1 Foundations

This chapter demonstrates the need for quantification in the definition of a risk management programme. In the first section, we introduce the foundations of risk management, based on the definition of an exposure: object of risk, peril, and consequences. We present the structure of the risk management decision process: (1) diagnosis of exposures, (2) risk treatment, and (3) audit and corrective actions. The design of a risk management program is the most significant part of step 2. Recent progresses in risk management show that this design should be addressed in a strategic, enterprise-wide manner, and therefore account for conflicting objectives and trade-offs. This means that risk cannot be limited any more to the downside effect but takes into account also the upside effect. The central objective of global risk management is enhancing opportunities while mitigating threats, i.e. driving up stockholders' value. *Therefore, risk quantification has become the cornerstone of effective strategic risk management*. In the second section, we propose a general approach for risk quantification: exposure quantifies the objects exposed, peril is quantified by a probability of occurrence, and consequences are quantified by a severity or impact, all these quantities being of course variable, and, most importantly, partially controllable.

RISK MANAGEMENT: PRINCIPLES AND PRACTICE

At a time when the world was fairly stable and the economy was based on scarce physical goods, purchasing insurance cover seemed the right answer to risk management: most of the perils were insurable, and the insurers acted as guardians of the mutualization process – eager to keep their costs down, they had even developed sophisticated ways to control those perils. Part of the deal in any insurance contract was to help the insured mitigate their risks so as to protect the overall mutuality. Furthermore, physical assets – plant and equipment – were essentials as customers were queuing to gobble up the production as soon as it was flowing again. Therefore, the insurer providing the capital necessary for rebuilding the production capacity was enough to pull the insured through a difficult time. However, even then, a more structured approach to risk management might have saved lives unduly wasted as they were altogether "cheap" for those liable for the deaths! Then in the 1960s and 1970s the pace started to accelerate, and in most of the developed world markets became mature. Marketing techniques became more sophisticated, creating differences and niches, while the offers among which customers could choose became increasingly differentiated. At the same time, services grew in importance, and producers became more and more intertwined. Other perils – economic (such as changes in customers' taste), natural (such as earthquake or flood), human (such as industrial intelligence or terrorism) – started to make evident the limitations of the "all insurance" approach. It was then that risk management started to emerge as a separate management field.

Furthermore, so many catastrophic events have taken place since the beginning of this century that it may seems frivolous to go back to 1 January, 2000 when the feared "Year 2000 bug" did not strike, or at least did not create the chaos that some predicted. However, in the developed

world, whose economy is heavily dependent on computer energy, all the entities involved, both public and private, had invested heavily to amend their information systems to stand off any problems. In addition, crisis teams had been set up to correct any last minute incident.

We know now that a number of "small" incidents did occur but have been fended off thanks to the experience gained through the preparation process. On the other hand, at the same time, metropolitan France lived through one of its worst recorded natural disasters during the last week of 1999. Mother Nature reminded French executives and elected officials that risk always occurs with dire consequences where it is not expected, where it has not been identified and analyzed beforehand. The immediate reaction is to call upon insurers or the state authorities for remedies!

However, the final lesson came when it was learned that in most public utilities, providing electricity and railways travel in France, for example, the "2000 readiness crisis management team" was on hand to make immediate decisions that helped reduce the impact on the economic life of the two consecutive tornadoes that destroyed many electrical lines and stopped trains in the middle of nowhere!

In spite of the current evolution, the risk management responsibility is still limited to insurance administration in too many private as well as public entities. This limited view of the function is even further restricted when the talents are spent on long bidding processes or hard annual bargaining with the insurance carriers, with the help of an intermediary, in order to limit premium budget increase for the next period, or, even better, to obtain significant cuts with improved cover. Of course, many risk managers are in charge of claims management. This means they can, on a day-to-day basis, contribute to the speedy conclusion of substantial loss compensations from the insurer.

On the other hand, technological breakthrough and complex economical networks combine to create an ever-expanding web of risks bearing down on the organizations. Each organization is part of a long chain comprising suppliers and subcontractors as well as customers. Furthermore, it is not enough to identify the risks of a given entity; the analysis must be expanded to include regional, state and even continental considerations. Zero inventories (procurement management) and zero defects (quality management) have increased both the frequency and severity of risks while widening the uncertainties involved.

Finally, what was perceived in the early 1980s as a new economical crisis, a new stage in the development process, is now clearly turning into a major shift in the worldwide markets. The phenomenon is so far-reaching that some call it a "rite of passage" from one era (the industrial) to the next (the post-industrial).

Indeed, some say we are leaving the era of the management of opportunities to enter the era of the management of risks. Opportunities refer to favourable uncertainties, the chances of gains, whereas risks should refer to both "unfavourable" uncertainties, the chances of losses only, i.e. threats, and opportunities. Therefore risk management is really the management of all uncertainties.

As far as local authorities (in France municipalities, departments and regions) and their associated bodies (in France SIVOM, SIVU, district and urban communities, etc.) are concerned, they are still far from having a clear vision of the exposures they are facing, although the movement is gaining momentum.

When contrasted with private entities, they have specific features that must be taken into account; laws define their missions. While they are shielded from some of the market risks, they must fulfil their purpose in the public interest under any circumstances. This is why they must follow a different logic while they enjoy some immunity. In many countries, they

are controlled by specific jurisdictions, like the CPA in the UK, the Regional Chambers of Accounts in France.

Local authority could benefit considerably from a "strategic approach to risk management" when considering the impact it could have, not only on the entity itself, its employees and its constituents, but also all the small and medium-sized businesses located within its jurisdiction. Over and above the traditional role of the risk manager professional as "keeper of the organization's own survival and well-being", in a local authority the risk manager could:

- Preserve and enhance public safety: plan for land occupation, industrial zoning, and public security (police), etc.
- Participate in recovering from natural and industrial catastrophes: responsibility for restoring public services, essential action plans for protecting people and property.
- Enhance economical well-being of the area: following a major catastrophe, the local authority may play a key role in the mending of the "economic cloth" or help to prevent a catastrophic impact by assisting small and medium-sized firms to develop some sort of risk management capacity.

In other words, the local authority may play a key role in transforming "reactive" risk management into "proactive" risk management in all economic actors under its jurisdiction; i.e. to turn risks into opportunities. In such a changing world, any student of risk management must therefore build his approach on a model that must remain his guideline throughout his study to ensure a certain degree of coherence.

But to enter the world of the management of uncertainties, a number of concepts must be defined as there is no clearly accepted language, outside of the ISO 73 document, not yet universally used and currently under revisions.

Definitions

The expression "risk management" is an open concept, still subject to a number of different interpretations, especially in Europe. Each professional has his own definition, based on his personal background and experience and the specifics of the firm's "culture" whose risks he manages. This reality does not enhance fruitful discussions between specialists. To make things worse, the same words are sometimes used to express different concepts.

Organization is the dynamic interaction of resources combined to achieve some defined permanent objectives. Resources can be broadly classified into five categories:

- *H*uman
- *T*echnical
- *I*nformation
- *P*artners (upstream, suppliers and subcontractors, and downstream, customers)
- *F*inancial

Risk (pure, speculative, and mixed) has many meanings and so we will try to avoid using it in this. However, it is so commonly found in risk management and insurance presentations that one must be aware of its possible meanings. There are basically four concepts described by this term:

- The uncertain event provoking the loss (see below "Peril").
- The resource exposed (see below "Object of risk").

- The financial consequences (see below "Loss").
- A global and subjective appreciation of the preceding factors (like the final comment by a field inspector in an insurance company after visiting an insured site: "good risk in its category").

The most common use refers to the first definition: the original cause of the loss suffered by the organization. In this sense, it is the uncertain event generating the loss that is the risk (*pure risk*) as opposed to those events that may result in either a gain or a loss (*speculative risk*). Those risks that cannot be easily classified in either category are called *mixed risks*.

In the original limited definition of the function, risk managers were only dealing with pure risk. Some use an even more restrictive term, i.e. "insurable risks". However, in this case, the risk manager is merely an insurance purchaser. It is clear that both adjectives are not equivalent.

The new "holistic" or "strategic" approach to risk management tends to blur this classification that for a long time was the cornerstone of risk management. Therefore, it is essential to introduce a further distinction.

Systematic and unsystematic risk

The systematic risk (nondiversifiable risk) is generated by nonprobabilistic events, i.e. that may happen simultaneously rather than due to pure chance. This means that the systematic risk does not lend itself to diversification, which requires constituting a large portfolio of uncorrelated risks. Losses generated by general economic conditions represent a systematic risk and all the economic actors suffer at the same time. When money markets tighten, interest rates increase for all organizations.

Typically these risks are not insurable. Imagine an insurance company offering a cover to protect the insured against a rise in interest rates. The company would not be able to build a diversified and balanced portfolio to mutualize this risk, as all their clients would be suffering losses simultaneously.

The unsystematic risk (diversifiable risk) is generated by a series of events the occurrence of which is fortuitous; they happen according to different probability distribution.

These risks are specific to each economic entity. For example, fire in a building is fortuitous and in a sufficiently diversified portfolio of buildings geographically spread, fires represent an unsystematic risk.

An insurance company can build a diversified portfolio by insuring a large number of buildings against fire provided they are sufficiently dispersed in a large territory. In using the impact of the law of large numbers, the insurance company is able to forecast with a good degree of precision the number, frequency, cost, and severity of the claims it will have to indemnify in a given insurance period. Therefore, it can offer the cover and compute a premium for each insured that will allow it to pay the total annual claims arising from fire in the insured buildings.[1]

Insurable risks

They are risks for which there exists an insurance market. That is to say, that some insurers are ready to grant cover in exchange for a premium (offer) acceptable for some potential buyers (demand). It would be of little interest to develop here a treaty on the elements that make a risk not only insurable and but also attractive for an insurance company to underwrite. The nonspecialist reader could easily read one of the many insurance initiation books. It suffices

[1] Cf. below: Insurable risks.

Table 1.1 Classification of perils

	Economic	Human			Natural	Industrial
		Intentional		*Unintentional*		
		Wise guy	*Criminal activity*			
Endogenous						
Exogenous						

here to state that the insurance process is based on the existence of a mutualization opportunity. The basic insurance principle is to share among many the financial burden of indemnifying the few that incur a given loss. In other words, from an individual's perspective, an exceptional uncertain threatening financial loss (claim) is transformed into a certain recurring limited annual cash outflow (premium).

It would be clearly unacceptable to use an outsource concept like "insurable risks", to define the domain of action of the risk management professional. Clearly, such an approach would call for a constantly modified boundary by the conditional existence of an insurance market rather than by an actual in-house process of exposure identification and evaluation.

Object of risk is any resource used by the organization and that is "at risk", i.e. that an adverse uncertain event (see below "Peril") can damage, destroy or make unavailable for the organization's use for a period of time, or indefinitely.

This term "object of risk" has been preferred to other terms like resources because it is a clearly defined concept already in use in the risk management information system GESTRISK based on the specifications drafted by the French risk managers association. It must be understood in a broad sense to include not only tangible assets, but also intangible assets and activities, with the cash flow thus generated. Objects of risk can be classified into five categories, based on the five categories of resources identified above.

Peril is the uncertain event (i.e. with probability strictly more than 0 and less than 1) that would generate a loss to the organization when it happens (any time in the future). The loss results from damage or destruction or unavailability of a resource essential for an organization's normal (or nominal) operations. In order to develop appropriate risk control and financing strategies, the perils can be best classified according to three criteria summarized in Table 1.1.

This table may require some explanation.

For the first column:

Endogenous:	**versus**	**Exogenous:**
An event that is generated by the organization itself or within the limit of the activities it controls (a fire starting on the premises, the release of a dangerous chemical into the atmosphere, the manufacturing of a substandard product, etc.).		An event that is generated from outside the area under the organization controls (a strike in a nearby factory creating unrest and blocking access to an industrial estate).

For the first line:

Economic:	Human:	Natural:	Industrial:
Resulting from an unexpected change in market conditions in the economic environment of the organization generating a sudden and tight constraint on it.	Resulting from human action (a fire breaks out in a warehouse from sparks during ill-protected welding operations, robbery in a jeweller's shop, etc.).	The probability of the event and its occurrence results from the action of nature – acts of God – (earthquake, hurricane, etc.).	Resulting from human activities but is not directly linked to a human act, voluntary or involuntary, like a fire while a factory is empty, water damages, etc.

In the case of "human perils", it can be:

Unintentional:	Intentional:
Resulting from error or negligence in the performance of a task:	The act of a person modifying a system intentionally to "improve" it but failing to properly document the changes for the other users.
	OR
At the time of the loss (cigarette butt close to a flammable material)	The act is performed or abstained from with the intention of generating a loss to a third party or gaining an illegal benefit for the person. In most cases, it is a criminal activity under the law in most countries. It should be further split between:
Before the loss occurred (absence of proper lining in a basement built in an area subject to flooding)	*"For profit"* where the person or organization involved in the attack is pursuing their personal financial interest (industrial spying, for example, blackmail, etc.).
	"Not for profit" where the person or organization is seeking to further a cause or remedy a wrongdoing (arson by an ex-employee, terrorist attack, etc.). *The terrorist attacks on New York and Washington on 11 September 2001 have illustrated how both essential and difficult it is to manage this peril.*

One final distinction must be made between perils and hazards (a common phrase in English insurance policies). It is of particular significance when applied to liability exposures where the hazard is generated by the action increasing potential liabilities (manufacture of a faulty product), whereas the peril itself is the claim put forward by a third party suffering the damage.

