



Business continuity management and risk

The role of standards

raising standards worldwide™

BSI
British Standards

A hand is shown in the upper left corner, placing a white domino with blue dots on a line of other white dominoes with blue dots. The dominoes are arranged in a slightly curved line on a light-colored surface. The background is a soft, out-of-focus white.

Executive summary

Greater awareness in recent years of the volatility of the risk environment, together with the regulatory impetus provided by corporate governance requirements, has placed effective risk management high on the corporate agenda. Changing attitudes to risk management have also resulted in the emergence of a more holistic and proactive approach to managing exposures.

During this evolutionary process, business continuity management (BCM) has emerged as an increasingly important element of an organization's risk mitigation strategy. Developing out of the areas of information security and disaster management, effective BCM can enable an organization to reduce its exposure to disruptive events, implement mechanisms to limit the impact of an incident on business processes and operations, and provide reputational resilience in the most difficult of circumstances.

However, a lack of consistency in approach, confusion over definitions and terms, and the inability to benchmark BCM strategies have hindered its development, and led to calls for a formal standard to be produced. Based upon proven methodologies, BS 25999 *Business continuity management* establishes the process, principles and terminology of effective business continuity management.

The rise of risk management up the corporate agenda reflects an increased understanding by organizations, both public and private, of their risk profiles and the need to effectively manage exposures. High-profile incidents such as Enron, 9/11, Hurricane Katrina, the summer floods in the United Kingdom, Northern Rock and Société Générale – as well as the regulatory structures implemented in some cases in the aftermath, such as Sarbanes-Oxley, Basel II and the Turnbull report – have served to shape attitudes to risk management and achieve greater boardroom awareness.

More proactive ...

Organizations are becoming increasingly proactive in their approach to managing their risk exposures and developing bespoke strategies rather than simply relying upon the parameters set by regulatory authorities. In tandem with this has been a change in the stance taken by regulators towards a more principles-based approach to regulation – a move that places the onus on organizations themselves to take greater responsibility for their risk management strategies.

Julia Graham, chief risk officer at DLA Piper and chair of the committee for BS 31100 *Code of practice for risk management*, believes that this change in the attitude of regulators is a very positive step, as it means that “organizations are then in a position to manage risk in line with their own context, nature, scale, complexity and jurisdictional spread of their business”.

Risk in a standard

In February 2008, BSI released the second draft of BS 31100 *Code of practice for risk management*. The standard is designed to provide a guide to risk management principles, models, frameworks and processes, in order to assist organizations to achieve their risk management objectives.

But can a concept as broad as risk management be captured effectively in a single standard? “The standard is intended to be high level and generic, and not specific to any business, country or discipline,” says Julia Graham, chief risk officer at DLA Piper and chair of the committee for BS 31100. “It is viewed as part of a family of standards.”

The discipline of risk management has, however, been the subject of many guidelines, documents and standards. “The committee which developed the standard looked long and hard at this issue – there are some excellent standards already available, which BS 31100 was not designed to replace,” explains Ms Graham. “Rather, BS 31100 is seen as a positional document which helps to set the overall risk scene, language, framework and process.”

RESEARCH

Business Barometer

According to the latest findings of BSI British Standards' annual Business Barometer, UK businesses are continuing to enhance their levels of disaster preparedness.

The survey of FTSE 250 companies in 2007 revealed that over 80% of respondents were confident their organization could continue to operate for up to a week following a disruption before experiencing serious detrimental effects. Almost two-thirds considered themselves ready to respond to a major IT failure, while 50% were fully prepared for a forced office relocation.

These figures reflect the fact that some 71% of respondents – up 10% from 2006 – now acknowledge the vital role played by BCM in ensuring their company remains competitive and wins new business in the future. With some 62% of businesses indicating that customers now require them to show that they have effective BCM measures in place – up 16% on the previous year – expectations are that this figure will continue to rise.

Commenting on the findings, Mike Low, director of BSI British Standards, says: "The scale of risk and opportunity in the FTSE 250 is enormous and these organizations are recognizing that BCM has to be at the heart of their operations." However, he emphasized that it was also crucial "for smaller organizations and those in other sectors to look seriously at how they would cope in the event of a disaster".

More holistic ...

This evolution is encouraging a much more holistic approach to the management of risk. Organizations are endeavouring to remove the silos which exist within their operations to achieve a more expansive and integrated risk strategy, founded upon an enhanced understanding of their risks, business processes and dependencies.

