

Overview and General Aspects

Operational Risks and Business Continuity: An Essayistic Overview

HEINRICH SCHETTLER, MARTIN J. WIECZOREK, MICHAEL PHILIPP
SQS Software Quality Systems AG (Germany)

Abstract: This article is intended to give a comprehensible introduction to operational risks and business continuity to an interested reader who is not necessarily an expert. Nowadays, business has become complex because of many factors: globalisation, distribution of services, new technologies and so on. Such factors lead to risks which we are sometimes not used to dealing with. However, none of those factors may be considered in isolation. They are, to a certain extent, always present and they have to be considered in their context. This is also necessary from the viewpoint of time, budget, and the quality of the corresponding activities.

After some historical examples of risk management, mainly in the context of trading and banking, the notion of robustness is introduced in an informal way and the driving forces in the field of operational risks today are discussed. An overview of strategies to control the risks to business processes is presented. Here the roles of business owners and of system and software suppliers are described, emphasising the issue of co-operation. In addition to the opportunities arising from risk management and business continuity planning, some limitations and open questions are sketched, indicating that there is no final patent remedy. As a conclusion, the needs for the balancing of risk control against other business activities and for its integration with those activities are outlined.

Keywords: Operational risks, Robustness, Risk management, Business continuity planning, Crisis management, Software and project risks, Benefits and costs, Risk map, Basel II

1 Introduction

While this article was being written, on September 11th 2001, the terrorist attacks on the World Trade Center and the Pentagon occurred. This catastrophe had many immediate political and economic effects. The other, more long-term effects cannot be predicted with today's knowledge and experience. Besides the human catastrophe this terrible event also highlights the enormous amount of interaction and interdependencies between business, technology and other kinds of infrastructure and their sensitivity to disturbances. This event has shown, in a horrible manner, the practical importance of operational risks and reminded us of the principal limitations of risk control.

Though the 11th of September is a striking example of a new quality of risk, we are used to dealing with risks. The glance at evolution and history in the next section will show this. Section 3 discusses current operational risks in the context of globalisation

and internationalisation, and Section 4 introduces the idea of robustness. Possibilities for dealing with operational risks will be discussed in Section 5 from two different viewpoints, namely the business process and the supplying of IT systems which support the business process. Section 6 will take a closer look at the problem of balancing all activities against operational risks with respect to benefits and costs, as well as opportunities and risks.

2 Examples of Risk Management in History

As a vivid example of risk management, observe a bird in the garden. How does the bird behave? Normally it is picking for worms or drinking water. That is its business process. When it is alarmed by strange, sometimes very small changes in its sensual field, the bird concentrates on the spot in which the changes have occurred (continuously operating early-warning system) and decides very quickly whether to escape (business continuity plan to shelter from substantial damage, e.g. by a cat), to continue observation of the spot or to continue exploiting its opportunities (worms). This comprises risk management behaviour, coded in DNA by biological evolution. In this way the bird achieves a certain amount of protection from dangers, e.g. cats. That is robustness of its “business process”.

Today we envision evolution as an optimisation process with the preservation of species as one of its goals. This optimisation process produces a certain amount of short-term inefficiency. Our bird does not use all of its time to pick worms, to drink water or to reproduce. If it did, the bird would have been eaten by a cat long ago, so that we would not observe it today.

In the following we give some historical examples of operational risks and their management from the field of trading, banking and insurance and consider the business system as a whole.

2.1 Trading

In addition to risk management by evolution, there is also a long tradition of conscious human risk management. One obvious step is reflected in the birth of the idea of risk in the 17th century [Broc96]. The Italian word *ris(i)co* meant “to sail around a rock”, which was a typical risk in those days in the business of trading with India.

In 1599 a trading company in the Netherlands sent four ships to India to buy pepper. Only two of the ships returned in 1601, demonstrating the risky side of trading. On the other hand, documents report profits of up to 300% [Brau86]. This resembles figures for successful start-up enterprises not so long ago.

What was the nature of the operational risks of trading? Rocks, bad weather, inaccurate maps, navigational mistakes and absence of information on what to sell or buy and where to do so. These risks mostly affected a single ship or a single trade, and in rare cases a small fleet, but they did not affect the worldwide trading system as a whole. To cope with their individual business risks, traders distributed their merchandise among several ships and diversified into different trades and locations. There were technological and procedural developments which increased the robustness of shipping. Copper hulls, simplification of steering and navigation, and differentiation and specialisation of work by centralising control of the ship in the hands of specially trained experts on the one hand, and leaving operational activities to semiskilled people, on the other hand, are only a few examples. The last feature allowed not only for better and quicker reaction in case of trouble (crisis management) but also the manning of many ships with people who had not previously worked on ships (efficiency and flexibility).

Another practice has had obvious consequences that have continued to the present day. As predecessors of our joint-stock companies, traders used to own and operate ships through shares, taking business opportunities and risks in common.

2.2 Banking and Insurance

Early forms of banking can be found in the Bible. Its medieval big-business form, for example as practised by the Fuggers, began by concentrating on financing the activities of kings and rulers such as conquests and wars. The careers of these bankers began to end when they overestimated the possibilities of a Spanish king and bid on a single horse.

A big opportunity arose in the context of trading in the form of a multiple function: on the one hand credit allowed traders to undertake expensive, long-term trading trips and reduced their financial risk, and on the other hand it allowed participants or investors to participate in the opportunities of trading and distributed the associated risks.

Financial risks were mitigated by comparatively small banking and insurance companies. In the beginning often a single company or businessman acted as trader, banker and insurer in one. The impacts of the bankruptcy of one such institution were also restricted.

A large operational risk, not only for banking, lay in the production of sound accounts, especially when the business was distributed over several locations and independent business transactions took place to a certain extent. Methods such as double-entry accounting (used for the first time by the Fuggers and in Upper Italy) and procedures for saving data and transferring information were used to prevent wrong accounting. These appear to be predecessors of practices such as two-phase commit protocols, re-routing and encryption techniques, which are nowadays used in computer networks to control similar risks. In addition, these risks accelerated the development

of mathematics as a key technology and of banking as the “engineering” discipline par excellence.

Probably the best known example of an early insurance business is Lloyds of London (which originated at the end of the 17th century), a co-operation of companies which originally insured ships. As one important part of its business, Lloyd’s operated an early warning system, which allowed the London headquarters to monitor as exactly and as quickly as possible the position and state of the insured ships. It is reported that Lloyd’s was even better informed than the ships’ owners. This knowledge protected Lloyd’s from insurance fraud and provided data to assess future claims by means of probability theory.

2.3 Business Network

Most of the operational risks of the 17th and 18th century arose from comparatively small, independent, isolated causes which affected single trades, ships or business partners. These risks did not affect the business network as a whole, which behaved in a stable and robust manner even under the conditions of the wars that were usual at that time.

One feature of this network was the great amount of flexibility and fault tolerance among the business partners regarding delays. Delays were a fact of life: delays in journeys by ship, delays in the transport of information and delays in the transport of bills of exchange between different branches. This indicated an inherent credit opportunity for the business partners, reflected in their business ethics, which were based to a great extent on mutual confidence. Prolongation of credit, time buffers and buffers for goods (warehouses) were basic measures to tackle the risks. As a framework, there evolved a stable and sufficiently effective but not very quick information network between business participants, which announced opportunities and risks.

