LUISS

Department
of Economics and Finance: Major in Management

Course of Management

Changes in entrepreneurial management: tackling risk management and business resilience

Prof. Francesca Capo
SUPERVISOR

Francesco Culcasi – 225271
CANDIDATE

Academic year 2019/2020

INDEX

Introduction

The era in which we live is characterized by numerous challenges that, in an increasingly insistent and continuous manner, call our society and our organizations to comparison; what we would have once called transient crises or extraordinary events, are now on the agenda. To demonstrate this, numerous examples can be given, such as: "natural disasters, terrorism, economic recession, mass migration, cyber threats, new technologies [...] and a number of other socio-political and economic trends. Operating under stable conditions is a utopia: ours has become an increasingly unpredictable environment; it is constantly evolving, offering opportunities and, at the same time, threatening numerous realities. Today, managing uncertainty and the unexpected represents a real challenge for many organizations.

The management of the company is carried out in compliance with the strategy decided by the managers and aimed at achieving the pre-established objectives. The strategy defines the fundamental paths of long-term management, decided on the basis of an in-depth assessment of the future evolution of the market and the environment in which the company will operate. The strategy is implemented through the implementation of plans concerning both the company and the business units, when present, and the different areas of management and support systems.

Strategy, Plans and Programs are aimed at guiding the management of the company in order to achieve long, medium- and short-term objectives. As a whole, they define a rather complex and articulated model which, in principle, should allow the company to operate on the market in such a way as to achieve its institutional goal: to produce satisfactory current economic results over time, assessed in relation to their ability to ensure responses in line with the expectations of its stakeholders. In order to prevent the pursuit of the objectives of plans and programs from being prevented by the occurrence of risks that can be identified and assessed ex-ante, companies make use of Risk Management, through which they decide how to deal with them. More specifically, after having identified and assessed the risks to which

it is exposed, the company decides on its "Risk Appetite", i.e. which of these risks it considers convenient to face directly, i.e. to take on its own, using the resources available, and which to transfer to third parties using insurance or other forms of transfer. In view of the above, it is clear that the subject of Risk Management is predictable risks, given that only such risks can be identified, assessed and subject to treatment. It is clear from the above that the logic that supports Risk Management is based on a "reactive approach", given that the treatment of the risks it envisages can only be carried out after the risks have been identified and assessed.

In reality, the pursuit of the Strategy through the implementation of the Plans and Programs, despite the valid recourse to risk management, can lead to different results from those set as objectives. This is due to the more or less significant differences that can be ascertained ex-post between the forecasts underlying the plans and programs and the actual performance of the market and the company's reference environment. These differences are determined by two orders of reasons: errors made when making the forecasts and unforeseen and unforeseeable events that occurred after their preparation.

The companies, following the occurrence of the first manifestations of these events, in order to contain their consequences, proceed to review and update the plans and programs, relying on the expectation that their effects may be reduced within a certain time, reasonably contained. However, if these expectations are not confirmed, as is the case in a large number of cases, and the company is unable to cope with unforeseen and unforeseeable risks, it would face a difficult and worrying situation. In particular, if it had to underestimate the extent of these adverse events, which, due to their significant economic consequences, may lead to a deterioration of its competitive position in the market, with consequent significant effects on its ability to create value, it could see its survival threatened. From what has been stated above, it emerges the need for the company to equip itself with a system that allows it to deal with unpredictable risks and in particular with those among them that, because of their scale, may threaten its survival, such as a fire of considerable size, a flood, an ostentatious attack or a pandemic in the society. The recourse to the use of Business Continuity Planning allows the company to outline the processes and actions that it will have to put in place to deal with unforeseen

disastrous events. Events that will be able to concern the processes of management, the activities, the human resources, the relationships of the enterprise with the external partners and a lot other still.

After having analyzed all the factors of risk that the company face and also the most used and efficient plans to overcome disasters, I decided to go into the theory which explains how companies adapt to changes and in particular the Business Resilience.

The term resilience has been used at the organizational level to describe the intrinsic characteristics of organizations that are able to respond faster to change, recover faster from unexpected events, and develop different ways to be efficient (Sutcliffe and Vogus, 2003).

In turbulent, dynamic and ever-changing market environments, only flexible, agile and dynamic organizations will be able to thrive. Often, in fact, companies must be able to go beyond mere survival, developing in complex, uncertain and threatening environments.

Unstable environments create frequent challenges, but even relatively stable markets are subject to shocks or periods of turbulence. Often these events are considered negative, but as Sutcliffe and Vogus explain, resilient organizations are able to make positive adjustments under difficult conditions. Resilient companies thrive because they have faced and overcome complicated challenges and made great efforts to increase their strategic flexibility - understood as the ability to change strategic perspectives in the short term and at low cost.

Resilience is therefore seen as an essential feature for an organization (and its members) to prevent and address various types of adversity.

CHAPTER 1: The concept of business risk

In the last decades, there has been an increasing in variability in the economic trends in world market which has made necessary for companies to have a risk management system that can support them in order to minimize the uncertainty.

Companies are constantly facing an increasing number and variety of risks and there is a growing recognition that risk must be managed taking into account the whole organization. All organizations are required to take a more practical approach to risk management that goes beyond statistics and analytics to future scenarios and planning.

The business risk is closely linked to the phenomena that fall within the scope of the sphere of the company and the changing relationships that are established between the company and the environment in which it operates. We can define it as the possibility that they occur and that they are affect the company, events that affect the economic performance of the business production activity for the market .

The genesis of business risk can be linked to the divergence between the distinctive features of the external environment and those of the organizational and operational structures of companies: while the environment is constantly evolving, the structures tend to be so rigid and resistant to change that they are not suitable for efficient and effective production activities.

During its existence, the company finds itself continuously interacting with the market and the environment in which it operates: it finds itself in a highly changing economic context. In the last few decades in particular, the company has witnessed an increase in the number and extent of the risks it faces, on the one hand, and an increase in its sensitivity to risk, on the other. The factors that have contributed to the increase in uncertainty and therefore the risks that the company is called upon to manage and face are:

- The increasing globalization of markets has led to an increase in the number, size and complexity of the risks that the company has had to face over time;
- The increased pressure on performance, resulting from the increased efficiency of regulated financial markets;

- The increase in pressure on companies, and in particular those that use regulated financial markets to finance themselves;
- The increase in the regulation of Corporate Governance, which requires companies to base their administration and management on the principles of transparency, integrity and accountability;
- The development of production technologies which, on the one hand, has enabled companies to create highly flexible integrated production systems but, on the other hand, has made these systems highly vulnerable;
- The development of information and telematic technologies, which has contributed to profound changes in the structure of business processes, concerning both basic activities and production and marketing activities;
- The increase in financial risks to which the company is exposed;
- The increase in the company's liability risks, as a result of the increase in the control of the different stakeholders and, more generally, the company's control over the company

These factors, both internal and external to the enterprise, contribute to the formation of the so-called enterprise risk system, which includes all the possible causes of the vulnerability to which the business activity is subject. The risk system as a whole includes both general and specific risks. The concept of general risk refers us to the corporate definition of risk: the risk is identified in the risk that the company is forced to bear following the possible occurrence of events that fall within its orbit; it is the set of possible positive and negative effects of a risky event on the situation.
economic, financial and asset situation of the company. The specific risks, on the other hand, are those
related to certain aspects of the business activity.

In the current market context, characterized by a widespread climate of uncertainty and constant volatility, companies are called to review their risk management policies, considering the evolution of the concept of risk management. In fact, it is necessary to build an integrated approach that involves all the fundamental aspects

of a company's life. Risk management, used to formulate risk-weighted strategies for the risk taken, must evolve towards an integrated approach with all business processes and that considers risk not only as a threat, but also as a source of opportunity and competitive advantage. The integrated approach required to risk management is that of Enterprise Risk Management systems, a framework that involves in an interactive and widespread way the different business functions according to overall managed processes

Companies therefore have started to consider the concept of risk as a result of different problematics that have influenced the markets. Has been found that its management can prevent the damage it can cause and, therefore, different analysis have been developed in order to forecast ex-ante the impact of those risks. It was also seen that companies that understand their risks better than their competitors are in a very powerful position because they are able to control it and to gain competitive advantage. Greater knowledge of risks provides the ability to deal with risk that intimidates competitors, to handle adversity better than competitors, and to manage risk at the lowest costs (Davenport and Bradley, 2000)

Although there are many studies related to the risk, economists have not yet come to give an unambiguous definition to the term. One problem that comes up against is the wide range of risks that can be found and analyzed, and this also partly justifies the inability to reach a common definition.

Every activity and every reality, in fact, can be subject to risk; the risk in investments in securities, the risk of pollution, the insurance risk are just a few examples.

Here we will aim to focus only on business risks, i.e. all those that undermine the activity of companies by creating potential problems that they will have to mitigate in order to prevent the achievement of their mission.

Even limited to this category, however, there is no single definition because, although it is a distinct class, it is also composed of multiple species. In fact, the business risks are many and different, so even here it can be complex to find a definition.

The importance of risk in entrepreneurial activity has been strongly emphasised and has been crucial since the 1990s. Many regulatory interventions have, in fact, entailed the obligation for companies to equip themselves with risk containment and internal control procedures, bringing to the attention of all companies the need to allocate adequate resources to the management of uncertainty. However, numerous contributions by authors who, long before the 1990s, focused their studies on the notion of risk are worthy of note.

- The American economist F.H. Knight was one of the main promoters of the distinction between risk and uncertainty. Uncertainty can occur in both measurable and non-measurable forms. In its measurable sense, uncertainty coincides with risk. Risk becomes apparent when events occur that are considered repeatable and therefore susceptible to statistical estimates. Knight's view is part of the so-called objectivistic current, which attributes to risk the connotations of objectivity and measurability;
- In contrast to Knight's interpretation, there is the subjective current, according to which the distinction between risk and uncertainty, is to be found in the nature of the events. De Finetti and Savage , exponents of this current, emphasize that the difference between risk and uncertainty is to be found in the knowledge of the events by the different actors on the basis of the information available to them, since the determination of each future scenario represents a common problem for both situations;
- For the German school, Friedrich Leitner attributed a single negative meaning to risk, calling it a threat to the company because it represents "the danger of the failure of an economic fact";
- For the Italian school, Corsani departed from Leitner's vision by defining risk as the differential between the expected and estimated results of the operator and those actually observed. Therefore, from this point of view, the risk can be both favorable and unfavorable, since the variation between expected and actual results can be both positive and negative;
- Finally, the definition of a more technical nature is the one offered by Segal, which claims that the risk is characterized by three fundamental aspects:

1. Risk is uncertainty: a good way to consider risk is that it occurs whenever there is less than 100% probability that an event will occur exactly as expected. In this perspective, any circumstance can lead to uncertainty and thus expose the risk.
2. Risk also includes "upward volatility": consider risk as the possibility that results may not be exactly the same as expected, but rather less or more than expected. Upward volatility' refers to all the chances of events occurring more positively than expected (upside risk), while downward volatility refers to all the chances of events occurring more negatively than expected (downside risk).
3. Risk is a deviation from expectations: the concept of loss linked to a risky event is incomplete, in the light of what has been said so far, as it excludes the concept of upward volatility and therefore a possible gain.

All of these theories show that there is no univocal definition but there are a number of elements that they have in common.

By contextualizing the risk in the company, it can be seen that it is in contrast to the opportunities. The latter are positive events, which can lead to changes in the plan set for the achievement of the objectives. Knowing how to exploit them is important for the manager, because it increases the value of the company. If it is easy to understand this, it is equally easy to recognize how risk management can lead to the ability to contain the destruction of value. For this reason, it is important to understand the right way to identify, measure, know and manage risk.

Two aspects can also be derived from the general definition of risk, namely quantitative and qualitative. As far as the qualitative risk is concerned, it can be inferred that the risk can lead to favorable variations (upside risk) and unfavorable variations. (downside risk). For the quantitative aspect, instead, the risk can be identified as a unit of measurement, that is the quantification of the expectation of loss. If typically, the concept of risk has a negative value, precisely because it has two sides, upside risk and down side risk, it becomes important to try to manage it in order to be able to take positive opportunities. In fact, risk is not only synonymous with loss, but can also be synonymous with extra-gain. The existence

of down-side risk, however, is crucial to define one of the fundamental concepts of finance: the higher the risk in business, the greater the potential financial reward is for the business owner. This explains the existence of trading activity on the market: in fact, we are constantly looking for something that, although it can have a high risk, allows us to give a higher remuneration than the alternatives. However, this aspect is strongly linked to the individual's risk aversion. In fact, there are risk averse and risk-loving individuals. The first ones are those who prefer something certain, even if it does not give much remuneration, because in them the fear of losing the invested capital prevails. The latter, on the other hand, are those in whom the desire for higher returns prevails rather than the fear of losing. These, in fact, prefer the riskier alternative between two alternatives that guarantee returns of different risks, if it is actually able to give a higher return.

