Section One

Achieving and maintaining business continuity: an executive overview

COPYRIGHTED MATERIAL

1

What are we planning for?

Geert Vancoppenolle – Belgium

Geert was formerly head of the Business Continuity Management practice of Accenture in Europe.

Introduction

Imagine that you have been asked to rebuild the business of the company that you work for in the immediate aftermath of a major disaster. Perhaps there has been a serious fire and you cannot make use of the existing IT infrastructure or of any other infrastructure elements within your current premises.

It is your responsibility to ensure that it should be possible to take orders within two hours. Customer deliveries must be possible within five days, except for your two most important customers for which it must be possible to deliver within the same day.

An immediate suggestion is that you will have to source your company's products from alternative plants within your company. These plants are not aware of the situation: moreover they may not have the capacity to modify production to cope with the scenario.

The customers, who are waiting for delivery, will flood you with questions regarding the affirmation of quality, accuracy and punctuality. Those who want to place orders will request guarantees of delivery. In the meantime, a number of suppliers will be waiting to deliver their goods, at the exact location that is unavailable to you.

Are you ready for it?

The example above might be what you are expected to do when your company is involved in a disaster. The event that caused the disaster could be anything: fire,

The Definitive Handbook of Business Continuity Management, Second Edition.
Edited by Andrew Hiles FBCI. © 2007 John Wiley & Sons Ltd.

power failure, unavailability of the IT infrastructure, evacuation of the installation and so on.

How long did it take to build your current business organization, providing customer service as it is doing today? The fact is that you have to plan to avoid or mitigate disasters before the event. Under extreme time pressures and the scrutiny of shareholders you must deal with all this in a crisis situation. I bet you wish you had prepared for this scenario!

This chapter poses the problem: What are we planning for through business continuity management? It not only defines ‘disaster’, but also explains outcomes and implications to our business organizations. The chapter is composed of four parts. The first part discusses the inherent dependencies and vulnerabilities of our business organizations. The second part discusses how unexpected events can lead to disaster and interrupt our business operations. The third part takes a look at what these disasters can do to our business: the damage, the impact and the business risks from operational interruptions. The last part asks the question about the objective of business continuity management: what should you expect to achieve through your business continuity plan?

Vulnerability of today’s business organizations

Business organizations: who should plan for business continuity?

By ‘business organizations’, we do not only mean commercial organizations that manufacture and sell products or that provide, for instance, financial services. A business organization in this context is any organization that provides services or goods, either to individual customers, to other business organizations, or to the public.

Examples of such business organizations include manufacturers, distribution companies, sales organizations, transport organizations such as railroads or airlines, utility companies such as electricity production and distribution, water, gas and telecommunications, and community services such as tax services, justice, emergency services, government and so on. Although not all these organizations are established to make profit, they all provide some service to somebody else, and have all built an operational structure to enable them to do so. In the context of this chapter, they are all called business organizations.

As all these organizations are equally at risk from the effects of a disaster that interrupts their operations, they should consider business continuity management if they are to optimize their chances of successful resumption of business following an interruption.

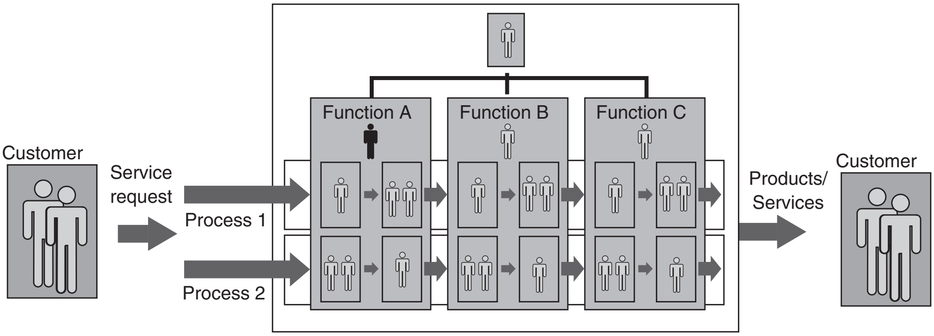


Figure 1.1—The business process

The business organizations of today

Driven by short cycle times, increased pressure to cut costs and to increase efficiency and customer orientation, today's organizations are organized around business processes to a greater extent than ever before. To deliver a product or a service to a customer, a chain of activities has to be performed. This chain of activities is called a business process (see Figure 1.1). Although in many organizations there is still a division into departments with a formal hierarchy, the actual business operations are typically organized and executed across departments, through these business processes, which are driven by information flows.

For the same reasons of efficiency and increased business value, companies are focusing themselves more and more on their activities where they can differentiate themselves in the market. For the other activities required to deliver the product or the service, many companies enter into partnerships with other organizations or outsource some of their activities. This means that the activities executed to deliver a product or a service to the customers extend beyond the boundaries of the company. Considering business processes, we have to look at the 'extended enterprise'.

Integrated organization

Each business organization always consists of three components (see Figure 1.2):

- Business processes – how products or services are delivered to the clients
- Participants – who participate in the execution of the business process
- Infrastructure and resources – used in the execution of the business process.