Loss (financial) is the negative financial consequences for an organization hit by a peril. Insurers usually estimate it either as:

- *A maximum loss* – possible or probable – (two concepts well known to the insurers either as PML or EML), whereas in the USA there is a third concept to take into account – the level of protection, or
- *An annual aggregate loss* (i.e. expected value annual loss due to several events).

Exposure

Based on the concept defined here above, an exposure is fully described by three elements, i.e. the financial consequences of a peril striking a given resource of the organization. But that definition should be revisited to include opportunities as well as threats. That is to say:

- Object of risk (resource at risk) – the resource that may be impacted by the outcome.
- Event (peril) – the random event that may impact positively or negatively the resource.
- Consequences on objectives (financial and other consequences) – as far as possible, they should be quantified in monetary terms, but some social and environmental impacts cannot always be translated into hard money.

Management

This is the term used to refer to the actions within an organization aimed at the following results:

- Plan (the team work)
- Organize (the team resources)
- Lead and motivate (team)
- Control and audit performance

This definition clearly positions the risk manager as a "manager" in charge of a budget and leader of a team. He must also report to an executive, justify the costs involved, and prove the efficiency of his operation, just like any other manager in the organization.

Risk management

Risk management is a continuous process to insure that proper consideration is given to uncertainty in all decisions made within the organization and that the proper documentation is kept for internal and external controls.

It comprises three steps: diagnosis of exposures, treatment of risk and audit of the risk management programmes.

Risk management is a continuous process for making and carrying out decisions that will reduce to an acceptable level the impact or uncertainties of the exposures bearing on an entity, i.e. within the risk appetite of the organization balancing opportunities and threats.

The decision process is divided into three steps. Implementing these decisions requires each practitioner to ensure proper management.

This definition clearly refers to an essential part of sound risk management, the continuous feedback loop. The "audit step" includes not only outside validation by a third party but also monitoring and reporting, i.e. understanding and tracking the risk decisions that have been made and how they relate to the objectives that have been set forth and also how they are implemented and reviewed periodically to ensure continuous pertinence with the evolution or the internal and external contexts as well as the organisation's own objectives.

Risk management objectives

An organization has been defined as a dynamic combination of resources organized to reach a set of goals and missions. Therefore, the definition of these objectives is a key element of any organization management.

In any event, economic efficiency will dictate the allocation of resources in the most economical way, i.e. to reach the most ambitious goal with the limited amount of resources available. This is the founding principle of the liberal economy system.

Under these conditions, it is clear that the unavailability of all or part of a given resource could prevent the organization from reaching its goals. The reasons for this "nonavailability" of resources include the occurrence of perils, or uncertain "accidental" events.

Within this framework, the objective of the risk management process can be defined as *the availability*, *under any set of circumstances*, *of the resources at a level compatible with the fundamental objectives of the organization*. This level can be refered to as "vital".

As a corollary, the risk manager must reach this goal while using as few resources as possible. Then again, a closer look at the organization's objectives is necessary to reach an operational definition of the goal of risk management.

Organizational objectives

The word organization is preferable to the more economic term of the firm so long as the risk management process can be applied not only to a profit seeking entity (firm) but also to a nonprofit organization and a public entity as well as a public or private hospital.

Individual organizations' goals may vary widely in content and wording; however, they can be usually classified into three broad categories.

Economic efficiency This concept can be expressed in a number of ways but it is always a variation on the central theme of the liberal economy system; i.e. the maximization of profit. Clearly for publicly traded companies as well as companies where ownership is distinct from management, the current expression would be creating long-term stockholder value which will have direct consequences for the "post-event objectives" below.

For a nonprofit organization it amounts to reaching the goals with the minimum possible resources or the maximum output for a given level of resources.

In public entities, like local government, the goal is always to minimize budget requirements to meet the constituents' basic needs. At a governmental level, a goal could be to minimize the defence budget while still providing for an adequate level of protection in times of both peace and war.

Environmental issues These focus on protecting the quality of the environment (air, water, and soil) and consist in essence of:

- Complying with legal and statutory obligations.
- Protecting the elements of the biosphere (environment in the traditional sense).
- Respecting the cultural traditions in all locations.

Ethics and good citizenship This encompasses a number of nonfinancial issues that executives must take into consideration in making decisions also refered to a "enterprise social responsibility": social improvements, humanitarian conduct, and artistic support. Among others:

- Artistic donations.
- Humanitarian foundations.
- Actions to improve life conditions.

Functional objectives The main departments of the organization are centred on the five classes of resource as listed above, i.e.:

- *H*uman (human resources VP)
- *T*echnical (operations VP)
- *I*nformation (information system VP or C.I.O.)
- *P*artners (marketing VP and purchasing or logistic VP)
- *F*inancial (CFO)

The main objectives of the organization (*permanent goals*) can be reached only if the main functions reached their subobjectives (*critical goals for the CEO*). More specifically the specific role of the finance director is to find the financial resources needed for the organization's smooth operation (*cash and fund management*) in the most favourable conditions (*cost of capital*).

Operational objectives (pre-event and post-event objectives)

In risk management manuals, objectives are often referred to as pre-loss and post-loss. This situation is due to the impact of the insurance terminology on risk management practices but the term event should always be preferred. On the other hand on a long-term vision the word "dysfunction" would encompass a broader spectrum of possibilities.

Risk management objectives have been derived traditionally from the objectives of the major departments that risk management is meant to assist in coping with their specific exposures.

This could be summarized in one sentence: *the risk manager's job is to ensure that, in any emergency situation, the organization has at its disposal adequate resources to allow it to attain its objectives under even the most strenuous circumstances*.

Among the resources that will be needed to get through the difficult phase is hard cash to face increased expenses and/or decreased revenues following the event. It is often the risk manager's direct responsibility to ensure that funds are available in the quantity and quality required.

More specifically, it is appropriate to distinguish pre-event and post-event objectives. If risk management is about planning ahead to reduce the uncertainties of the future, then it should be concerned in priority with post-event objectives.

Post-event objectives (rupture in the production process) In any case, the minimum objective will be the organization's survival. However, for each of the four main classes of resources a continuum of objectives may be derived from the basic survival:

- *Technical, information and commercial*: continuity of operations is in fact a very demanding objective. However, it is inescapable sometimes in an industry where public health and safety is at stake, or permanence in a market is a prerequisite to stay in business. One may think of the registrar office in a municipality, the primary school system, or in healthcare of the electricity supply for an operating theatre. The continuum is based on the maximum downtime allowed. Clearly the shorter it is, the most expensive the investment in risk control. Therefore it is very important to measure with great care the "acceptable downtime".
- *Financial*: beyond survival, the financial objectives can be classified in increasing constraint order.
  – *No loss*: keep the organization in the "black" even in the year in which the loss occurs.
  – *Maintain profit level*: the "average" profit level achieved in the past is maintained even when the loss occurs.
  – *Sustain growth*: the growth is maintained throughout the period whatever happens.
  When a very large public holds the company stocks, the firm's financial results are essential for its enduring independence. Sudden variation in the earnings per share or dividend can be heavily penalized at the stock exchange with sharp declines in share prices. This may attract raiders and endanger also the executives' jobs! The finance theory would show that the long-term growth rate is a key to the profit learnings ratio.
- *Humanitarian*: these goals encompass all the negative impacts that the organization's activities may have on its socio-economic and cultural environment. This includes suppliers and subcontractors, customers, local communities and the labour force.

Pre-event objectives (economic efficiency) Before the events' occurrence, it is clear that the risk management goal will be centred on economic efficiency, i.e. the risk management programme must be as lean as possible while providing for the completion of the post-event objectives assigned to it.

Other significant objectives

- *Reduce uncertainties*, i.e. the variability (standard deviation) of the financial results to a level compatible with top management "appetite for risk" (some say that the risk manager's job is to "buy his boss a good night's sleep").
- *Abide by the common laws and all the statutory laws* that apply to the organization's activities and locations.
- *Harmony with the "society" goals*: it can be useful to remember that the society or community goals can be reflected at two levels:
  – The *laws* that represent the wishes of the people through the electoral bodies representing them (legislative power).
  – *Ethic and "good citizenship"* for which the strict adherence to the law is not enough and the organization must strive at anticipating the cultural and humanitarian expectations of the society.

Conflict between objectives

It is easy to understand, with no need for lengthy explanations, that as one escalates along the continuum of post-event objectives, one will draw more on the financial resources of the organization and therefore will tend to increase, rather than decrease, the overall cost of risk.

Risk management decision process

The analytical approach to managing risks is defined through a matrix to reflect the dual activity of the risk manager practitioner:

- A manager, as such, must go through the managing process of planning, organizing, leading, and controlling (horizontal axis).
- A decider going through the three steps routine of the risk management decision process as described below (vertical axis).

Step 1–Diagnosis of exposures

The diagnosis of exposures cannot be conducted without a clear understanding of the organization's goals and strategy. A systems approach to risk analysis allows the risk manager to define a portfolio of exposures for the firm and to draft a risk map to illustrate the major risks that should draw top management's attention. The objectives and mission of the organization should also be subjected to a risk analysis, in light of the ethics and values publicly announced by the organization and in the light of public beliefs.

Exposure identification is the single most vital part of the risk management process; it consists of listing the exposure "portfolio" of the organization in terms of resources and the perils that may affect them. The analysis is aimed at measuring the probable or possible impacts on the organization of each exposure in terms of probability and severity. The financial consequences should have priority but others like social, human, and environmental should also be factored into the best of the ability. The assessment phase will take into account the existing treatment mechanisms to measure their efficiency and assess further improvements needed.

Actually, once an exposure is recognized, uncertainty is somewhat reduced as a volatility can be assessed and a problem once identified can lead to some kind of solution. The "hidden exposure" is always more threatening as, evidently, when it strikes, there is no plan to cope with it, no risk management technique to either reduce the consequences or finance them.

The risk management practitioner can use a number of tools during the investigation process, and these are listed below. However, tools without a method lead nowhere and we will describe one such method for using properly all the tools available. The one we have chosen is called "risk centres".

Identification tools It is all too obvious that, for a given organization, exposure identification requires a thorough understanding of both the organization itself, for endogenous perils, and of its environments, for exogenous perils. The term environment refers here not only to the economic partners of the organization, the entities it is trading with. It encompasses the overall economy, the social, legal, and cultural components as well.

Therefore, the risk identification tools are instruments to describe and analyze the organization and its environments.

- Financial and accounting records:
  These are key to understanding what the main features of an organization are. They consist of the following documents.
  - The *balance sheet* gives a first approach to the physical assets held by the organization and on the liability side; it may be possible to spot any outstanding liability stemming from that exposure. It gives also a hint to the current situation of the organization, the main ratios, where it stands in working capital and debt to equity ratio.
  - The *income statement* gives an idea of the profitability of the organization, its main profit centre and their contribution to the profits (a key to evaluating losses of revenues).
  - The *sources and uses of funds statement* identifies the main flow of long-term funds and the congruence between sources and uses.
  - The *annual report* contains also other valuable information such as the auditors' report, lease equipment, some contracts, and human resources status.
- Marketing, purchasing and other documents:
  All documents given to customers, including packaging and user's notice may be instrumental in understanding potential product liabilities. Procedure manuals can illustrate potential defects in the administrative processes leading to quality problems, etc. Reading union panels may point to possible safety questions and other morale questions raised by the workers' representatives. Special attention must be given to all contractual agreements as they bring potential liabilities.
- Production and flow charts:
  These identify the flows of goods and services within the organization and with its main economic partners, both up-and downstream, suppliers and customers. They help in identifying bottlenecks and locating the weaknesses in the logistics or distribution network.
- Standards questionnaires:
  They are sometimes called also "checklists"; they were formerly regarded mainly as guidelines for the insurance underwriters. If limited to a short-list of questions, they can offer the newly appointed or assigned risk management professional a quick approach to all the sites from his office. Each operational manager answers the same set of questions, which allows for a quick consistent overview.

  Their limit is twofold. Being "standards", they are not always well adapted to the specifics of a given organization, or of each site. If they are designed to be broad in scope, both for resources and perils, they could be long and fastidious. But the operational managers might not take the time to answer.

  On the other hand, often they emanate from insurers. Therefore, their focus is mostly on "insurable risks" that may not be the most serious facing a given organization. In that case, they are based either on the covers generally granted or on the exclusion of the "all risks" policies.
- Historical data and scenario analysis:
  As illustrated in the recent book by Peter L. Bernstein,[2] the first breakthrough in modern management dates from the day when Pascal established the founding stone for what was to become modern statistics. Trying to establish a trend for the future from the experience

[2] Bernstein, Peter L. 1996. *Against the Gods. The Remarkable Story of Risk*, John Wiley & Sons, Inc., New York.

of the past was the first break from the "fear of the gods", the first step towards modern management.