The fact that the risk also has negative aspects does not mean that it should be totally eliminated, but neither does it mean that the consequences should be accepted without taking any action. Risk management thus becomes fundamental and requires understanding which risks to accept and how to manage them, which risks to eliminate and how to do so and which risks you can predict and how to govern them. All this requires the need to define a degree of risk tolerance, i.e. a range of volatility with respect to the target, which we are willing to accept.
Once we analyzed the “historical approach” to the difference’s definitions of business risks, we are going to see what are the factors that determine the risks.

1.1 Factors of risks: internal and external

There are many sources and factors that can both influence business decisions and act on uncertain events, determining their outcome and causing them to deviate from expected results. These are both external factors, and so not completely controllable and influenceable by the company, and internal factors which are directly manageable.

External factors

This category includes, first of all, natural phenomena: "the company operates in a natural environment even before the economic-social environment". (Riviezzo C., 2010:14). We are therefore referring to all those phenomena that are beyond man's control, that are difficult to predict and that can generate very considerable damage. They can derive both from physical phenomena, i.e. linked to the force of nature (atmospheric agents such as hail, lightning, drought, earthquakes, landslides and landslides, floods...), and biological phenomena, i.e. pathogens (parasites, bacteria, viruses) that can affect both production factors and people. Each company will be exposed to these risks in a more or less significant way, depending on the type of activity carried out. It is a fact that, despite the evolution of forecasting methodologies, the company is not able to fully control them.

Secondly, all those factors linked to the economic and social environment in which the company operates can be identified. The environment represents all that is external, affects the company and determines its existence" (Riviezzo C., 2010:17). It is possible to distinguish between:

-general environment: it includes all those factors that are broadly and generically related to the economic, political and social context in which the company is inserted. It refers, for example, to movements in macroeconomic variables (inflation, distribution of wealth, etc.), changes in the financial market (interest rates, exchange rates, etc.), regulatory interventions (the enactment of new more or less restrictive laws or rules governing the relationships between the various parties operating in the company);

-specific market of the company: this refers to all those factors that affect the conditions of the markets in which the company carries out all the operations essential and necessary to its existence and the achievement of the company's objectives. We look in particular at the outlet market in which the company offers its products and services, with the aim of better satisfying its target customers. Risk factors in this case may be variations in the number and type of competitors; changes in consumer confidence, in their tastes, in their behavior, in fashion; technological advances and in research and development, or even the launch of new products and variations in pricing policies.

Internal factors

This second category includes all those factors linked to the specific operational choices adopted by the company management, it therefore refers to everything that has to do with the specific operational choices made by the company's management, in particular organizational, financial, economic and strategic policies which, in line with the company culture and corporate objectives, are adopted on a daily basis in the performance of normal business activities.

Organizational policies concern, for example, "the rational allocation of all the company's existing or new resources" (Riviezzo C., 2010:17), then the management of resources, the selection and organisation of personnel or the information system.

Financial policies, on the other hand, concern the financial structure and therefore all the choices on the sources of financing from which to draw on the capital invested: the self-financing choices, dividend policy, ownership structure, debt ratio, any financial instruments to be used, investment or financing opportunities.

Economic policies, on the other hand, concern the commercial aspect, i.e. all the characteristic operations of the company, linked to its core business. We therefore refer to the operations that are carried out both on the input market, i.e. the acquisition of production factors, supply relationships, cost structure, payment of debts; and on the output market, i.e. the distribution channels, the structure of the outlet market, the conditions for the settlement of receivables.

Finally, strategic policies concern market positioning strategies, promotional activities, pricing strategies, the study of competitors' behavior and how to react to changes in demand. This then refers to all those strategies that are adopted by the company to be able to stay on the market and be competitive.

1.2 Types of business risks

In order to better understand and manage risks, they usually are classified in a practical approach, in fact, for the purposes of the daily management of business activities, the Casualty Actuarial Society (CAS) states that it is possible to divide business risks into macro-categories, within which they can be further subdivided: pure risks (hazard), financial, strategic and operational risks.

Font: marketing91.com

1. FINANCIAL RISK are associated with potential losses resulting from changes in financial markets. It is possible to distinguish between internal financial risks, those that depend on the financial structure choices made by management, or decisions regarding the sources of financial resources to cover the company's invested capital; and external risks, those that depend on the performance of the financial markets and any macroeconomic or financial variables. "They are conditioned by the ability of the company both to achieve a balanced ratio between equity and debt and to optimize the availability of liquid resources" (Prandi P). These risks may affect companies that use long-term indebtedness, in relation to possible changes in interest rates; or companies listed on regulated markets that are therefore exposed to the volatility of securities in relation to market conditions; or companies that are unlisted and without financial instruments, but which, for example, have significant import/export relations with foreign countries and must therefore monitor exchange rate trends.

The risks that are included in this categories are:

- interest rate risk. It is represented by the uncertainty associated with the trend in interest rates: significant fluctuations in interest rates can lead to large variations in the cost of financing sources and therefore in the structure of liabilities.

- exchange rate risk. It derives from possible adverse fluctuations in exchange rates between two currencies, which have an impact on the value of transactions carried out in currencies other than the national currency. These fluctuations may be due both to the amount of transactions carried out, whether they are purchases and sales of goods and services or receivables and payables in foreign currency, and to the economic, cultural and political situation of the foreign country with which exchanges are made. These are unexpected fluctuations that the company is unable to predict and control directly; however, it has the possibility of limiting the economic and financial effects of such risks through adjustments to commercial, production and purchasing strategies, or through trading in ad hoc derivative instruments.
- credit risk. This category of risk considers the potential losses that the company may incur in relation to the counterparty's inability to meet its obligations. Reference is made, in the case of companies of a non-financial nature, to two fundamental aspects. The first is linked to a reduction in the creditworthiness of the counterparty in the eyes of the banks, which could worsen its economic and financial conditions and affect its ability to meet its obligations on a regular basis. The second aspect, on the other hand, is linked to the customer's actual inability to fulfil: the financial loss generated by the actual non-payment is therefore identified (there is essentially a loss on receivables).
- the risk of inflation. It depends on fluctuations in the inflation rate in relation to changes in the economic policy choices made by the country in which the company is located. It is therefore a risk that cannot be completely controlled by management, as it cannot directly affect the performance of macroeconomic variables; however, there is the possibility of providing transfer and hedging instruments also for this risk.
- liquidity risk. It manifests itself in a situation of difficulty due to time lags between income and expenditure that make it impossible to find liquid resources to meet maturing obligations in a timely and economic manner. This refers, for example, to the payment of financial liabilities or supply payables.
- the price risk of raw materials. This risk depends on fluctuations in the price of raw materials (commodities) needed in the company's characteristic processing and

transformation process, such as to jeopardize productivity and the ability to generate margins. What is assessed will be the impact of the price of the commodities used on production costs: it is in fact the cost of salt that is most affected by significant changes in raw material prices. If the latter also increase, the cost of sales increases, generating a decrease in the gross margin.

2. STRATEGIC RISKS depend on the degree of success of the company's highest level strategic choices. External and internal sources of randomness can affect these decisions, determining the positive or negative outcome of the strategies implemented; it is up to top management to consider these sources and take effective measures to anticipate and limit the potential harmful effects. These risks are therefore linked to the company's specific operations, the business objectives set and the choices made to achieve them, as well as changes in the business environment in which the company operates; they may depend, for example, on incorrect considerations in market positioning, poor responsiveness to changes in the operating environment, incorrect business decisions, inability and inadequacy in the timely implementation of strategies.

The category includes:

- counterparty risk. It is linked to the inability of the counterparty (e.g. the client) to fulfil its obligations, which arose before the final settlement of the transaction. This is a risk arising from mismatching between the initial contract and the actual behavior of the client, in relation to the timing and manner of performance.
- concentration risk. This is defined as "the risk arising from exposures to counterparties, groups of connected counterparties and counterparties in the same sector or exercising the same activity or belonging to the same geographical area" . This is essentially the risk that a company may incur in losses, even significant ones, in relation to large exposures to a single counterparty, a single company or a group of related companies, belonging to the same sector or geographical area, which are in a situation of difficulty or default.

- reputational risk. This is the risk of incurring a reduction in profits in relation to the negative perception of the company's image by those with whom it enters into relations, i.e. customers, suppliers, shareholders, investors, etc.. The image is a fundamental element for the company and rather delicate: wrong production, commercial or strategic decisions can have very negative consequences on the perception of reliability, quality and credibility of the company by external parties. For most companies, the perception by the market, customer loyalty, the image of excellence, the quality of products and services offered, are of vital importance for the success of the business and the achievement of business objectives. Damage to the image can therefore result in the following effects strongly negative both to business relationships and to the accessibility to the sources of funding.
- compliance risk. This is the risk arising from non-compliance with regulations, in the specific case of mandatory rules (laws or regulations) or self-regulation (statutes, self-regulatory codes). Such violations may result in judicial or administrative sanctions, significant financial losses and reputational damages. The management of such risk presupposes proactively addressing the complexity in which the company operates and therefore the development, by the specific compliance function, of risk management methodologies not only in a manner consistent with the company's strategies and operations, but also and above all in compliance with the specific regulations governing the company's activities.
- country risk. This is a type of risk that mainly affects companies that have relations with foreign countries. It is in fact the set of risks that derive from the economic, legislative, political and socio-cultural differences between the various countries. Significant differences in economic and technological development, political tensions, backward or less liberal regulations, can therefore represent significant obstacles to the success of commercial and financial relations between companies from different countries.

3. OPERATIONAL RISKS are pure risks that inevitably arise with the exercise of business activity as they are linked to the company's operations. The "New Basel II Accord "provides a definition of operational risks that can be applied in a general

way to all companies: they are "the risk of suffering losses resulting from inadequate or failing procedures, human resources and internal systems, or from external events". These are therefore the possible negative effects of uncertain events that may affect the company in relation to the mismatch between the resources available and the needs arising from management. These include, for example, human errors, inadequacy of systems, interruptions of activities, contractual failures, irregularities in accounting, errors in strategic planning, etc. Within this category, four different types of risks can be identified, depending on the sources that can determine them:

-human resources; these are possible losses resulting from negligence, inexperience, lack of preparation, misinformation and lack of updating of staff, as well as possible human errors, distractions, uninformed managerial decisions, unauthorized activities, violations of rules, incommunicability, internal tensions among staff. We therefore refer to damaging events resulting from lack of competence or integrity of persons within the company;

-information systems; these are the possible losses resulting from the lack of availability, accessibility and efficiency of information systems. The activity of the majority of companies is currently essential for technological and IT resources, both as regards production software, data collection and information on customers, suppliers and competitors, and the dissemination of information, both internally and externally. Damage often significant can therefore be caused, for example, by application programming errors, interruptions in the operation of systems, malfunctioning of information channels, lack of precision in the data collected or difficulty in accessing them, easy violation of databases by unauthorized parties; -internal processes; reference is made to damage resulting from the inadequacy of procedures, processes and internal controls, the obsolescence of plant and machinery, or the unavailability of resources or know-how required and necessary to the various processes. These are, for example, inconsistencies or errors in the definition of roles and responsibilities, errors in the formation and performance of procedures, accounting errors, wrong decisions regarding the risk management function itself.

-exogenous factors; this includes all random events linked to factors external to the company, which do not depend on it and therefore cannot be influenced by management decisions. This refers both to changes in the political, economic, legislative and cultural context and to criminal activities such as theft, fraud, terrorist attacks and natural disasters.

4. BUSINESS RISK This is the risk associated with the type of activity carried out. Contrary to the operational risk, which is linked to the company and is therefore an endogenous risk, the business risk is the typical risk of all companies that belong to the same sector and are, therefore, exogenous. They arise from external events caused by changes in the environment and competitive variations. Problems that arise when the company tries to create and maintain a competitive position (Lam, 2003).

Examples of this risk are the uncertainty of demand, technological development, business cyclicality, various distribution policies or changes in the number of competitors.

Cyclicality, for example, is the risk linked to the variability of the company's revenues in the economic situation. It depends on the sector to which it belongs.

It should not be confused with the seasonality of the business, which consists of the periods in which I produce and sell the product. It, precisely because it concerns revenues, also influences the whole pursuit of the company's objectives, therefore it is a variable to be considered.

After having identify the different kinds of risks and how to identify them, another fundamental analysis is the risk treatments. It basically consist in selecting and implementing the most suitable measures to modify the company's risk profile, in line with the objectives of the company and the risk manager.

In concrete terms, it is a the process of making decisions that have an impact on the risks previously analyzed, assessed and possibly integrated, and that allow the

effective and efficient functioning of the organization, as well as ensuring compliance with laws and regulations.

The way the risk is treated is ex ante or ex post.

Ex ante are all the risk treatments that can modify all the possible economic effect before they occur and are:

-risk avoidance consist in give up, if possible, to take a certain risk. The organization recognizes that other management measures are not appropriate to contain or are too onerous compared to the benefits of taking a particular category of risk. For this reason it has the right not to support projects that involve the assumption of risk, avoiding to incur in management solutions that are not suitable from a strategic point of view. For example, the decision not to invest in an activity very profitable but outside the core business but just as risky so that the company's risk appetite exceeds the maximum threshold set by management.