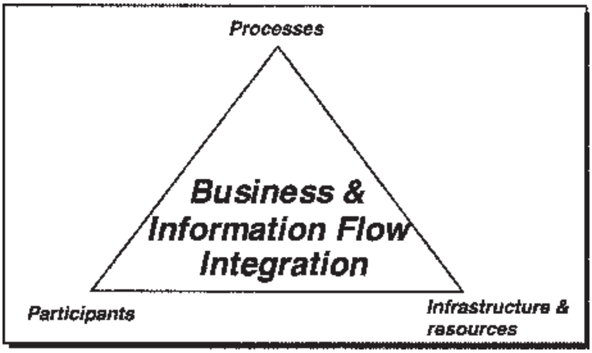

Processes
Business & Information Flow Integration
Participants
Infrastructure & resources

Figure 1.2—Elements of a business organization

These elements of the organization are integrated through information flows. Because of the high level of integration of business operations and information flows, it is difficult to separate any of these elements from the others. It is these elements together that allow an organization to execute its business operations. Also, when you think about how you will bring about the resumption of business after a disaster, you cannot separate any of the elements of the organization from the others. For instance, if you consider only IT, or just a single department, then you will probably not achieve business resumption, because you are overlooking the integration of dependencies throughout the organization.

Business dependencies and vulnerabilities

Each business process depends on a number of critical elements. In a business process a number of persons or departments are involved, who execute one or more activities and pass the resulting information on to the next participant in the business process.

A first dependency is human resources, where a minimum number is required with the appropriate skills and knowledge to be able to execute the business activities. Other dependencies are resources and infrastructure elements. These can be logistical resources, utilities, office infrastructure, manufacturing infrastructure, information technology or financial resources. Examples of logistical resources are loading and stocking areas, transport facilities, weighbridges and so on. The extent to which business operations depend on these critical items means that there is a higher vulnerability to business interruptions. These vulnerabilities include, for instance, single points of failures in the IT architecture and network. When such a component becomes unavailable, many or all of the critical information flows to support business operations are interrupted.

Within each business process, there are a number of key activities. When such key business activities can no longer be executed because of an unexpected event,

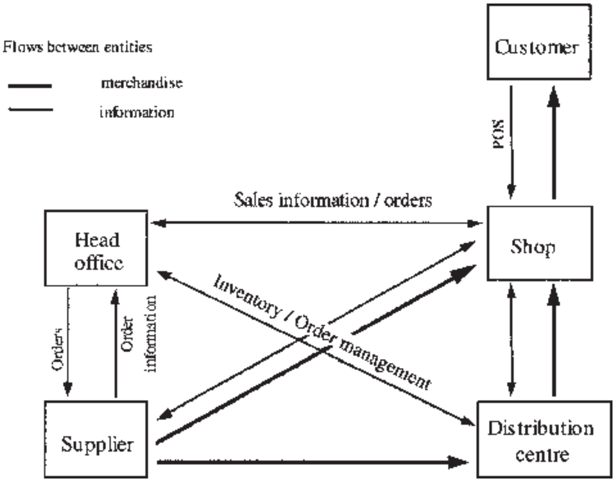


Figure 1.3—Retail replenishment

the result could be an interruption of the business process that is part of the value chain to the customer.

To illustrate this, let's take the example of the replenishment cycle of a supermarket chain (Figure 1.3). In this case there is a complex information flow that starts from the POS terminals in the shops. Each shop sends daily information on the local stock levels to the head office. The information from all shops is consolidated and processed to issue orders to the suppliers. A second information flow provides input to the distribution centres, allowing them to plan the distribution to the shops. For each group of products, there are different supply cycles and deadlines within this replenishment cycle.

Continuity of the replenishment depends on this complex activity chain, where there is an integration of information flows and merchandise flows. Throughout the chain, several departments and locations interact on a regular basis. Within the chain, there are a number of subprocesses, each with its own dependencies and vulnerabilities, for example reception and transfer of goods for transport to the stores. The information flows go through a number of servers and networks.

Within business continuity management it is impossible to duplicate every process – this would be too expensive. Nor is it sufficient just to provide backup for one or more elements; as discussed above, due to the interdependencies, this would be insufficient to effectively recover the full process.

To be able to provide continuity of this complex cycle when an unexpected event interrupts the chain, the business continuity plan will have to organize the business process differently by using a limited alternative infrastructure and by temporarily redefining the cycle times and deadlines.

External dependencies

Business organizations are not only dependent on elements within the company. No business organization is an island. Each depends on a number of external resources and outside organizations. These external resources are often beyond its immediate control. Examples are electricity, water, telecommunications and so on. Although your organization cannot control the delivery of these services and therefore cannot prevent interruptions, it is your organization alone that can and will have to manage the impact on your business operations should these external dependencies fail. Likewise, the participants in the business processes are both internal and external to the company. Examples are suppliers, business partners, agents, distributors, banks, factors of invoices, insurers and public authorities.

The business activities that provide customer service extend beyond the company boundaries. The concept of 'extended enterprise' is very applicable. This means – again – that you are dependent on elements that are beyond your immediate control. You will have to handle the consequences to your business when they become unavailable.

These external dependencies are very critical for any company participating in a supply chain (Figure 1.4). These companies are, for instance, particularly dependent on a number of external information flows. Examples are order-entry and delivery notes, reception of invoices, payments to and from the bank, and ability to ship.

Companies are also dependent on the execution of business activities outside their own organization. This is especially true with the increased level of outsourcing and business partnerships. Examples of hi-tech outsourcing include information and communications technology, contact centres, web services and application services. Other services that are frequently outsourced are facilities management, security, cleaning, catering, transport, distribution, packaging, back-office functions and financial services. Although these external companies are responsible for their own business continuity management to resume their business, you are responsible for managing the impact on your business operations of a disaster within these companies.

