequences.

For example, a large fire could occur that completely destroys a warehouse of a distribution and logistics company. Although the magnitude of the event may be large, if the company has produced plans to cope with such an event, the impact on the overall business may be much less than would otherwise be anticipated.

9. Risk likelihood and impact

Large organizations frequently make use of a risk matrix as a means of summarizing their risk profile. The risk matrix is very useful and can be used for a range of applications. It can also be used to identify the type of risk response that is most likely to be employed. Figure 3 illustrates the occasions when each of the responses tolerate, treat, transfer and terminate are most likely to be employed for the current level of risk.

Impact is not the same as magnitude, because a risk may have a high magnitude in terms of the size of the event, but the impact may be smaller. For example, a road transport company may suffer the complete loss of one of its vehicles but, depending on the exact circumstances, this may have a very small overall impact on the business. This will be especially true if the company did not have sufficient work to fully utilize the type of vehicle involved in the loss.

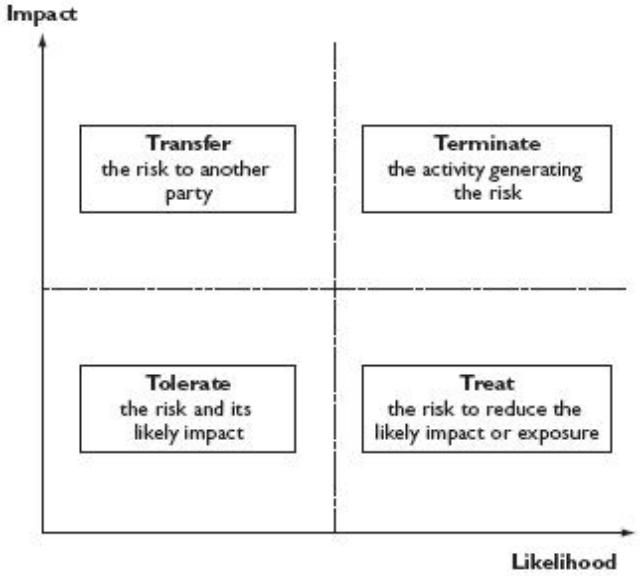

Fig. 3 Risk matrix and the 4Ts of hazard management

When assessing a risk for the first time you should assume there are no controls already in place. The subsequent two assessments are completed with:

1) those controls already in place and

2) with any additional controls needed to reduce the risk further.

The assessor should assign values for the identified 'likelihood' of occurrence (A) and the severity of the 'Impact' (B). By multiplying 'A' and 'B' together you get the rating score, which gives an indication of how important the risk is. The thick black line is the "line of tolerance". Those risks that are plotted above the line (score 10 – 25) are "out of tolerance" and should be referred for further consideration.

LIKELIHOOD (A)						
	Very Likely 5	**5**	**10**	**15**	**20**	**25**
	Likely 4	**4**	**8**	**12**	**16**	**20**
	Feasible 3	**3**	**6**	**9**	**12**	**15**
	Slight 2	**2**	**4**	**6**	**8**	**10**
	Very unlikely 1	**1**	**2**	**3**	**4**	**5**
		Insignificant 1	**Minor** 2	**Significant** 3	**Major** 4	**Critical** 5
	IMPACT (B)					

Fig. 3 Sample Risk Assessment Matrix:
Green = Low risk, Yellow = Moderate Risk, Amber = High Risk, Red = Extremely High risk

Likelihood of Occurrence (A)		**Severity of Impact (B)**	
1- Very unlikely (hasn't occurred before)		1 - Insignificant (have no effect)	
2 - Slight	(rarely occurs)	2 - Minor	(little effect)
3 - Feasible	(possible, but not common)	3 - Significant	(may pose a problem)
4 - Likely again)	(has before, will	4 - Major	(Will pose a problem)
5 - Very Likely	(occurs frequently)	5 - Critical	(Immediate action required)

E - *Extremely High Risk* - Activities in this category contain unacceptable levels of risk, including catastrophic and critical injuries that are highly likely to occur. Organizations should consider whether they should eliminate or modify activities that still have an "E" rating after applying all reasonable risk management strategies.

H - *High Risk* - Activities in this category contain potentially serious risks that are likely to occur. Application of proactive risk management strategies to reduce the risk is advised. Organizations should consider ways to modify or eliminate unacceptable risks.

M - *Moderate Risk* - Activities in this category contain some level of risk that is unlikely to occur. Organizations should consider what can be done to manage the risk to prevent any negative outcomes.

L - *Low Risk* - Activities in this category contain minimal risks and are unlikely to occur. Organizations can proceed with these activities as planned.

10. Risk and uncertainty

Risk is sometimes defined as uncertainty of outcomes. This is a somewhat technical, but nevertheless useful definition and it is particularly applicable to the management of control risks. Control risks are the most difficult to identify and define, but are often associated with projects. The overall intention of a project is to deliver the desired outcomes on time, within budget and to specification.