-risk reduction consists in minimizing the probability of occurrence and the impact of risky events through the adoption of prevention and protection techniques. Preventive measures consist of reducing the probability of occurrence of adverse scenarios and/or increasing the probability for positive scenarios. For example, it is estimated that an investment, e.g. a new wood processing plant, could be much more profitable if it was not located close to the river which often overflows and renders the plant unusable, if an expense for raising the embankments were to be made, this would decrease the possibility of the adverse event occurring, thus increasing the plant's productivity and profitability.

The protective measures, on the other hand, act on the reduction of the impact of the negative scenario, without minimally altering its probability.

-risk differentiation It is a management tool suitable for those risks that are characterized by a reduced systematic component and that lend themselves to management logics aimed at reducing the overall riskiness of the company. it is particularly effective when there is a low degree of correlation between pure non-catastrophic risks and other types of risks.

-risk transfer hedging consists of taking a risky position as opposed to the one you wish to manage that takes advantage of the principle of offsetting to reduce the overall risk to which the organization is exposed. For example, the taking out of an

insurance policy that covers those risks that are unlikely but significantly harmful, such as natural disasters or fires that risk substantially damaging the tangible assets of a company.

-risk sharing : These strategies lie between transfer and retention and consist in sharing risks with other companies through the creation of contracts, such as joint ventures, or ad hoc companies into which the capital to be invested flows. In this way, both profits and losses from the investments made are shared.

-risk retention: is the assumption of a risk within the company without taking any explicit measures to transfer it. This occurs when the adoption of open management measures is not economically viable. The company may choose to adopt self insurance solutions.

Ex post are all the possible actions that can be implemented after the risky event has occurred and are damage limitation and mitigations measures.

The growing importance of indirect damages and damages related to the possible interruption of production activity has led to the development of a number of disciplines that have the specific objective of planning measures to contain and reduce physical and image damage to be adopted following serious accidents.

These disciplines are:

business continuity plan and crisis management.

1.3 Business risks evaluation and corporate impact of risky events

As many experts on the subject say, when considering risk, five elements must be evaluated: risk concept, risk process, risk awareness, risk measurement and risk control.

1. Risk concept is the phase in which the concept of risk is defined and must be understood and internalized by all those who operate within the company.

To better understand the notion of risk, it is interesting to identify some elements that characterize it: exposure, volatility, probability, time horizon, correlation and finally capital (Lam, 2003).

An example of what an exposure is the credit that a company has against a client, the amount of this credit represents the maximum loss that the company could incur if the client does not pay. Volatility, on the other hand, indicates how much the target outcome could vary. Generally, a really high volatility is synonymous of really high risk.

The time horizon is another determined element of risk, in fact, the more distant an event is in time the less predictable the results it will achieve and the riskier it is.

Knowing the time horizon allows you to manage future risks today, with the advantage of incurring fewer costs because they are less likely to actually occur. On the other hand, managing short-term risks can lead to higher costs precisely because there is more information that can confirm their occurrence.

As a result of the time horizon one can distinguish between possible and probable event. A probable event is something that we already know in what probability it will occur, because over time we have been able to analyze the situation that has allowed us to define a probability distribution. Otherwise, the possible event refers to something unknown, of which I do not know what will happen. The latter presents the highest risk situation because I have no information about it and therefore have no way of predicting anything. It is associated with what are called unexpected risks.

Another component is the correlation: it identifies the similarity of "behavior" between two risks. If two risks behave in the same way they are correlated, and this leads to an overall high risk. The concept of correlation is very important in portfolio risk diversification strategies.

The last element is capital, i.e. the amount of resources that you decide to leave available to deal with sudden risks. This level depends on internal choices or goals that the company sets itself, such as maintaining a certain

level of rating. In fact, the more a company wants to have high ratings, the more it must have resources to cover the risks that may occur.

2. Risk awareness It is the initial stage of any risk management process. It consists of ensuring that everyone within the organization is able to recognize the possible risks, to consider their consequences and to be able to communicate the risk and its characteristics. To allow a proper risk awareness we must define all the types of risks to which our company could be subject and assign names that are for all terms to uniquely identify that risk. This step avoids
misunderstandings that could occur between the various operators and allows to have an efficency risk management.
In addition to recognizing internal risks, it is also important to know what external risks are linked to variables such as technological innovation, economic trends, regulatory changes and other events. These risks are difficult to manage internally, but they must be taken into account to try to contain their effects.
There are various techniques to identify risks. These are scenario analysis, historical analysis and finally process mapping.
Scenario analysis is the technique that involves the definition of different possible scenarios of the economy and how business choices can be influenced. This technique makes it possible to understand the risks that may arise because different situations have been foreseen and for each one all the problems that may lead to a variation in the pursuit of the objectives have been highlighted.
Historical analysis consists in keeping a sort of record of everything that has happened over time and how it has been dealt with. This allows us to know what risks have occurred in the past and how often, thus allowing us to define a probability distribution as well as a risk map. In this way it is possible to list the different risks to which the company may be subject and understand their effects. In this type of technique it may also include risk

analysis of companies in the same sector, always with a view to have a complete picture of the possible risks. However, the limit of this technique is that the significant risks are typically infrequent and therefore the historical analysis is not exhaustive.

Finally, the process mapping technique consists in defining a detailed map of all the processes that are carried out in the company and then proceed to evaluate all the possible changes that could occur in each single activity. This method also makes it possible to divide who does what and therefore to know to whom to assign the competences in terms of the application of risk management policies. The limit here is not being able to identify those risks that are in the middle between one activity and another.

3. Risk measurement This is the stage at which a value is placed on the assessment of the elements from which the risk may arise. Knowing the amount of risk that can occur allows you to understand what you have to manage. In fact, it is important that the company defines a level of risk tolerance that identifies the part that it decides to keep inside and the part that it will outsource.

   The level of tolerability will therefore highlight the amount of unexpected risk of which I am not sure it will occur and that is what I am managing.

   In addition, outsourcing means incurring a cost, because there is also a price-quantity relationship at risk level. In fact, deciding to outsource the risk involves paying for the service they offer. Therefore, the more risk you decide to tolerate, the lower will be the cost I will have to pay for its management. Risk measurement is not easy because there is often insufficient historical data available. Therefore, two measurement techniques can be distinguished: quantitative analysis and qualitative analysis.

   The former is based on probability distributions that have also been built up from past experience.

   However, if sufficient data are not available, a qualitative risk analysis can be carried out. It consists of collecting information about the possible events

and the use of expert opinions on the possibility of the event and its impacts. It is mainly based on estimates (Shi, 2004).

Once a probability has been attributed to the various events, it is useful to classify the risks according not only to this variable but also to the severity of the effects. This phase is the basis for the next one, which consists of the risk process, since it allows to understand the different characteristics of the risks and therefore to define a correct management policy.

In order to better identify risks, Lam suggests considering losses, accidents, the manager's risk assessment and risk indicators (Lam, 2003).

As far as losses and accidents are concerned, it becomes essential to create a database in which to collect all the data relating to them. In fact, by doing so, a history is built that can be useful to understand possible future risks.

Management's assessment of risk is to have a clear idea of the risks to which the company is subject and what uncertainties may prevent the pursuit of objectives. This analysis is based on the use of the past experience of the manager, who has knowledge of the company's risks over time.

Finally, build a table with risk indicators to allow the control of all possible events that give rise to risk. They should give not only an ex-post analysis, but also a prospective analysis of events, in order to provide useful information for management.

4. Risk process Once the risk has been identified, it becomes crucial to decide how to deal with it; this is what is done in the risk process.

   In fact, the risk management strategy and therefore the tools to be used are defined. These can be: the taking out of insurance, the use of derivatives or the modification of certain internal policies. The choice depends on the type of risk and how much risk I want to outsource. In fact, I can choose to remove all the risk, eliminate only part of it and keep the tolerable one, or I can keep all the risk.

   I also need to know that if I decide to remove all the risk, this means removing not only the negative risk, but also the positive risk. Awareness of this is especially important in order to avoid wrong assessments of the

work of the Chief Risk Officer (CRO) or risk managers. In fact, the possibility of also removing the positive risk means eliminating extra gain and this could be understood negatively. The essential thing is to understand that this policy has made it possible to remove the possible negative risk, which would have damaged resources if it had occurred.

On the other hand, a hedging instrument must be such as to cover as much risk as possible and must last as long as the exposure lasts. If dynamic strategies are used, it becomes fundamental to have a careful management that, the more I have instruments that last less than the risk, the more complex and expensive it becomes.

Both the insurance and the use of derivatives are a way to transfer the risk to third parties. In fact, derivative contracts are pure risk trading instruments where there is an exchange of underlying assets that allows the risk to be transferred externally. Another way to outsource risk is the use of contracts such as the transfer of risk to the consumer or the subcontracting of certain risky activities.

Moreover, at this stage, the choices could also lead to a change in the corporate strategy if it turns out to be too risky.

All the policies that will be adopted, however, will have to be accepted by everyone and this can often be a problem due to the different risk aversion of the various actors.

5. Risk control It is the final step in any risk management process and is to assess whether the management choices are applied correctly and whether they are correct to avoid a large part of the risks. In fact, if the risk is managed correctly, the company will have no losses and may even have profits, while the counterparty, which has taken over the risk, has potentially accumulated all the losses.

   Moreover, as stated above, precisely because up-side risk also exists, it could be that the final post-hedging result has led to a loss compared to non-hedging. This does not mean that the strategy adopted was not correct, as it absorbed all the down-side risk, only that ex-ante, it is not possible to know

whether I will have positive risk or negative risk. This forecasting problem is typical of risk management activity, so it can be useful to research policies that are not too restrictive, and this is partly allowed thanks to the proliferation of derivative instruments.

In this phase it is also necessary to optimize the risk-return ratio, i.e. to assess whether the management strategies that have been adopted allow to support the company's growth and profitability. In fact, risk management is an expensive activity, so it becomes important to assess whether the cost incurred has been useful to prevent the risk or there has been a waste of resources. The already mentioned price-quantity relationship that is also present in this activity must, therefore, be kept under control.

In order to assess the correct application of the previously defined strategy, it must also be assessed whether the endogenous variables, which may give rise to risk, have undergone changes such as to influence their success. In fact, in the course of the management activity, some variables that belong to the external environment, such as, for example, the performance of the economy, could induce to modify the strategy even during the course of the work.

Regardless of the origin, nature and type of the risky events, they affect the company in a more or less serious way, with different consequences on the economic and financial situation and financial equilibrium. Depending on how the risks impact on the life of the company and the effects they produce, it is possible to distinguish between:

-direct impacts; essentially, the directly observable consequences of risky events affecting the company's resources by reducing their value are considered. Some examples can be fires, thefts, accidents at work,...;

-indirect impacts; these are those effects indirectly related to company assets, often as a result of direct impacts and which can amplify the negative consequences of damaging events that occur;

-consequential impacts; these are those damages that the company's image may suffer in relation to the occurrence of a risky event that compromises the perception that the external subjects with whom the company comes into contact have of the company's image, its reliability, and the quality of the products. This may result in reputational damage with possible loss of market share.

The first two types of impacts act at an immediate level, as they refer to all those situations "in which the negative effects of a business failure are directly reflected on the stakeholders and the socio-economic context of reference" (Fortuna F., 2012:21); precisely for this reason they can be limited through specific prevention and coverage tools. On the contrary, the last type of impact acts at a systemic level: in addition to the negative consequences for the company itself, the following can consequently be produced

knock-on effects also on other economies and others who somehow come into contact with the enterprise. They therefore have a broader and more incisive scope and are not insurable because they are not directly predictable and quantifiable.

CHAPTER 2: Plans for overcoming disasters

After talked about the different kind of risks that companies can face during its life, we now have to focus to the different plans that firms have to use in order to overcoming risky events.

In order to deal with unexpected events of considerable magnitude, companies must overcome the "reactive logic" of Risk Management - foresee and assess risks and then decide how to deal with them - and make use of a system based on "proactive logic": the possibility of the occurrence of unforeseeable events, which may have significant consequences on their management, and prepare to deal with them in a timely and effective manner. In order to deal with these events, companies use Business Continuity Planning, i.e. a system that allows them to maintain the continuity of their management processes or promptly restore it when it is compromised due to the occurrence of an unforeseen adverse event of considerable magnitude (Lindors, Tittel, 2017). Therefore, the Business Continuity Plan is a fundamental component of Business Continuity Management, since the latter concerns the continuity of the entire company. The construction of the Business Continuity Plan is based on the Business Impact Analysis. The latter identifies in advance unforeseen but possible adverse events and quantifies the losses that could be generated on management processes, assessed in terms of costs. This analysis also helps to assess whether some "non-core activities" of the business management are to be managed in outsourcing and the risks that may arise. Basically the Business Impact Analysis helps to analyze the processes of the entire company and to determine which of them are more exposed to unexpected adverse events in order to prepare in advance the plan of their response.