Disaster can strike, within your organization as well

Unexpected events and incidents can become disasters

When one thinks of disaster, such examples as fire, flood, terrorist action, hurricane and so on immediately come to mind. Although there are regions where some of these threats are more real than elsewhere, the reality shows us that disasters come in a variety of guises. It does not have to be a large-scale event to

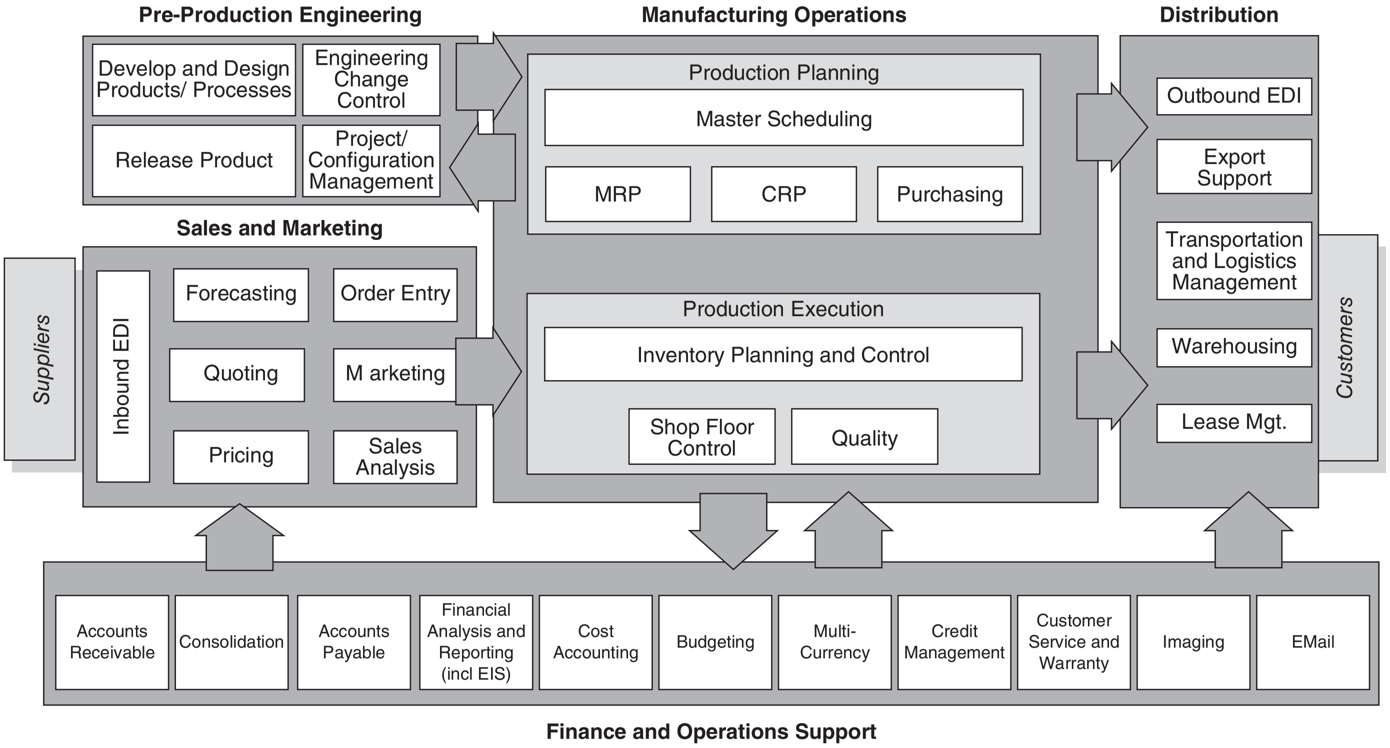


Figure 1.4—The complex business activity chain

mean disaster for your company. Neither does it have to be an event that causes extensive damage to the infrastructure.

Imagine, for instance, an event in your neighbourhood (your industry park or in the city centre) that requires an evacuation of the whole area until the problem is solved, which could be hours or even days. Your computers will still run, your telephones will still ring, and your business infrastructure will be unharmed. But you cannot use it. You cannot answer the telephone. You cannot enter the building. Such circumstances can be disastrous to your business.

Or consider a utilities company that starts a new service. But demand is so unexpectedly high that there is insufficient capacity to support the demand, and the service is reduced to the point of a business interruption. Is this a disaster? Probably, because the image will be damaged such that it will be extremely difficult to restore it.

Even small incidents, over only a short period, can create a disaster if they affect a key dependency. Consider the example of a fish farm, where an electricity failure of very short duration disturbed the temperature of the pools, causing the death or contamination of much of the stock. The effect was the loss of a breeding cycle of three years. Plenty of additional examples of events causing business interruptions can be found in the appendices at the end of this book, demonstrating that disasters do come in all shapes and sizes.

Classification of disasters

A possible classification of business disasters can be according to the type of event. Such classification includes the following groups:

- Acts of nature – e.g. hurricane, flood, etc.
- External man-made events – e.g. terrorism, evacuation, security intrusion, etc.
- Internal unintentional events – e.g. accidental loss of files, computer failure, etc.
- Internal intentional events – e.g. strike, sabotage, data deletion, financial wrong-doing, etc.
- Legal, regulatory, compliance or governance failure, which could be either intentional or unintentional
- Business failure – e.g. caused by inappropriate and unsuccessful business strategies or management.

Such classification has its merits in driving emergency plans and crisis management, where the event itself must be managed in order to protect people and assets, and to mitigate damage. When it comes to business continuity management, where the objective is to resume business operations, a different classification of disasters is more effective.

Some companies ask themselves if they should include the loss of the head office in the scope of the business continuity plan, especially as the probability of the destruction of the head office is considered to be low. Basically, this is the wrong, or at least an incomplete question. Your business continuity management should not be driven by eliminating risks according only to their probability but rather by considering what would be the effect and impact on your business if an unexpected event were to occur, whatever the event. In that sense, for business continuity management as a method of achieving business resumption, potential events and disasters could be better classified according to their business impact.

