RISK AND/OR RESILIENCE MANAGEMENT

Jean-Paul Louisot*

Abstract

Risk management aims at managing all the uncertainties that may interfere with the objectives and missions of the organization. Resilience engineering aims at building its capacity to get over disturbances or stress while keeping the functionalities needed to survive, and possibly thrive. A recently open debate on an Internet blog launched by the risk managers of the Scottish Widows Bank seems to arise from what some professionals see as two competing branches of the management sciences. Whereas through the development of ERM – Enterprise-wide Risk Management – risk management is emerging at last to become a science, as well as an art and a practice, the mentioned above centered on the role of a newly forged name "resilience management". This opens a new front of the many debates that could derail the path to maturity of Risk Management as a science and reopen new silos much as Business Impact Analysis, BIA, or continuity management, might do if a clear distinction is not made between science, objectives and tools. However, because organizations are so interconnected today in the supply cloud that it is inevitable that they will face catastrophic risk and this is why resilience needs to be a core objective of any risk management plan? Whereas traditional risk management techniques alone may not be adequate to deal with such pervasive and insipient risk scenarios, resilience is ingrained into ERM.

Keywords: Resilience, Risk-Management, Enterprise-wide Risk Management, Strategic Redevelopment, Continuity, Risk to Reputation, Stakeholders

**Docteur ès Sciences de Gestion de la Sorbonne, Anc. Université Paris 1 Panthéon-Sorbonne, Institut Catholique de Lille, Directeur Pédagogique de CARM_Institute, Veuves*

1 Risk management objectives & resilience: how do they meet?

The core objective of any risk management effort is to ensure the organization survival whatever the circumstances it may be confronted to. In a financial approach to survival, one might say that all that will be needed is enough cash to go through the period following a damageable event; however this will be enough only if the organization can retain its stakeholders' trust and confidence through the episode. Although burning through cash may also be seen by stakeholders as a reduction in their value or if insurance was available at a nominal cost, an inappropriate use of assets.

However, even this prime objective may prove beyond the reach of some organizations under dire and exceptional circumstances; this is more specifically true when it comes to liabilities or environment damages. When referring to environment such events at the EXXON Valdez and more recently the explosion of the deep-sea petroleum-drilling rig Deepwater Horizon in the Gulf of Mexico come to mind. In fact, in most extreme catastrophes, the decision may be to limit their probability to a level such that stakeholders will "live with it." Their perception of the threat is such that the benefits of the activities of the organization prevail over the risk so that the organization retains what the British call the "social license to operate". With the explosion of social media, it has become of utmost importance for any organization to reach a proper balance taking into account all stakeholders' interests and expectations when making decisions at all levels; it may even prove the best way to ensure long term value for the stockholders.

On the other hand, a risk management objective limited to survival may well prove below the expectations of the stakeholders, even more so at a time when most large organization s recognize their exposure to procurement cloud collapse. When it comes to black swans, stakeholders will often recognize that a temporary disruption may prove unavoidable. But for exposures that could be qualified as moderate, that can be reasonably expected to occur over a five or ten years horizon, they remain volatile year in year out, the major economic players will request more and more to be satisfied that the tools of continuity put in place by their suppliers and sub-contractors will limit the consequences of any event on their own activities. Furthermore, the "survival objective" would not address the point of the economic result of the organization and the profits might take the stockholders on a rollercoaster that would not help the stock price for public companies. By the same token, economic partners might question

the long-term viability of the organization. In the case of non for profit, the rollercoaster ride by those in need can only exacerbate, for example, their need for government assistance which introduces more government debt and perhaps taxes. The sine wave magnifies with such disruptions. At the end of the day, it might discourage donors who would feel that the management of the organization *"does not know what they are doing."*

Other constituencies, like state, local authorities, and consumers could also be alerted by the perception of a chaotic short sighted management. In such a context, top management must assign other more forcing objectives to risk management such as maximum acceptable downtime, stabilizing financial results, corporate social responsibility, in other terms the impact of ethical choices or the organizational Values. In other terms, they must decide on the conditions they wish the organization to rebound after a serious, or even catastrophic. Depending on the organization, the goal may be to retain or gain market shares, maintain or improve profit, reach out to more people in need, etc.