However, there arose threats to the business system. Vital points, which controlled the business system and made it vulnerable to chain reactions, developed. From the 17th to the 18th century, the city of Amsterdam in the Netherlands developed into the central European trade centre and storeroom – a warehouse and banking place in one. For a long time, there were no real threats to this location in spite of various wars.

A decline of the Netherlands and Amsterdam took place in the second half of the 18th century, accompanied by crises in the credit business, which had Amsterdam as its centre. These crises were induced by an increase in bills without sufficient underlying value. The crises ended in the occupation of Amsterdam by foreign troops and a revolution in 1787, which was the first major predecessor of the French Revolution in 1789. These impacts were not anticipated by the important businessmen in Amsterdam. These businessmen furthered the crises by initiating and multiplying the uncontrolled use of excessively large amounts of paper.

Today globalisation and internationalisation are sometimes identified as new sources of operational risks. But in the 17th and 18th centuries there was already a business network which spanned the world. Until then its density had increased at a modest velocity. Globalisation and internationalisation are thus old but ongoing processes.

3 Operational Risks Today

On February 10, 2001, a German newspaper [FAZ101] reported an incident concerning an underwater cable which connects China with North America. This cable is used for Internet traffic and had been damaged near Shanghai, probably by a fishing net. The interruption lasted about half a day and caused a lot of trouble for businesses and private users, even after the traffic had been re-routed to a second cable. This example shows the need to look for interactions that are not obvious but nevertheless possible. It shows the need to look at the sometimes hidden vital or critical points upon which a great deal of business depends. The Y2K activities reminded us of the importance of the supply of energy, water and communication services.

On May 16, 2001 the same German newspaper [FAZ201] reported that the second largest daily loss ever recorded, measured in absolute figures, had occurred on the London Stock Exchange on May 15th. Somebody had entered the wrong input into a computer program and “suddenly” released a series of very quick selling orders for British stocks. A typical chain reaction. The impacts were obvious. The reasons why – as usual in such cases – were not published. London Stock Exchange officials announced that the security precautions of one member would have to be checked. This example is only one of many examples and shows what can happen if only a short reaction time is available. This situation, perhaps in combination with panic, allows only Pavlov-like, formal reaction schemes. It is remarkable that the subsequent sellers tried to reduce their clients’ risks, but by doing so only achieved the contrary.¹ Efficiency- or time-optimised processes tend to react very sensitively to small, unpredicted variations in their inputs and their environment.

To get an overview of the vast number of possible risks, we need some ordering scheme. The Basel Committee on Banking Supervision, for instance, proposes the risk areas listed in Table for the banking industry [BASE]. We shall use this table in our overview of operational risks as an example of how to structure risks for the purpose of understanding their causes and of facilitating risk control.

¹ The residual risk from the measures to control risk was greater than the initial risk.

Table 1: Risk areas according to the Basel Committee on Banking Supervision

Risk area	Description
External factors	External factors summarise all interactions of a banking enterprise with its clients, external business partners and environment.
Processes	All internal business, management and service processes performed by the organisation to fulfil its tasks including their internal interactions (e.g. by “material flow”).
Systems	This area addresses the technical infrastructure to perform the banking processes; especially IT and Telecommunication (TC) infrastructure facilities such as business premises, buildings and associated technology. We interpret “Systems” not only in the sense of IT but in a wider sense.
People	This area addresses all the persons performing the business of the banking organisation, from senior management to the operational level.

3.1 External Factors

Obviously, the above-mentioned example of the trawler that cut an Internet cable fits into the field of environmental interactions, which has an enormous potential for dangers that are not so easy to predict.

In general, within the area of external factors, risks might be associated with:

- material flow with banking partners (e.g. in the context of international payment transactions)
- supply and services provided by external partners (e.g. supply of business data, as in the case of Reuters; supply of parts of banking services such as credit card management; IT operations; facility supply; and energy supply)
- criminal activities, for example by external defrauders, hackers or terrorists (new opportunities are presented, for example, by new client interfaces)
- political developments
- natural disasters such as earthquakes, hurricanes and so on.

The only item in this list for which there seems to be no increase of risk is the field of natural disasters. Such risks are traditionally mitigated by the appropriate engineering of buildings and by insurance. Risks (or more exactly the knowledge of them) can possibly be increased or decreased through new scientific insights, for example, about the danger presented to locations by earthquakes. The relevance of risks from criminal activities is obvious. The stability of the political environment varies from country to country. But at the moment we believe that the probability of unpredictable developments is increasing.

In today's business world there is a tendency to outsource business parts or services as separate enterprises. This obviously increases the number of business interfaces which have to perform properly. The robustness of an external partner is not so easily judged as the robustness of an internal department. Figure 1 presents our view of the relevant interfaces in the context of financial business.

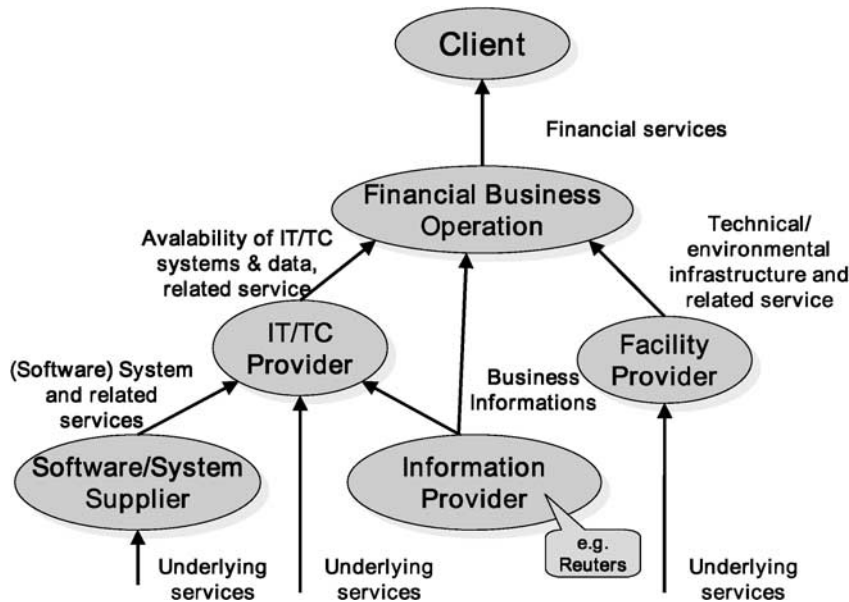


Figure 1: Differentiation of work between business process and suppliers

As an additional effect, an external partner will provide its services to several customers. The coincidence of high-volume service needs by several customers, for example, might influence each of these customers in a sometimes unpredictable way.

Often, internal service departments have informal knowledge about the usage of their service and direct contacts people in the business processes. This knowledge and these contacts help such departments to react properly and quickly in disturbances or crises.

The patent remedy in this situation is a service-level agreement (SLA). This is an appropriate form for such needs but does not prescribe the content of the service in a comprehensive manner. Rather, SLAs tend to concentrate on normal business, and there might be a considerable residual risk resulting from the specifics of this type of co-operation.