Such classification according to effect could be:

- Failure of an individual infrastructure element, including single points of failure
- Longer-term interruption of a critical information flow
- Longer-term interruption of a critical business activity chain or business process
- Local longer-term business interruption
- Complete business interruption.

Experience shows that, in many cases, the effect of an unexpected event cascades into larger impact levels. This again underlines why, for business continuity management to be effective, it must be driven in terms of managing the business impact, rather than handling the event. Many examples of this are to be found in the Appendix section of this book.

Disasters do happen

It is still a widespread belief that disasters only happen to others, and that the probability of a disaster is so low that investment in business continuity management cannot be justified with ease. However, statistics show that disasters do happen, and you could be the unfortunate victim today!

In 2004, the Gartner Group determined that the average cost of downtime worldwide was $42 000 per hour. They also found that the average network experiences 175 hours of downtime each year. Even if an organization is far below the average downtime and is down for 100 hours in a year, that time would equate to potentially $4 200 000 in lost revenue.

A research report from the Yankee Group shows that more than half of the questioned companies lost over $1000 per hour because of system downtime. Another 9% indicated that their losses were $50 000 or more per hour. Statistics suggest the average downtime event lasts 48 minutes.

And this is just IT.

As organizations have many more key dependencies that are not IT, the probability of business interruptions is in reality much higher. And when your organization is larger, you will have more key dependencies and vulnerabilities, hence it is more probable that your organization will suffer a business interruption at some point in time. Although smaller organizations have fewer dependencies, they are usually more important, hence an occurrence of a disaster here usually has a higher impact.

Another myth is that when a disaster happens, organizations are flexible enough to survive, even without a business continuity plan. On this topic, there is some variance in the statistics. But all mention a figure between 60% and 90% of companies without business continuity plans, and that suffer the loss of a key facility, go to the wall within 24 months of a disaster. And those that do survive typically never reach the same level of business that they would have obtained without the disaster occurring.

The business risks of unexpected events interrupting operations

Consequences of unexpected events interrupting operations

The immediate consequence of an unexpected event is the damage that it generates. This is the area where insurance can assist you in managing a disaster. In terms of business continuity, immediate physical damage is not the most important concern. Of greater importance is the impact on business operations, and how this can be overcome in order to resume the business and survive as a company.

Damage, impact and long-term effects

An unexpected event can cause damage to infrastructure elements and resources supporting business operations. Examples can be buildings, computers, networks, machinery, etc. The damage can be such that the infrastructure element is destroyed or unavailable for an extended period of time.

The direct consequences of such events can be twofold:

- Unavailability of infrastructure elements or resources
- Loss of information.

In terms of Business Continuity Management, it is important to make the distinction between damage caused by the event and the impact on the business because of the unavailability or the loss of information.

Next to the impact on business operations, one must also consider the long-term effects of such unexpected events. These are business impacts that are still felt long after the business has been resumed and operations have returned to normal. Examples are:

- Loss of market share
- Lower share price
- Lower credit rating
- Loss of brand value
- Loss of company image, public confidence and credibility
- Loss of key staff, who may move to competitors.

All these elements must be considered and will drive the business continuity management.

The direct impact: unavailability and loss of information

Alternative business operations

Unavailability of IT infrastructure has always been the focus of the traditional IT disaster recovery planning, which focused mainly on replacement or switching to alternative infrastructure. It is clear that it can rarely be cost justified to duplicate all your resources – priorities must be identified. It is often very difficult to decide how far one should go in these arrangements.

As it is rarely possible to duplicate the complete business infrastructure after a disaster, business operations will have to be organized with only limited infrastructure available. Executing the most critical business activities with this limited infrastructure and personnel is one of the fundamental challenges of business continuity management.

Very probably, given the limited infrastructure and resources, the information flows and the business operations will have to be reorganized in order to meet the business objectives at a minimum acceptable level.

Loss of information

After a disaster, one will typically restart from the last available backups (which have hopefully been stored off-site!) (see Figure 1.5). If you can restart from backups (many do not), this means that all transactions that had been entered

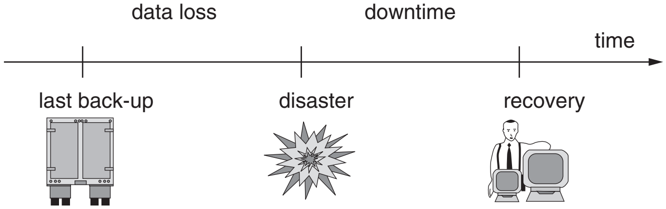


Figure 1.5—Typical IT recovery cycle

since the backups were taken will not be on the system after the restore. This information may well be lost. Also one must consider the synchronization of the data restored from different backups taken at different times. For instance, the backup of orders entered can be taken later than the backup of the financial systems, including the accounts receivable. It is as if your organization has gone back in time, but each system to a different time zone, and you have to match between time zones.

In addition to the time mismatch, the business events associated with the lost transactions will have been executed. For instance:

- Invoices will have been sent out
- Orders will have been received
- Goods will have been manufactured, lost or shipped
- Payments will have been made.

All this, but there may not be a trace of these events in the information systems. Even now, most organizations do not back up data in real time. Typically, there will be a periodic full image backup, followed by incremental backups of just the changed data. The changed data then needs to be applied to the last full image backup as part of the recovery process. Perhaps some of this information will be contained in incremental backups. But even with data mirroring, there will still be paper transactions that have not been entered in IT systems.

Thus a recovery point objective needs to be established – that is, the time to which data must be restored (e.g. start of day, end of day or some timed checkpoints throughout the day).