The use of historical data, i.e. past losses experience, of a given organization remains the first source for establishing forecast as to the level of losses for the years to come. However, there are serious limits to the use of probability or trending, the first being to have a sufficient number of adequate data (law of the large numbers) and the second the underlying hypothesis calling for a stable environment (probability) or a stable evolution of the environment (trend analysis).

Therefore, it is clear that historical data are most useful for large organizations and high frequency losses, which lend themselves to probability laws. Such is not the case for high severity, low frequency losses. For this category, it is possible to tap from others' experience through statistics gathered by the insurers and consolidated by their professional associations.

It is also important to analyze the chain of events that led to losses or potential losses with techniques like fault tree analysis.

- Internal and external experts:
  Risk managers are necessarily generalists with some knowledge of all the activities in which the organization engages. Conversely, they cannot be experts in all these varied areas and therefore must rely occasionally on experts' opinion.

  They may be specialists in given scientific or technical fields but also in financial matters (bankers or financial institutions), insurance (brokers, underwriters, reinsurers) or legal (lawyers). In some cases, psychologists or sociologists may prove useful to understand specific populations or reaction under stress, for example.
- Site inspection (visit):
  However, direct contact with operational mangers on their sites cannot be replaced by "homework". The risk management professional has a specific perception for risks and a fresh look at things that may allow for the unearthing of specific exposure going otherwise unnoticed.

Risk centres method The various tools listed above provide the risk management professional with a general idea of the main exposures that the entity is confronted with. However, this paperwork is not enough and must be enhanced by visits to the various sites of the entity. This must be done in a systemic and logical manner.

Practically, each consultant has developed a method for identifying and analyzing clients' exposures. However, few have published it in an orderly fashion. The method developed here is one of the few "public" views. First published by Yves Maquet,[3] a consultant, it is reproduced here with substantial changes introduced by the authors.

This method is built upon a model that views the entity as a dynamic combination of five main categories of resources to reach a goal, or a set of goals, assigned to the board of directors by the stockholders' annual meeting. The five categories of resources are the following for this model:

- $H =$ human: beware, not all human resources are "employees".
- $T =$ technical: here limited to the plant and equipment under the control of the organization itself, whether owned, leased or under custody and care.

[3] Maquet, Yves 1991. *Des Priues d'assurance an financement des risques*, Bruglant, Brussds.

- $I =$ information: all information flows within the organization as well as those exchanges with all its socio-economic partners, whether stored or processed, be they computerized or not.
- $P =$ partners: all the goods and services exchanged with the partners both upstream (suppliers and subcontractors) and downstream (customers and clients) but also administrations and consumers' unions, etc.
- $F =$ financial: all financial flows running through the organization. In a free market economic model it represents the reverse flow of goods and services with its natural and necessary "accumulation" to allow a correct operation of the "economic pump".

In this approach, we are still concerned with reaching goals and objectives. Losses are only seen in light of their impact on these goals and objectives. An exposure is worth consideration only insofar as it threatens those goals.

Thus the risk centre method stems from a strategic vision with success as the only acceptable outcome. But success for the whole organization relies on the individual success of each manager. Thus the entity, or system, is divided into subsystems, or risk centres, using its reporting hierarchy as a guideline.

One must only remember that a "permanent" objective of a manager is divided into as many critical objectives as he has people reporting to him. The idea being that if all of these critical objectives are not met, the manager will not be able to meet his own permanent objectives. The permanent objective of the manager is a critical objective for his boss, and conversely, all his critical objectives are permanent objectives of his subordinates.

Hence, following down the lines of authorities in a given organization, it can be split into as many small entities as necessary. These small or "individual" firms represent the "risk centres".

Where should the process stop? Each individual risk centre must still be a "living entity" with all five classes of resources and a clearly defined objective necessary to the overall firm objectives. It is a "monocellular" firm in which the "boss", the manager, can grasp the frontier of his domain and thus has a good vision of his exposures while still enjoying a degree of freedom to decide how best to manage his "micro business".

In fact, the risk centre method is one more application of a universal approach to "big problems", often used in physics and mathematics. A problem that is too big and unmanageable should be split into as many small problems as necessary to be manageable.

The various identification tools are then used to establish a diagnosis of the exposures facing each individual risk centre. However, at this stage, the interview with the risk centre manager will play an essential part in the success of the process. As it is a time-consuming process, the centres should be ranked on the basis of their contribution to the overall goals of the organization, or better even their capacity at ruining the chances of reaching those goals. Therefore, an overview of the main exposures should be developed as early as possible in the risk management process, if only to establish a list of priorities for the risk manager's efforts.

The way to conduct such an interview with the risk centre manager is summarized in Table 1.2.

Questions 1 and 2 aim at evaluating the manager's understanding of the expectation of his superiors, his position in the overall organization and the resources he uses to achieve his own missions. Questions 3 and 4 try to develop a contingency planning specific for the centre.

Question 3 puts the manager in an impossible situation where he would not have access to a vital resource, plant, and equipment or personnel. He is then threatened in his inner security

Table 1.2 Interview with a risk centre manager (Example)

Question 1–Goals and Objectives
What are the goals and objectives, the missions of your service or department?

Question 2–Resources
- What is your organization?
- What are your personnel, your office space, work area tools and equipment?
- Where do your products, your raw materials, your information come from?
- Where do you send your production, information?
- What means of communication do you use?

Question 3–Key Scenarios
Assume your entire location burns down tonight, without injuring any of your employees. *Tomorrow morning when your employees report to work, how do you manage to start production again?*

Assume now, on the contrary, that you have no workers reporting to work tomorrow morning (strike, no access open, etc.) while your plant is intact.
How do you manage to start production under these circumstances?

Clearly the purpose of these questions is to assess what resources are "vital", and which are "additional" when the question is survival of the organization under extreme duress . Therefore, the questions assume total lack of one of the resources.

Question 4–How Do You Propose To Fend Off These Exposures
- Now
- pre-event: prevention/reduction
- Later
- post-event: survival or contingency planning, crisis management

and forced to imagine a disaster from which to recover. This artificial stress may bring out some creative solutions to be used in the crisis management manual.

Question 4 aims at designing a new harmony between objective and resources that was temporarily destroyed by the unfortunate scenario. The question is a management one where the peril is secondary and the absence of the resource for whatever cause is the central idea. Insurance and classical risk controls are not essential here. The concept of "vital" resources refers to those resources just barely sufficient to live temporarily through a difficult time.

The next step consists of taking into account the difficulties in implementing different loss control measures than nobody knows better than the centre's manager himself. He, more than anybody else, can determine what level of tolerance for uncertainty and the level of mishap that is acceptable for his "constituencies". It is even possible that, with a good risk mapping, the manager will be able to reallocate his resources before the occurrence of any traumatic experience. He could thus avoid any catastrophic consequence (loss reduction) and provide for the contingency planning to be implemented in case of an emergency to preserve as far as possible the goals assigned to him by the organization (survival planning). Most of the time the investment cost involved will prove to be limited as the field manager will know where to go to get the most cost-efficient "alternative resource". He job is to know all the threads of his trade.

However, this microscopic approach at the "risk centre" level is not sufficient, and it is essential to have a broader view, a system's approach that will include the relationship between all the risk centres, their interaction with each other, and their environment(s). The overall

planning, the consolidation process, requires an understanding of the organization and of its long-term strategy that is conceivable only at the executive level.

It is clear that this process will follow the hierarchical pyramid from bottom to top. When a risk centre manager reaches the limits of his autonomy the ball must be passed on to the next level of management up to the CEO or the executive board. The risk manager must be a facilitator along this process and he is in charge of the presentation of the final picture to the board, laying down the options open for decisions.

Of course, along that line, the risk mapping is reduced to the essential issues, those exposures that could send the organization to the rocks.

No process can be totally exhaustive, however qualified are the persons in charge. It is therefore always necessary that a review be done regularly, whenever possible by outside expertise (consultant, internal audit, peer review). This is implied in step 3 of the risk management decision process. The "circle of risk management" may prove useful at this stage.

Step 2–Risk treatment

The loss control aspect of the risk mediation process is challenged to transcend traditional hazards to cover all types of potential losses: legal, procurement, production, markets, partners' and contractual. The risk financing portion of mitigation must be integrated in a global finance strategy – not only to benefit from the new alternative risk transfer offerings but also because it simply makes sense. With all risks in the same portfolio, the financing possibilities open up. Modern risk financing is no longer a simple dosage between retention and transfer, i.e. buying insurance with different levels of deductible, per occurrence or per accumulation over a period.

Some economists even theorize that insurance mechanisms may be rejected entirely by large concerns (where it is viewed as economically inefficient) since each individual stockholder can mitigate risks through a balanced portfolio diversification. This theoretical approach, however, does not take into account the fact that small investors cannot sufficiently diversify. And it negates the social efficiency of insurance mechanisms. While reducing profit fluctuations induced by large losses, insurance may protect employment as well as the assets of small investors. (The choice of systematic insurance transfer should be revisited, however, for large holding companies, especially in a time when the price of insurance is experiencing manifold increases.)

In order to effectively treat all the exposures identified and analyzed during the diagnosis process, the first step is to proceed with as wide a check as possible of all measures that could be applied to the situation. In other terms, what instruments of loss control or loss financing could be included in a risk management programme acceptable to top management, fulfilling the goals and objectives of the organization and reasonably easy to implement by all those involved.

Review of risk management alternatives (step 2.1) For each exposure, there should be an exhaustive "brainstorming" session to insure that no stone remains unturned. For the risk management professional, hired as a consultant to audit a risk management department, the most striking defect is the failure to use one's imagination to find new solutions to new risks. It seems that most risk managers stick to old recipes. For each instrument that could be used, their impact on reducing long-term uncertainties should be measured against their cost.

The risk management professional must always keep in mind that he has two sets of tools, loss control and loss financing:

- Loss control techniques:
  These techniques are to be planned ahead, before any event causing loss has occurred. However, some are activated at all times (pre-loss measures) or only at the time of the event or after (post-loss measures). They are all aimed at reducing the economical impact of adverse events on the organization. Basically, they reduce one of the two major components of the economical consequences: Frequency (or probability) and Severity.

  The techniques aiming at reducing Frequency are broadly classified under the term *"loss prevention"*: they prevent accidents from occurring (*by acting on the chain of event, or causes, leading to them*).

  The techniques aiming at reducing Severity are broadly classified under the term *"loss reduction"*: they prevent accidents from spreading damaging effects (*by acting on the chain of event increasing the losses, or consequences, after they occur*).
- Risk financing techniques:
  Except under some rare and specific circumstances listed in Chapter 2, loss control techniques do not reduce the risk to Zero. Therefore, the occurrence a sizeable loss remains a possibility that cannot be ignored due to the potentially severe impact it might have on the organization's current flows of cash. It is therefore mandatory for the organization to establish some kind of "safe source of cash" to be tapped under specific duress.

  As is described further in step 4, funds may come from within the organization itself or from without. The first case is called Retention, the second Transfer. Actually, theses crude definitions will be reviewed to reflect more recent developments in risk management. More specifically, in risk financing, the actual source of funds at the time of the claim (or need) is less important than who bears the uncertainties (the risk) to decide whether the programme is retention or transfer.

Risk management programme development and approval (step 2.2) Organizational goals are at the heart of modern risk management, therefore the definition based on "success" is the right one: an exposure, a risk, is a potential chain of event or scenario that could prevent the organization from reaching its goals. This stresses that designing an appropriate risk management programme will always mean designing a programme that best allows the permanent or long-term goals to be reached.

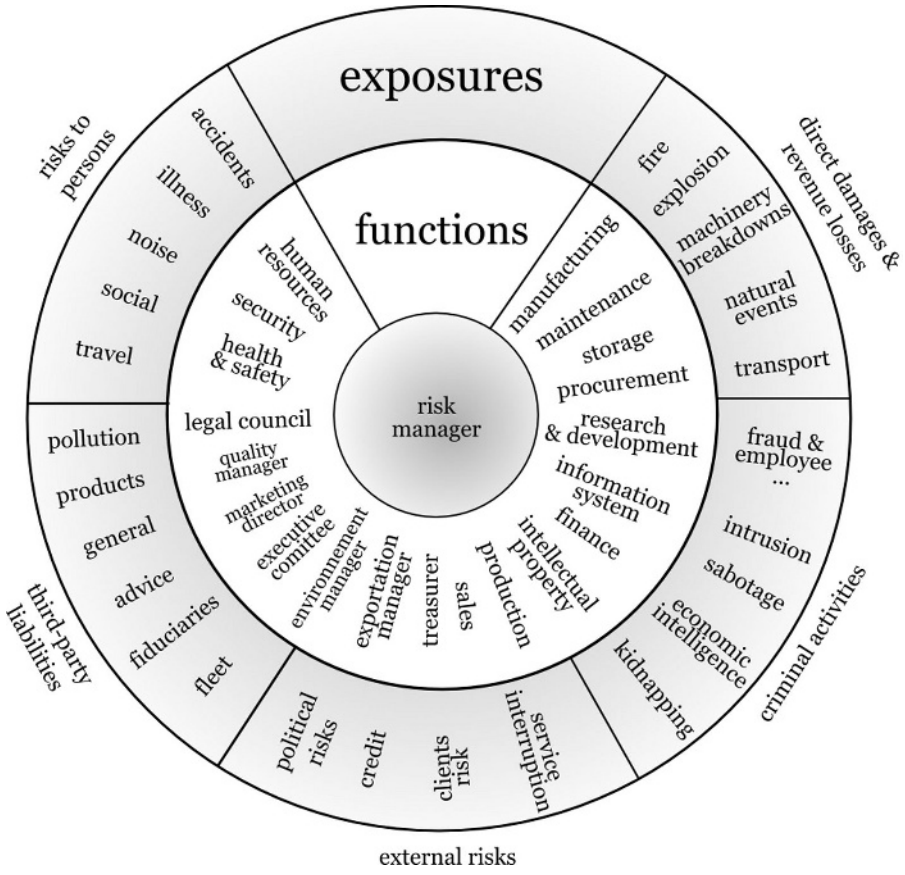
In other terms there can be no "best risk management programme" without a direct reference to long-term organizational goals, but also each departmental goal. At this stage, it is essential to have a comprehensive or global approach. There are different words used to describe it: holistic (France), integrated (UK) or enterprise (USA). Strategic risk management is of the essence of any strategy. Some authors have coined an expression to refer to a traditional "pure" risk or "insurable" risk approach naming it "suboptimal risk management".