With no need for long developments here, as top management set higher post-event objectives, risk management will require more resources, including finances. Therefore there in an increasing conflict between the general pre-event objective of economic efficiency and the choice of an improved rebound post-event. In other terms, the increase of overall "cost of risk" might be questioned by the owners and the financial analysts.

This is a clear illustration of the need to assess risk management efforts over the medium or long term, i.e. at least ten years, whereas the financial markets tend to force CEOs to manage short terms results, annual if not quarterly. If more resources are diverted towards risk management, these are not used to boost development and improve the return on capital and the short term results are less convincing.

To justify these « non-essential » efforts, it is necessary to broaden the horizon to take into account a major event could occur at any time and probably during a ten year period many major events could disrupt the organization. However, financial analysts should develop models taking into account the degree of potential failure when most firm are valued on a present value approach that has a built in hypothesis of an infinite future. What techniques can measure a long-term benefit to the company? To provide an answer to this question, it proved necessary to introduce a new concept that is gaining momentum in the strategic thinking at all levels; it is a way to assess a longer term management including elements such as sustainable development and corporate social responsibility. The concept of resilience is borrowed from metallurgy, but used also in psychology and sociology is resilience.

Any academic development on risk management, must refer to it, and a growing number of annual reports for global companies include it in their risk presentation. Although this explosion is relatively new in the last five years, as early as the nineties, the Canadian Auditors Associations provided the first definition in a guide for its members. In metallurgy, the resilience of a metal measures its capacity to regain its elastic qualities after a stress, mechanic or thermic; in social sciences, it measures the capacity of an individual, or an organization, to adapt to a rapidly changing environment.

Among the topics is the taunting issue that companies must improve flexibility without deviating from their core missions. However, the way in which they carry the mission may have to adapt to changing expectations. For example, it may not be efficient for a single product company diversify because that would dilute its efforts to provide optimal benefits to consumers for its desired product. In the same time, it should remain keenly aware should the consumers' taste move away from its one product and move ahead of its competitors or substitutes to anticipate such evolution.

As far as risk management is concerned, resilience measures or assesses the capacity of an organization to recoup after a major disturbance, or survive a crisis. This will typically require that the organization will be able to fulfil its major obligations to its main stakeholders, i.e.:

- society, comply with laws and regulations;
- personnel, retain employment levels & pays salaries;
- economic partner, secure contractual terms and conditions;
- stockholders, maintain profitability & dividends.

2 Evolution & explosion of Risk-management, what of change management?

To understand the role of the concept of resilience in the current risk management landscape, it is necessary to review briefly the evolution that risk-management went through during the last two decades. The explosion of risk management as a practice in many organization is such that many professional programs in universities now include risk-management as a fundamental branch of the management sciences. Few academics and professionals envisioned this evolution but clearly they have seen continuity and crisis management as becoming important processes in any organization. And is that not, what resilience is about?

In this context, risk management foremost objective is resilience. And this concept is applicable to all branches of industry and services, even though financial institutions seems at the forefront of the movement. One of the participants of a recent debate on the Internet suggest that that resilience is the surplus of the capacity of an organization to face a major disturbance, and the damages it might incur in a

given situation. The higher the difference, the margin, the higher the resilience. However, the limit of that vision is that is looks only at the financial resources, thus ignoring in fact human, technical, partners and information resources. Including, what will develop on the social media, and the impact on the organization's reputation.

Furthermore, the capacity of an organization to develop the right response in any event is directly linked with its suppleness and adaptability. This means that the management style and structure have a direct impact on the organisation resilience. A very hierarchical and bureaucratic organization whose personnel adheres strictly to fixed processes, with no leeway to act according to circumstances, even in the case of a crisis, where he must gain prior authorization from his hierarchy for any change like, for example, the implementation of a continuity plan. Only organizations that can offer a capacity for change can survive like a building erected to resist earthquake. This issue reflects a debate not yet resolved in the ISO 31000:2009 standard, where the need for "risk-owners", the operational managers to be in charge of managing the risks at their level, requires that they have both the responsibility and the authority it the ERM – Enterprise-wide Risk Management – is to be effective.