It would be unrealistic for the project manager to assume that only adverse aspects of the ground conditions will be discovered. Likewise, it would be unwise for the project manager to assume that conditions will be better than he has been advised, just because he wants that to be the case.

Because control risks cause uncertainty, it may be considered that an organization will have an aversion to these risks. Perhaps, the real aversion is to the potential variability in outcomes. A certain level of deviation from the project plan can be tolerated, but it must not be too great. Tolerance in relation to control risks can be considered to have the same meaning as in the manufacture of engineering components, where the components must be of a certain size, within acceptable tolerance limits.

11. Business continuity planning

There has been considerable interest in the subjects of business continuity planning (BCP) and disaster recovery planning (DRP) in recent times. This illustrates the importance of BCP as an integral part of risk management. This increased concern has been reinforced by the potential for major disruption posed by extreme weather events, terrorist attacks, civil emergencies and the fear of a fl u pandemic.

In simple terms, BCP is how an organization prepares for future incidents that could jeopardize its existence. The range of incidents that should be covered will include everything from local events like fires through to regional disruption such as earthquakes or national security incidents and extend to international events like terrorism and pandemics.

British Standard BS 31100 defines business continuity planning as a ‘holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response to

safeguard the interests of its key stakeholders, reputation, brand and value-creating activities'.

In case of a serious incident such as loss of access to premises or failure of a major part of an organization, it is important to have in place a well defined, documented and tested disaster recovery plan. Such plans inevitably focus on recovery of access to IT systems and data, but also commonly cover the provision of alternative premises (if needed) and other facilities, as well as setting out plans for communications with employees and with other stakeholders such as suppliers, customers and the media at a time of crisis.

Business continuity plans build upon this by setting out longer-term plans for restoration of 'business as usual' in the immediate aftermath of a disaster. A business continuity plan is an important part of reducing the impact of a hazard incident. The plan should include arrangements for reducing the damage caused during the incident and containing the cost of recovery from it.

Disaster recovery plans are a particular component of business continuity planning. If a computer system fails to operate correctly or data has become corrupted, the organization will need emergency procedures to ensure that the data can be recovered and/or ensure that the organization continues in existence.

For a printing firm IT systems are fundamental to the operation of the company, because the computer systems process orders, schedule printing and manage invoicing. For such a company, it may be appropriate to arrange for a mobile emergency computer facility to be available in case of major IT failure. If this decision is taken, a contract should be set up with an outside company for a duplicate computer to be delivered in a trailer to the premises of the company. The duplicate computer would then be connected and the operations would be controlled from the duplicate computer in the trailer. The success of this arrangement will depend on the availability of information from backup disks that should be produced at least once per day and possibly several times per day.

The overriding principles appropriate to successful business continuity planning are that the business continuity plan (BCP) should be:

- comprehensive;
- cost-effective;
- practical;
- effective;
- maintained;
- practiced.

It is important that the BCP should cover all the operations and premises of the organization to ensure that the plan can facilitate a complete resumption of normal business operations. It is also important that the plan is cost-effective and proportionate to the risk exposures.

The BCP must be practical and easily understood by staff and others who are involved in the execution of the plan. Overall, the BCP must be effective in that it will recognize the urgency of certain business components or functions and identify responsibilities for ensuring timely resumption of normal work.

In order to guarantee that the BCP will be effective, it needs to be tested, maintained and practiced. All members of staff need to be familiar with the intended operation of the plan and training will need to be provided. The lessons learnt during testing and practice of the business recovery plan should be incorporated into the plan so that it becomes more effective.

Testing of business continuity plans is an essential component of ensuring that they will be appropriate and effective. However, testing of plans can be time-consuming and, in some circumstances, disruptive and costly. Even the simple example of a fi re evacuation drill from a building illustrates that the testing of procedures is inevitably going to disrupt normal routine operations.

There is an obvious link between BCP and enterprise risk management (ERM). ERM is concerned with the risks facing the whole organization and BCP takes an approach that business continuity arrangements should be in place. The BCP approach is to look at the continuity of operations across the whole organization. Ensuring continuity is obviously part of an ERM approach. It should therefore be considered that BCP is part of ERM, but it is not the whole of ERM activity. Nevertheless, there is a strong similarity in approach and the business continuity and disaster recovery activities should take place within the context of a broader ERM initiative, as appropriate.

Continuation of core business processes is also the basis of business continuity planning. The difference in emphasis is that ERM seeks to identify the risks that could impact the core processes. BCP seeks to identify the critical business functions that need to be maintained in order to achieve continuation of the business. The approaches are complementary and there is a good deal of similarity between BCP and this style of ERM.

BIBLIOGRAPHY

1. R. Gallati, **"**Risk management and capital adequacy", McGraw-Hill Companies, 2003
2. P. Hopkin, "Fundamentals of risk management", The Institute of Risk Management, 2010
3. Ministerul Finanțelor Publice, Metodologie de implementare a standardului de control intern "Managementul riscurilor", 2007