Regardless of the size of the business, in order to remain competitive, it is vital that it maintains and increases its customer base. In this regard, it is clear that there is no better proof of being able to do so than to demonstrate that it is capable of defending continuity of management even after major adverse events have occurred.

The restoration of the IT system is of fundamental importance for the company, since it supports all processes, the relationships between processes and the entire communications system within the company and with its internal and external stakeholders. The future of the company depends on the human resources on which the company bases the implementation of its management processes and on the continuity, it is able to ensure them. The company that has the skills and abilities to deal effectively with unforeseen adverse events, in addition to ensuring its continuity and development, is able to increase the customer loyalty, to strengthen its reputation and increase its market value.

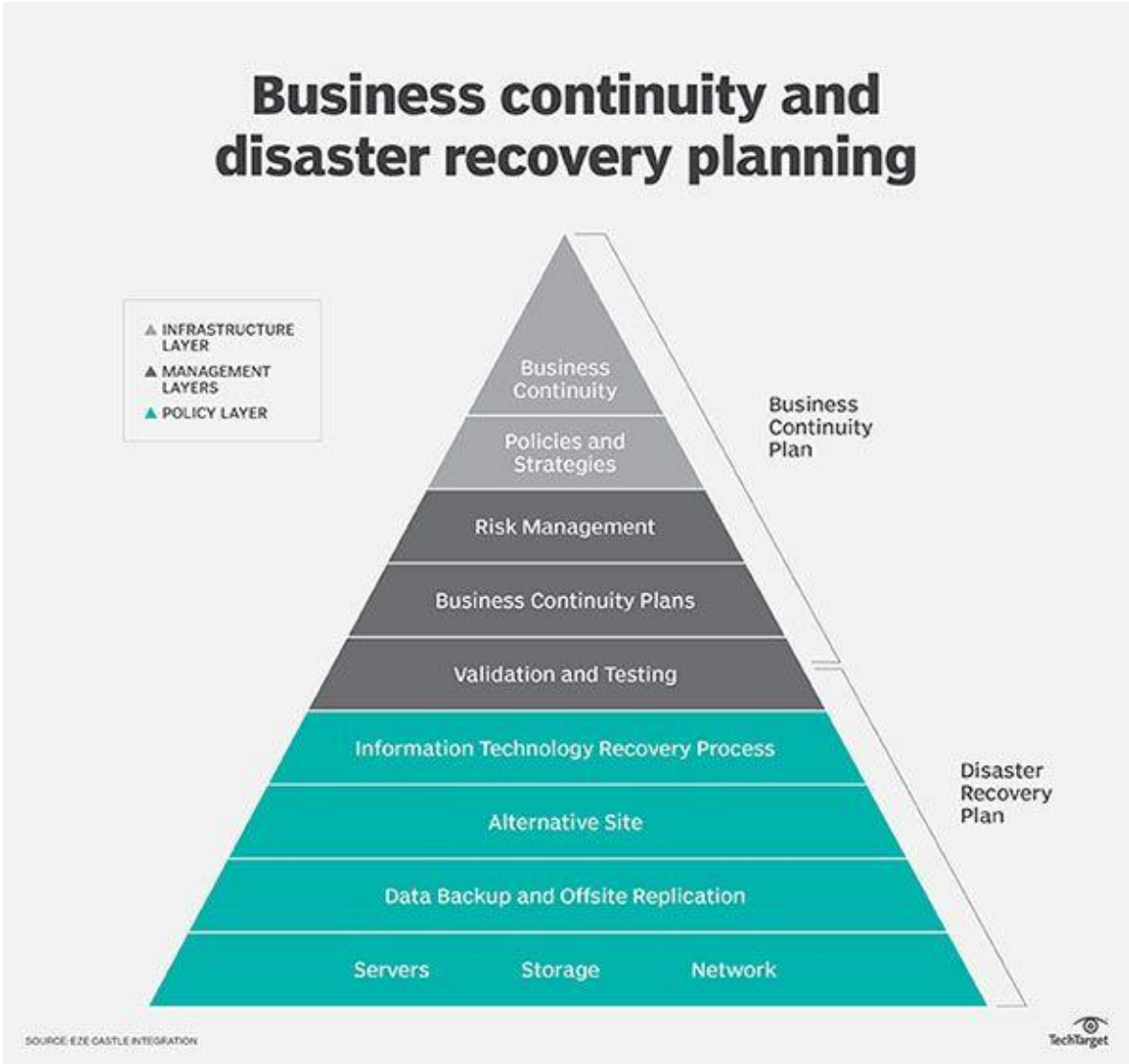
A disaster for a company can affect disparate sectors, such as buildings, human resources, IT systems, paper documentation, and can cause a great damage, sometimes severely compromising the company's ordinary operations. It should not be thought that the disaster is just a catastrophic event such as Hurricane Katrina or the tsunami. Even staff errors, causing loss of data, can represent a disaster for the organization.

Disasters, understood as accidents, are quite frequent events in companies. Therefore, there is a need (a growing trend over the years) to adopt solutions to prevent the economic damage resulting from downtime, to limit the consequences of disasters and to restore the entire business, once affected by the adverse event.

Today the issue discussed so far has been addressed through Business Continuity (BC), the most widespread and recognized methodology for managing disasters, through the prevention and, if necessary, the recovery of existing infrastructure, data and systems. The aim is to ensure business continuity as much as possible. Guaranteeing continuity means not only setting up the environment and infrastructures capable of mitigating the risk of an unforeseen break, but also planning the most appropriate moves to carry out corrective actions in a short time and with contained costs. Key factors of a BC are given by the planning and the chosen strategy: Business Continuity is not only data backup. The methodology aims to identify what are the risks of the system, where it may be subject to threats and what impacts they may have on it.

In preventing all cases of disaster, it should also be considered how the entire business is affected: in such a scenario a Disaster Recovery solution is adopted, which provides the procedures and technical infrastructure to keep critical services active in case of unavailability of the IT infrastructure that delivers them.

When studying a solution for business continuity, procedures are planned for all cases identified. Among these, there is the possibility to identify the worst case, which describes a scenario where the event has had such a strong impact that it has resulted in permanent, or almost permanent, losses. In such a context, it is no longer simply a matter of ensuring continuity, but of implementing a series of procedures to reactivate the entire business. The task of Disaster Recovery is just that, i.e. to set up alternative structures and procedures to bring all business activities back to life: the solution generally involves a transfer of operations to a replacement site. Also in this case there is an activity planning and a reference plan, always included in the wider Business Continuity plan.



Font: techtarget

2.1 Into the Business Continuity Plan

What we have said so far should not make us think that a Business Continuity solution should be applied to every company. The implementation of a BC has first of all a cost, so precise evaluations must be made on the convenience of developing it. Usually it is the large companies that have an interest in having a BC plan; for small, or even medium-sized companies, such an investment may not be justified. In addition, a BC solution must be motivated by the fact that there is a real likelihood that a disaster could occur and that there are threats that could cause it.

Understanding which threats may affect the organization and where it is vulnerable is the task of risk analysis (typical risk management activity); this determines, based on the results obtained, the implementation or not of a Business Continuity plan.

Summing up, we can therefore say that Business Continuity means a process consisting in the prevention and management of situations of serious unavailability of IT systems, through the provision of alternative procedures and resources to ensure the critical business services.

2.1.1 Objects of Business Continuity

The Business Continuity therefore has several typical objects that are addressed in the definition of the plan:

- provide an immediate, measured and accurate response to an emergency;
- facilitate the recovery of business operations to reduce the overall impact of an event and at the same time bring critical business functions back to life within a certain period of time;
- minimize total loss;
- Provide procedures and resource lists to assist the recovery of data processing functions considered critical to supporting business functions and IT applications;
- document procedures in clear and defined terms, so that staff are fully aware of the actions to be taken;
- identify suppliers;
- avoid a confusing response during the fault period by training staff with sufficient advance notice and providing it with clear and precise documentation;
- document the procedures for storing, safeguarding and retrieving data, information, documents and supplies;
- provide guidelines for behavior to be followed during the breakdown, in order to ensure a timely resumption of services;
- describe the actions, resources and materials to return critical operations to an alternate site in the event that the primary site has suffered a failure for an extended period of time;
- repair or replace damaged facilities within an extremely short period of time.

Like typical projects, the Business Continuity project is based on three fundamental processes, which determine its life cycle:

1. planning
2. execution
3. control

The planning phase generally aims to build the plan and strategies to be implemented to ensure business continuity. The planning has two aspects, one preventive and one reactive.

The preventive aspect consists in determining the activities to be carried out, before the disaster, or the adverse event, affects the systems to be protected. The activities concern the preparation of infrastructures and technologies capable of carrying out business operations when the primary system is at a standstill.

The reactive aspect, on the other hand, is the determination of those activities that must be carried out after the disaster has occurred. The difference with respect to what has been said previously lies in the fact that the hypothesis is being considered that the site, or the system, on which the business activities are carried out is destroyed, or in any case made permanently or for a prolonged period of time unavailable. In this case, which is the worst-case scenario, the actions to be taken to transfer normal operations from the site of origin to the secondary site are planned.

The execution of the plan activities is carried out first of all for the first (proactive) phase, which is designed to prevent interruptions. The second phase is clearly implemented following the disaster.

Monitoring is carried out not only on the execution of the activities but also on the plan itself. The continuous review of the plan is in fact essential to ensure the effectiveness of Business Continuity. Part of the control is also given by the verification of the plan, carried out in order to determine its operation.

The reason why a Business Continuity plan is implemented is because the organization believes that there are threats that can produce a standstill in business activities. The identification of such threats takes place as part of one of the first of the Risk Management activities: risk analysis. Only after the results obtained from

the analysis it is established whether to start a planning process of the BC, when the real presence of threats is underlined, with a high probability that they occur.

The drafting of a Business Continuity plan is the product of a process of analysis and organization that can be summarized in five steps.

1. Project Management and Initiation: the phase that creates the project team that will support the project management function.

2. Business Impact Analysis (BIA): is the process by which all business functions are analyzed to understand the impact that a failure could have on them. The loss load is estimated in time periods, relative to the absence of service. We also try to understand for how many units of time the absence of service could be tolerable. This is an activity included in risk management and is after risk analysis.

3. Recovery Strategies: is the phase that identifies the best recovery alternatives.

4. Plan Design and Development: it is the phase in which the results obtained during the

the BIA and write down the actions identified.

5. Testing, Maintenance, Awareness, and Training: this is the phase that establishes which processes must be activated to test recovery strategies and to maintain the BC plan.

During the first phase, the organizational aspects through which to prepare for the problem are addressed. An attention role is played by the project management, which establishes which elements are necessary to carry out the project and establishes the best strategies to implement the solution. Another task of project management is to establish the project team, including officials and technical specialists, and to draw up the work plan, which sets objectives, organizational methods and identifies tasks and responsibilities.

The second phase, Business Impact Analysis, aims to determine what impacts the system may have if the threatening events identified during the risk analysis are exerted. This activity is also included in the scope of Risk Management, which is why we will not go into the subject in more detail in the next chapter.

The third and fourth phases concern the activities of defining technical and organizational strategies, which lead to the definition of the technical design and the continuity plan.

The last phase, among those listed, takes into consideration testing and maintenance, as well as the communication of activities, aimed at making the staff operational and instructing them on how to proceed. The Plan must be subjected to suitably defined tests to verify its validity ex-ante. Many companies test the plan not only at the end of its preparation but also two or four times during the year. The most common tests are the "Table-top exercise", the "Structured walk-through", the "Disasters simulation testing". The "Table-top Exercise" consists of a meeting in which the plan is examined in depth to ascertain the existence of any gaps to be filled and to verify that all the business units have been included. In the Structured walk-through, each team member thoroughly analyzes the components of the plan to identify their weaknesses. Often, the team works by testing against a particular model. Some companies use role-playing in structuring the process of this test. Any weaknesses highlighted should be corrected and an updated Plan should be distributed to all staff involved.

It is a good practice to carry out an annual full-scale test to ascertain whether it is necessary to remove some staff members or to integrate them with people who have particular skills.

Finally, a simulated test of the feared disaster event should be carried out annually. For this test it is necessary to create an environment that simulates a real disaster, considering its consequences on machinery and equipment, the information system, staff, supplies, as well as partner companies and the staff of the business organization. The purpose of the simulation is to verify whether the company is able to perform critical functions during the occurrence of the adverse event. During each test phase of the Business Continuity Plan it is frequent to include new members in the team in order to discover gaps and delays in information that team members may have overlooked.

Performing the Business Continuity Plan test requires considerable effort. Once the test has been completed, some parts of the Plan will be confirmed while others, the most critical ones, will have to receive the appropriate in-depth analysis, which may result in adjustments to the Plan.