3.2 Processes

This area addresses the internal business, management and service processes performed by the bank to fulfil its tasks, including their internal interactions, e.g. by “material” and/or service flow. A characteristic feature of banking is the worldwide distribution of interacting branches. Along with this, there is an increasing coupling of banking processes between those branches, e.g. for the purpose of international payment transactions or worldwide stock trading. Activities such as these are subject to the continuous control of a central office, with sometimes very short reaction times. This coupling is intensified by the desire to shorten and streamline transaction workflow for reasons of efficiency and competitive advantage. Looking at risks, there is a higher sensitivity to disturbances of all kinds and a growing potential of chain-reaction-like failures, as in the stock-trading example at the beginning of this section.

Another interesting feature of today’s world is the accelerated concentration of business through mergers and acquisitions. If these efforts reach the level of operational business they often result in a restructuring of the operational processes. This can sometimes change the work of a lot of people in a comparably short time, thus temporarily increasing the potential of operational risks owing to a lack of synchronisation or co-ordination of work. For instance, restructuring tends to cut off informal work-arounds practised in the case of disturbances, thus impairing robustness. This effect might be intensified if change management is not actively performed. Internal restructuring efforts, most often performed with the aim of raising efficiency, can have similar impacts.

The remedy in this situation is called “standardisation of normal business”, most often by means of a large amount of documentation. Apart from the sometimes underestimated cost, which is a operational risk in itself, the standardisation paradigm ignores fluctuations in the environment and, especially, in the individual and time-dependent variations of the strengths and weaknesses of human resources.

3.3 Systems

Systems are the main technical resources of business. The risk associated with them depends upon two factors. The first is their vital nature for business or, to put it differently, their potential to cause damage to business. The second is the probability of failures, which correlates with the error-proneness of the system.

Obviously, the vital nature of IT and TK systems is high in banking. A bank’s ledger, for example, seems today to be practically impossible to maintain without the support of IT systems. Moreover, business processes in a spatially distributed environment are difficult to perform without IT systems. This difficulty is strengthened by the growing velocity and amount of interaction. Consequently, the potential damage is increasing.

In addition, the error-proneness appears to be increasing.² First – as a very rough indicator – there is the growth in system volume. This is induced, especially, by growth in functionality, in the number and velocity of interactions with partner systems and users and, last not least, in the requirements for robustness.

The functional interdependency of a bank's systems suggests that we should no longer view them as a collection of (independent) systems but as a single, large system with many subsystems and components. A special case is the integration of IT “dinosaur” systems which have behaved well for decades in stand-alone operation but display strange behaviour if integrated.

The second factor which increases error-proneness is that the engineering abilities and capacities to develop and operate such systems are still not as mature as those for their smaller, more independent predecessors. This results in a lower quality of work and products.

The third factor is the widespread use of new technologies. Products based on new technologies are naturally not as robust as those based on well-known technologies and reveal a greater error-proneness.

A further risk-relevant effect today is indicated by the common failures of local area networks and intranets caused by bottleneck situations, which have an impact on many application systems.

In areas of technical infrastructure such as air conditioning, fire protection and access control systems, there is also a tendency towards more widespread integration and automation, thus increasing not only opportunities but also operational risks.

In his description of experiences in the field of large-scale, technically supported businesses, Perrow [Perr99] analysed accidents resulting from unexpected interactions in complex systems such as nuclear and chemical plants and aircraft and shipping logistics, within their organisational and environmental contexts. These disciplines have a long tradition and experience in the normal operation and risk engineering of huge, complex technical systems and business procedures. However, “regularly” occurring accidents such as the ICE train catastrophe in Germany in 1999, the fire at Düsseldorf airport, the explosion in a chemical plant near Toulouse in September 2001, the Kursk disaster, the explosion of a firework plant in the Netherlands, the crash of Concorde near Paris in 2000, the collision between a US atomic submarine and a Japanese trawler in 2000, and other events show the inherent limitations of risk management in spite of our experience and more mature knowledge.

² Not on the level of single components but on the level of complete systems.

3.4 People

The field of operational risks caused by people can be further divided into the area of general human error and the area of conscious violation of rules. Important examples of the violation of rules are fraud, theft and sabotage. In addition, internal enterprise rules have to be obeyed. A well-known example is the case of Nick Leeson. Owing to the variety of possible situations, rules of all kinds must to some extent include discretionary powers that allow appropriate actions for a specific situation. But we are not perfect; we cannot guarantee that the use of these power will always be appropriate. But how do we regard such risks in daily business?

In the London Stock Exchange example given at the beginning of this section, it is plausible to assume that time pressure played an important role. Time pressure might be a normal problem faced by professionals in stock trading, but that doesn't change the fact that traders share the usual human limitations and that there is an individual variation in capabilities too. Time pressure seems to be spreading and intensifying mainly as a result of the use of IT systems to accelerate business. This, for example, affects the operators of interconnected IT systems with very short overall transaction times, high throughput and enormous vitality for perhaps worldwide distributed business processes. Systematic examinations, as cited by Masing [Masi88], confirm the common-sense knowledge of a super-linear increase in the probability of human error with the time available.

Short reaction times are not such a problem when events of this type can be predicted through experience and prepared for in sufficient detail, and when the participants master the routines to tackle them (this especially applies to the field of business continuity plans). But in the case of new businesses and technology, a certain number of events will arise which we cannot yet predict, and we must not forget the rare events with high damage potential waiting to occur with the currently used technology. In such cases a risk component lies in the element of surprise followed by panic or an otherwise wrong reaction, as in the classic *Titanic* accident.³

The growing interdependency within business, its spatial distribution and the growing technical dependencies make it more and more difficult for us to see the complicated and partially "hidden" cause-effect chains in sufficient detail, especially when only a short time is available. The ability to react properly depends mainly on the skills and qualifications of the people involved.

The voluminous and complex interactions in normal business are usually managed by use of more and more detailed standards, which govern the activities of the business process participants. Possible negative effects of standardisation are boredom, "over-

³ When the iceberg was seen, the commanding officer tried to get the ship out of its way. Most probably, he unintentionally caused the sinking of the *Titanic* in this way.

routine” and an awareness oriented towards only the standardised rules. This weakens the robustness on the individual level and increases the sensitivity of business to disturbances.

3.5 Coincidental Risks

Even the best scheme for the classification of risks cannot prevent events from occurring that cross the borders of predefined risk areas such as those defined in Table 1. The possibility of such coincidences must be considered.

To show this, we shall take an example from the airport area. Someone placed an oversized piece of luggage on the baggage transport system of an airport. Such systems are very large, interconnecting almost all operational areas of an airport. On its way through the system, the piece ripped away one “head” of a sprinkler system. The sprinkler system did what it should do under these circumstances: it sprinkled. Some distance below, a LAN router was installed; it was not vital for the core business of the airport but was important for the airport’s internal processes in a large area. The water destroyed the router, which in turn greatly disturbed the internal processes. This problem lasted more than a day before complete recovery. Clearly a coincidence, but what were the causes? The baggage transport system was designed to transport oversized luggage. But this special oversize item seems to have been new on this path. Because of the baggage system’s size and complexity, no luggage operator can ever know all possible paths. The engineer planning the router did not take account of the fact that there was a sprinkler a few dozen metres above the position of the router and the possibility of interaction with water. Besides the coincidental aspect, this event highlights the problem of maintaining an overview of huge, complex, expanding systems.