There is a new approach to resilience for which the concept goes far beyond risk-management, and even its thought process. In this context, resilience is the capacity of the organisation, and its staff, to adapt under all circumstances to changes, challenges, failures, and even ruptures or crisis. Thus resilience is key to the success of any strategy whatever the uncertainties of the future. However, resilience seems natural in some organisations' culture where individual initiatives are encouraged. May be an illustration will help at this stage, if one stumbles and falls, it might be worth catching the one Euro coin found on the ground before getting up! This is what Bertrand Robert has conceptualized under the construction of "creative rupture" that invites an organisation in such a situation to conduct a new SWOT analysis to reinvent its strategy so that it can take advantage of the evolution in its internal context (strength and weaknesses) and external context (threats and opportunities).

For example, in a positive/negative sense, the companies that supplied the infamous FEMA trailers had to change their ideas of distribution after the disaster from summer fun seekers to disaster homes. The issue of capitalizing on ruptures, is summarized in one question: Can the organization think of creative alternative uses of their products or creative new products that work within the framework of the economy or society after a disaster? With a daily regional paper in France, that would be destroyed with no chance of rebirth in case of a fire in its printing shop, we imagined to use the resources to develop an online paper and redevelop the land for apartments building as it was in a desirable location in a middle size city in the heart of France.

In the management of change, communication systems play an important role, all the more critical in the time of stress, it is essential that communication be a continuous process linking the organization with its stakeholders and building or comforting their trust, the communication on risk is only a part of a bigger picture. The communication in time of a crisis is efficient only so far as it rests on the institutional communication. Resilience requires also the development of a consistent and robust communication process with all stakeholders at all time.

3 The heart of the debate might it be differing visions of resilience?

In some industries, failure is not an option, as is the case for aeronautics and space, resilience is at the heart of any project, and the system must be developed to ensure success. In such a context, the entire organization must be governed, prepared, and trained for the resilience of all its operations. In such a situation, what is the relationship between resilience and risk management? The system is subjected to a system safety analysis that is part of the risk management framework.

If the risk-management program is part of the missions, developed during the conceptual stage and implemented even before the system is operational, then all risks should be identified and information provided even to those in charge of the conception; it is the most efficient way to reduce the probability of anything wrong happening and enhance the capacity of coping with the unexpected. On the other hand, if the implementation of risk management is delayed until the beginning of operations, it can identify emerging risks new threats, weaknesses, and exposures to prioritize them and propose an improvement process, but it may prove lacking as an add on rather than a built in process.

Some professionals and academics might suggest that in such a context, risk management may not be known under that name as it is part of the overall project engineering integrated into sound management incorporating "lean management", "legal compliance". As far as I am concerned what is described here is a real holistic and integrated risk management, i.e. ERM. In a proper system safety approach, risks are assessed, and treated as early as the conception phase and resilience a definite mission of the system. One could summarize in a proverb: "*It is better to prevent than to cure"…*

3.1 Resilience & standards

In the United Kingdom, the organization in charge of standardization, the BSI, recently published BS

65000[1] centered on resilience, but at the public level. There are a number of other standards that touch on the subject, without being exhaustive here[2]. From an attentive study of those documents, it springs that risk and resilience are related concepts; however, most professionals would agree that resilience is a key objective for all organizations as they tend to manage their resources so that they can adapt to changes, even radical changes and ruptures.

However, within this enlarged framework, resilience would extend far beyond risk-management to all the protective functions including, but not limited to, IT security, Physical security, health and safety, environment management, etc. Therefore, it must be envisioned within 360° approach combining culture, strategy, and change. It is in fact a definition of a mature ERM including continuity management, to reduce the impact of potential disruptions, and the learning process needed to make quick decision under stress even with scarce information in a time of a crisis.