The verification and validation of the plan is a fundamental point in the completion of planning activities. Its importance stems from the fact that test results can lead to considerations about important changes in the action plan, to be made to ensure that the business is safeguarded. Failure to verify the plan, with formal approval, is potentially damaging as it may be ineffective once proven in a real situation.

As far as the maintenance of the plan is concerned, we can say that even in this phase the phase is very complex. Keeping the plan up to date means checking that the planned actions still have value over time. It is possible that for certain threats, certain strategic choices are no longer effective. In addition, some application or infrastructure changes may also lead to changes at the recovery site.

Ultimately, we want to specify that the Business Continuity plan is not unique, but consists of a series of plans. In fact, given the complexity of the work to be done and the need to involve different business functions, the BC includes a set of procedures and plans for business continuity and business recovery. Each plan has a specific function within the BC, as it concerns the management of specific activities. Five components are included in the plan and are:

- Business recovery;
- Business resumption;
- Disaster recovery;
- Contingency plan;
- Crisis Management.

2.1.2 Crisis management and Contingency plan

How we can see, Crisis Management is part of Business Continuity Planning. In fact, any unforeseen adverse event of considerable magnitude that has serious consequences on the management of the company, requires the availability of a Crisis Management Plan, which is an important component of the Business Continuity Plan. Its relevant dimensions concern:

- the definition of the crisis;
- how do you arrive at the definition of the "crisis";
- the components of the Crisis Management Plan;
- how the Crisis Management Plan is implemented.

The "crisis" can be defined as an unforeseen event of considerable magnitude that when it occurs has serious consequences on the company's management, machinery, plant, information systems, personnel, and others, causing the production to stop. The block of production causes a number of knock-on effects. A crisis can have internal or external origins. It can be small or large. Depending on the severity of the crisis, the company may be exposed to adverse publicity, which may lead to a decline in the value of its shares, with a consequent decrease in the convenience of investors to buy them. From what has been said, it emerges the importance that when the crisis occurs there is an immediate response in order to manage it with high professionalism and competence, aiming in completing it in the shortest possible time (Woo, Gallgan, 2015).

The Crisis Management Plan is a component of the Business Continuity Plan. It, if well elaborated and documented, is the fundamental tool of crisis management. As such, the Business Continuity Plan has the function of facilitating communication between all stakeholders, particularly interested in the security of the company, as well as forecasting the actions to be taken to assess the impact of the crisis on external stakeholders, to support interaction with the media during the crisis and, above all, those to be taken to contain its negative consequences.

In the elaboration of the Crisis Management Plan must be defined:

- The Crisis Management Team, which should include high-level managers who have the necessary expertise and experience to manage a crisis. The team should also include people with specific expertise in crisis management;

- the organizational responsibilities of the Team. Although each team member should be assigned a specific task related to particular functions, duties and responsibilities, in the course of crisis management the operational logic of the team members should always be that of their continuous and mutual interaction as required to achieve the objective assigned to them. Sub-teams - which will operate under the direction of the most important member of the team - are composed of

people with different types of skills, able to perform the tasks assigned to them in crisis management;

-evaluation and correction: during the management of the crisis, the different actors in charge of the crisis will have to evaluate the responses to be given to the different problems faced and decide on the corrective actions to be taken to eliminate the detected deviations from the objectives pursued;

-the list of contacts. A regularly updated list of contacts must be compiled and maintained to ensure relations with stakeholders;
-the Command Centre. A Command Centre to manage emergency operations in Crisis Management should be the focal point for crisis management;

-Logistics. Logistic support for notification, mobility, and operation of crisis centers should be clearly defined;

-Public Relations. In a crisis situation the last thing a company needs is a "hostile press". A member of the team should be responsible for managing relations with the press, making them as transparent and comprehensive as possible, compatible with the levels of confidentiality to be safeguarded, avoiding any contradiction between communications fed during the crisis (Pillai, 2015).

Crisis management tests the decision-making skills of the company's management and staff. This is because if decisions are made very quickly there is a risk of basing them on incorrect or inadequate information. For the same reason if you wait to obtain more correct information you risk paralysis of the analysis is the lengthening of the time of decisions or non-decisions. It must also be avoided that crisis managers are immersed with a vast mass of information.
There should not be confused Crisis Management with Contingency Planning. Both are components of "Business Continuity Management", which allows the company to cope with and overcome major adverse events, but they have different objectives and are implemented with different processes. The "Contingency Planning" differs

from Crisis Management because it concerns the process by which the company identifies the potential adverse risks to which it is exposed and develops a comprehensive plan that allows it both to respond to any threat or adverse event and to achieve a return to normal in the shortest possible time. Therefore, Contingency Planning expresses a proactive strategy that places more importance on preparing for the unexpected event than on responding to it. Conversely, Crisis Management is the process of managing the response to a major adverse event after it has occurred. It is the expression of a reactive strategy that gives more importance to the response than to the preparation. The Contingency Plan identifies and prioritizes resources that are critical to the continuity and survival of the business. Critical resources include the computer system, communications system, plant and machinery, warehouses and human resources. The Contingency Plan identifies potential threats for each critical resource and develops an action plan to respond to any threat situation that may occur. The management of the plan is entrusted to a team of experts responsible for the different aspects of the response, including communications, resource allocation and management as a whole. Companies regularly review the Contingency Plan and update it taking into account the evolution of the threats to which they are exposed (Linton, 1698).

2.2 Into the Disaster Recovery Plan

Events of catastrophic proportions, such as Hurricane Katrina in 2005 and September 11, 2001 or even the pandemic which is currently going on highlighted the importance of Disaster Recovery as a social security in order to keep an organization's business alive. The temporary loss of a service can be very costly and even lead to company failure.

Disaster Recovery (or more briefly DR) can be defined as one of the possible solutions for business continuity following a disaster that can be contemplated in a Business Continuity plan. As such, the solution relates to ensuring the continuity of the business, even in the presence of extreme cases, where the disaster coincides

with a catastrophic event that has as its consequences the permanent loss of data, applications and infrastructure supporting the activity.

Disaster Recovery provides the procedures and technical infrastructure to keep critical services active in case of infrastructure unavailability.

The objective of a DR is to ensure the survival of the business and to plan how it should remain so. The survival of the business is normally guaranteed by alternative infrastructures and applications.

An organization's systems may consist of applications and data that are more or less critical because they have a particularly important economic value. Usually the criticality of systems, as seen above, is determined through risk analysis.

MANAGEMENT OF A DISASTER RECOVERY PLAN

The path through which the management of a Disaster Recovery within an organization matures is in fact essential for the solution proposal to be effective.

The guidelines provided by Gartner define a series of stages through which to conduct the management of a recovery.

FIRST STAGE:

At this first point it is assumed that the organization does not have any recovery plan, or that the plan exists, but that it was made in the past to be archived and then no longer maintained, let alone tested. Also included at this stage is the possibility that DR plans exist, but that they only partially cover the system or data that the company's business needs. At this stage, the risk to business operations is always very high. Hence the need to implement a Disaster Recovery solution that can take 6-12 months of work, during which time it is possible to better understand what needs are required.

SECOND STAGE:

At this stage, a project team is assembled to understand the DR management drivers in order to determine the existing shortcomings in the organization and to define the investments to be made in order to implement a plan. It is precisely at this point that the organization understands that there is a real need to implement a Disaster Recovery.

Usually at this stage is also attributable to the execution of the BIA (at least in the initial phase), in order to determine the criticality of the key processes of the company. The Business Impact Analysis is formally conducted in project terms.

THIRD STAGE

At this stage, the implementation of the Disaster Recovery solution, or Business Continuity, takes place in a more detailed and formal way: the management has as a driver the evolution of the business activities already active and their integration with those planned. The Business Impact Analysis processes are formalized annually, and the DR requirements are already defined during the first steps of the projects, concerning the development of new applications and new infrastructures. It is becoming increasingly important to have a more formal DR organization to ensure a life cycle approach.

Disaster Recovery management becomes an effective business function within the organization. Responsibilities in this area can be defined by the Business Continuity Manager (BCM), who typically resides outside the organization and takes care of risk management, security or centralized operations.

FOURTH STAGE

At this level, the concept of Business Continuity is well established within the organization.

The management of the BC is a formal process, included in the business organization, and there is a real planning, with a plan associated with it.

An interesting survey by Gartner (How to Conduct a Disaster Recovery Management Self-Assessment, John P Morency, Donna Scott) shows that, among a hundred organizations examined, a high percentage of them have already considered formally relying on Disaster Recovery solutions, with very high levels of management.

Currently, as seen, it cannot be said that all the organizations present have a Recovery solution or that they know it. The culture of safety in this field has become more widespread following disasters that are sadly known all over the planet, due

to the seriousness of the damage done. In addition to this, the spread of Business Continuity and Disaster Recovery has had its reasons in the increasing evolution of technologies and the increasing dependence of organizations on IT.

Some data, coming from statistical surveys (source: Gartner), state that in the last ten years, in the USA, tornadoes have caused about 102 emergencies.

In California, the terrible earthquake of 94 caused damage equivalent to 6 billion euros. Also in the United States, one in four companies said they have faced disaster in the last five years.

Now only 68% of companies in the US have a Business Continuity Plan and only 55% of them have formally approved it.

Today, out of five companies affected by a major disaster, two fail to reopen, one reopens, failing within two years. One then wonders why there is a lack of due anti-disaster procedures within companies. Some of these reasons are given by the following points:

Legal requirements (Legislative Decree 196 for example).

"Due diligence "4;

Basel-25;

Insurance issues;

Fiscal balance sheet certification issues;

Obligations towards stakeholders.

Another reason why some companies, with a culture not focused on safety, or better not aware of the importance of Disaster Recovery, decide not to invest

on a preventive solution, against attacks, is due to the high investment that the project involves. Since the costs are considerable, companies can sometimes be discouraged from implementing such a solution.

CHAPTER 3: BUSINESS RESILIENCE

Disasters, crises and other unexpected events have the potential to damage the management of the company and the processes that make it up, to interrupt the continuity of the business flow with consequences on its profitability. As a result, customer relations may be made problematic both by negative events and by the inadequacy of the actions taken in response to the events that have occurred. In fact, its easily evident the criticality of the actions taken to respond to the sudden events that have occurred, aimed at containing the damage produced by them and allowing the recovery process to begin. The system that allows so much is "Resilience". It allows the company to adapt to the market and the environment also following the occurrence of unforeseen events of considerable magnitude, i.e. "disruptions". These events, which the increased dynamism of the market and the environment, make it increasingly frequent and increasingly worrying for the extent of the consequences they may generate on the management of the company, on its competitive positioning and on its ability to create value (Braman, 2017).

The adaptation of the company to the market and the environment has a critical value, given the high dynamism that characterizes them in the present and that, in all probability, will characterize them more and more in the future. No company has the oracle to predict future developments. Change is constantly accelerating, a new or destructive technology can emerge at any moment and upset the plans carefully elaborated by the enterprise. Resilient firms are prepared to take greater risks and respond quickly to sudden changes when they occur. They are better able to cope with the situation when they skip the plans that have been drawn up in line with the strategy decided upon. Companies that show that they have a higher risk tolerance have an extra advantage over those who do not.

The "Business Resilience" is a system that, while incorporating Business Continuity, Disaster Recovery and Crisis Management, has a broader scope than the same, since it is aimed at dealing with unforeseen adverse events across the board, capable of causing radical changes of different magnitudes in its management, and in particular in its business areas, with a view to ensuring its valid

competitive positioning to which its survival and, where conditions permit, its development is linked.

Business Resilience, fundamentally, is the ability of the company to adapt to unforeseen changes of considerable magnitude, i.e. disruptions, and to maintain, or promptly recover, the continuity of its management, its activities, safeguarding its competitive positioning, the value of its brand, its image and, most importantly, its ability to create value (Selleri, 2017).

3.1 The four capabilities of resilience

The valid use of Resilience is based on four fundamental capabilities. The first is Responsiveness, i.e. the ability to implement tactical plans developed before the occurrence of a disaster or crisis. This capability must be implemented in a cross-functional manner to cover all critical areas of business management. The second is Protection, i.e. the ability that allows the company to have coverage against identified threats and, where possible, against non-identifiable threats. Protection also includes Contingency Plans and alternative actions that will be implemented in the event of adverse events of such magnitude as to be disruptions. The third capability is the Response, which concerns the process to be implemented immediately after and during a crisis. It is essential that the Response has been identified before the crisis begins. In fact, if the bodies of the company were to try to identify it during an emergency, they would already have failed. The fourth response capability is Recovery, which is about the process to be put in place to enable the company to return to the situation that existed before the adverse event occurred as quickly as possible. Often the mistake of considering Recovery as equivalent to the implementation of the Disaster Recovery Plan is made. It is that the latter is aimed at recovering the activity only at a basic level, which makes it more than a simple response. Recovery, on the other hand, has a very different tactical purpose. In fact, it focuses on maintaining or recovering the level of existing management activities before the adverse event occurs.