Therefore, the risk management mission is to guarantee the long-term "safety" or achievement of the organization's goals. That is why some use the phrase "strategic risk planning" rather than "risk management programme" which may have too narrow a connotation (limited to pure risk).

At the end of the day, the final say in such an important matter has to rest with the board of directors whose job is to make sure that top management goals are aligned with the shareholders' objectives, with due consideration given to other stakeholders' interest in order not to

jeopardize the company's social licence to operate. In simple terms, it is the board that must set the "risk appetite" of the company and communicate it in operational terms for all in charge of implementing the risk management strategy.

Risk management programme implementation (step 2.3) The circle of risk management (see below) represented 25-year-old breakthrough that led the risk management professional out of "insurance manager duties". It is like an orientation table for any risk manager. Placed at the centre, he has a key to understand his organization's risk management issues and responsibility.



Circle of risk management

One of the primary concerns of risk management professionals is that they usually have a limited role in the actual implementation of the programme they have designed. In most cases, they only implement the global financing programmes. And even in that area, their direct implication is still too often limited to buying insurance covers.

However, this aspect should not be underestimated; the insurance budget in a large international conglomerate can be very substantial, even in excess of one billion euros. When they get involved in the management of captive insurance or reinsurance they are obviously more visible to top management due to the investment funds involved with the reserving practices.

For all the other elements of the risk management programme, dealing with organization, production facilities, products and distribution channels, suppliers, and subcontractors, the risk manager is only the coordination point. He is more in the position of an internal consultant and must be able to communicate and convince the managers. At the previous stage, the need to consolidate in one overall strategic risk management programme has also been stressed.

A comprehensive and rational risk management programme will aim at reaching the overall goals of the organization. Those who benefit from such an approach are not always those who have to pay the costs. Therefore, one of the keys to the successful implementation of all risk management programmes is the management costs allocation system. It must "naturally" drive the operational managers to implement at their level all the investments and the daily chores needed for a complete implementation. These points will be addressed again further.

Step 3–Audit and corrective actions

Top executives' interest in the audit process extends to the risk management sphere, and corporate governance issues have made this step a critical aspect of extended risk management. A case could be made for the internal auditor to be the natural owner of this step, but this remains an open debate.

However, the audit step of the risk management process cannot be performed only by a third party, be it internal or external; it is essential that all the operational managers in charge of managing the risks linked with their activity perform also the self-assessment audit with the assistance of the risk management professional. This monitoring and reporting exercise will allow for a proper documentation of the activities involved with managing risks and ensuring that the decisions have been made rationally taking into account the objectives and limitations of the organization, as well as the priorities set by top management and the board. Thus the continuous feedback loop will be effectively closed allowing for a proper evaluation of the changes in the organization's internal and external context as well as the evolution in the company's goals to adapt to stockholders' owners' social and economical circumstances. The risk register recommended by the Australian Standards is a good tool for assigning responsibility and following the risk management strategy implementation.

There is, however, a trend for internal auditors (encouraged by external audit firms ready to assist with their consulting branch) to go beyond the auditing phase and pose as the legitimate owner of the entire risk management strategy of the firm. Thus, the risk manager may be reduced to insurance buying and managing, or made redundant through a complete outsourcing of risk management competencies. Regardless of which department is in charge of the process, it should always be completed with the help and support of the risk management team. If the risk manager is an "internal consultant" with no hierarchical authority to implement most of the approved programmes, then he must directly, or through an internal audit department, make sure that the programme is not only fully implemented but also proves to be efficient in reaching the assigned goals.

The word "audit" is indeed appropriate at this stage. However, the word "diagnosis" is preferred for the first step where "audit" is still too often used. An "audit process" aims at comparing an ideal situation with the reality found. Reality is contrasted with a set of standards, both qualitative and quantitative and the sources for the differences are sought to explain and correct the situation when needed.

For those not familiar with audit processes, it is important to remember that there are essentially two classes of standards:

- *Result standards:* they help measure the progress made over a given period when comparing the standard at the end of the period with
  - Beginning levels,
  - Desired ending levels,
  - Results for the main competitors (benchmarking).
- *Activity standards:* they measure the efforts deployed during the period without references to the results achieved.

The main benefit of using such a classification to measure the efficiency of the risk management department is that it is parallel to those used when auditing any department in an organization.

However, one must always keep in mind that it is much more reliable to use such an approach constantly for "frequency exposures" where it is relatively easy and safe to measure the improvements, the reduced number of incidents and the reduced overall "costs of risk". Such is not the case with "severity exposures" where efficiency is hard to trace as costs may be relatively "hard numbers" whereas the results may require a long period to be evaluated.

Let us illustrate briefly. Even in the wake of such ecological catastrophes as the Exxon Valdez and more recently the Erika, some challenges still remain. Tankers pay dues in the harbours on the basis of their draft and double-hulled tankers are penalized as they can carry less crude oil due to the internal "skin"! Even though new tankers have to be double skinned, some of the old ones, which are not, are still allowed to sail until phased out.

STATE OF THE ART AND THE TRENDS IN RISK MANAGEMENT

Risk profile, risk map or risk matrix

Prior to examining more closely the different techniques to mediate risks, it is essential to stress again that risk management is an "economic function" and that the impact is usually measured on the basis of two parameters. In the long run, the cost is measured by the expected value:

Frequency $\times$ Severity

However, using the multiplication sign is potentially misleading, as, in a human time scale, this may be totally irrelevant as a basis for decision making. It is more proper to use the vector (F, S) to draw a curve that will separate, for each organization, each board of directors, the acceptable and the unacceptable. In fact bearing in mind the definition of risk as the uncertainty of the outcome of a situation, or the spread of result, one could argue that the vector to consider has three dimensions (F, S, σ) where σ is the standard deviation of the annual cost.

On the other hand, the product $(F \times S)$ can be used as a reliable measure of the expected cost of risk for the "frequency" exposure class where the probability of occurrence is such that the law of large numbers applies: thus the organization can budget its expenses on the basis of the expected value of the cost of risk (see D below).

As a conclusion from an exposure diagnosis process, the exposures of a given organization could be summarized in a four quadrant matrix where both frequency and severity are qualified as "high" or "low". *Each organization has to decide for itself what it will call "high" and what it will accept as "low" based on a number of considerations among which are financial strength, stability of cash flows, profits levels and stability, and other subjective elements.*

The four quadrants can be read as follows:

Table 1.3 Simplified risk matrix

	Frequency	
Severity	Low	High
Low	(A)	(C)
High	(D)	(B)

- (A) – Low frequency and severity: these are exposures that have practically no significant impact on the profits. They can be dealt with if and when they occur, as the cash in hand is sufficient to take care of them. They can be practically ignored and do not require any monitoring.
- (B) – High frequency and Severity: these are exposures that no organization should allow to exist. They are typically treated by the risk "avoidance" or "suppression" techniques: do not engage in such a project or get out of it as fast as possible when identified. These extreme situations are rare and should not happen when the risk manager is taken on board any project team very early in the process.

  For all practical reasons, the risk manager domain is restricted to the two last quadrants.
- (C) – High frequency, low severity: as mentioned above, this is an area where the laws of statistics can apply even within the limits of the organization. There is enough "risk mutualization" to forecast with a "reasonable" degree of precision the losses for next year based on the past experience and the likely evolution. Let us say that the forecast can be held true within a range that does not interfere seriously with the budgeting process.

  However, this implies that the organization has collected and recorded reasonably dependable statistical data on past losses as a basis for forecasting future losses and measuring the probable impact of proposed loss control measures.

  In effect, this quadrant contains not so much "risks" as costs to be contained and budgeted as accurately as possible. However, it must be kept in mind that:
  – "Loss prevention" (reducing the frequency or probability of a loss) measures have both immediate and long-term costs for the organization,
  – Claims management is crucial for cost monitoring and that, if no insurance cover is purchased where the insurer does it within the "insurance premium", the organization will incur costs if it is done internally or fees if it is outsourced from a third party,
  – All scenarios should be analyzed including the chances for a very bad year with exceptional frequency and/or severity to place an unbearable burden on the organization.

  On the whole, this class of exposure lends itself well to retention financing where a first line can even be budgeted and charged against current cash flows with no specific exceptional risk financing mechanisms.
- (D) – Low frequency, high severity: this is the quadrant where the risk management professional expertise is most essential. Expected losses in the long run may require a century or a millennium time span to have any meaning. Therefore, this is utterly incompatible with the framework of a human organization. Should the event take place, the consequences for the organization are such that it cannot start up again without a massive injection of external funds. This is one of the main functions of the insurance community, to bring in fresh capital at a time of extreme duress. Hence, the expression coined by some: "the insurer is the banker of the exceptional situations".

That is to say, the covers offered are adequate for a reasonable premium, reasonably stable through time and above all secured by adequate solvency. *The insurer must be able to pay the large claims when called upon to do so!*

This is also where "loss reduction", i.e. limiting the severity of any claim, is essential.

Furthermore, all perils, all dysfunction cannot be assured; some are not insurable by law or by statistical impossibility. In some cases not enough insurers are attracted for a functional market to exist. Then, if and when such an event will occur internal sources of funds will have to be tapped, including investment money set aside for some new development programme that may have to be shelved temporarily as priorities are changed by an unexpected chain of events.

The preceding matrix is but a simplified version of what is now commonly called a risk map or risk matrix.

Risk mapping is a tool that allows classifying, comparing, and prioritizing exposures so that efficient action plans can be developed to mediate or treat them, or benefit from them to draw a competitive edge, putting to best use all available resources. In other words, it is a dynamic graphic representation of the ever-evolving organizational risk profile. Hence, each organization must develop its own specific risk map.

Risk mapping is also an excellent audit and communication tool both internally and externally for the risk manager and the executives of the organization.

However, the model used above, a matrix with only four quadrants may prove far too limited to gain an understanding of one organisation's risks. In practice at the cross, point, representing the mean probability and the mean impact the bulk, more than 80%, of the cost of risk is concentrated. Therefore, risk evaluation will be greatly improved with matrices that will be 4×4, 4×6, 6×4 or 6×6 depending on how fine an assessment is needed. Note that it is highly recommended to select an even number of possibilities on both axes to prevent those involved in the assessment process to take "the middle road."

Furthermore, the categories must be meaningful in the eyes of the "assessor", i.e.

- On the probability axis: Once a day, once a month, for high frequency, once a year, once every two years, once every five years, for the medium frequency as it is likely to happen during the tenure of any executive, and once every fifty years, once a century, once a millennium, for rare event that no one should have to live through and yet be prepared for should it happen due to the dire consequences;
- On the impact axis: for low impact refer to annual profit give a good grasp to a board of director (less than one per mil, one percent, etc.) whereas for medium range impacts a reference to the annual cash flow or gross revenues may prove more meaningful and finally for the very severe impacts may be compared to total assets, or net worth, some times more than a 100%!

This approach will give an immediate insight into what is "essential" or "strategic" and what should be left to the field managers to cope with.

Finally, it should be noted that more than a "permanent risk map" the risk matrix is only a temporary tool to help decision maker that is immediately obsolete when the deciders have moved forward and changed the "risk landscape."

Risk financing and strategic financing

Strategic risk management is still a long way from being the norm. On the other hand, large conglomerates participating in the globalization process have already perceived the gains to be made at the efficient frontier in managing risks in a holistic fashion. Financial analysts and CFOs have been trained in the same universities where the gospel is diversification and uncorrelated risks, pure and speculative alike.

The two fundamental objectives of the finance department remain solvency and optimum return on assets. That means conducting a long-term sustained growth, protected from most uncertainties. At this stage, one must keep in mind that the current development in finance theory rests on the assumption that strategies are built on arbitrage between risk and return and that at the efficient frontier, the board's appetite for risk is key to the return achieved. If the stockholders want more return, they have to bear more risk, as measured as the volatility of future results.