When analysing the impact of information loss, one must consider how that lost information can be retrieved:

- Would you be able to reconstitute this information within your organization (the paper audit trail could be burnt in the fire), or will you have to ask your customers, suppliers, trading partners and banks for assistance?
- How will that affect your reputation?
- How much effort will this information retrieval entail?
- In the meantime, can you continue your business operations?
- How can you integrate the retrieved information in your information systems, without re-executing the associated business events?
- Can you guarantee the integrity and completeness of the retrieved information?

Consider, for instance, an air cargo company. Consignments are tracked by a computer system. Restarting after a disaster from the last backup, in the worst case 24 hours old, means that information on all consignment movements in the last 24 hours would be lost. On top of that there may be no way of knowing from internal sources which consignments had been transported in that timeframe: loss of the systems might not cause the physical movement of consignments to stop. The company either has to recompose all transactions by manually collecting information from its worldwide agents and partners (nearly impossible to achieve completeness), or it has to perform a total inventory of all its warehouses and stop business operations until completion of the inventory.

Loss of information due to a disaster is not limited to data on computers. What about all the information stored in binders, folders (with, for instance, customer information), contracts, property deeds, the archives, the legally required vital records, the paper client files, the business knowledge spread over the place, etc. Depending on the event, part of this information can be lost too. You must also consider the potential impact on your business of losing this information.

The indirect impact: rippling effects on business operations

Each business process consists of a chain of activities that are executed typically by different departments. An unexpected event can interrupt a business activity, and/or interrupt an information flow supporting a business process. If the event is such that the business activity (or several activities) can no longer be executed, the impact could stretch out towards the entire business process.

Consider, for instance, in the process of handling requests for loans, that the business activity of checking the credit position of the requester can no longer be executed. Either the loan is granted without the credit verification, which creates a financial risk, or the entire business process is halted, which will increase the risk of losing business opportunities (the customer will go elsewhere). The business impact of unavailability of key supporting infrastructure or resources can have chain effects throughout the process and even on other business processes. An example is the case of a distribution environment, where the goods tracking is done through bar codes. If the scanning of incoming goods is not possible for a certain period of time, there will be an impact on the full process. Either the process of transfer of incoming and outgoing goods is continued, with risk of losing track of goods, or the goods transfer process is stopped, with all the consequences of shortage of storage capacity for other incoming goods and of not being able to deliver the goods in time. The business impact will largely increase, as soon as external parties become involved. The higher the external visibility of the event, the more considerable and long lasting the business impact will be.

The effect of an unexpected event impacting business operations can easily ripple through the company. Even a relatively small event in an environment where many activities depend on each other can have a tremendous impact. Consider, for instance, the replenishment process for a supermarket chain. A WAN failure at a bad time, which lasts long enough, can in the end create a logistical nightmare, impact customer satisfaction because of empty shelves, and create a large financial impact in an industry where net margins are already slim (Figure 1.6).

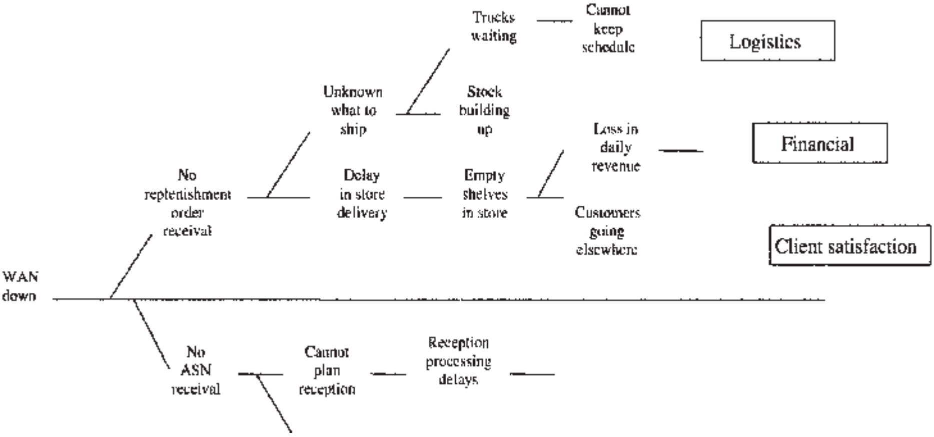


Figure 1.6—Effect diagram

As no organization is an island, the rippling effects of a business interruption can even go beyond the company's boundaries. This is particularly true for companies that are an integral component of a wider supply chain – that is most of us! If, because of a business interruption, you deliver late, your reliability may well be brought into question for a considerable period of time – often well after the actual crisis.

In some cases, when a company participating in a supply chain is hit by a disaster, this could ripple down throughout the supply chain. Each company within the chain will have to deal with the impact of this on its own business operations through its business continuity management.

The long-term impact: image, market position, growth or decline

Even long after you have recovered from a disaster, and have returned to normal business operations, you will feel long-term impact. Depending on how good your business continuity plan has proven to be, you will suffer some long-term impacts that can in the worst case even drive you out of business. These long-term impacts can include:

- Loss of customers
- Weakened financial position (for instance, reduced cash flow)
- Lost market share
- Loss of investor confidence
- Liabilities
- Eroded public image
- Etc.

Your share price is a good indicator of the degree of long-term impact. Typically, shortly after a disaster, as your shareholders learn about the disaster through the media, share price will drop. Depending on how positive the perception is of you coping with the disaster, the share price will rise. Whether it ever reaches the level it would have had without the disaster is a good indication of the long-term impact. This means that it is not only important to have an effective business continuity plan, but also that you must handle the outside world perception of the effectiveness of your plan. You will have to include media management and public relations as an integral component of an overall business continuity management strategy.