Resilience is the system that allows the company to adapt dynamically to changes in the market and the environment. Its importance has grown over time in parallel

with the continuous acceleration of technological development. No company has the capabilities to predict the future development of technology. Change is constantly accelerating: a new or destructive technology can emerge at any time and distort the plans carefully worked out by the company in line with the strategy decided. Only resilient companies are prepared to take greater risks and respond quickly to unforeseen changes when they occur. They are better able to cope with the situation when they skip plans that were previously drawn up in line with the decided strategy. Companies that have a higher risk tolerance have an extra advantage over those that do not.

3.2 The evolution of resilience

In recent years, Resilience has been recognized as having a broader scope than that described above, given its "ability to enable the company to anticipate and react to future change, not only to ensure the continuity of its management, but also to achieve its evolution in response to change. Resilience puts the company in a position to decide before change becomes unmanageable. In this logic, the British Standard BS 65000 defines Resilience as "the ability of the enterprise to anticipate, prepare for, and respond and adapt to incremental change and disruptions in order to survive and prosper" (Owen, 2016). In other words, Resilience is recognized as the ability to enable the company to cope with unforeseeable adverse events produced by change and to take advantage of opportunities that may arise during an in-depth analysis of its evolutionary trend.

According to a more advanced approach than that set out above, Resilience would have a broader scope than that of enabling the company to cope with unforeseeable adverse events with a view to ensuring its survival and, when the conditions emerge, its development. In fact, it is recognized as having a much broader scope, since it would be able to allow the company to acquire, in parallel with the development of the skills and abilities that it had to equip itself with for its effective implementation, the ability to manage any sudden change of considerable magnitude: to face unpredictable changes with negative value, to grasp and turn to its advantage unpredictable events with positive value (Ivezic, 2017).

As part of the new orientation towards Resilience, those in charge of the company are primarily called upon to provide it with the necessary skills and abilities to enable it to cope with unforeseeable adverse events of considerable magnitude and to return to the existing situation before they occur and the resulting crisis takes hold. Secondly, in connection with the acquisition of the necessary skills and abilities, they must allow the company to evolve in the direction of becoming more skillful and stronger, as well as being able to identify and cope with unforeseen and unforeseeable adverse events, and also to be able to promptly seize and turn to its own advantage the opportunities that the change in the market and in the environment is opening up. In this logic, Resilience is consolidated with Antifragility.

N. Taleb proposed to go beyond Business Resilience by proposing the Antifragility approach, a term coined by N. Taleb to define "that category of things that not only gain from chaos, but need it to survive and develop". Antifragility, according to Taleb, is "a property of systems that increases their capacity, their resistance, their robustness, as a result of stressors, shocks, volatility, disturbances, errors, faults, attacks or failures" (Satell, 2013). In parallel with the increase in the dynamism of the market and the environment, the company uses Resilience to manage a variety of changes, not only negative but also positive, in this logic it increasingly assumes the characteristics of both an "immune system" and an "evolutionary system". In other words, a system that, on the one hand, defends the company from the attacks of aggressive and unpredictable events, allowing it to maintain a constructive relationship with the market and the environment and, on the other, allows it to research and implement its relationship with the market on an innovative basis. For all that has now been said, Resilience goes beyond its original ability to allow the company to face the crisis situations in which it may find itself, since it is characterized by a proactive approach to crisis-generating events. This evolution builds a bridge between Resilience and Antifragility. But so much can happen on condition that the company knows how to internalize the ability to adapt to any change that may profoundly affect the smooth running of its management.

Technological innovations create numerous opportunities for businesses but at the same time make them more vulnerable as they become increasingly complex,

virtual, interdependent. Understanding the scale of the potential impact of technologies requires in-depth knowledge of the technology(s) of interest to the enterprise and sound basic knowledge. Technology management should guide the design and implementation of Resilience in the enterprise so that it can use it to its full advantage and be more resilient to other changes in the environment. It is clear from what we have said that building a Resilience system is a prerequisite for the company to take risks. The importance for the company to take risks is clear, as Mark Zuckerberg, founder of Facebook, says: "The biggest risk for the company is not to take any risk. In a rapidly changing world, the only strategic risk that guarantees failure is not taking risks.

Resilience allows the company to manage the unpredictable risks of considerable adverse value, generated by changes in the market and the environment in which it operates, which, if not dealt with promptly when they occur, could generate devastating consequences on its management, such as to compromise its continuity. As we have had the opportunity to say before, the capabilities required by resilience, in connection with the identification of the threats to be faced, can allow the company to identify strategic opportunities from which it can benefit more or less significantly in terms of increasing its competitive advantage and, in close connection, increasing its value creation. Resilience can generate this result when, when faced with a threat, it is the most valid response, not only a more or less structured intervention aimed at containing damage or loss and recovering the continuity of the management compromised by the same, but a more articulated response, aimed at neutralizing it and taking advantage of it. This is what happens when the company's management, making use of the skills and abilities required by Resilience, is able to identify and face a potential threat to its competitive position, linked to the possibility of using a new emerging technology by a company that is a direct competitor of the company, promptly deciding on an initiative aimed at translating it into an opportunity. It is clear that in this situation the most direct and most promising response to the threat can take place, if the required conditions are met, through a decisive recourse to innovation. Only by behaving in this way can the company make the most of the new technology by first developing new products with which to neutralize or contain the extent of the threats of the competing

company or companies. In the management of resilience, innovation can emerge from the latent state when, in analyzing a threat in order to decide the most effective way to deal with it, new potentials for the enterprise emerge that justify a careful and thorough evaluation of their scope which, if it ends with highly positive results, will lead to the planning and development of one or more innovation projects.

3.3 Black Swan events

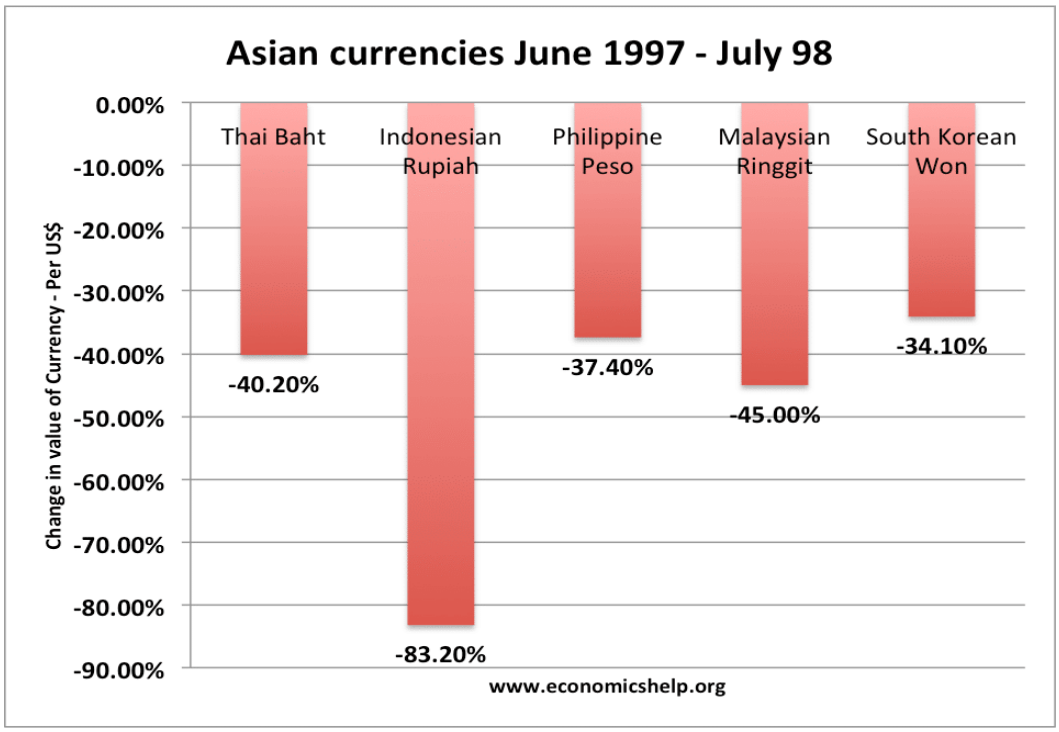
The Black Swan is the metaphor that Nassim Taleb, finance professor, writer and for many years Wall Street trader, coined for those random and difficult to predict financial events, whose negative consequences are far-reaching for everyone.
In most cases, investors' excessive appetites for risk and their sudden fears are at the root of Black Swan events.
Although the risks inherent in the markets can never be completely eliminated, it is essential for economic and financial operators to adhere scrupulously to certain golden rules. Prudence, diligence, risk diversification and hedging, portfolio rebalancing and monitoring are necessary at least to contain unforeseeable shocks.
Based on the Black Swan theory, Faisal Khan, a columnist with multiple interests in global economic trends, has retraced the financial history of the last twenty years, highlighting nine events related to the case. It is an instructive reconstruction, able to help us keep in mind the effects of financial excesses, but it is also useful to note their frequency. A financially catastrophic event occurred on average every two years or so.

1 - Asian Financial Crisis (1997)
It broke out at the end of the surprising economic development of the Asian Tigers (South Korea, Thailand, Malaysia, Indonesia, Singapore and the Philippines), the crisis produced losses of over seventy percent in the value of the currencies and stock markets of those countries.
The region's tumultuous export-driven development of economies in the region generated a strong inflow of direct (i.e. short-term) investment from abroad, which pushed up real estate prices. Stimulated by the abundance of financial resources,

governments and businesses were encouraged to borrow heavily from banks to support ambitious infrastructure projects and robust spending programs. The monetary restrictions of the U.S. Federal Reserve, which raised the dollar exchange rate, were reflected in the currencies of some of those exporting countries that were linked to the American currency.

The bursting of the Thai real estate market bubble was brought about by the collapse of the real estate and financial entities of Somprasong Land and Finance One in early 1997. Thai Bhat, the Thai currency, after wide fluctuations, was massively devalued, spreading instability to the economies of neighboring countries. The Ringgit of Malaysia, the Indonesian Rupee and the Singapore Dollar followed the fate of Thai.

The International Monetary Fund intervened with short-term loans of 110 billion dollars to Thailand, Indonesia and South Korea, imposing strict fiscal conditions (more taxes and less public spending), privatizations and higher interest rates. By 1999, they had pulled themselves out of the crisis and rejoined the growth path of the Asian continent.



Font: economicshelp.org

The massive loss of value of South East Asian currencies

2 - Internet bubble (2000)

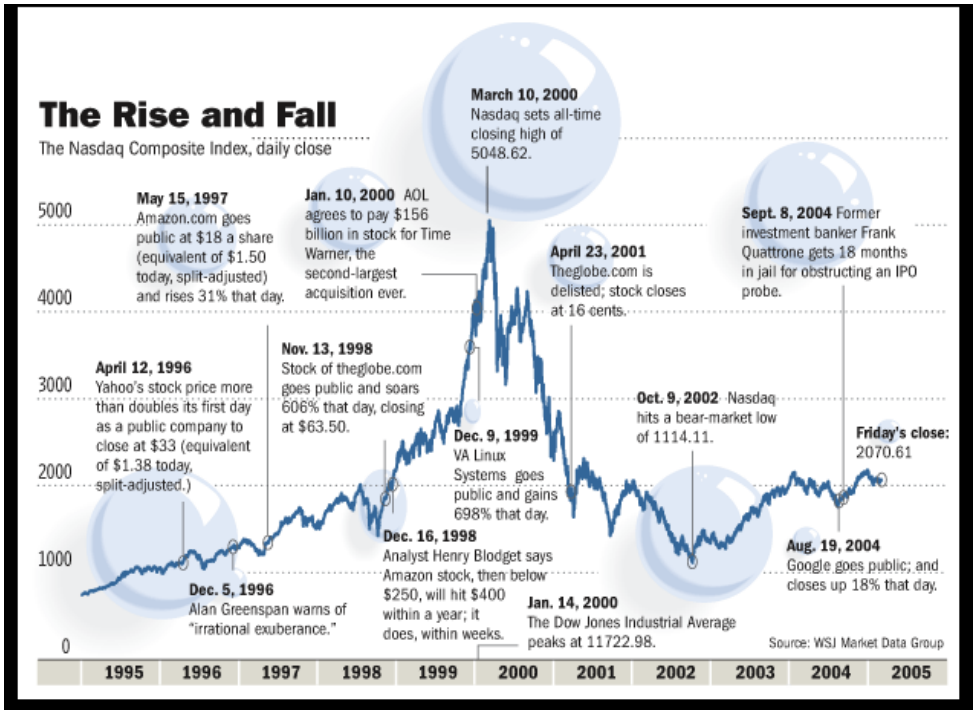
The technology bubble that exploded at the beginning of the millennium is a classic example of the unsustainability of markets, when asset valuations are completely unrealistic, being fueled by the abundance of financial resources channeled into them.

Financial analysts of the time were captivated by the rush generated by the excitement of the advent of the Internet and investors blindly believed in a market, which eventually exploded.