When applied to the realm of risks, beyond the specific financial risks from which it was designed in the first place, the portfolio approach to risk financing leads to a first and fundamental choice between pre- and post-financing of risks. In order that the value to the stockholders be maximized, i.e. the long-term market price of the stock, post-financing will always provide a higher present value of future flows of cash as the funds can be invested in higher return assets. However, two considerations are essential:

- Risk management fundamental mission: it is not so much to eliminate exposures or even to curb the cost of risk than to make sure that only those risks that provide a good return are borne by the organization, i.e. it will cope with the volatility of the cash flows generated by the uncertainty of the outcomes.
- Retention/transfer optimal choice: as mentioned earlier, the origin of the funds, from inside or from outside the organization, is originally the key to distinguishing between retention and transfer. Within the framework of portfolio analysis, the main question is who bears the risk in any given situation, i.e. the uncertainty of the outcome. Therefore, when risk is measured by the standard deviation of the outcome, even the purchase of insurance cover transfers the volatility to the insurer, i.e. the risk, at least according to the terms and conditions of the insurance contract. The optimal equilibrium will have to trade off return for a chance of failure through the "cash flow at risk approach".

From risk management to strategic risk management

Beyond the traditional definition of risk management including only the management of accidental risks, the following lists illustrate some of the "risks" that could be associated with the concept of risk management in a much broader sense.

- Financial risks like:
  - *Banking risks (or lenders' risk)*: loan officers in the banking industry use the term to refer to the quality of a portfolio of loans, that is to say, the ability of the borrowers to repay the instalments in full and on time.
  - *Liquidity risk*: CFOs and treasurers are responsible for the congruence between in- and outflows of cash. They must make sure that the organization will meet is obligation at all times (including those times following a large accident when exceptional sources of funds must be secured).

  - *Foreign exchange risk*: brokers at the exchanges are very attentive to fluctuations in interest rate and currency movements, as they have to hedge daily their positions to avoid risk or seek return.
  - *Interest rate risks*: long-term financing bears an interest and the change in the time structure of interest may have an impact on the solvency or the return of the actors in the financial markets.
  - *Investment risk*: Whether dealing with large individual projects or large stock funds, investment managers are aware of the fundamental finance principle: risk and return are linked, the higher the risk, the higher the return. In the case of portfolio, the fiduciary must understand the investor's risk appetite and whether they are in for a long haul of short-term gains. In the latter, the choice concerns when to buy and when to sell using short-term up or down trends in the market. In the former, the strategy must rely on the fundamentals of the corporation whose stocks or bonds they keep, sell or contemplate buying.
- Nonfinancial risks like:
  - *Health risk (or hazard)*: healthcare specialists are trained to stop epidemics and pandemics, restore or maintain public hygiene, and more generally promote a healthy environment for the general public.
  - *Project risk*: pilots of major projects like the construction of a dam, a power plant or skyscraper, or the launching of a satellite have two key indicators to follow: time and costs. Therefore they must swiftly manage any incident occurring during the construction or preparation. (Project risk management is key to project management and a specialty of risk management where cost and timing are the main factors.)
  - *Military risk (foreign war)*: the members of the strategic defence staff of any country must be very careful with the confidentiality of their decisions and proposals. They also have to prepare alternative strategies for any foreign operations.
  - *Weather conditions risk*: meteorologists work at developing models to predict tornadoes and other climactic situations impacting the life of the people as early as possible to enhance decision-making processes.

Clearly, all these examples illustrate situations where it is legitimate to use the concept of risk management. Indeed, in all these situations, the aim is to find appropriate means to manage uncertainty, to reduce the range of possible outcomes, and to develop a capacity to react when confronted with adverse conditions.

Some academic circles and even some professionals fear that the term "risk management" is tainted by its origin in the insurance world – even in workers' compensation covers for that matter. This is the reason why a new phrase has been coined: "strategic risk management". The underlying idea is that in all situations where there is uncertainty about the future, a probabilistic approach is difficult. The main differences between the traditional view of risk management and this new approach can be summarized in three points:

- Strategic risk management is concerned with all risks, pure as well as speculative.
- Strategic risk management's central goal is economic efficiency. It is not limited to restoring a situation following an accident. Therefore, it is geared towards growth; change management in an essentially positive approach rather than the negative approach of the traditional view of risk management. (*Economic efficiency or growth could be even replaced by optimum value to stakeholders in a more ethical centred approach*.)
- Strategic risk management is in essence systemic. It is not only analytical, it views the organization as an open living body, as a whole. If the identification of individual exposures

remains essential, combining them in a dynamic system is the key to this approach. All the objectives of the organization must be assessed, the strength and weaknesses evaluated as well as opportunities and threats stemming from its environment. A global optimum for the system is the only possible mission.

In this broader perspective, traditional risk management is not obsolete. It appears only as one of the many facets of strategic risk management. When the term managing risk is changed to managing uncertainty, it must be applied to all dimensions of the organization's strategy.

From managing physical assets to managing reputation

In the last two decades of the twentieth century the world economy experienced what must be seen now as a complete paradigm change. Globalization is only the most visible part of the iceberg; in fact the rise of a 'nonphysical' economy as the major proportion of the world's wealth is undoubtedly the most significant evolution. The value of intangible assets became the most important part of the market value of any firm traded on the stock exchange: when compared to the value of the physical assets, the total value of the firm (measured by the share price multiplied by the number of outstanding shares) reached peaks that ranged from 10 to 100 times.

The financial explanation is simple: the value of the firm is equal to the present value of the future stream of dividends expected from that firm, discounted at a rate which takes into account of the level of risk and the expected growth.

However, the model could not explain the level of shares in a company that had never turned any profit and might not in the near future; in fact what gave them value were *expectations*. This "added value" is now commonly called "reputation". Does it really exist? The stock market provides the answer: even after the collapse of the stock market in 2002/2004 only partially recouped since then with some significant recent rebounds, the value of "not-accounted-for" intangible assets – the difference between physical asset value and market price – is still significant. As a matter of fact, this is not only true for traded shares but even for private transactions when smaller firms are integrated into larger concerns. Reputation, whether it exists or not, has a significant impact on the economy, representing probably between 60 and 70 % of developed countries' wealth.

In short, up until recently risk management has been dealing with what has become less than a third of the wealth of the organizations it serves. It is high time reputation risks were assessed and mitigated.

All information – whether written, spoken, or via a computer programme – that flows in, through, and out of the organization is of vital importance. It is a source of exposure, through loss of data, degradation, or disclosure resulting from equipment failure, human error, or wilful intrusion. It contributes to the survival of any organization because of the importance of the "intangible assets" value stemming from the flow of information. It is so important that a specific diagnosis and risk management programme for information exposures is essential. (Among major information exposures, the "Y2K bug" was an illustration of a well-managed exposure resulting in only minor interruption.) Internet connections and firewalls remain a constant challenge. Nevertheless, all CEOs should remember that the human brain is the easiest way to carry information (and secrets) out of the organization: the best risk control technique is a proactive human resource policy. Furthermore, all human beings are not only rational but also emotional and social animals, and using a purely rational approach to information risk as

a way to manage it when intangible assets are exposed would be very short-sighted. Indeed, most organizations, with sometimes a push from public opinion, consumers' associations or even trading partners, are being made more and more aware of a major exposure: *the risk to reputation (image*, *brand)*.

This is the risk that an organization's reputation can be tainted, either by real mismanagement or simply in the public's or its economic partners' perception. For the purpose of this chapter, "reputation" is defined broadly and includes both the stakeholders' subjective appreciation of the organization and the intangible assets like brands and image that can be separately valued. The degradation may have different origins: dramatic accidents, questioning of management's wisdom, product defect and ill-organized or untimely product recall, or defamation, to quote but a few.

Consider Exxon and the pollution of Alaska waters by the *Exxon Valdez*, or Shell and the consumers' boycott following the *Piper Alpha* affair more recently BP and the Alaskan pipeline; Perrier never fully recovered after toluene traces were found; whether Firestone has rebounded after the SUV tyre recall? (Thanks largely to out-of-court settlements in most of the cases, coupled with the effort made in Formula 1 car racing that resulted in tremendous success since the 2003 world championship – outstanding adherence under slippery conditions!) We can add more recent examples: British Airways flights grounded for several days in the summer of 2005 over social unrest at its outsourced catering supplier, KPMG admitting to illicit advice to clients, major brokers drawn into a controversy over commissions and tempered tender offer processes, major pharmaceutical firms delaying recall of major products, etc.

The media's increased scrutiny, relaying public interest in all aspects of each organization's management, imposes on all boards of directors a need always to act as if under a "glass roof", where every move and every thought can be made public. In all areas of management, therefore, decisions and their implementation must be at all times consistent with the set of values set forth by the organization.

This is of the utmost importance in the areas grouped under the heading "corporate social responsibility" – encompassing employment practices, impact on the environment and sustainable development, human rights, involvement in local communities (especially in emerging economies) and relationships with business partners.

To summarize, reputation is the result of a lengthy project to build trust, through consistent efforts, with all stakeholders, while the world is growing less and less trusting and the different stakeholders may have diverse, indeed contrary interests in the organization.

The main consequence for risk managers is that maximizing value to stockholders will require managing risks in such a way that reputation is enhanced and risks to reputation mitigated. Clearly, sound risk management is one of the pillar of good governance.

From risk manager to chief risk officer

As briefly explained above, in the recent past risk management went through a tremendous evolution and appears to have grown from a set of technical skills into both a discipline in itself and a part of the broader field of management sciences.

Since the mid-1990s, this reality has been illustrated in many organizations by the creation or expansion of the internal risk management professional's status. However, more recently, in the UK among others, a reverse trend has appeared with the separation of risk financing (assigned to the CFO) and loss control (to the operational), thus questioning the pertinence of a risk manager altogether. In the meantime, corporate governance tends to be embodied in a

new function. Could it be then that one of the major risks to be managed by a risk manager would be his own career?

But in the same time, both Australian and British corporations are encouraged to create risk committees in their board staffed only with independent directors, i.e. nonexecutive, to ensure proper consideration is given to these important issues.

Whatever the framework, consultant, part-time executive or manager, depending on the size and scope of the risks to be managed, there is an ever-broadening field of competencies for the next generation risk management professional.

These apparently conflicting trends can be reconciled when one realizes that risk management is truly transversal as risks will stem from and touch all the activities conducted within and without the organization. Therefore, the risk management professional is only a facilitator of the risk management process that must be owned by the risk management practitioners, i.e. all in charge of an activity for the organization.

In the USA, some corporations, mostly in the financial sector, have recognized the necessity to include the risk management process at the highest level, i.e. in the executive suite. For those risk persons who sit in the executive meetings, they have forged a new title reflecting their executive status.

Traditionally, members of the executive committee have become "chief officer", like the chief executive officer, chief administrative officer, chief financial officer, etc. So the new person would be the CRO (chief risk officer), and should report to the risk committee at the board level.

French entrepreneurs could smile at this recent discovery made in the New World. As early as 1898, Henri Fayol, a French engineer and entrepreneur, considered as one of the founders of modern management, identified "safety", i.e. protecting persons and assets, as one of the six main functions of a firm.

He identified clearly the strategic security director, the ancestor of the CRO. It took nearly 60 years for Fayol to be translated in English and 40 more years for the American establishment to read him. But how much longer will be needed for the French establishment to rediscover him?

Will this new risk manager, this new CRO, whatever the title, be the person to find a new "meaning" for words such as risk, safety, security, threat and opportunity, sustainability?

Why is risk quantification needed?

In the context within which organizations must operate today, it is all too clear that the traditional and reactive approach of the insurance purchaser protecting the assets of the organization must be replaced by a dynamic and proactive vision aimed at achieving the organization's mission, goals and objectives under any stress or surprise. It requires a new expanded definition of "risks". The "new" risk manager must think and look beyond the organization's frontiers, more specifically to include all the economic partners, indeed all the stakeholders of the organization. Special attention will have to be devoted to the procurement chain and the interdependences of all parties.

This is a major reason why risk management professional conferences in Europe and Australia as well as in America have given some thought to developing a new title to evidence the evolution of the risk management scope and duties. How to name this new strategic manager of risks when clearly purchasing insurance is no longer the sole answer to managing risks?

With this rapid evolution of the "risk domain" comprising more and more noninsurable risks, new approaches to risk management have become necessary to be an effective risk manager.

Defining the competencies required is a very daunting task, let alone finding the individual to possess them!

The Australian standards were revised in 2004, and the British standards developed jointly by ALARM, AIRMIC, and the IRM are now accepted by FERMA and have been translated into more than 20 languages. If interpreted as a road map to effective ERM (enterprise-wide risk management) rather than a compliance reference, then these frameworks do provide a track to explore an ISO commission an RN chaired by K. Knight is currently developing an international "RN framework" inspired from the Australian Standards. But whatever the itinerary preferred, all managers will need to develop a risk register and quantify the possible or probable consequences of risks to make rational decisions that can be disclosed to the authorities and the public. In many circumstances the data available are not reliable and complete enough to open the gates for traditional probability and trend analysis, other toolboxes may be required to develop satisfactory quantification models to help decision makers include a proper evaluation of uncertainty in any strategic or operational decision.