The importance of the public image of your company cannot be stressed enough. Even with the most effective and successful business resumption plan, if the public, investors, shareholders and so on get a negative perception, it could ruin all your efforts. Sound communication management, coupled with effective crisis management, is essential for survival beyond a disaster. For a company whose success is heavily dependent on its share price, the above-mentioned effect on share price alone should create a strong justification for investment in business continuity management.

In industries with intense competition, loss of customers or loss of market share might be something you will never recover from. Typically, this will generate a downsizing, and dependent on the flexibility of your organization, can even mean that you are pushed out of the market.

The business risks of an interruption in ICT operations becomes more critical every year. In 2006 Gartner EXP surveyed 1400 CIOs in more than 30 countries, representing more than US$90 billion in IT spending.[1] Marcus Blosch, vice president and research director at Gartner EXP, said:

> The survey results make it very clear that business expectations of IT have changed dramatically and executives are expecting their CIOs to move beyond concerns about cost, security and quality to help grow the business.

An unexpected event interrupting information flows or business operations can be considered a risk to the extent that it would create a material business risk for your company. A business risk is a threat that an event or action will adversely affect your organization's ability to successfully achieve its business objectives and execute its strategies – in other words the achievement of business mission. This implies that you have to look at IT or other business interruptions in the context of the key business risks for your company.

For example, a key business risk in the automotive components industry (and many other manufacturing industries) can be 'not being able to deliver parts where they are needed at the exact time they are needed'. In this industry, price and effectiveness are critical drivers that have enforced short cycle times through integrated logistics. Any disruption in business operations that would result in late

[1] *Growing IT's Contribution: The 2006 CIO Agenda*, Gartner EXP 2006.

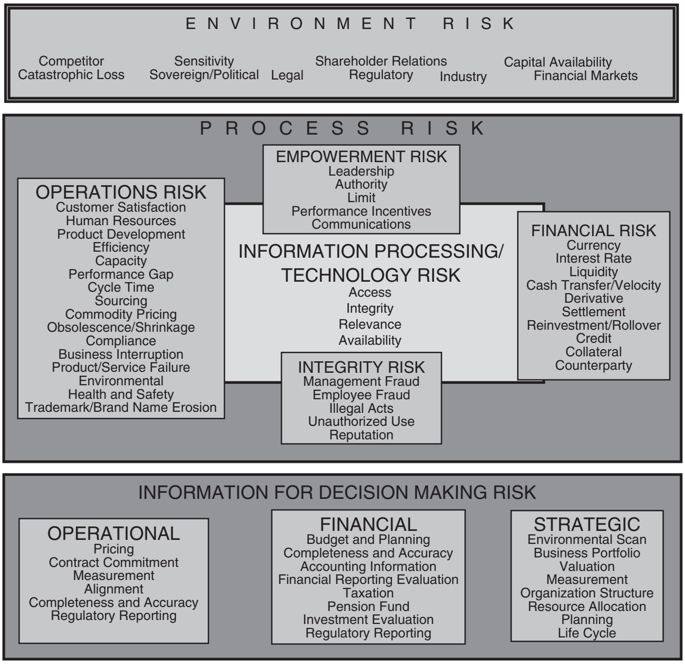


Figure 1.7—The Business Risk Model™. © Accenture

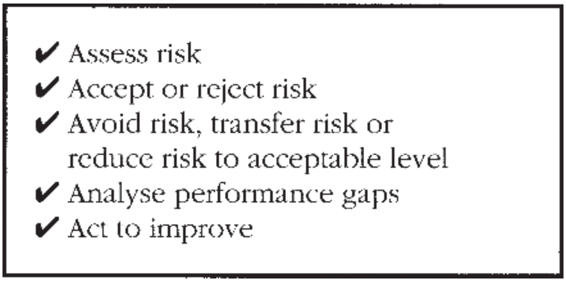
delivery or loss of efficiency is a key risk that subsequently must be covered in business continuity management for such companies.

When going through this exercise, it is important that you use a reference framework of business risks, specific for your business environment. Such a framework allows you not to dwell on symptoms or the obvious, but to focus on what is essential for your business success. An example of such framework is the Business Risk Model™, developed by Accenture for each industry segment (Figure 1.7).

Analysing your key business risks and performing a gap analysis with your current protection will allow you to set priorities. It also allows you to focus your investments towards those areas where you have the most benefit, namely covering the largest business risks for your company of an interruption in business operations.

Risk management: gamble or hedge?

Business continuity management is in the first place more about management of business interruption risks than about shopping around for solutions. The largest



✔ Assess risk
✔ Accept or reject risk
✔ Avoid risk, transfer risk or reduce risk to acceptable level
✔ Analyse performance gaps
✔ Act to improve

Figure 1.8—'The five As' of risk management

mistake one can make about business continuity management is thinking 'I have a business continuity plan, nothing can happen to me'. Every business continuity management is based on assumptions, and on risk management decisions. These include items such as maximum allowable downtime, disaster scenarios to include single point of failure assumptions, acceptance of certain risks and finding a balance between cost and benefits.

No business continuity management will ever cover all areas and all risks. The target is to cover the business risks that are key for your company, and to cover the business processes that are most critical for your business success. To reach that target, basically each business continuity management exercise is a risk management exercise, which is always based on the 'five As' of risk management (Figure 1.8).

By analysing the business risks of an interruption of business operations and the business impact, decisions can be made with regard to what level of risk can be accepted and what risks must be reduced to an acceptable level through business continuity management. It is important to realize that, when agreeing to accept a risk, this decision also includes acceptance of the consequences in the event that the worst happens.