Examples such as this show the growing potential of coincidence. Driven by potential business opportunities, with new clients and products, the operational business processes and their underlying infrastructure are sometimes changed on the basis of a technology which is not yet mature and, especially, not robust enough. The speed-up of business transactions and business changes challenges the abilities of the stakeholders, as does the increasing linking of technical and business process components, resulting in an increase of operational risks that cannot be ignored. Obviously, this development is amplified by threats external to the operational business.

4 Robustness

Robustness is the ability of business processes, organisations or technical systems to continue business and to protect their substance effectively from damage in the case of

disturbances, incidents and accidents. Roughly speaking, robustness is the ability to survive in the case of trouble. Therefore robustness is the goal of risk management.

The historical examples given in Section 2 indicate that the following strategies and general “tools” were used to maintain and improve robustness:

- early warning and awareness
- skill and practice in coping with risks
- flexibility and fault tolerance
- diversification in all levels of business
- fallback resources and procedures (e.g. “business continuity plans” and resources)
- abstract resources such as buffers of time (e.g. the buffers provided simply by the slowness of processes) and buffers of credit or budget
- process improvements (e.g. double-entry accounting)
- technological improvements (e.g. in shipping).

Today we use the same strategies and tools to control risks, but they have a more up-to-date look.

The historical examples indicate loose coupling to be an important feature of robust systems. The development of vital points, however, increased the vulnerability of the business system.

The look at operational risks today in Section 3 reveals coincidences as indicators of a new quality of operational risks. The possibility of coincidences is due to the complexity of the business system and, especially, the complex technical infrastructure. Complexity enables an enormous amount of dangerous interaction, which did not have time to occur before now. Thus, complexity is the opposite of loose coupling, which for a long time helped the business system to be robust.

The effects of complexity are intensified by the increasing lack of transparency of the business system. There may be not only obvious vital points but also, perhaps, hidden vital points, which will be revealed only by the occurrence of a disaster.

The historical examples indicate that there was some slowness in business processes, which gave time to control undesired developments. The speeding up of processes today cuts down the most important resource of risk management: time.

5 What Can Be Done?

The general answer is easy to give and well known from risk management. To achieve robustness you must prevent risks from influencing your business and/or limit the damage to a tolerable residual risk level if the former is not possible. This is most often done by the introduction of redundancies in the form of fallback procedures and re-

sources into business. But the problem is that these redundancies have to fit your risks, the environment you are working in and your operational possibilities.

The most important prerequisite for controlling risks is knowing them. You must have a sound map of your risks, which includes all of the “devils in the detail” arising from the specifics of the business operation and environment.

The task has to be shared by business processes and IT suppliers, whose different roles are discussed in the following sections.

5.1 From the Viewpoint of the Business Process

What does robustness mean in the case of a business process?

1. The process must protect people from injuries in all cases. This goal is required not only by business but also by ethics and, most often, by law.
2. The process must protect its substantial resources from damage; in particular it allow for the recovery of business activities. The main resources are people, essential business data and documents, the process infrastructure, and, last but not least, the company's reputation.
3. The process must deliver its intended output, e.g. banking services or products, even in the presence of disturbances such as the breakdown of IT systems.

The fulfilment of these goals guarantees business continuity. The first and the second goal focus mainly on risks to the substance of the business process, the third focuses mainly on risks to its operational results.

In order to reach these goals, you must be able to manage a crisis and to reduce the extent and frequency of crises through the specific preparation of business continuity measures and a sound knowledge of the underlying risks.

5.1.1 Crisis Management Capability

The capability to manage crises is the basic part of business continuity and a prerequisite for all its components. Roughly speaking, it is the ability to act whatever happens. If there is an event which has not been specially prepared for, the company is able to act appropriately as an organisation. Put in greater detail, it is able to inform all people involved in the crisis, especially those who are not aware of it but could suffer from it or have a role in coping with it. Someone can get an overview of the situation and can direct the resources and act in an effective, efficient manner, directed by the goals mentioned above. The company can do all of this as fast as necessary or, more correctly, as fast as possible, because at the beginning of the crisis you will not (completely) know

what has happened, what can happen and what is necessary. This speed can only be achieved through the thorough preparation of an information and decision network which spans the business process, its business partners in the workflow and its IT and facility providers.

Since crises are rare, the routine of daily business does not suffice as preparation. To achieve and maintain a bit of routine, simulations and training should be performed with all people who could possibly be involved. A classical example is an evacuation exercise. The WTC accident showed that this was not a superfluous game. But some abilities cannot be trained. There are people who have a natural ability to perform this kind of job; this ability is especially valuable if it is combined with profound knowledge and experience of processes and infrastructure. These people are chosen to become real crisis managers.

An important precondition for crisis management is an appropriate infrastructure, especially the means to communicate with those involved wherever they might be, even if the standard means of communication no longer works.

In addition to a general capability to perform troubleshooting, crisis management provides the organisational, informational and decision framework for the more specialised components of business continuity.

5.1.2 Business Continuity Capability

You can achieve business continuity capability if you prepare for specific risky events by planning in advance. The benefits of this preparation, namely the reduction of risks, should balance the costs.

A simple, fictitious example: if a bank (or a bank department) is exposed to the risk that the payment transaction system might break down for a considerable amount of time, the bank can prepare, train and practise manual procedures to handle these situations in such a way that business continues and the business impacts of the risk are minimised.

If the payment transaction system recovers, the preparation allows the bank to update the payment transaction database and to return to normal business. Sometimes, however, the system recovery takes too long. In this case the bank is prepared to shut the business down completely and to inform and pacify its clients. If the bank were not to inform them, their anger would in most cases be even greater. If, finally, the system recovery is completed, the bank is prepared to recover its business from the state it was in at the time of business shutdown.

In addition, the bank is prepared to continue business, if need be, with reduced capacity. In a similar way it is able to handle all the risks relevant to the goals presented above. As a main issue here, the bank is prepared to protect people and business assets such as its data and documents, business infrastructure and reputation from damage.

To be prepared implies the availability of sufficient fallback manpower (in the simplest case, hours of overtime) and the appropriate technical and organisational fallback infrastructure has to be guaranteed. This can range from the provision of paper forms not used in normal operation, up to disaster recovery sites where business continues if the business premises are no longer available. The business continuity plans should fit the abilities of all participants.

As with crisis management, the aspect of training is very important, especially if the underlying risks imply a large damage potential but are rare. Similarly, periodic checks ensure the existence and availability of the fallback infrastructure.

The most important prerequisite for preparation through business continuity plans is a sufficient amount of time, followed by the availability of appropriate resources. But the preparation can only be performed if there is concrete, sound, current knowledge of the risks to which your business is exposed.

5.1.3 Risk Awareness Capability

You can only handle your operational risks if you know them. A map of the current risks which provides all of the information needed to judge risks and to decide on the appropriate action, has to be worked out. To keep the map up to date, some kind of early warning and supervisory system should be operated to observe all areas in which short- and long-term problems might arise.

The knowledge about risks (the map) should be organised to support the localisation of the causes of risk and thus give hints about the starting points of well-directed risk control. Because there might be many risks to consider in detail, the map should be structured by risk areas as shown in Section 3. An important means of calibrating this map is to evaluate the experiences of problems (occurrences of risks) in the company.