RISK QUANTIFICATION – A KNOWLEDGE-BASED APPROACH

Introduction

In the first section of this chapter, we have presented what we believe are the foundations of risk management:

- The definition of an exposure: object or resources at risk, peril, and consequences. Thus defining an organisation as a portfolio of exposures.
- The three-step risk management process: diagnosis of exposures, risk treatment, and audit; the risk treatment step being further decomposed in design, development, and implementation phases of the risk management programme.

We have also demonstrated that quantification is the key element for strategic – or holistic – risk management, as only a proper evaluation of uncertainties allows for rational decision making.

In this section, we will show how a knowledge perspective on risk could support the design of a risk management programme, at both tactical and strategic levels. One of the key tasks of the risk manager, i.e. to design a risk management programme and have it approved, can be represented as an "influence diagram".

Causal structure of risk

Risks are situations where damaging events may occur but are not fully predictable. Recognizing some degree of unpredictability in these situations does not mean that they are totally random events.

Most of the risks that we will consider throughout this book are partially driven by a series of factors, or drivers. These drivers are conditions that would make the occurrence of the risk more probable, or more severe.

From a scientific viewpoint, causation is the foundation of determinism: identifying *all* the causes of a given phenomenon would allow predicting the occurrence and unfolding of this event. Similarly, the probability theory is the mathematical perspective on uncertainty. In situations where an event is totally unpredictable, the laws of probability can help to envision and quantify the possible futures.

Knowledge is the reduction of uncertainty – when we gain a better understanding of a phenomenon, the random part of the outcome decreases compared to the deterministic part.

Some authors introduce a subtle distinction between *uncertainty* and *variability*, the latter being an intrinsic randomness of a phenomenon that cannot be reduced. In the framework of deterministic physics, there is no such thing as variability, and apparent randomness is only the result of incomplete knowledge. Invoking Heisenberg's "uncertainty principle" in a discussion on risk quantification may seem disproportionate. However, in so doing, we understand the principle as stating that the ultimate knowledge is not reachable, rather than that events are random by nature: "In the sharp formulation of the law of causality (if we know the present exactly, we can calculate the future) it is not the conclusion that is wrong but the premise".[4]

Uncertainty and knowledge

For the purpose of this discussion, we can summarize our position as follows: uncertainty results from an incomplete knowledge, and complete knowledge is unreachable.

Our perspective on risk quantification will rely heavily on this dialectic between knowledge and uncertainty.

Specific knowledge of a phenomenon is represented by a causal structure. When working with a specific device or machine, the possibility of a misuse leading to an accident depends both on the experience of the user and on the complexity of the device. "Experience" and "complexity" are key drivers for this risk.

However, these drivers are not sufficient to create a deterministic model. If we know that the user is "experienced" and the machine "simple", this does not mean that there is no risk at all. Several other factors can interfere: the user may be tired or disturbed, the machine may not have been reset properly by the previous user, etc. The occurrence of the risk is still a random event, but the probability of this event depends on the drivers.

Thus we simply recognize that (1) some key drivers have some influence on the possible occurrence of the risk, and (2) even if these drivers are known, the occurrence of the risk remains unpredictable.

The formalization of causal probabilistic graphs (Bayesian networks) is particularly adapted to represent this mixture of knowledge and uncertainty. We will use this formalism as a tool throughout this book. Causal graphs and Bayesian networks will be described in detail in Chapter 2 Toolbox. We provide here only a brief introduction to this formalization.

Figure 1.1 represents the causal structure – the "knowledge", i.e. the causal relationships between the *nodes* (the variables).

Here, both the "User experience" and the "Machine complexity" influence the possible occurrence of an "Accident". Since the actual occurrence of an accident cannot be predicted from the knowledge of these two causes only, the "Accident" is a random variable. The probability distribution of this variable is conditioned by the two drivers. As "Accident" is a binary (yes/no) variable, its distribution is fully characterized by the probability of occurrence of an accident.

Of course, each node can be determined by one or more drivers, and can be the driver of other nodes in the more complex graph. For instance, in the elementary illustration here, we could introduce the idea that the experience of the user cannot be measured directly, but is

[4] Heisenberg, W. 1927. Über den ausch aulichen Inhalt der quantentheoretischen Kinematik und Mechanik, *Zeitschrift für Physik*, 43, 172–198.

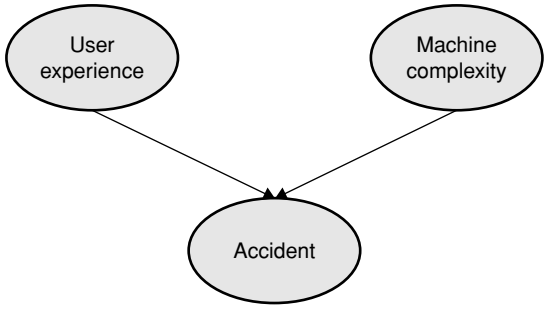


Figure 1.1 Illustration of causal structure of a risk

partially conditioned by her age. Older users are typically more experienced, although they can be new in the job.

A risk management programme itself can be described through an abstract causal graph. Before introducing this graph, which represents the cornerstone of our approach, we need to introduce two other types of nodes in causal graphs.

Decision nodes represent drivers that are chosen rather than observed. If we use the above model for a prospective risk analysis in a workshop, the choice of an equipment supplier can be a driver of the machine complexity. On the other hand, the management could increase the level of qualification of the users by implementing a training programme. Therefore, the final probability of accident would be – partially – influenced by some management decisions, Figure 1.2.

Utility nodes usually represent cost, or profit, variables driven by other variables. They can also represent other quantifiable measures, which cannot be reduced to costs, such as human casualties.

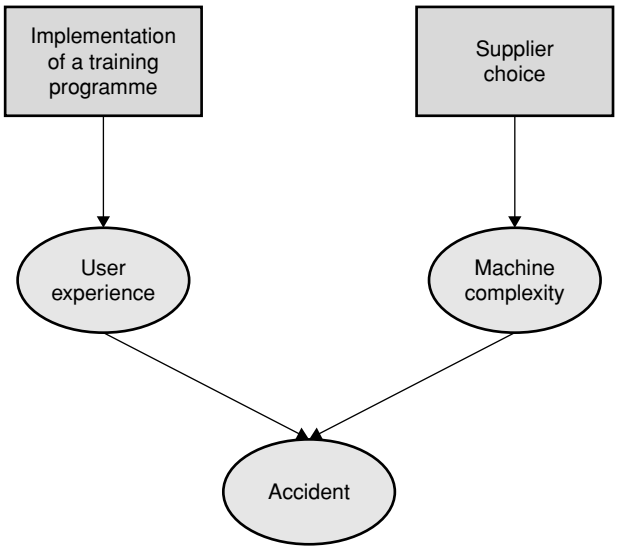


Figure 1.2 Management decisions in the casual structure of a risk

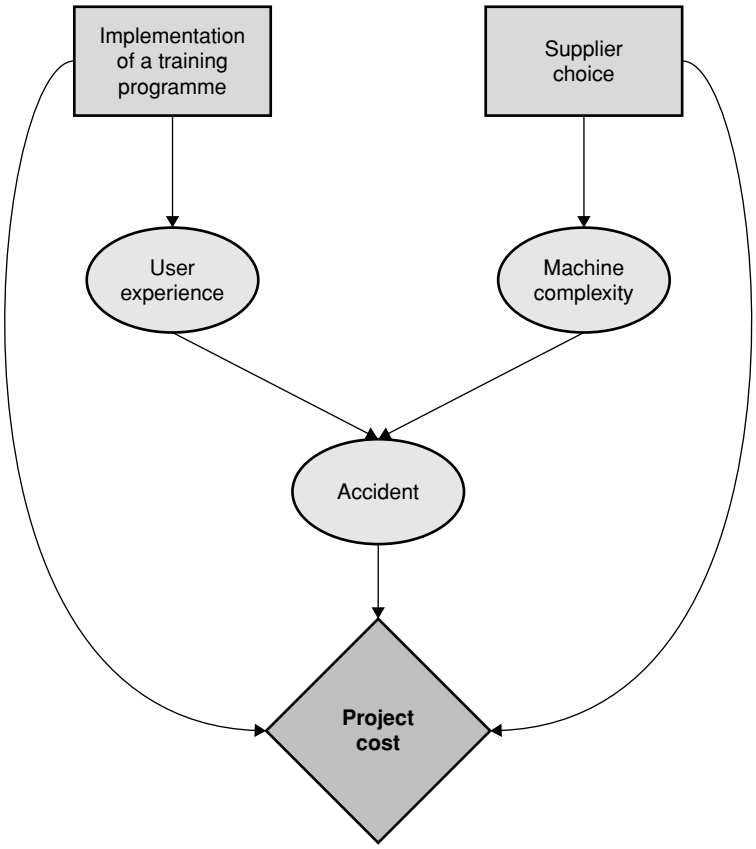


Figure 1.3 Probabilistic economic analysis of a project

Further to the factory point of view risk analysis initiated above, a probabilistic economic analysis can be carried out, through the introduction of cost elements: total accident costs, training costs, and machine costs, Figure 1.3.

Figures 1.1–1.3 are built according to the conventions used in "influence diagrams". An influence diagram is a visual representation of a decision problem. Influence diagrams offer an intuitive way to represent decisions, uncertainties, objectives, and their mutual interactions.

We will use the following conventions throughout this book:

- A rectangle represents a decision.
- An ellipse represents a random variable.
- A diamond represents an objective, cost or utility.
- An arrow represents an *influence*, or *causal dependency*.

We will now try to generalize this simple example to show how causal graphs can be used to formally represent the risk management process.

Building a quantitative causal model of risk

In the first section of this chapter, we have shown that risk assessment is supported by the notion of *exposure* as the basic concept of risk.

An exposure is defined by three elements:

- The resource at risk, or risk object.
- The peril or random event to which the resource is exposed.
- The consequence, i.e. the possible impact – financial or other – when the resource is "hit" by the peril.

For each of these notions, we propose a quantitative counterpart, which would be generally described as a partially random variable – a conditioned random variable.

Before describing in detail this quantification, we must clarify the qualitative and quantitative notions of exposure. From a qualitative point of view, an exposure is a risk. From a quantitative point of view, the exposure will measure the number of resources exposed to a risk.

The exposed resources are quantified by exposure. Exposure is measured by an appropriate quantitative measurement of the exposed resource, such as typically the number of units, the acreage, the volume, etc. In the context of quantifying operational risk for a bank (Basel 2), an apparently similar risk can have different resources exposed, and, hence, different exposures. When considering credit card *external* fraud risks, the exposed resource is the credit card itself. Credit cards can be lost or stolen, and therefore the number of cards is the measurement of exposure to this risk. On the other hand, when considering *internal* fraud risks, the risk can result from a group of employees able to duplicate existing cards and issue fraudulent transactions under some circumstances. In this situation, the exposed resources are the employees of the firm, not the cards. Rather, the number of duplicated cards would be a factor of severity.

In the case of natural events, the same type of distinction may apply. Resources exposed to a tropical storm would be houses, since the storm would hit each of them individually. As a consequence, the number of houses in a specific area would be the correct exposure measurement. On the other hand, the appropriate measurement for a tidal wave, or tsunami, exposure would be the coast length. Here, the number of houses built close to the shore would be an indicator of severity rather than of exposure.

The peril is quantified by a probability of occurrence. This probability is defined as the average expected number of disasters that may happen for one unit of exposure during one unit of time. If the probability of a factory fire in a particular area is estimated at 0.05 %, this means that on average, we expect that 1 of 2000 plants will experience a fire next year.

Exposure and probability of occurrence must be defined in a consistent way. Consider the risk of terrorist attacks on planes. Assume that the main risk is that a terrorist would succeed in boarding a plane with a bomb. Assume further that the probability that he would succeed is 10^{-6} (one in a million), given the quality of controls in place. The appropriate exposure is neither the number of passengers – depending on which plane is involved, an Embrayer, a Boeing 727 or 777 or an Airbus A380 – nor the number of planes in a given company fleet. The appropriate exposure is obviously the number of *flights*. In the same domain, assume that the probability of an individual suffering a heart attack within one year is 0.1 %.[5] We can then estimate the probability of both the pilot and the co-pilot being struck during the same flight. In this example, the appropriate exposure measurement is not the number of flights, but rather the cumulated hours of flight for this company.

Most perils can be described by a binary indicator: the peril will or will not happen. For some of them, such as earthquakes or other natural hazards, the peril occurrence must be further

[5] This evaluation would be focused on the typical airline pilot profile (male, 35–55, good physical condition).

qualified by intensity. For instance, earthquake intensity is usually measured on either Richter or Mercalli scales.

Occurrence and intensity

Intensity is a general notion that could be used for all perils, provided that, as a convention, only 0 and 100 % intensity are observable for "yes or no" perils.

This would also make the three notions of exposure, occurrence and severity more consistent: they are random variables characterized by a probability distribution. The specific case of the yes/no peril can be described by only one figure: the probability of occurrence.

The consequences of a peril are quantified by a severity or impact indicator: financial losses, human casualties, breach of ethics, long-term impact, etc.

When quantifying the consequences of a peril, the disaster is assumed to have already happened. The occurrence is considered certain, but the consequences are still uncertain, and will be represented as a random variable.

When a continuous intensity measurement is applicable, it should not be confused with severity or impact. An earthquake may be very intense, but still have no impact at all, if happening in the heart of a desert.