Before going into defining solutions within a business continuity management, it is important that you do not make assumptions with a 'wet finger' approach. To return to the air cargo example, IT had assumed within its disaster recovery planning that restarting from yesterday's backup would be sufficient. We have discussed before what that meant in terms of loss of information and what would be the business impact.

It is important that risk management decisions are taken on an informed basis. Only in this way can a business continuity strategy be defined that will meet the business requirements and will cover the key risks. This is the difference between hedging and gambling: you gamble when you make assumptions, for instance, purely based on the probability of an event or based on 'gut feeling'. You hedge when you take risk management decisions based on a careful analysis of the business risk, on the potential business impact and on the key dependencies and vulnerabilities in perspective of your business objectives. Hedging is assessing the magnitude of the risks and taking informed and balanced decisions.

Business continuity management is about hedging the business risks of operational interruptions, deriving a business continuity strategy from this that meets the business objectives, and implementing this strategy.

Business continuity: what does survival mean to you?

So, you need business continuity management. It is a question of business survival. You want to manage the risks of a business interruption due to an unexpected event. But your business organization is complex. You cannot duplicate it all; this is just too expensive. Even duplicating only the most critical infrastructure is probably still very expensive and difficult to justify. Besides, what is critical and what is not, and to what level? Not all elements in your business organization are equally critical, yet they are interdependent because they are part of these activity chains.

What do you have to protect your business against? You cannot foresee all possible events. How far do you need to go? Where will you start? More important, where will you stop? How do you identify your priorities? How do you ensure that you invest in the right places? Could it be that you spend more than you should?

Before you actually start your business continuity management project, there is an important question to ask yourself: ‘What is your objective, what do you want to obtain from your business continuity management?’ At first sight, the answer is obvious: you want to be able to continue doing business after a disaster, to resume business activities and continue to serve your customers.

Consider the approach to business continuity management that you intend to take, and the project organization you intend to establish to build the plan. Compare the focus areas of that approach against what your objectives of business continuity management are.

Considering the different approaches to business continuity management that we see organizations apply, there are basically three kinds of objectives, each matching a different approach:

- Rebuild the infrastructure. Here the focus is on alternative facilities and sites and on solutions to minimize downtime of key infrastructure and systems.
- Resumption of business activities. The focus is on setting up an organization and the required facilities to enable key staff to resume their activities.
- Continuity in customer service at an acceptable level. The focus is on defining what level of customer service must be maintained throughout a disaster, and what is required to achieve that level of customer service.

The following sections discuss each of these objectives and approaches. They describe what are the benefits, what are the outcomes and what are the pitfalls or potential shortcomings of each of these.

Rebuilding the infrastructure

The objective in this approach is to rebuild the critical infrastructure that has been damaged in a disaster. The idea is that as soon as the damaged infrastructure is available again (albeit in a different location), the business activities can be resumed as before because the required infrastructure is the same.

Lists are created of mission critical activities including computer systems, networks, manufacturing infrastructure, contact centres, web services, office space and any other essential infrastructure elements. The selection of these critical infrastructure elements is based on a business impact analysis and a risk analysis. The maximum allowable downtime is defined (maximum acceptable outage and recovery time objective, which are usually the same), when required differentiated per group of infrastructure elements. With this list in hand and the determination of recovery time objective, alternative solutions are considered and a cost/benefit analysis is made. The critical success factor in this approach is to have a sufficient mission critical infrastructure duplicated so that business activities can be resumed in a similar way to how they were executed previously.

Once the solutions are selected, plans must be built to bring them into action. This is the mechanism to switch on these alternative systems and infrastructure elements. Because of cost considerations, we see the list of mission critical infrastructure elements very often trimmed down to the barest essentials (and sometimes less than that), for which the least costly option is chosen.

Although the thinking process in the beginning is business oriented through the business impact analysis, we very often see a too intense focus on systems and office space without sufficient verification as to whether business activities in the end can effectively be resumed. What we also see happen too often is that a reduced version of this approach is chosen to create a feeling of safety. Very often it is only the central IT system and communications that are considered within the scope of business continuity management, the concept being that without this system the company would not be able to survive a disaster. Consequently, the lowest cost options are considered in respect of hot-site or short-term delivery of a replacement system in the mistaken belief that this solution will ensure the company's survival. An example illustrating this is the replenishment cycle mentioned before. The company concerned decided to duplicate, through server mirroring, only the most critical within the chain of systems and networks supporting the replenishment information flow, without considering how the replenishment process would be resumed with only this single server available.

A further problem follows this narrow vision of protection of only the most critical infrastructure elements. This is in the testing component of the process. In many instances, testing focuses on making the alternative infrastructure available but too rarely considers the practical application of mission critical business activities based upon this limited infrastructure. Although the intention is correct, the outcome of this approach is infrastructure replacement, not necessarily business continuity. Relatively few companies can afford such an extensive duplication of infrastructure.

When a disaster does occur, we very often see these limited investments prove to be ineffective in providing business resumption. Stories abound of companies that went bankrupt even though their central computer system was recovered within hours of the disaster.

Resumption of business activities

Having witnessed the pitfalls of a purely infrastructure-oriented approach to business continuity management, many organizations have added the dimension of resumption of business activities to their approach.

Another key driver in the approach focusing on resumption of business activities is the awareness that central systems are only part of the infrastructure supporting the business activities. PC networks and client/server architectures have created critical dependencies throughout the enterprise. In this approach, the activities of the employees are considered. A list is made of what the mission critical activities are and what is required to be able to execute them. Again, a business impact analysis and risk analysis are instrumental in determining the level of criticality of these activities.