The removal of these silos has contributed to the emergence of business continuity management (BCM) as an integral part of an organization's risk management strategy. Seen for decades as an IT and disaster recovery-related issue, BCM is now gaining a much more prominent position in the risk mitigation mechanisms of many organizations.

In the majority of cases, business continuity has evolved independently from risk management operations. James Crask, resilience policy manager at the Civil Contingencies Secretariat, attributes this to the factors that have driven its development. "In many organizations risk management has traditionally been driven by finance, while business continuity has developed from security and crisis management arrangements. Because they have often developed independently of each other they are frequently situated in different parts of an organization, meaning they could be moving in different directions." However, Mr Crask is confident that attitudes are now changing and that, increasingly, companies are realising that these two disciplines should be working together.

Ms Graham views risk management and business continuity as two parts of the same governance framework. "Risk management provides the umbrella under which a variety of risk management categories and capabilities can reside," she says. "Business continuity is part of risk management and notably part of an organization's risk control environment."

More integrated ...

While still in its relative infancy as a discipline compared to risk management, components of business continuity can be found in virtually all organizations. It is basic common sense to ensure measures are in place so that activities essential to the delivery of products or services are protected. Therefore, they can still be maintained should an incident occur. Yet the effectiveness of such processes is highly dependent upon the extent to which these measures are integrated into the organization.

Attitudes are changing as companies realize that risk management and business continuity disciplines should be working together.

“Traditionally most organizations understand the core components of their business and are aware of what needs to be protected,” says Mr Crask. “That is where they build in continuity. However, what they have failed to do is view the organization as a whole, obtain the full support of senior management, understand interdependencies, embed business continuity into the culture of the operation and ensure that employees are aware of their roles and undergo regular training.”

*BCM is less about the plan itself
and more about ensuring that
the requirements are built into
every facet of the business.*

There is also a tendency on the part of some companies to limit the scope of business continuity to the areas of incident management and risk mitigation, believes Steve Mellish, head of business continuity at Sainsbury's. “This in my opinion doesn't make for a really effective business continuity capability. You need to have – and understand – the whole picture to devise a business continuity capability that really ensures that it meets the business requirements and is fit-for-purpose.”

The value of BCM can only be achieved if it becomes an integral part of the operational structure of an organization. Business continuity is less about the plan itself and more about ensuring that the requirements are built into every facet of the business, starting with the internal operations and extending out along the supply chain.

Adding value to the business

If an organization successfully integrates a robust and effective BCM plan into every facet of its operations, then the potential benefits that can be gained are extensive.

Providing assurance

One of the primary aims of an effective BCM strategy is to provide a level of assurance that, in the event of a disruptive incident, the organization can not only continue to provide critical services but also become fully operational again in as short a time frame as possible – no matter how severe the disruption.

Peter Sierwald, director of Phoenix Continuity Services, describes the goal of effective business continuity: “A sound BCM strategy provides assurance that all necessary aspects of the organization's value chain can be protected and recovered to an acceptable level of emergency operation at an acceptable cost.”

CASE STUDY

Bits not pieces

The development of a standard for information and communication technology (ICT) continuity is no easy task, particularly given the increasing complexity and interdependency of the systems involved.

The situation is further compounded by the fact that few organizations have a thorough understanding of the systems that they operate. "Systems are complex enough to manage when we understand their end-to-end make-up," says Oscar O'Connor, an adviser with Adam Continuity, "but when we do not, we are simply asking for trouble."

The British Standard for ICT continuity, BS 25777, is designed to provide guidance on how to apply business continuity principles to an organization's ICT systems. Employing the same basic structure as BS 25999, the standard is designed to enable companies to implement appropriate levels of resilience for ICT services, as well as the processes required to respond to and recover from a disruptive incident.

"BS 25777 aims to ensure that not only are the organization's ICT services as resilient and recoverable as is appropriate," says Mr O'Connor, "but also that the organization's BCM requirements for ICT support are completely covered."

Competitive advantage

In an increasingly volatile environment, the ability to offer such levels of assurance through the implementation of a well-structured BCM plan is becoming a discernible competitive advantage. The value of having mechanisms in place that enable you to limit the detrimental impact of an event on your business activities, thereby enabling you to outperform competitor organizations during a crisis and return to normal levels of service in a shorter time frame, is immense.

Being able to demonstrate that, even in the most trying circumstances, an organization is capable of maintaining operations, can impress clients.

Strengthening client relationships

From the perspective of existing – and potential – clients, being able to demonstrate that, even in the most trying of circumstances, an organization is capable of maintaining its operations can serve not only to strengthen existing relationships but also stimulate new ones. Such a competitive benefit is encouraging the emergence of a more proactive commercial approach to business continuity rather than simply viewing it as a mechanism for managing a disruption to operations.