In order to obtain an overview of the risks and for the purpose of prioritisation, the “greatness” of each risk should be determined by evaluating the probability of harmful business impact and the size of this impact. In many cases, however, you might not evaluate these factors explicitly. In such case risk indicators or qualitative evaluations which correlate to some extent, on their own or in combination, with the “greatness” of the risk may help.

On the basis of the risk map, the company decides on the necessity of actions to improve its business continuity capability, and the company uses the map to judge the success of actions already taken. In particular the risk map supports the balancing of the costs of business continuity measures against the amount of risk reduction achieved by them. The activities towards business continuity start with the most urgent and important risks in the map.

Which sources of information should be used in the early warning system? Some heuristics:

- The company investigates possible fields of risk in a systematic way, whenever it is not sufficiently sure of them. It looks especially at signs of unexpected interactions with “long-distance effects”.
- It analyses changes, especially the entry of innovations into the risk areas, not when they are carried out but when they are planned.
- It investigates problems in daily business, especially peculiar events and disturbances without any obvious explanation. By looking at variations of their cause–effect chains, you might discover variants associated with very big risks.
- Technical monitoring devices are used to collect indications of risks.
- Not only the documented or explicit knowledge of all people involved in the process but also their “feeling” about risks are taken into account.
- External sources of risk are taken into account.

To finish the description of risk awareness capability, a very important feature must be mentioned. There has to be an awareness of the limits of knowledge about risk. This knowledge will never be as sound as the knowledge about things which did happen.

A specific limit is caused by the restricted risk scope of a company. From the viewpoint of a single bank, for example, it is difficult to map the risks for the entire area of worldwide banking business or for business in general. This task is attempted by legislative authorities supported by organisations such as the above-mentioned Basel Committee on Banking Supervision (see [BIS] and [BASE]), which prepares worldwide risk assessments and general measures to control risks for the worldwide banking systems. Owing to a broader statistical basis, those institutions are able to detect risks that a single bank would never perceive. Considerations of risks beyond the scope of a single bank have resulted in laws such as the German KontraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich) and MaH (Mindestanforderungen an das Betreiben von Handelsgeschäften).

In the area of operational risks we are still far away from over-engineering. But too much preparation also seems not to be good, and not only because of cost reasons. There should be a tolerated level of risk background noise. This offers the best opportunity for real-life practice in handling risks. That’s why the fire brigade is not unhappy to carry out some limited operations regularly.

5.2 From the Viewpoint of the Software System Supplier

As indicated in Section 3.3, the supplier of software and IT systems provides a basis for business opportunities, but at the same time operational business risks.

The region of risks with respect to an IT system can be broken down according to the localisation of possible faults. Risks can be caused by

- faulty interaction within the system (e.g. risks induced by faulty components)
- faulty interaction between the system and its partner systems through interfaces (e.g. risks induced by the increase of interactions in worldwide networks)
- faulty interaction between persons and the system (e.g. qualitative and quantitative changes in the context of new types of end-users in e-business)
- faulty system behaviour as a result of disturbances in its environment or in its underlying services (which may be widely distributed systems with reduced control of the environment, e.g. heterogeneous Internet clients of end-users).

The furthest evolved techniques to handle risks by means of the development process concentrate on the first item in this list. With the other three items, there is an increase in risk. The development of appropriate means is ongoing but not yet completed.

In addition, this increase is mixed up with a growing pressure of time on software development. You have to develop faster than usual and, in parallel, you have to discover a significant amount of operational and technical virgin soil. As a not too rare result, there are fewer opportunities carried out than expected and some very poor compromises for example in the case of Internet/Intranet portals.

As a background for the following discussion, Figure 2 depicts the main structure of the software development process and its main interaction paths with a business process.

The development process consists of a construction part and a quality assurance part. The development is triggered by a request from a business process for improved

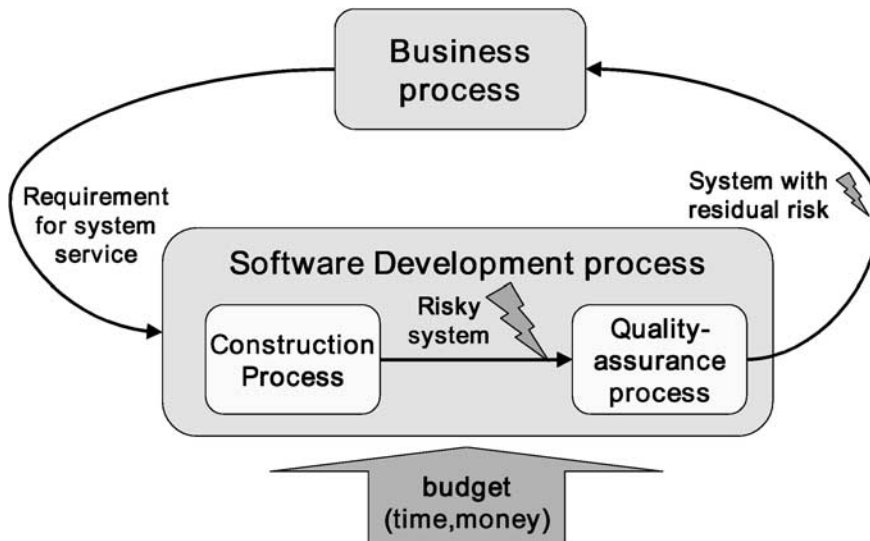


Figure 2: Structure of development process

support. This is often the first source of risk, owing to potential failings in the transfer of understanding and knowledge of requirements, technical/economical feasibility and associated imponderables between the client and the development process. This is especially relevant if there only is an abstract vision of a business opportunity that has not yet been broken down to the operational, procedural level and the specific tasks the system is to fulfil. If a breakdown exists, it is expected to be unstable, because it has not yet been proved and improved by practice. This, combined with the (naturally) lower maturity of new technologies and techniques, is often unsuccessfully handled as a “normal” project. The amounts of practical research and learning necessary on the business process and supplier sides are not considered.

The construction part of the development process produces the software system, which – in addition to the initial faults caused by mutual misunderstanding – is extremely likely to contain faults added during the construction process. The main factor influencing the quality and quantity of risks is the abilities of the developers and their managers, as individuals and as teams. But even in the best case there always will be some considerable residual risks.

The extreme likeliness of faults in construction is the basis of quality assurance’s livelihood. Quality assurance acts as a sensor for faults, which, in combination with a defined threshold, helps to control a software delivery valve that allows systems to pass to the business process. Naturally, even when the valve opens there is sometimes a considerable amount of residual risk. There are, in principle, the following reasons for risk:

- the human counterparts of sensors and valves and their constraints (“Nobody is perfect”)
- statistical errors induced by checking the behaviour of the system only in comparatively small samples
- the level of risk the business process is prepared for and willing to accept.

If necessary, these residual risks must be explicitly controlled by business continuity measures within the business process. This is often omitted, and that is one reason why the period after roll-out is sometimes accompanied by a feeling of subliminal horror.

5.2.1 Robustness of Systems

A special challenge of software development is to improve the robustness of software systems. Traditionally this is interpreted as some appropriate behaviour in the case of false operation by a typical experienced user. For example, the system should not break down if the user enters a syntactically wrong input.

Today, this topic is enriched by new groups of users who only occasionally work with the system, have no training, are less patient and have – from the developers’ viewpoint – fantastic ideas for bringing the system down or corrupting its data.