Fire is a particular case, which in our opinion should be considered as a yes/no peril, even though it can be limited or catastrophic. Indeed, a fire ceases if it is not fed by oxygen and flammable goods. Therefore a fire's intensity is defined only by its consequences.

Quantification of a risk

Exposure, occurrence (or intensity), and impact are the three random variables that fully define a risk. Quantifying these variables is the first step of risk quantification, which corresponds to the "Risk assessment" step of the risk management three-step process described above.

This assessment is probabilistic, since each of these variables is potentially random.

Exposure, frequency, and probability

The risk management literature often qualifies risk using two main concepts: frequency and severity. Severity is the expected cost of an accident or a disaster, or, more precisely, the distribution of this cost when an accident occurs. We believe that frequency is not a well-defined concept since it measures the probability of an accident or a disaster *given the present resources exposed*. Change of frequency may have two causes: change in exposure, or change in probability.

For instance, since 1970 the probability of an airline accident has constantly decreased to about 1.5 accidents for 1 million take-offs or landings in 2000. However, the exposure – i.e. the number of take-offs or landings – is constantly increasing, and hence the number of accidents does not show a clear downward trend, Figure 1.4.

This gives the public the wrong perception of an increasing risk, whereas the individual traveller is now more than 10 times safer today than in 1970.

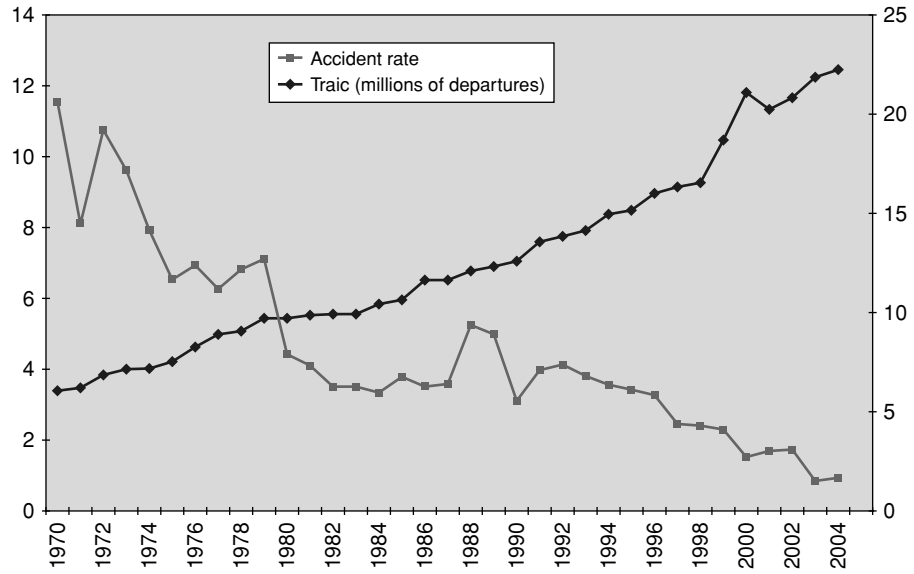


Figure 1.4 Parallel evolution of airline accident rate and traffic

This example also shows the importance of an appropriate definition of exposure, as the *number of resources "independently" exposed to a given peril*.

Some studies on transport safety use a "km.passenger" as a measurement of exposure, usually reporting the "casualties per 100 million km.passenger" as a measurement of frequency. This may be an appropriate indicator from an economic point of view, but "km.passenger" is not a correct measurement for exposure, at least for air transport. Indeed, a "km.passenger" is not a resource independently exposed to the risk of a take-off or landing crash – which are by far the most dangerous phases of a flight. When a crash occurs on a long-distance flight, several hundreds of thousands of "km.passengers" are hit simultaneously. It is not possible to define the individual probability of one "km.passenger" being hit.

A change of transport structure, for instance increasing the share of long-distance flights would artificially reduce the risk, although the overall safety would not be improved. This is shown in Figure 1.5, where the casualties per 100 million km.passenger have decreased three times faster (from 0.05 to 0.005 in 10 years) than the number of accidents per million departures (from 3.25 to 0.9), during the period from 1996 to 2004. This is probably due to an increase in long-distance and large carriers' share of the overall traffic.

Another problem with this measurement is that it also entangles exposure, probability, *and* severity.

This "casualties per 100 million of km.passenger" indicator may increase if either: (1) the short-carrier share increases, (2) the actual safety of aircrafts decreases, or (3) the size of air carriers increases. Again, this might be an interesting indicator for a global "cost-of-risk" analysis, but this will not help in understanding the drivers of this cost.

Exposure, occurrence, and impact drivers

Each of the three variables described above can be influenced, at least partially, by some drivers.

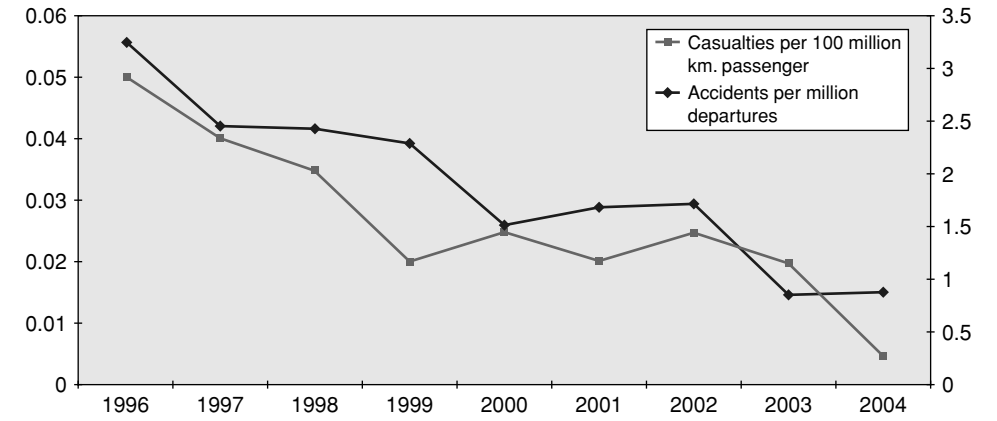


Figure 1.5 Parallel evolution of different frequency measurements for airline accidents

For instance, an airline company may analyse the risk exposure attached to a partial renewal of its fleet with large aircrafts. This would decrease the exposure to terrorist attacks since it would lower the number of flights. Similarly, a reduced number of flights would lower the workload of the security officers, and allow more thorough checks, finally reducing the probability of an attack. On the other hand, should a disaster occur, obviously it would have more severe consequences, since on average twice as many passengers would be on board.

But if the traffic increases due to economic conditions leading to a higher demand for air travel, the company would have to increase the number of flights anyway.

In that particular case, we see that:

- Drivers to exposure (number of flights) are: demand and company policy.
- Drivers to occurrence are: workload of, which is in turn driven by number of, flights and number of security officers.
- Drivers to severity are: demand and airline policy.

Controlling exposure, occurrence, and impact

Controlling exposure, occurrence and impact reflects the three main approaches to risk reduction.

Controlling exposure is related to *avoidance*: a resource exposed to risk is usually a resource exposed also to an opportunity. If an airline decides not to increase its traffic, its exposure to take-off or landing accidents will not be increased, but this means also that some opportunities would be lost.

Controlling occurrence is related to *prevention*: reducing the probability of a given risk is performed through an analysis and improvement of the situation before the accident happens.

Controlling impact is related to *protection*: reducing the severity of a given accident is performed through an analysis and improvement of the hypothetical situation if the accident would happen.

Controllable, predictable, observable, and hidden drivers

Four categories of drivers can be identified:

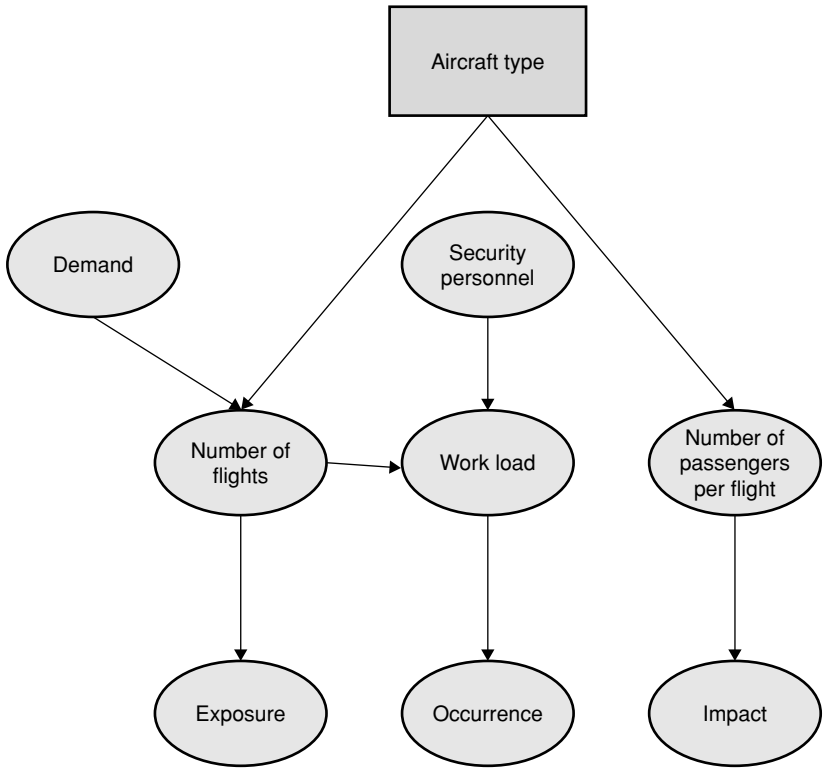


Figure 1.6 Drivers of risk exposure variables (exposure, occurrence, and impact)

- *Controllable drivers* can be influenced by some decision: in our example, the number of passengers per flight will be modified by the aircraft type selection.
- *Predictable drivers* cannot be really influenced by a decision, but their evolution can be predicted to some extent: in our example, the demand can be partially predicted – using external economic forecasts.[6]
- *Observable drivers* cannot be influenced, or predicted. They can be only observed after the facts, a posteriori. Observable drivers should not normally be included in a causal model of risk, since they cannot be used in a prospective evaluation.
- *Hidden drivers* cannot be measured directly, not even a posteriori, but may be controlled to some extent. For instance, the hostility of potential terrorists cannot be measured; however, it can be reduced through communication actions.

Cost of decisions

This first analysis shows that controllable drivers are obviously the most interesting: they are the levers of risk control or mitigation.

[6] In that particular example, the airline could partially drive its demand on this line through its pricing policy which could drive its market share. However, since the reaction of the competition cannot be predicted, it could be more rational to consider that demand is not controllable.

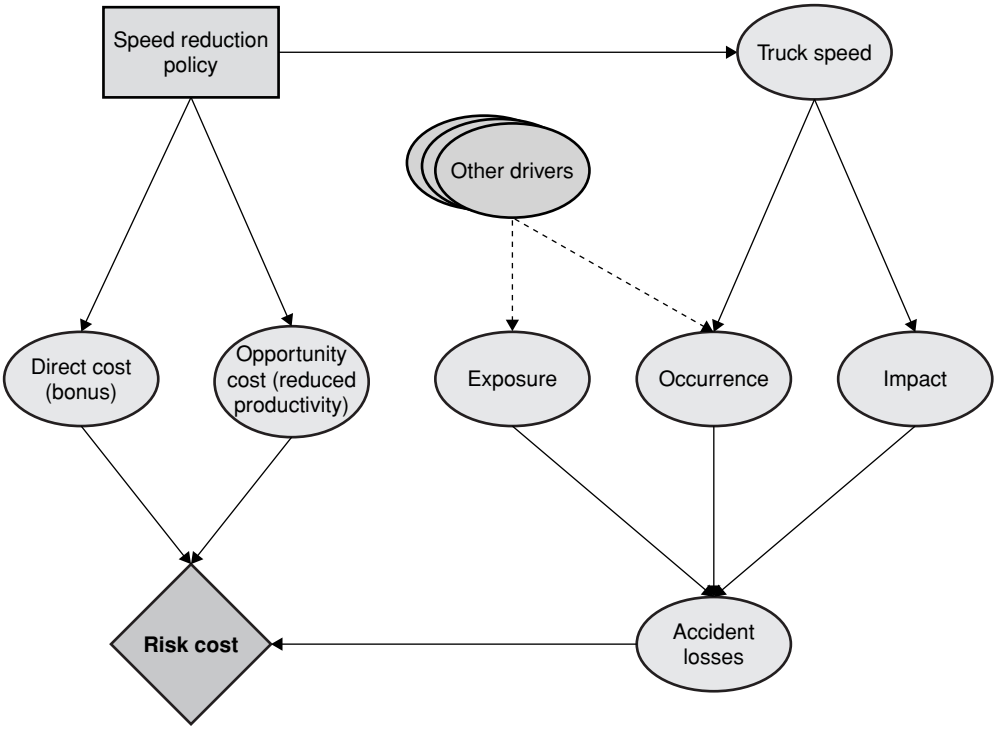


Figure 1.7 How risk mitigation actions impact risk cost

In most cases, implementing a risk control measure will:

- Change the distribution of some risk driver, at either the exposure, occurrence, or impact level.
- Have a direct cost, related to the implementation itself.
- Have an indirect or opportunity cost, related to the potential impact on business.