The sirens of speculation made them forget the fundamental parameters, represented by the analysis of business plans, trends and revenue streams of listed companies.

The Nasdaq index grew from less than 1000 in 1995 to 5048 in March 2000. Large companies like Dell&Cisco then placed huge sales orders on the market, spreading panic among investors. In a short time the market lost 10%. With the outflow of capital, the shares of technology companies, which had reached disproportionate prices, lost their value. The fall of the Nasdaq index reached such proportions that it took 15 years to recover the level of the time.

The chart below gives an idea of the violence of the bursting financial bubble.



Font: new.gcase.org

3 - Terrorist attack of 9 September (2001)

While the debate continues as to whether the financial crises of 2000 and 2008 could be prevented, or at least mitigated, the terrorist attacks on New York took everyone by surprise. The financial markets were still under the effects of the technology bubble of a year earlier. Since there were no fundamental trends to analyze, one can only look at the numbers when the markets reopened on 17 September, after the longest closure since 1933.

It was decided to avoid chaos and panic from sales. On the first day of reopening the Nyse's losses were over 7%. There were massive sales of airline and insurance company stocks, for understandable reasons. The week closed with losses of Dow Jones by 14 percent and Standard & Poor by 11.6 percent. A stock market capitalization of $1.4 trillion was wiped out in a few days. The downward correction ended a year later, in October 2002.

The public and private costs of the terrorist attack of September 11, 2001 are shown in the graph below and concern the financing of military spending, the costs of physical damage suffered by the air attacks, security spending, and the impact on economic activities, totaling over 3,000 billion dollars.

4 - Global financial meltdown (2008)

The greatest financial meltdown of our time, second only to the Great Depression of the 1930s, began in September 2008.

The sub-prime mortgage bubble, which supported an out-of-control housing loan market, eventually burst.

The tolerance of banks and other financial entities in granting credit, generated by years of stable economic development, low inflation and high levels of employment, had in fact exceeded all prudence. The Federal Reserve played a major role before, during and after the disaster.

Between March 2000 and December 2001, it encouraged interest rates to fall rapidly from 6 to 1.75 per cent, producing "easy money" that the more aggressive

bankers were ready to distribute among borrowers, being less and less attentive to their ability to repay.

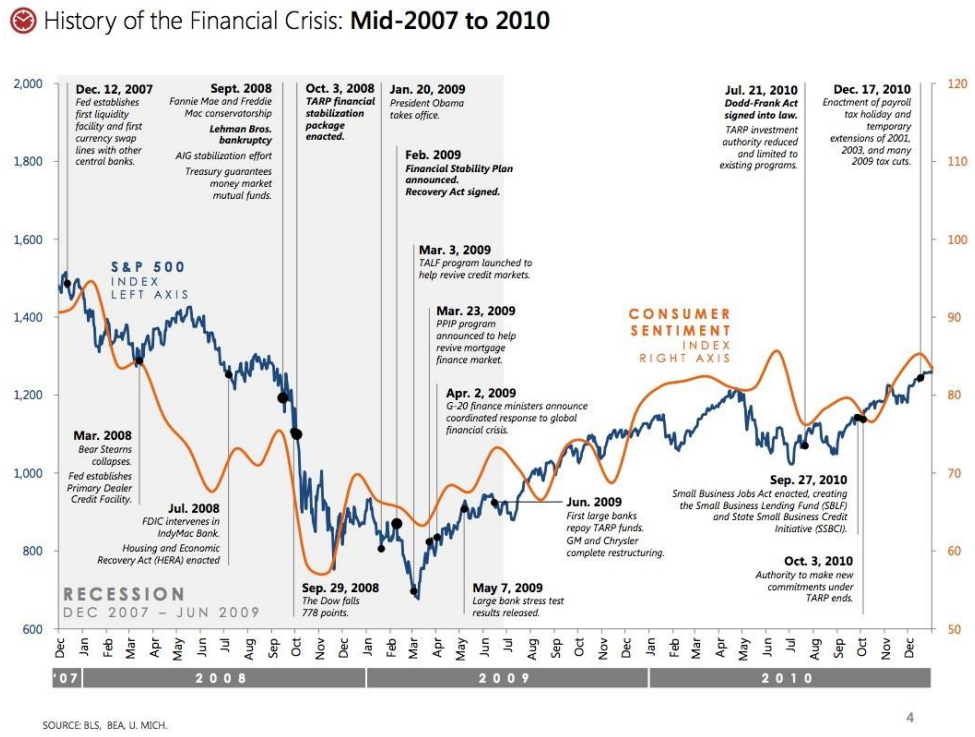
In March 2008, the investment bank Bear Stearns suffered the sale of shares by investors worried about losses on a large number of assets held, represented by mortgage-backed securities, which were beginning to default. Exposure to these toxic securities was extended not only to the United States, but also to financial institutions, corporations and pension funds in the rest of the world.

The Bear bailout requested from JP Morgan Chase obtained the Fed's guarantee for only $30 billion. A domino effect erupted in September 2008. With the collapse of the real estate market, the big world player Lehman Brothers also went bankrupt. Fannie Mae and Freddie Mac, the two financial entities that insured almost 90% of U.S. housing loans, also went into crisis. The government had to buy them both for 187 billion dollars, also intervening in the rescue of the largest insurance company, AIG, for another 85 billion dollars. It sold credit default swaps as insurance for mortgage-backed securities.

The U.S. government eventually approved an emergency plan called Tarp (Troubled Asset Relief Program) for $700 billion to provide liquidity to a financial system that had suddenly become short of it.

It was followed by other governments with similar interventions and there was tight regulation to limit the risk-taking propensity of the major intermediaries, the best known of which was the Dodd-Frank reform bill named after representatives of the two antagonistic parties in the US Congress.

In Europe, the crisis dictated for years the expansionary policies of the ECB, gave impetus to the launch of the Banking Union (2014) and the introduction of rules for intervention in the event of a crisis of systemic banks (resolution and bail-in).



Font: pewreaserch.org

5 - European sovereign debt crisis (2009)

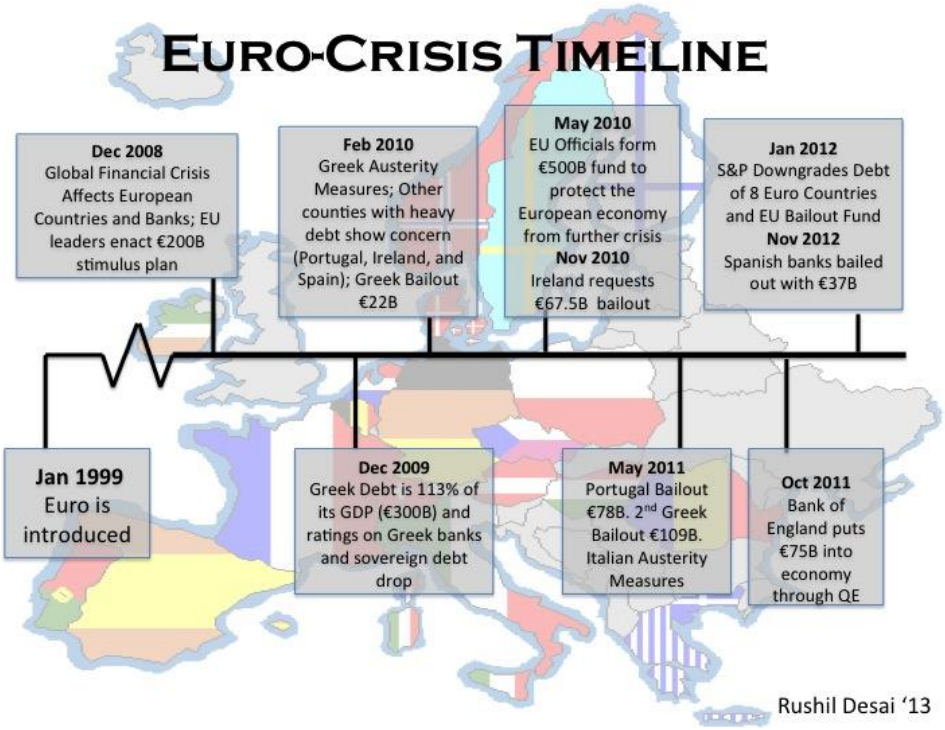
The European financial crisis came in the wake of the biggest US financial meltdown in 2008.

The first signs came with the failure of the Icelandic banking system, the effects of which spread to Portugal, Italy, Ireland, Greece and Spain, which became known as PIIGS.

The underlying reason was the enormous public debt they accumulated, with difficulties in refinancing them.

As was the case with the United States, the intervention of the European Central Bank was necessary. The duration of the European crisis was much longer. Although most of those countries pulled themselves out of the worst moment, the conditions are still far from satisfactory, with many of them struggling with low growth rates and high public debt. Greece is the best known example, with the double intervention of international support, imposed at a very high social price.

The European problems are not yet over, given the Brexit affair, the growth of political movements that do not recognize themselves in the traditional parties and express aversion to the economic policies of the Union, without being able to propose viable alternatives. These factors cast uncertainty on Europe's economic prospects.



Font: eurozonecrisistimeline.weekbly.com

6 - Fukushima nuclear disaster (2011)

A natural disaster that caused a high number of deaths, but also serious financial upheavals in Japan (the third largest economy in the world) and in the neighboring area was the earthquake of magnitude 8.9 and subsequent tsunami with ocean waves of over 30 meters that hit the northeast coast of the country in March 2011. The dead were 28,000.

On the economic level the devastation was of various kinds. The stock markets recorded losses of 16% for the Nikkei, 2.4 for the Dow, 9.5 for Topix and 4 for the Dax.

The Tsunami waves damaged the Fukushima nuclear power plant, causing radioactive material to spill, which took months to stop.

The disaster destroyed 138,000 buildings, causing hundreds of millions of dollars' worth of damage. The affected region produced between 6 and 8% of the national GDP. A further 11 of the 50 nuclear power plants in operation throughout the country were shut down as a precaution or due to damage, reducing electricity generation capacity by 40%.

Japan had to import oil, which caused further damage. Another negative consequence was the closure of some commercial ports from which the exported goods departed. The disaster occurred when Japan was just emerging from two decades of deflation and stagnation.

7 - Oil crisis (2014)

Much of the first decade of the new millennium saw sustained development of both advanced and emerging economies in Latin America and Asia.

This situation has led to a strong demand for goods, as happens in any cyclical expansionary phase, starting with oil.

China has been the major player in this boom, with double-digit development and an insatiable appetite for raw materials. The boom prompted the US and Canada to extract their oil, the former from the shale of North Dakota through fracking and the latter from the oil sands of the State of Alberta. Libya, which returned under Western control in 2011, also increased its daily oil production from 5 million barrels in 2008 to 8.5 million barrels in 2014.

At the time of the slowdown of the Chinese economy, the oversupply of oil and the collapse in demand for goods led to the halving of the price of the barrel from 110 dollars to 50. Since then, the price of oil has started to rise again very slowly, also suffering competition from renewable energy as a long-term movement. The economies of the OPEC countries and Canada have been affected.

9 - BREXIT (2016)

Finally, there is the endless saga of Brexit, a partnership with the European Union that has turned into a confused divorce, with no solutions in sight. It has been a conflicted relationship since the signing of the Maastrich Treaty in 1992, with the

creation of a single currency area and the transfer of national powers to the European institutions.

Britain did not adopt the Euro and overcoming strong resistance eventually joined the Union's social policies but continued to demand exemptions and special treatment. In short, it was a conflicting report until the 2016 vote in favour of leaving the Union.

The reaction of the financial markets in the face of the Brexit was one of fall, with the pound and the euro both weakened

The price of gold, an asset that serves as a traditional hedge against such risks, rose by 6%. The deadline of 29 March 2019, which was to mark the end of the report, was exceeded without agreement. The resignation of Prime Minister Teresa May these days is bound to increase the difficulties for an acceptable solution. The uncertainties are bound to damage the economic interests of both parties in the long term.

3.4 Last Black Swan event: COVID-19

The COVID-19 affair will leave its mark. This is clearly first and foremost a humanitarian shock. But immediately afterwards it will be seen that it is also an economic shock. The data is unclear and not very comparable. The forecasts are extremely complex.

The impact of the new coronavirus (COVID-19) on global trade is evidence that ecosystems are particularly vulnerable to risks outside their sphere of influence and control. The ecosystem of production chains extends to include companies around the world: companies buy goods and services from global suppliers who, in turn, source them from others. The commerce sector offers an essential service, but when even a networked part has to cope with the impact of an event like COVID-19, the ecosystem as a whole is subject to disruption. As a result, no company is immune. While interdependence makes the whole system more efficient, it can also lead to risks and fragility that are not immediately visible. With global growth driven by Asian consumers, any disruption on the other side of the world can have negative spill-over effects on a large scale. And because each chain has its own weak link, companies can also be subject to unexpected disruptions along their supply chain.