3.2 Engineering resilience & ecology

The concept of resilience is so widely used that it covers different realities as the following:

- ***Engineering or reactive resilience***: Engineering resilience would be the velocity of return to a new stable state following a disturbance which implies to focalize on the speed of functioning. It is the issue of the organization reactivity, including the acceptable degraded functioning state and/or downtime a key parameter of any continuity management effort.
- ***Ecological or proactive resilience:*** Ecological resilience would take into account the unavoidable change within and without a system, like entropy, and aims at finding a new equilibrium within the new contextual framework thus reflecting the capacity of the organization to adapt and thrive. This proactive resilience rests on the flexibility of the organization that allows it to find positive answers to disturbances and could be also defined as a pre-event resilience founded on environmental sciences, thus key to sustainable development.

3.3 Risks & resilience

With this new paradigm over resilience, some professionals envision risk management as a part of resilience management. However such an approach would mean that risk management is limited to manage known risks. As a revision of Donald Rumsfeld remark, that would mean that risk management is expected to cope neither with the "known-unknown", i.e. emerging risks, nor with the "unknown- unknown", i.e. the Black Swans. Woods and Wreathall[3] develop a model or resilience in analogy with the stress-tension approach. They identify the initial response to an event as the uniform response of the whole organization when it has the capacity to meet the challenge. This is what they call the first level of reactive capacity, do they have in mind risk management? The second level of response is the capacity to adjust to a new situation and that would be the real deep resilience where the organization can no more rest on planned responses, processes, and resources whereas the answers go far beyond the limits of the first degree adaptation[4]. In their framework, risk management would only allow to anticipate on the probable and the possible, and true resilience would come only with the second order of change to adapt.

3.4 The right answer to different levels of disturbance

In a global and integrated approach, risk management cannot be limited in scope to known risks or to situations where prior continuity plans can be implemented to go over the difficulty encountered like an automatic pilot on a plane. In real life, it must address both reactive and proactive resilience. Efficient risk management applies to complex systems, interacting in an ever growing web of interdependencies, thus by essence in an unstable equilibrium. When the system moves away from its built-in balance, corrective measures must be implemented that will restore a balance. However, these swings out of the ordinary are still too often called "crisis" whereas all emergency situations are not conducive to crisis; naming crisis situations that are merely unexpected, or out of the probable, can have to negative impacts:

- A craze effect that could generate a crisis ; and
- A blasé attitude form staff that will not react as promptly as needed when a real crisis will loom.

This situation of unenlightened catastrophism » is clearly identified in a recent book by Dylan Evans[5] when he suggests that *"transforming low probability events in quasi-certainties when these events are perceived as particularly formidable by stakeholders is an approach of worst case scenario that can induce dreadful decisions."* This is the exact reason why it is crucial for the organizations survival and resilience that those in position of authority react un a gradual manner to the nature and potential severity of given circumstances.

Whereas the level of disturbance of a complex system is a continuum, we have chosen to illustrate the preceding remarks based on the description in four

[1] BS 65000 - Guidance for Organisational Resilience

[2] Business Continuity ISO 22301 , Risk Management ISO 31000, Crisis Management BS 11200 published Sept 2014, Resilience November 2014, and Business Collaboration BS 11000

[3] See bibliography

[4] Woods & Wreathall, 2008, p.146

[5] Evans Dylan, Risk Intelligence, New York (USA), Simon & Chuster, inc; (2012)

states proposes, among others, in the November 2007 issue of the Harvard Business Review, that is to say:

- ***Simple state***: It is the state for which the system has been set up, the nominal state and it is based on "best practices", an unstable equilibrium rarely maintained, but with the following characteristics:
  - ✓ Stability, clear cause/effect relationships;
  - ✓ Slow evolution, order and accomplishment;
  - ✓ Avoid complacency.
- ***Complicated state***: it is a state where expertise is essential and the domain of "good practices". It is the state in which operational managers, risk owners, can handle daily variations within the possible and it is characterized by:
  - ✓ Multiples possible responses, analysis of different solutions, readiness to listen to non-conventional thoughts;
  - ✓ ***Beware:*** making timely decisions is more important than to wait for the best.
- ***Complex state***: This is the state where innovating solution must be investigated ahead of the situation to plan for action, it is still in the hands of the operational managers but it requires a formal planning process. It is where business continuity plans are an efficient tool and it is characterized by:
  - ✓ Only experience feedback will lead to a good understanding the chain of events;
  - ✓ It is essential to size innovation, embrace creativity and new management models;
  - ✓ ***Beware:*** there is a risk to attempt a return to the pre-event situation without taking into account the new context.
- ***State of chaos or rupture*** : This is the state when acting fast is essential but with a strategic vision that is beyond operational managers and require the input of top management and even may be the board of directors, it is the level of disturbance that call for a *Strategic Redeployment Planning (SDP)* and the state is characterized by:
  - ✓ Impossibility to discern stable cause/effect pattern, no manageable schemes;
  - ✓ Some degree of order must be restored to return to a complex state, may be different from the pre-event equilibrium;
  - ✓ Communication must be transparent and specific with instruction coming from top management to implement swift strategic changes if need be *(it is not the time for dialogue)*
  - ✓ ***Beware:*** This is an ideal situation to implement innovations and strategic U turns *(change management)*

4 How to strengthen the resistance to risks? Ten "best practices"[6]

In terms of resilience, experience feedback is a key factor in the learning process. However, the experience of the organization may not prove enough to strengthen its resilience; lessons must be learned also from situations experienced by other organizations in the same industry, or similar contexts. At the end of the process, it is all about transmuting threats into opportunities to ensure optimal value creation.

However, it is important also to keep a clear mind and a vision far beyond the organization's backyard, best practices may be found in other branches, other part of the world, may be even from prospective substitutes. It is through a cooperation with the World Economic Forum that PricewaterhouseCoopers (PwC) has gathered a wealth of experiences from international experts and CEOs, mainly on corruption risks, cyber-risks, and risks in the procurement cloud, as well as natural catastrophes, but that could easily be extended to all other forms of risks. PwC came up with a list of ten "best practices" to strengthen the resilience of an organization:

- ***Educate permanently to instill the organization's Values***: Even if only a small part of an organization is going through a problem it can put in jeopardy the whole; this is why a strong common culture and shared values are vital for its resilience. For example, to limit risks linked to corruption the Royal HaskoningDHV[7] (RHDHV) has introduced a complete program of further education to embed integrity at all levels in the organization.

"Business integrity goes far beyond corruption, collusion and fraud; it includes also personal attitudes and behaviors"[8]

- ***Collaborate to promote information transparency:*** Within huge complex and global networks, transparent information from individual actors for decision makers enhances risk resilient decision making. The Barrick Gold Corporation[9] strengthened the effectiveness of its due diligence process regarding corruption and procurement through cooperation with NGO operating global networks; thanks to this decision they improved third parties' confidence in the information.

[6] Ed Simmons - Price Water Coopers - Access the World Economic Forum's full report here: Leading Practices Exchange: Managing Risk

[7] RHDHV is an international firm consulting in engineering and project management.

[8] Anti-corruption Practice 2 – UNDCP (United Nations Development Programme)

[9] Barrick Gold Corporation is a Canadian firm specialized in gold mining.

"A collective approach is recommended for transparency and due diligence to curb risks, and specifically those linked to corruption"[10]

• ***Promote zero tolerance for any breach on risks handling:*** There are some risky events that should be deemed unacceptable by organizations, and which all involved should clearly understand to be so. To limit corruption risks, Skanska[11]put in place a "five zero" internal policy. The five pillars to conduct a project are: zero non profitable projects, zero environmental hazard; zero workers comp, zero ethical breach, and zero quality defect.