For instance, consider a cargo company deciding to take a harder line on truck speed limitation. The company may decide to award a bonus to the compliant drivers. This company will incur directly the cost of the bonus (direct costs), but may also initially face a drop in revenue, or need to hire more drivers to serve its customers. Of course, this policy will reduce the probability and impact of accidents.

Risk financing

The second element in the treatment step of the risk management process is usually to develop a risk financing strategy, including a more effective use of insurance and other sources of capital.

This strategy will have an impact on the cost of the retained risks and on the cost of financing, which could also be analyzed through an influence diagram.

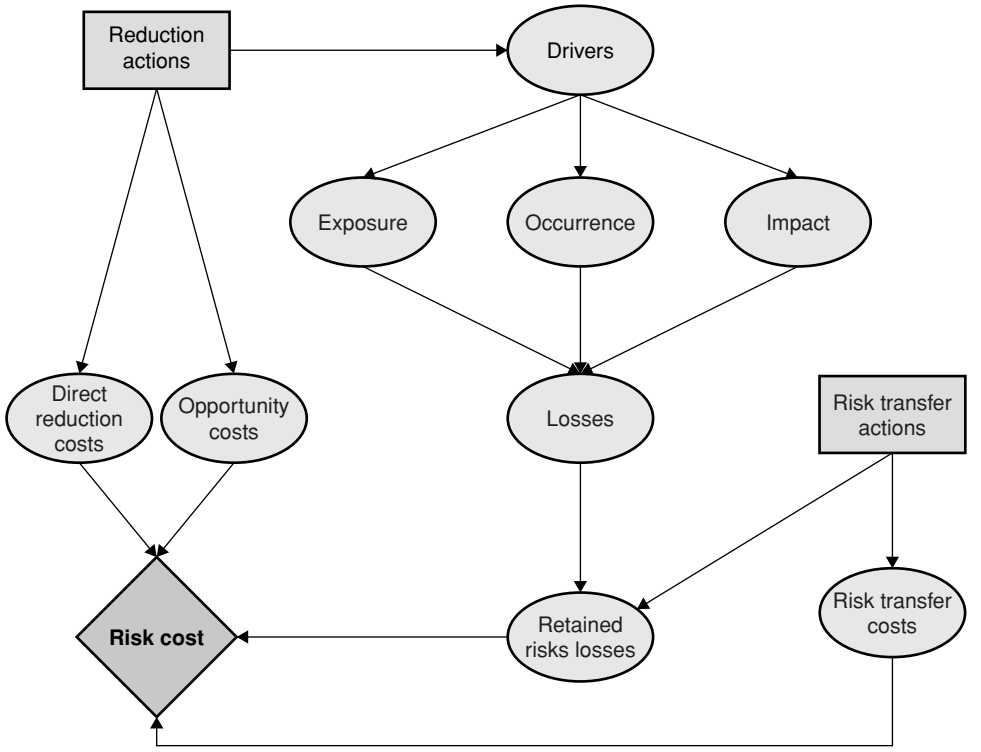


Figure 1.8 The risk management programme as an influence diagram

Risk management programme as an influence diagram

From this first general analysis of the risk management process, we can derive a general causal graph for risk management, Figure 1.8.

This graph can be analysed in detail as follows:

- "Exposure", "occurrence", and "impact" are random variables partially determined by risk "Drivers". These "Drivers" may of course be multiple and potentially dependent. This type of dependence is not represented in this abstract version of the graph, but would be in a specific model for a particular risk or risk portfolio.
- "Losses" is a random variable whose distribution depends on exposure, occurrence, and Impact. "Reduction actions" modify the "Drivers", and, consequently, the "Losses". "Reduction actions" are human decisions. The choice of actions will of course depend of the risk cost analysis, but it is considered to be free. This is why decisions have no direct causes in this graph, or more generally in influence diagrams.
- The cost of reduction actions, "Direct reduction costs", depends on the reduction actions implemented, as does "Opportunity costs".
- "Risk transfer actions" implement various methods for financing the possible losses. The "Retained risk losses" distribution depends on both the total losses distribution – before financing – and the risk transfer actions selected.

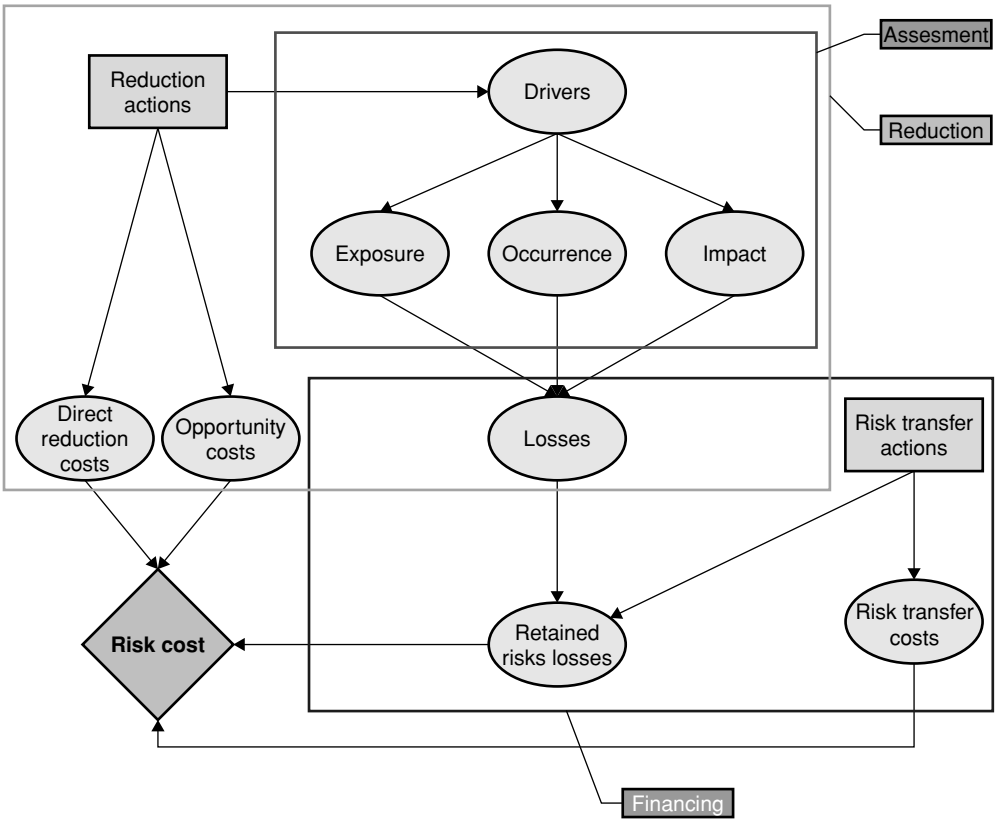


Figure 1.9 Risk assessment, control, and financing as parts of the risk management influence diagram

- The final objective node, "Risk cost", is computed as the sum of reduction costs, opportunity costs, retained risk losses, and risk transfer costs.

This diagram captures most of the risk management process. The three steps of this process (assessment, reduction, and financing) are represented by subparts of these graphs, as shown in Figure 1.9.

Modelling an individual risk or the risk management programme

Before going further in this discussion, there is one point we would like to make clear. The formalization of causal graphs allows describing a model for both a single risk and the global risk management programme.

The airline terrorist risk model and cargo road accident model are examples of individual risk models. Such individual models may be simply juxtaposed when designing a risk management programme. They would certainly interact, at least through the limitation of financial resources. Figure 1.10 shows how the constraints on money allocation for risk mitigation could be represented in a causal graph.

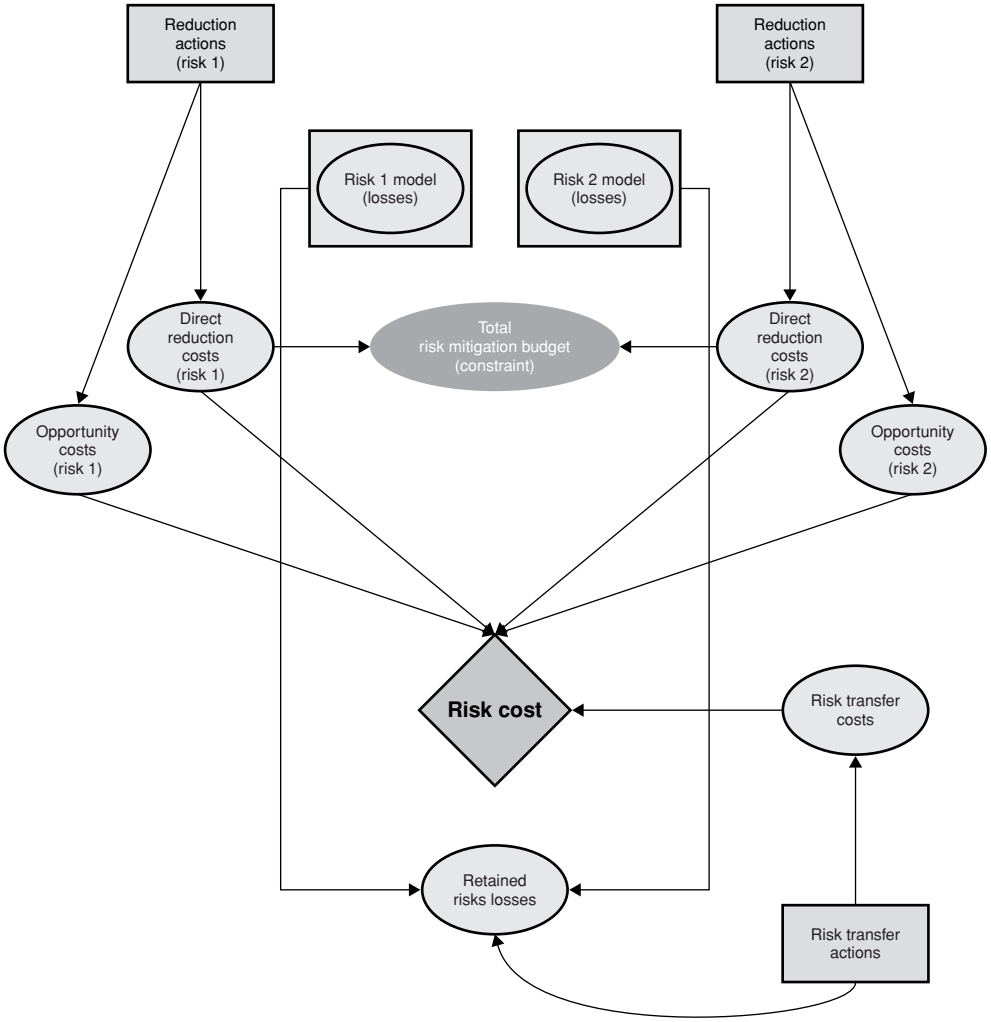


Figure 1.10 Interaction of multiple risks

In this example, we consider only two risks risk1 and risk2, although the discussion could be easily extended to any number of risk models. Causal models of loss distribution for each of these risks are represented in a compact way. Reduction actions are available for each of these risks. These actions cannot be selected independently, as the total budget allocated for risk mitigation expenses is limited: therefore the total costs undertaken for reduction of risk1 and risk2 cannot exceed the budget.

Although it is in theory possible to aggregate all individual risk models into a global model, in practice this would be far too complex. The global risk model of the organization should be considered at a synthetic level. Each risk model would be replaced by a simplified risk cost model, and risk costs models would be aggregated into a global risk model. In Chapter 3, we will discuss how a specific risk model can be transformed into a synthetic risk cost model, and also exhibit risk models considered at different levels.

SUMMARY

Risk management is currently maturing into a fully fledged branch of managerial sciences dealing with the handling of uncertainty to which any organization is confronted due to more or less predictable changes in the internal and external context in which it operates as well as evolutions in their ownership and stakeholders that may modify their objectives.

Global risk management is involved in the design and implementation of strategies that will incorporate provisions for adaptations to these changing conditions and provide sentinel events to warn of possible ruptures as early as possible. This will deliver value by facilitating prompt reaction and pre-emptive actions to allow managers to reach their objectives, goals, and missions under any circumstances and cope with surprises, even of cataclysmic proportions.

However, this organizational resilience can be achieved only through the implementation of a continuous process of risk management at all levels in the organization stemming from a clearly defined risk management strategy approved by the board in which risk appetite is defined and communicated. This three-step process, diagnosis of exposures, risk treatment or mitigation plan, loops through the review and audit process of the risk management programmes to ensure that the key objectives are at the centre of all decision making and achieved through a proper implementation of the plans.

Judgement can be applied to decision making in risk related issues, but rational and transparent processes called for by good governance practices require that risks be quantified as widely as possible. When data are insufficient, unavailable or irrelevant, expertise must be called upon to quantify impacts as well as likelihoods. This is precisely what this book is about. It will guide the reader through the quantification tools appropriate at all three steps of the risk management process: diagnosis to set priority, loss control and loss financing to select the most efficient methods with one major goal in mind – long-term value to stakeholders and audit to validate the results and improve the future.