The Fukushima nuclear disaster in 2011 triggered an unforeseen shock for the world's automakers. Supply chains depended on a single electronics component manufacturer. The close proximity of its plants to the nuclear power plant led to its closure. This event caused an abrupt cut of about 40% of the global supply of microcontrollers, a type of custom chip used in automobiles, to stop car production worldwide.

Examples like this reinforce the idea that a company's supply chain is a strategic element. So how can companies effectively manage the risk of unforeseen disruptions?

1. The immediate priority is to take care of employees and their families. Timely dissemination of information is necessary to ensure that official recommendations are widely disseminated. In an attempt to limit contagion from COVID-19, employees from affected countries were not able to go to work regularly but, thanks to remote work, productivity could be maintained. The considerations that emerge during prolonged periods of working from home range from the most practical to the personal, from broadband speed to employee welfare.

2. The next step is to discover hidden dependencies through an end-to-end review of a supply chain. Through the mapping of suppliers and buyers, companies can draw up plans to protect themselves from disruptions down to the component level. Later, as roads, ports and loading facilities are also affected by disruptions, alternative logistics and distribution options may be required. In the month following the introduction of the first travel restrictions related to the Covid-19 outbreak, about half of planned departures on one of the main cargo routes from Asia to Europe were cancelled. Having visibility into all operations, from procurement to production and distribution, will enable companies to prepare emergency options in advance.

3. Once immediate impacts have been reduced, companies must prepare to meet latent demand that requires agility, as it can lead to peak orders. The availability of funding allows resources to be allocated quickly and flexibly to add capacity and avoid bottlenecks.

4. Finally, to try to anticipate future disruptions, companies should consider diversification of the supply chain. A wider range of suppliers in different geographical areas reduces the risk of a country being cut off. Stanley Black and Decker, the world's largest tool manufacturer, has recently expanded production in the US to avoid being dependent on a single geographic area.

The combination of these actions increases resilience, a feature that becomes increasingly important as potential disruptions multiply: whether infectious diseases, such as SARS, Ebola or COVID-19; environmental, such as Fukushima; financial, such as the global crisis; or political instability. The World Economic Forum's Global Risks Report paints an uncertain scenario, highlighting the intensification of environmental risks. Failure to mitigate and adapt to climate change is the main risk in terms of impact, followed by biodiversity loss.

As time goes by, the distances between companies and their suppliers may narrow. Both to be closer to the consumer and to reduce risks. However, it would be short-sighted to break these links that govern global growth. Indeed, using only national suppliers would reduce the ability to be resilient. It is essential to have a range of options available, as goods, services and expertise on the ground may not be available, competitive or even uncertain. As climate change causes disruptions to global trade, policy-makers must be careful not to add additional barriers to trade, as has been the case in recent years, but to lighten the burden.
Companies cannot control a volatile and uncertain external environment, but they can adopt a flexible response. As threats multiply, resilience becomes a key factor. Companies that stand out are those that can anticipate external disturbances.

Scenarios and comparisons

1. The key issue to be resolved in this crisis has been the ability of health care systems to cope with peak conditions. Health care systems designed with an efficiency criterion prove to be proportionate to conditions considered normal but

cannot withstand excessive peaks in demand for hospitalization; the resilience of these systems is the project of the future.

2. The decision to minimize human losses due to the disease, under these conditions, translates into a blow to the economy if politics deals with the issue in a generic way and does not seek a balance between the two problems, trying to block the contacts of the truly infected but leaving the majority of the population on the move;

3. The consequences can be imagined according to two alternative scenarios: a. a. a strengthening of the economically and physically stronger people, classes and countries with a worsening of the conditions of all the others; b. a paradigm shift with the search for more measured operations in resilience-oriented contexts.

Instead of using Resilience, Nassim Taleb prefers "anti-fragility". A resilient system recovers well after crises. An anti-fragile system improves in crises. Conceptual differences, but not necessarily fundamental. Also because we have to understand the substance of the problem.

The health care system under stress for the coronavirus shows how monomaniacal concentration on efficiency at all times reduces resilience and effectiveness during crises, in peak cases. Basically, as long as everything goes well, it cuts to the bone and when needed, it lacks flab. In Italy, where the true numbers of infected people have always been reported and the deaths have been attributed to the virus and not to other debilitating diseases, the answer has been to block the country so as not to collapse the health system (which would have caused an unacceptable number of deaths). In addition, a great deal of money was spent to increase the production capacity of the hospitals a little. The best was solidarity with the hospitals: resilience in Italy is in society. In France they had put aside the so-called "health reserve" and called back into service the people who were needed and who were already prepared to operate (Le Monde).

The resilience project is very different from the efficiency project: and should be adopted for essential public systems. It is about building systems that are redundant, flexible, without fragility: this implies a strong relationship with the community,

access to resources put in reserve, the possibility of using people who are prepared but usually do something else, and so on.

Between reducing the number of deaths and containing the negative effects on the economy, the search for balance is essential.

Some countries have chosen to aim to save as many lives as possible, putting the resulting economic crisis in the background. Other countries have chosen to aim to save the economy by sweeping the health issue under the carpet as far as possible. It is clear that the sense of responsibility applied to different values and emotions in different cases. And it is also clear that intelligence was measured by the ability to intervene harshly against the propagation of the virus without generic actions but through very targeted operations: an idea that is not science fiction is to use mobile phones, big data and artificial intelligence to predict who is infected or is really at risk of becoming infected and then stop it, letting others live almost normally. In Europe it seems more difficult to do this than in other countries: but could privacy be more resilient than inflexible? A temporary reduction in privacy for times of great crisis, which makes it possible to follow each person to identify who is really likely to be infected and therefore to infect them, can lead to targeted measures. (Reuters).

The scenario that sees the distance between rich and poor widens is very likely. If, however, a change in mentality becomes much more attractive, the scenario in which the community takes matters into its own hands and builds an important set of mutual aid structures and skills suitable for resilience. It cannot be the state that makes this choice. It has to be the community, helped by the state and private individuals. Social innovation is essential to think and realize this project of resilient society, able to reallocate resources quickly and effectively to deal with various crises, predictable and unpredictable.

The only certainty we have for the future is that there will be more and more unpredictable crises: normality changes as complexity grows. Connections enrich everyone's possibilities but multiply contagions. Climate change will create

unstable conditions and unprecedented environmental changes. Opportunities for criminals, multinationals and governments will lead to unforeseen conflicts. The stable scenario desired and assumed by neoliberalism is unrealistic. It never was. It will be less and less so.

CONCLUSION

Through this work it has been possible to fully understand how essential it is in the company to manage risks effectively and efficiently. This favors the achievement of greater business performance than the non-management of the same and therefore becomes a reason that influences the execution. From the analysis carried out so far, it has been possible to verify how different the strategies that a company can employ when a risk arises and therefore it becomes fundamental to analyze the situation in order to find the best feasible solution. It will have to allow the management of the risk which does not only mean its elimination, but also the possibility of exploiting some positive aspects or tolerating some of the negative ones. In fact, it has been possible to understand how often it is difficult or economically not convenient to eliminate the risk completely and therefore it is useful to define a level of risk that you are willing to bear.

The next step was to analyze what are the possible plans to overcome all disasters. It was seen then, the business continuity plan that allows the business continuity following negative events, and also all the procedures of the disaster recovery plan. After having analyzed the business risks and the different plans, it was fundamental to deepen in data aspects the dynamic and complex relationships that the company is called to build and maintain over time in response to the change of the market and the environment. In this complex and changeable adaptation to the change of the market and the environment, the company is called to anticipate the "turning points", i.e. the situations in which, to ensure the continuity of its management, it must make a profound change in its strategy, such as to reposition itself in competitive terms on the market. In other words, the company continuously proceeds to adapt to the market, mainly by increasing the efficiency of its management processes and improving the products offered to customers. By

proceeding in this way, it ensures the continuity of its management, leveraging the efficient and effective use of available resources. Over time, however, the increase in the intensity of change in the environment and the market makes it increasingly difficult and challenging for the company to achieve a balance with them to the point where it realizes that this dynamic balance can no longer be achieved except through its radical and new strategic repositioning on the same. This is the "Turning Point" that imposes to the enterprise the decision and the implementation of a strategy that allows it to overcome the competitive position reached on the market in order to realize a radically new one. The process that makes this deep and radical change of the competitive position of the enterprise on the market possible is that of "Innovation" able to create a new market.

After analyzing how the company can cope with unforeseen and unforeseeable events in order to ensure, through dynamic adaptation to the market, its continuity, I dwelt on the resilient thinking in the business organization making an analysis of the latest black swan events that have hit the economic world. Among these, it seemed relevant to me to dwell on the event that in this period is having a devastating impact on all sectors: the COVID 19, with the hope that this sad period of human history can end as soon as possible.

REFERENCES

Braman R.J. (2017), *How to create a Business Resilience Plan and Why*, Facebook 26 January 2017.Linton L. (1698), *Continuity Vs Crisis Management*, https://yourbusiness.azcentral.com.

Carlson C. (2008), Innovation: The Five Discipline for Creating What Customers Want, *Crown Business*.

Chan Kim W. and Mauborgne R. (2015), *How to create Uncontested Market Space and Make the Competition Irrelevant*.

Christensen C. (2016), *Competing against luck, The Story of Customer Choise*.

Denning S. (2015), How To Make The Whole Organization Agile, *Forbes*, July 2015.

Denning S. (2016), The four Keys You Need to Achieve Strategic Agility, *Forbes*, May 2017.

Denning S. (2017), Moving To Blue Ocean Strategy: A Five-Step Process To Make The Shift, *Forbes*, September 2017.

Denning S. (2017), Beyond Agile Operations: How To Achieve The Holy Grail Of Strategic Agility, *Forbes*, February 2017.

Ivezic M. (2017), *Enterprise Resilience-resilience- A model to survive and thrive in a world of change*;

https://www.linkedin.com, in L. Selleri, Cambiamento dell'Ambiente e Vulnerabilità dell'Impresa: il ruolo integrato Dell'ER della Resilienza e dell'Antifragilità nel fronteggiamento del Rischo e dell'Incertezza, *Economia Aziendale Online*, n. 2/2017.

Lindros K. and Tittel E. (2017), *How to create an effective business continuity plan*. CIO.

Owen S. (2016), *The Role of Risk Management in Disruption & Innovation*, https://www.linkedin.com/pulse/role- risk-magement-disruption-innovationstephani.

Pillai J. (2015), *Difference between DR, BC and Crisis Management*. http://www.Stay in business.com.

PwC (2016), *The Future of Industry: Brings Down the Walls*.

. Selleri L. (2016), L'Enterprise Risk Management quale sistema di protezione e di creazione di valore; *Economia Aziendale Online*, n. 3/2016.

Selleri L. (2017), Cambiamento dell'ambiente e vulnerabilità d'impresa:il ruoo integrato dell'ERM, della Resilienza e dell'Antifragilità nel fronteggiamento del Rischio e dell'Incertezza; *Economia Aziendale Online*, n. 2 /2017.

Thiel P. (2014), Zero to One, *Crown Business*.

Thiel P. (2016), Competition is for losers, *Wall Street Journal*, 30 April 2016.

Woo R. and Gallgan M. (2015), *Crisis Leadership: Five Principles for Managing the Unexpected*, http:// deloitte. Wsj. Com/risk and compliance.

CAS Enterprise Risk Management Committee, 2003, "Overview of enterprise risk management", 99-164.

Covello V., Mumpower J., 1985, "Risk Analysis and Risk Management: an Historical Perspective", Risk Analysis 5 (2), 103-124.

D'Arcy S., Brogan J., 2001, "Enterprise risk management", Journal of Risk Management of Korea 12 (1).

Dickinson G., 2001, "Enterprise risk management: its origins and conceptual foundation", The Geneva Papers on Risk and Insurance 26 (3), 360-366.

Golshan N., Rasid S., 2012, "What leads firms to Enterprise Risk Management adoption? A literature review", International Conference on Economics, Business and Marketing Management 29.

Knight Frank, 1971, "Risk, uncertainty and profit", Chicago University Press, Chicago

Pagach D., Warr R., 2010, "The effects of Enterprise Risk Management on firm performance".

AIIA, & PWC. (2006). La gestione del rischio aziendale. Milano: Il Sole 24 Ore.

Giorgino, M., & Travaglini, F. (2008). Il risk management nelle imprese italiane. Come progettare e costruire sistemi e soluzioni per la gestione dei rischi d'impresa. Il Sole 24 Ore.

Allen R.S., Haley P.P., Harris G.M., Fowler S.N., Pruthi R., *Resilience: Definitions, Ambiguities, and Applications*, In Resnick B., Gwyther L., Roberto K., *Resilience in Aging*, Springer, New York, 2011

Coutu D., *Organizational structure: How Resilience Works*, Harvard Business Review, pp. 46−55, 2002

Crouhy M., Galai D., Mark R., *Risk Management*, McGraw-Hill, New York, 2001