The result of this analysis is typically a scheme of what number of staff (and the associated office space and infrastructure) is required by what day after a disaster. The idea is to gradually resume the business activities elsewhere, starting with the most critical ones, until full business resumption or until the return to the old facilities is possible. The benefit of this approach is that it links business activities to required infrastructure, providing a much better guarantee for effective business resumption in the case of a disaster. The critical success factors of this approach are the criteria that are used to prioritize business activities.

The most important pitfall of this approach is that it very easily results in building departmental recovery plans, where each department within the company will build its plan to resume the critical business activities executed within its department but in isolation of the whole. What is missing here is business integration. For instance, one department is dependent on being provided with input from another department to execute one of its key activities. Perhaps the provision of that input is considered non-critical by the provider department but is absolutely crucial to the operation of the receiving department. Very often, departmental recovery plans lack a business process orientation, where business processes cross over a number of departments.

Another pitfall is that the criteria to define business criticality of the activities are not uniform over the departments, and/or are not linked to the business objectives or the key business drivers of the company. We often see business continuity plans using this approach focus much more on the business activities as objectives on their own, instead of focusing on the resumption of the key business activities to enable continuity in service delivery.

Continuity in customer service at an acceptable level

The continuity solution is the preferred (and sometimes the only) option for organizations having high volume, high value, transaction-based activities. Infrastructure replication and resilience is now generally considered essential for banking, dealing and online web-based businesses or contact centres and for telecommunications companies. For compliance reasons, many financial institutions have to follow this route. The more reliant the organization is on its technological infrastructure, the more likely it is that this approach will be followed.

When a CIO of a global bank was asked how they justified the massive spend on infrastructure resilience, he replied: ‘It’s simply part of the cost of being in business.’ On another occasion, a CIO requested a consultant to find an Internet service provider that would guarantee 100% availability and be prepared to pay consequential cost if they failed to do so. ‘No ISP will guarantee that,’ responded the consultant, ‘but why do you need it?’ The CIO replied: ‘Because we can lose a billion dollars in eight minutes.’

The case for infrastructure resilience can be powerful. Following 9/11, according to Fitch First Database, the Bank of New York lost some $900 million while Citigroup lost around $830 million. The UK Bishopsgate terrorist bomb in 1993 cost various UK banks a total of around $500 million.

For many other organizations, it may not be justifiable to duplicate all critical infrastructure, since that infrastructure alone does not provide business continuity. Moreover, it may be very difficult to obtain integrated business resumption through a mere resumption of individual business activities. In this case it is clear that selections will have to be made about what to replicate and that a structured approach to make these selections is the key to success. Making these selections is essentially business risk management, and is an executive level responsibility. It concerns the management of business interruption risks in the context of reaching the business objectives and safeguarding the key business drivers.

Typical management objectives of business continuity management are to:

- Provide continuity in customer service at a minimum acceptable level
- Limit the impact on the financial position of the company.

Defining what is the minimum level of customer service that is to be maintained throughout a disaster is critical in this approach. This requires a top-down analysis of business drivers and objectives, the key business processes supporting these business drivers and their key dependencies and vulnerabilities. In many cases, this will be determined by contractual commitments and service level agreements.

The goal of the business continuity plan is to build the business operational capability to reach these service levels. These will eventually include provision of alternative key infrastructure, resumption of key business processes and associated business activities, organization measures to execute the business resumption and many more.

Conclusion

Business continuity management is about being able to continue 'without missing a beat' or being prepared to rebuild your business organization after a disaster in order to provide continuity in customer service at a minimum acceptable level, to limit the impact on the financial position, and in the long term to survive as a business organization.

Today's business organizations are driven by business processes, which are chains of activities that are executed across departments. Each organization consists of an integration of business processes, the participants in these processes and the infrastructure and resources supporting these business processes. Within each business process, there are a number of critical dependencies, which can include: human resources, logistical infrastructure, information technology, key activities, and dependencies beyond the organization's boundaries. Unexpected events can at all times interrupt business operations. These do not have to be large-scale events or do not even have to cause extensive damage to mean a disaster to an organization.

Because unexpected events do come in all shapes and sizes, and considering the objective of business continuity management of being able to resume business operations, potential events and disasters can be better classified according to effect, rather than type of event. Statistics show that business interruptions do occur, more frequently than one would expect. They also show that you should be prepared if you want to optimize your chances to stay in business.

The effects of a disaster are not limited to the damage that it causes. They also include the business impact of unavailability and loss of information. The business effects and losses associated with extended interruptions of the critical business activities can be very high. Even after the resumption of business, the impact of a disaster can still be felt through loss of customers, a fall in the share price, and in an erosion of the organization's image, perception and credibility in the marketplace.

An unexpected event interrupting business operations can be considered a risk to the extent that it would materialize a key business risk for the organization. A business risk is a threat that an event or action will adversely affect the organization's ability to successfully achieve its business objectives and execute its strategies.

No business continuity management will ever be able to cover all business areas and all risks. The target is to cover the business risks that are key for your organization, and to cover the business processes that are essential for your business success. To reach that target, basically business continuity management is a business risk management exercise. It is important that risk management decisions are taken on an informed basis. Only in this way can a business continuity strategy be defined that will meet the business requirements and that will cover the key risks.

Business continuity management is about:

- Hedging the business risks of operational interruptions
- Forming a business continuity strategy from this that meets the business objectives
- Implementing this strategy.

Finally, it is very important to define your objective clearly: non-stop operations providing continuity in customer service, rebuilding the infrastructure, resuming business activities all at an acceptable service level. Having defined your objective, you have to apply an approach that meets that objective, and stay focused on that objective, throughout the business continuity management project.