"The three-step approach – pre-qualification, performance evaluation, and suppliers' development – allows to eliminate problematic suppliers." [12]

• ***Question permanently the hypotheses:*** At a time of accelerated change, the hypotheses on which were based the risk-resilient decisions are not valid anymore. The WHO questions continually the hypotheses that lead to the manufacturing of anti-flu vaccine anticipating virus mutations. In 2009, the aftermath of the H1N1 pandemic lead WHO to question the hypothesis according to which major pharmaceutical companies could increase their manufacturing in developing countries. Therefore, WHO helped the development of local productions of vaccine in these countries that resulted in an improved access to vaccination for the populations.

"It is essential to develop and implement a process to monitor and question the underlying hypotheses for the protection."[13]

• ***Support staff, so that they support the organization***: If the staff of an organization are not personally resilient, then the organization itself cannot be resilient, all the more during or in the aftermath of a crisis. During the nineties, following hurricane Andrew landing in Florida, local employers took many initiatives, as part of their pre-event planning, to help their local employees to recoup. These firms' assessment was that the assistance provided to their staff would help them support their employers and enhance the local economy resilience.

"It might be counter-intuitive that companies already stricken by a disaster increase their own burden by taking responsibility for additional risks and use its capital for the benefit of their employees. However, evidence proves that a swift return to work of the employees motivated for the restauration of their employer, it is probable that the employer would take longer to recover, and may be even never recover."[14]

• ***Make decisions on independent and reliable data bases and information:*** In a time of a rupture, or a crisis, data can be corrupted or lose credibility whereas robust informed decisions rest on the availability of specific and reliable data. The Japanese subsidiary of Deutsche Bank was able to make sound decision during the Fukushima Daiichi disaster thanks to independently collected data, at a time when other sources provided conflicting information.

"It is essential for organizations to rely on informed and exact assessment to make decisions in a time of a crisis."[15]

• ***Rehearse and prepare for a crisis with drills:*** Although organizations are not often challenged by crisis, they may still happen at any time and top management, as well as risk management professionals must be ready for action as early as the warning signs. There again, Deutsche Bank has developed a global program to train managers in crisis management through a series of real situation drills so that they develop the skills needed to act swiftly and with confidence in such situations.

"Specific plans are less useful than the capacity to develop a plan under stress when the situation requires. At a time when catastrophic risks are more and more global due to increasingly complex web of interconnections, a local and swift response is vital."[16]

• ***Set up alarm systems that will facilitate swift and early decision making:*** In most crisis, speed is of the essence. Therefore, information and systems that bring an early detection of threats are essential as they allow the organization to react even before the impact on its activity. To ensure a protection against an increasing number of cyberattacks, the US government has set up an agency specialized in the detection of emerging threats to alert critical infrastructure organizations, and the development of specific loss reduction strategies.

"Governments should set up agencies to alert economic agents on emerging cyber risks and loss control strategies for threats on critical infrastructures."[17]

• ***Place the responsibility for resilience on top management:*** Resilient organizations are able to identify trends, adapt to changing contexts, and ensure collaboration throughout the organization. But this can be achieved only if top management is involved in the project. Because of the ever increasing number of cyberattacks, among other threats, financial institutions have moved the responsibility of cybersecurity from the IT department to the CEO in all subsidiaries, with an overview by the board of directors. In the same time, the risk owners will have

[10] Anti-corruption Practice 4 – UNDCP (United Nations Development Programme)
[11] Skanska is a Swedish firm in the field of building infrastructures for International projects.
[12] Anti-corruption Practice 7 – UNDCP (United Nations Development Programme)
[13] Catastrophic Risk Practice 2 - United Nations Office for Disaster Risk Reduction (UNISDR)
[14] Catastrophic Risk Practice 4 - United Nations Office for Disaster Risk Reduction (UNISDR)
[15] Catastrophic Risk Practice 5 - United Nations Office for Disaster Risk Reduction (UNISDR)
[16] Catastrophic Risk Practice 15 - United Nations Office for Disaster Risk Reduction (UNISDR)
[17] Cyber Risk Practice 1 - United Nations Office for Disaster Risk Reduction (UNISDR)

to be in a position to react to risk that materialize at their level, hence the responsivity for managing risk within their scope of action must be coupled with the authority to act swiftly when something goes awry.