A further aspect is that the interfaces with partner systems, for example in a world-wide network, tend to be less well known and reliable than they used to be in the smaller LAN context. This often comes along with the increasing rate of change of interconnected systems. There appears to be a development comparable to the above-mentioned new groups of users, as indicated by everyday test engineering experience.

Furthermore, increasing variation in software and hardware platforms and associated services, which is emerging especially in e-business, may give rise to more risks. To conclude this summary, we should mention the widely discussed topic of system misuse (e.g. viruses and hacking).

Therefore, an expanded catalogue of robustness maxims for software development should include:

- Protect the system, especially its data, from wrong inputs.
- Protect the system from misuse.
- Let the system run as long as possible to perform its task (if necessary only partially), even if some interfaces have temporarily broken down or behave strangely and/or some parts of the platform behave (temporarily) strangely or don't work. This is especially important in the case of requirements for high availability.
- Let the system monitor for and detect peculiar behaviour that could involve intolerable risk potential, and if necessary let the system cry for help or even shut down (early warning).
- Minimise the irritation of users and operators in cases of disturbance (in such cases there is reason enough for irritation).
- Construct the robustness features such that their reliability is appropriate to the situations in which they are used.
- Be sure that the robustness features are not a reason for additional failures. Their reliability must be even better than that of the system in a state of normal operation.

Now, which opportunities does the software supplier have in order to improve the robustness of a system?

5.2.2 Software Construction

The common background of software development is characterised by increasing limitations on time, budget and/or resources. This requires aids for a more exact prioritisation of the various tasks. These aids should focus on the expected error-proneness of the system that is being developed which controls the probability of failures, and on the vitality or damage potential of the parts and features of the system when it is used in business processes. In other words, this prioritisation should depend upon the risks which might arise from system or software failures in the business process.

As an illustration: a small, simple module within a process control system had the task of enabling the communication between all of the programs of the system. The task of programming the module was given to an inexperienced newcomer. So the error-proneness of the module was high in spite of the simplicity of the task. Naturally the module contained some faults; still, the newcomer had performed his work comparatively well. The failures did not occur during normal operation but only in a few rare but practically relevant stress situations with considerable damage potential (high vitality). The faults were discovered by chance before the system went into operation. Whether the usual standard test procedure on the system level would have discovered the faults was not certain.

In this example, the risk was not seen by the team leader, owing to the module's simplicity.⁴ He did not consider in detail the relevance of the module within the system and for production; the module should at least have been intensively checked or, even better, programmed by a more experienced programmer. Why didn't the team leader consider this?

The example highlights a lack of understanding of the system's use in the business process as one source of risk. The example also suggests that faults "like" to concentrate on interfaces. So there is a considerable error-proneness in the coupling of programs in particular. This includes all types of shared use of static data (databases and files), on-line interfaces between programs and systems, the synchronisation of programs and the effects of temporarily unavailable platform/network resources. This is very similar to phenomena in and between organisations.

A detailed risk map can serve as an aid to enhancing the mutual comprehension of system use in the business process and the practical awareness of associated risks. The risk mapping should be integrated into the process of specification of requirements and functionality to supplement the usual attitude of looking for and believing in opportunities. This image of the risks which the business process might incur in the case of system misbehaviour can help to focus the construction processes according to the relevance and error-proneness of the system and to protect it better from its own weaknesses.

5.2.3 Quality Assurance

Quality assurance processes have to improve the accuracy of quality assurance efforts. Thus, they have to incorporate more explicitly and in more detail the risks to business processes from system misbehaviour. To do this, the understanding of the business process and its context must also be improved.

⁴ This module is another example of a vital point.

A software system's "right to exist" depends upon its support of business processes. So quality goals depend mainly on the amount of software induced risk the business process is able to tolerate or to handle. The testing and quality assurance measures must be directed towards reducing risk to this tolerable level. As mentioned above, one factor of this risk is the damage potential within the business process, the other factor is the error-proneness of the software delivered by software construction. This second factor controls the probability of system failures. It depends, on the one hand, on the amount of software delivered and, on the other hand, on the quality of the construction work. So the strengths and weaknesses of the construction process, of its suppliers and of its environment influence the risk to a large extent.

So – as a means of synchronising the joint efforts of construction and quality assurance to deliver a system with tolerable risks – there is a need for the above-mentioned map of risks to be shared with the construction process. Experiences from test consulting confirm the importance of this need.

One result of quality assurance should be a specification of the residual risks for business after roll-out, in addition to the usual quality declaration. This specification should address, in particular, the system's "teething troubles" following roll-out, and risks with low probability or frequency but high damage potential. Information such as this would allow business processes to improve the accuracy and cost-effectiveness of their business continuity measures.

There is one considerable limitation to testing which arises from the tighter coupling of systems within the production network: the increasing difficulty in simulating the totality of widespread, interconnected operational systems in testing laboratories. However, it seems to be possible to improve the strategies for the selection of test targets according to the associated risks. The rate of change of systems does not allow a complete integration test whenever one of the partner systems is updated.

In the previous sections we discussed the benefits of risk control, especially through quality assurance as a reduction of business process operational risks. Today it is more or less a standard task, supported by an appropriate controlling infrastructure, to calculate the costs with sufficient precision and timeliness. Reductions in risks and residual risks will, most often, be estimated not explicitly, but by rules of thumb or by guessing. If done by experts, this is not the worst way to act, but this does not work as reliably and efficiently as is necessary.

5.2.4 Operational Risks of IT Projects

From our experience – with no claim to completeness – the following are currently the main elements in the operational risk of IT projects:

- Difficult time constraints, sometimes caused by a predefined market entrance, might result in best-case planning that leads to significant delays.

- Quality deficits in deliveries, resulting in unexpected, significant problems in the business process. Time constraints are not the only possible source, others are indicated below.
- “Virgin soil” in business practices and the manner of using systems for business (e.g. e-business), resulting in necessary but not sufficiently predictable trial-and-error work on the side of the business process and within development.
- “Virgin soil” in system and development platforms and tools, at least from the viewpoint of the available development resources. Sometimes, even technological innovations without any engineering expertise.
- An increasing number of co-operation partners external to the project, accompanied by spatially distributed work. This is often a direct result of the above-mentioned increasing number of technical interfaces in the systems and, in addition, the tendency towards outsourcing. Owing to the project’s sensitivity to disturbances at its interfaces, the project risks increase. Self-organisational practices may no longer work, and existing project standards sometimes do not fit the new situation.
- Intercultural, sometimes worldwide co-operation within project teams.
- Even if there is a sufficient budget, too few or insufficiently qualified people.

Clearly the basic ideas for managing the operational risks of IT projects are the same as for business processes. However, IT projects are most often structured according a particular process model containing several phases, e.g. requirements analysis, architecture and design, implementation, test, and roll-out, including initial operation. Each phase is more or less subject to its special kinds of risks, which must be considered thoroughly. The phases finish with milestones, which contain a fundamental decision on schedule, budget and resources that is concentrated on the subsequent phase (forecast). The most important of these decisions is obviously the decision on the initial plan. Therefore the decisions incorporate a significant damage potential, which should be examined through risk assessments as a part of the project’s early warning system. Furthermore, the project management should be integrated with a component of continuous risk and problem management to protect it from problems and risks which are relevant during the project’s duration.