"Cyber resilient strategies should be developed at the board of directors' level in each organization so that it can efficiently identify trends, adapt continuously to business contexts, and be able to implement an efficient response to systemic chaos and ensure continuity of operations, to the best of its ability."[18]

- ***Share knowledge and experience within a network of reliable and trustworthy partners:*** Procurement clouds, critical interdependencies, systemic threats, these are only illustrations of the many networks the resilience of which is essential for the resilience of each organization which is only but a knot. Sharing information and know-how, sometimes very sensitive, in a network of partners with whom the work with trust and confidence, will improve the resilience not only of the organization, but also the entire network. The fight against cyber threats on critical infrastructures lead by the Australian government rests on a network of trusted and experienced organizations to share critical information and security strategies that facilitate quick responses and resilient defenses.

"Sharing knowledge with trust between private and public stakeholders improves the understanding of cyberattacks and the response necessary to curb those that could strike critical infrastructures."[19]

5 It is too early to risk a conclusion – a status report

The debate is still at an early stage and will be further fueled by the multiplication of sources and changing nature of uncertainties in the world imply that all organizations need to adapt permanently. However, it is all to cleat that the core mission of risk management will remain to assess all risks and offer solutions to curb their probability or their impact, not only known risks, but also emerging risks as well as those not even imagined today.

Events that occur rarely, or even that never occurred before, sometimes called Black Swans, are particularly difficult to handle and require a lot of attention; however, their management should not divert from the more common risks the systematic management of which not only reduces sources of inefficiencies in the organization, but also participate in the preparation of all staff for the handling of the dire situations. This will be effective only if the increasing independencies are recognized and the efforts are extended to and shared with all the partners as not a single organization is in a position to identify and mitigate all the threats that could disrupt the network emerging from within or without its known frontiers.

It is therefore necessary for the whole network to develop its adaptation capabilities based on a common foundation. But is there a way to achieve such a compatibility? It will require a social learning process engaging all citizens, an understanding of Paradoxal management[20], and a culture of co-evolution[21], rather than letting the Darwinian principle of natural selection be applied in these situations. It is essential to take advantage of punctual equilibrium offered by a wide functional diversity. It is then easy to understand how resilience puts an organization in a position to size the opportunities to improve or innovate that are offered by the changes in its internal and external context.

It is critical for an effective risk management that shared exposures and interdependencies are recognized and jointly managed. No organization lives in an autarkic state and the disruption suffered by some can impact the whole network like a shock wave. The British government has clearly identified the need when it ruled that risk managers in local authorities are requested to set up an active dialogue with all the risk-managers of public and private entities present on the territory. Le gouvernement britannique a bien identifié ce besoin en exigeant des risk-managers dans les territoires qu'ils mettent en place une concertation effective avec les risk-managers de tous les acteurs publics et privés actifs sur le territoire.

Developing a diagnostic or the entire system is all the more important that an organization may be surprised by a situation that may seem random or unpredictable whereas it is the inevitable consequence of a chain of events that was not identified proactively. True resilience, therefore, requires an in depth understanding of the internal and external contexts in which the organization operates, which is precisely one of the recommendation of the ISO 31000:20009 standard, and positioning the organization in these contexts. If this first step was to be ignored, the rest of the risk management efforts would be practically sterile, as the organization would not be in a position to curb its major threats, and enhance its best opportunities.

To reach the level of knowledge of the context needed, the approach must be dynamic and identify the main force lines of change. It is armed with this understanding of the systems potential weaknesses that the organization can identify its thresholds of fragility, assess how robust is the system, measure the

[18] Cyber Risk Practice 2 - United Nations Office for Disaster Risk Reduction (UNISDR)

[19] Cyber Risk Practice 5 - United Nations Office for Disaster Risk Reduction (UNISDR)

[20] Paradoxal management rests on the conviction expresses in a formula suggested by Bernard Nadoulek: "A company in which there is no order cannot survive, but a company without disorder cannot evolve." This conviction is the prerequisite in any collaborative management.