Explicit project continuity plans – as the project counterpart of business continuity plans – and appropriate crisis management might be necessary for phases and activities with high, time-stressed interactions with a large number of project partners, especially during integration testing, roll-out and initial operation. The project continuity plan dedicated to roll-out has to match the business continuity plans for system operation and the business process on the side of the business holder. Emergency services provided by the software supplier should be a part of the system support for the business process after the project has finished, for example as part of a service-level agreement between the software supplier and the business process. This becomes especially important if the quality goals of the project are to be relaxed owing to time con-

straints or, equivalently, the residual risks to the business processes from software and system failures are to be systematically increased.

A similar kind of coupling between a project and a business process (in latter being partially simulated) takes place during testing activities, especially integration testing. These activities might require a specialised continuity plan, which can be a predecessor of the plan used during operation after roll-out. The integration test phase also presents an opportunity to check and improve this plan in advance of operation.

To protect its own business, the software supplier should perform one risk management shared by all projects. The people involved in each project should thoroughly analyse all the problems and risks encountered during its duration and recommend measures to protect future projects from problems and risks. This input should be systematically evaluated by the management to obtain a complete, consistent risk map, which includes all projects, and to define the appropriate risk control measures, considering synergy effects between projects.

5.2.5 A “Cultural” Factor in the Background

We see a general “cultural” factor which tends to de-integrate the necessary team play between the business process and IT development as the root of many problems and risks.

This can be sketched in extreme fashion as follows. Often developers do not know and understand the odds and ends of the business process in sufficient detail to construct an appropriate system or to test it. “I only have to build the system. What the user will do with it is none of my business!” In addition, they tend to assume that everybody knows the abilities and limitations of the technologies used, even if they are new. Fascinated by new technologies, the developers tend to overestimate their technical opportunities.

In contrast, the representatives of the business process tend to take for granted that everybody, including developers, knows and understands all of the odds and ends of the business. In addition, they do not believe that there might be odds and ends in the technical field too, though these are especially possible in view of the new fascinating technologies. On this basis, both sides come to an operational consensus, whose gaps do not become obvious in detail.

The initial trigger for an operational risk is often a simple misunderstanding, sometimes enhanced by an overestimation of technological opportunities and/or time pressure.

The engineers of development processes concentrate on formally nice, consistent frameworks. But such frameworks do not take sufficiently into account the fact that the developers and business representatives involved did not learn effective communication with the goal of mutual understanding. This – the problem of different languages

and social interaction – is not unique to software development and its clients. However, other engineering disciplines have already gained more experience in neutralising its effects. One concept used here is called “Simultaneous Engineering” (see [KaBr95] for a short description). The basic strategies are to involve all the stakeholders of a development project from its beginning and to enable interdisciplinary teamwork.

5.3 Which Risks Remain?

The previous sections have indicated that a lot can be done to control risks. But which risks remain after one has taken these measures to control risks? Clearly, there are the residual risks in the risk map, which the company does not want to mitigate. The company is sure that it can tolerate their impacts if they occur.

Many of these residual risks and the initially identified risks are well known, in the sense that they have occurred in the way identified or a comparable way, such that they could be studied in reality, modelled and prepared for. We learn to prevent a disaster from the experience of the disaster.

We observe that, in addition to those well-known risks, risks with very low probability but very high damage potential remain, for instance in the context of business and technological innovations and/or in a dependency upon environmental influences. We can think of the London Stock Exchange example (see Section 3) as a comparably small event and September 11th 2001 as a big one. How should they be tackled?

The general goal should be to offer protection from these risks, at least to the extent that some limits of damage are impossible to cross. A traditional example here is the famous four-eye principle, used not only in banking but also elsewhere as a business equivalent of an emergency brake. Sometimes the emergency brake might even imply the abandonment of possible technologies, if they are not robust enough for business or their impacts on business processes are not definitely controllable or sufficiently known.

To some extent it is helpful to systematise risk assessment techniques for the examination of limited areas with a high potential for risks. This will work if there are practicable models. An example of specialised risk assessments is the Y2K activities, which not only controlled the risk addressed but, in addition, increased the knowledge of interdependencies and revealed many possibly risky interactions in the neighbourhood of Y2K problems.

When the risks are not exactly known but they announce themselves in a timely way through perceivable harbingers, it is possible to adjust the early warning systems to look for them. The operator of a worldwide early warning system could be a supranational banking institution such as the Basel Committee (see above). In co-operation with the individual banks, such an institution could perceive signs of risks (e.g. by statistical means) that an individual bank or an individual state would rarely see. In addi-

tion, the institution would also have an opportunity to examine the net interactions between the individual banks. Such institutions, in co-operation with states, would be able to establish limits for tolerable residual risks.

One approach of risk management is to consider some worst-case scenario in order to study the causes and impacts linked to it and to define useful measures for control. It would be very useful to know such a worst-case scenario for the operational risks of a bank or of the banking system as a whole. Is it similar to the WTC attack? Might it be even worse, owing to a small software error which spreads undiscovered in a very short time across a worldwide banking network and causes uncontrollable damage? If the WTC was not the single “heart” in the “middle” of the banking system, is there such a “heart” which could be hit? All of this is unknown to us. What seems to be clear is that a Super MCA (Maximum Credible Accident) must have greater dimensions than the WTC attack.

In spite of all the possible technical, scientific, organisational and method-related tools, the most important device for discovering “new” risks is our brain, which can be triggered first by our gut feeling (as with opportunities) on the basis of experiences which have not yet been systematised and scientifically formalised. We should train our most valuable tools on the target.⁵

Concluding this section we say in summary that there is no guaranteed way to have no risks but that there is a usable possible way to have fewer risks.

6 Balancing

As indicated in the previous sections, there is a need to balance the benefits against the costs for each risk control measure. Benefit is gained through risk reduction; cost is incurred through the corresponding activities. This balancing might imply that some well-known risks will not be mitigated.

But there are some more general balancing tasks: the integrated consideration and balancing of robustness against other components the goals of business processes and, especially, integrated consideration and balancing against business opportunities.

⁵ At this point, however, we do not favour uncontrolled Murphy-like thinking or superstition. Such an approach misleads and produces so many risk scenarios that nobody ever will be able to judge them.

6.1 Balancing of Goals

Clearly, risk management, including business continuity planning for the purpose of robustness, is not the only goal of a business process.⁶ This is evident in the concept of “business continuity” itself, which implicitly refers to normal business.

Figure 3 depicts an abstract scheme for the various components of the goals which have to be considered and balanced in an overall examination. The priorities given to those factors seem to be reasonable in many cases and situations.

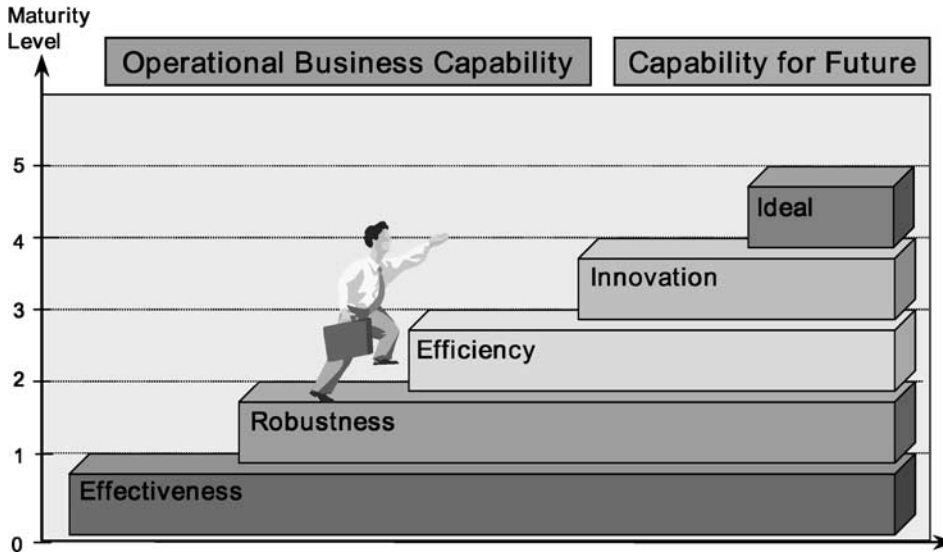


Figure 3: Factors in benefit-cost balancing

The first component of the goals of a business process is that the process should perform under normal circumstances in an effective and sufficiently efficient way. The second goal is to achieve robustness. The third is to be effective and robust in the most efficient manner, and the last two components refer to the process’s ability to take advantage of opportunities arising from innovation. The totality of the components reflects the business process’s interest in its short- and long-term life.

Normal business, and restricted business in the case of incidents and accidents generate the cash flows to finance normal, robust, efficient business and its future, as well as to make a profit. The relative importance of the business goals varies depending on the particular situation of an enterprise and with time. In recent years there has some-

⁶ The following remarks refer, accordingly, to support and supply processes.

times been a general emphasis on innovation alone. Today the focus seems to be shifting towards robustness, in reaction to the developments in the field of the operational risks mentioned above.

However, neither of those factors should be considered in isolation. They are always both present in business and influence each other, at the very least because there is only one budget to sponsor them.

6.2 Balancing of Opportunity Against Risk

As a typical example of balancing opportunity against risk, let us consider an IT system which is to be developed to automate a manual banking operation, i.e. to increase the efficiency of work. In the business process, each individual case in which the system is used will offer some benefit in terms of cost reduction. The amount of cost reduction varies depending on the specifics of the situation, but clearly there is some upper boundary to the amount. Owing to the nature of the banking process, the IT system must modify the contents of some very important databases (e.g. accounts, assets or clients), which are substantial in the context of the bank as a whole.

Of course, nobody is perfect, including the managers, architects, developers, quality assurers and component suppliers of the IT system. Therefore software errors which cause malfunctions, thus inducing financial losses in business processes, must be taken into account. These losses might be small if only a small amount of work has to be repeated, as might happen if the software is used wrongly, but they might be enormous if the above-mentioned databases are corrupted. From the bank's viewpoint, the permanent corruption of the databases might be equivalent to bankruptcy and an infinite loss.

To obtain an overview of the individual benefits and losses, we may represent them together in one figure. The combined distribution of benefits and losses for the various possible cases in which the IT system is used might possibly look like that in Figure 4.

The asymmetry of the distribution is obvious. Its most remarkable features are a concentration of probability on the benefit or opportunity side, in combination with practically infinitely large values with very low probability on the loss or risk side. We presume that distributions of comparable shape⁷ and behaviour represent many situations, perhaps even the overall operational opportunity and risk of a bank.

In decision situations, e.g. a decision on the use of the above IT system, we are used to considering mainly the expectation value of such a distribution. This we assume to be located near the peak on the benefit side and to be clearly positive, so the decision seems to be clear and easy. An almost imperceptible increase on the loss side, however, might cause the expectation value to become negative. So we tend to ignore the varia-

⁷ However, we think that it is possible to have more than one peak.

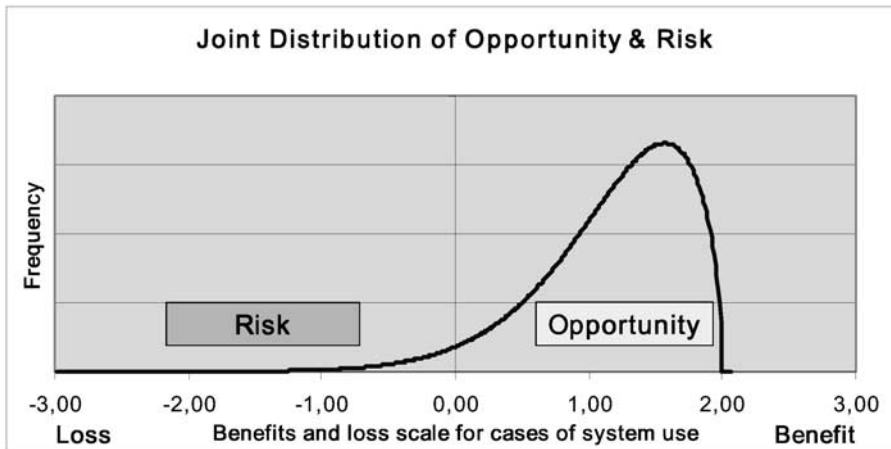


Figure 4: Distribution of opportunity and risk

tion of the distribution. Mostly we do not even try to calculate such figures or to gather the underlying qualitative and quantitative information.

The opportunity side of the distribution is comparably easy to fit because there is much empirical background data. This side reflects successful, normal daily business. On the side of very large losses or great damage, it is practically impossible to predict or calculate the probabilities with sufficient accuracy if there is a lack of empirical data and practicable modelling techniques (see also Section 5.3). Examples are cases of new technologies or business architectures. There is therefore a diffuse grey area of ignorance, which might be interpreted as a high risk in itself. As one example of the relevance of this potential, remember the accident at the Three Mile Island nuclear power plant in Pennsylvania, which occurred after years of nuclear power plant operation in the US; and we should not forget the 11th of September 2001.

How do we behave in such situations? We tend to “think positive” and to ignore our ignorance. So we end up again with the relevance of the “human factor”.

7 Concluding Remarks

Systematic risk management and business continuity planning help to achieve robustness to a large extent. But the risk potential of rare events remains, revealing itself from time to time in unexpected and enormous catastrophes. This risk potential is continuously being replenished by new technologies and new engineering of business processes; in summary, mainly in the context of technological and/or organisational innovations.

One possible way to tackle these risks would be to structure the business in such a way that its worst-case scenario would imply only a restricted impact. To give a rather simple idea of what we mean: the attack on the WTC and its aftermath were possible only because the WTC contained a combination of many innocent people, a high level of business traffic; and a great amount of infrastructure and investments, and, we should not forget, it had an enormous symbolic value, and all at a single location.

To finish, let's return to history. One prototype of protection from danger is represented by the clumsy medieval knight with his heavy armour, which didn't allow him to get out of the way. The other prototype is the mobile bowman with only his weapons, whose mobility was his most efficient protection and who conquered the knight. The main prerequisite for his efficacy was his room to manoeuvre.

Either way has its drawbacks, but in the interest of long-term survival and efficiency we think that we need more room to perceive existing risks, to control them and perhaps to discover the opportunity in them.

Business Continuity

IT Risk Management for International Corporations

Wieczorek, M.; Naujoks, U.; Bartlett, B. (Eds.)

2002, XVI, 216 p. 56 illus., Softcover

ISBN: 978-3-540-43051-3