[21] Coevolution is the dynamic of evolution implying the interaction between genes and culture over a long time horizon.

degree of leeway at all levels. This in depth analysis allows to come to grips with anarchy, i.e. the stages of evolution that the organization must go through to adapt to the new realities, and take into account the various scales that influence the main stakeholders' interest. At the end, the most efficient approach would be to build the hyperspace of danger[22] of all the stakeholders to decipher the complexity of the network in which the organization is involved.

In this perspective, the traditional concept of resilience, called engineering here above, which would entail a return to the ex-ante situation, might prove dangerous if it means resisting to change, instead of adapting to it. Furthermore, in the first place, why return to the situation that let the dreaded event happen? The organization would not learn from its mistake and reinstate the even causes that generated the disturbance.

This is why assessing the level of disturbance as suggested above is essential for the best use of resources allocated to the management of risks. More precisely, the distinction between situations where prior continuity planning will return the organization to a new stability, without major change in the strategy, and those situations that call for a "strategic redeployment plan" where top management will be called upon to reassess the existing strategy.

In addition, contrary, to what some suggests, risk management cannot be limited to managing known risks, but also, and mainly, it must ready the organization to confront the unexpected, the unknown. The natural extension of traditional risk management, linked to insurance covers, is to work on Black Swans, and thus make the organization more robust.

Resilience i.e. the continuing development and adaptation of an organization in a context experiencing a constant evolution, has become a fundamental objective of top management. Risk-Management is the core function that contribute to building and preserving resilience provided it goes beyond the daily management of known risks and embraces a long term vision. However, this is possible only within the scope of ERM – Enterprise-wide Risk Management –, global and integrated extended to all the actors of the organization, internal as well as external, which supposes a share vision, shared values and a permanent effort of education and training.

There are many activities that contribute to the science of risk management, and its implementation within all organizations. They include continuity management, economic intelligence, health and safety, security, etc. that are all essential to the building and strengthening of resilience. However, risk management can be fully effective only if it is involved at all levels, strategic, tactic, and operational.

The board of directors must back all the efforts of risk management and tackle directly all the exposures whose impact is potentially strategic but they must be weary of only an inside-out vision and be sure to put in place instruments to obtain an outside-in vision that only questioning external and internal stakeholders can bring. It is the only way to take into account on all decision making the expectations and perceptions of stakeholders. It is the condition for the organization's strategy remain relevant and, provide products and services that meet the short, medium, and long term expectations of its economic partners while meeting its social responsibility obligations; thus keeping its "social license to operate".

Resilience finds its real existence, its soul, in the organization's reputation that must be patiently built and preserved throughout the tribulations of the world; but are not risk to reputation at the heart of risk management?

However important reputation is, a company might maintain its good reputation to the end but simply expire because of the weight of disaster? The case of Cantor Fitzgerald was called to my attention. In the WTC 9/11 disaster Cantor Fitzgerald lost almost all of its people. It was known for its great management and compassion—but in the end it suffered unmercifully from the disaster. It managed to survive, but how did it do so and is it the same compassionate company it was before?

References

1. Evans Dylan, *Risk Intelligence*, New York (USA), Simon & Chuster, inc; (2012)
2. Gauthier- Gaillard Sophie & Louisot Jean-Paul – Diagnostic des risques – AFNOR, 2nde Edition (2014)
3. Kauffman, S. A. (1991). Anti-chaos and adaptation. Scientific American, 265(2), 78-84.
4. Louisot Jean-Paul, 100 Questions pour comprendre la gestion des risques – AFNOR, 2nde Edition (2014)
5. Walker, B., Holling, C. S., Carpenter, S. R., & Kinzig, A. (2004). Resilience, adaptability and transformability in social--ecological systems. Ecology and society, 9(2), 5.
6. Woods, D. D., & Wreathall, J. (2008). Stress-strain plots as a basis for assessing system resilience. Resilience Engineering: Remaining Sensitive to the Possibility of Failure, 1, 145-161.

[22] See Georges-Yves Kervern, "Latest advances in Cindyinics" – Economica Paris, 1994