Tendering for business

In recent years there has been a marked rise in the number of companies that now stipulate that an organization must have a BCM plan as a prerequisite for a bidding process. “We have seen more organizations over the last year asking about business continuity during the tendering process than we have ever seen before,” confirms Simon Beesley, operations excellence manager at TDG.

Preserving and enhancing reputation

Reputational risk is considered by many organizations to be the number one risk they face. Taking years, if not decades, to build up, a company’s reputation can lie in tatters in an instant. While the aim of a BCM plan is both to limit an organization’s exposure to a disruptive event and to improve its ability to return to normal service quickly in the aftermath of any such incident, by succeeding on these two fronts the organization will not only preserve but actually enhance its reputation.

Increasing share value

The effective management of a crisis not only provides a defence mechanism for your bottom line by enabling you to continue to operate, it can also provide long-term share value benefits. In *The Impact of Catastrophes on Shareholder Value*, Rory Knight and Deborah Pretty examined how shareholder value was affected by a major incident.

They found that while share prices initially crashed, those organizations which managed the crisis effectively saw their share value not only return to pre-incident levels, but actually rise above them – which was then sustained for a long period of time. In contrast, those organizations that mismanaged the disruption never saw their share price recover to the same position.

A worthwhile investment

Martin Caddick, head of UK business continuity management at Marsh, believes that in order to encourage board level buy-in to business continuity, you must make members aware that BCM is an effective investment. By adopting a more holistic view of risk and BCM, such investments can provide much greater bang for your risk buck. “You can potentially reduce your levels of insurance, spend less on protection measures and even reduce expenditure on BCM,” he says, “while at the same time enhancing your overall protection.”

You can reduce expenditure on insurance, protection measures and even BCM, while at the same time enhancing overall protection.

Understanding your organization

In another recent survey by Marsh, *The Upside to Business Continuity*, respondents were asked to highlight the benefits of BCM they had experienced over the last 12 months. Surprisingly, over 50% of respondents found that they had achieved a better understanding of their business, while 37% highlighted improved risk-intelligent decision making.

Mr Beesley believes that by gaining a thorough understanding of your business processes you can then see areas where these processes can be enhanced or streamlined to facilitate the overall stability of your operation. “Any time when you start a project which looks at how your business processes operate, you will always find ways of improving these processes.”

CASE STUDY

As strong as the weakest link

Following a review of its approach to BCM in 2007, TDG, a supply chain management company, launched a pilot project to provide its site in Rugby with a business continuity management system developed and implemented following the BS 25999 code of practice.

“The way we used to approach BCM as an organization was that it was pretty much every site for itself, with little in the way of central control,” says Simon Beesley, operations excellence manager at TDG, who is responsible for the project.

Admitting that he knew “nothing” about BCM before beginning the project, Mr Beesley enrolled on a one-day introductory workshop to BS 25999 – hosted by BSI – which enabled him to understand how to apply the standard within his organization. “In terms of providing a framework for this project, BS 25999 was incredibly helpful,” he explains. “It is written in plain English and provides a clear process that you can follow.”

While it was important to ensure that senior management were involved in the project from the start, he also highlighted the

importance of involving those people “on the shop floor”, as they are best placed to describe their particular operations and also to propose solutions should a disruption occur. “As long as you engage the people that understand each part of your business and ask them the right questions, the process can become a very straightforward one.”

It is imperative that those who will manage the disruption also develop the business continuity management system. “The approach that we are taking at TDG is that my role is to support the sites in implementing their plans, not to develop them,” he explains. Local ownership of the project must be established so that each site can develop its own bespoke solutions based upon the templates and guidance provided.

While acknowledging that being the first logistics company to achieve BS 25999 certification has provided TDG with a unique selling point, Mr Beesley is keen to point out that this is not why TDG undertook the project. “It should never be about ‘getting the badge’, but rather about companies gaining real benefit from going through the process.”

By obtaining a thorough understanding of your organization you gain “an improved understanding of the risks you face, both within the walls of your organization and across the wider supply chain, ” says Mr Beesley. He believes this process has helped his organisation to enhance relationships not only internally, but also with external customers and suppliers.

Establishing best practice

However, despite the myriad benefits which business continuity can bring to the table, its effectiveness has been hindered by the relative lack of clear guidance on the processes required to implement a successful BCM strategy.

Prior to the publication of BS 25999, there were a number of business continuity guidelines in existence, such as BSI’s PAS 56:2003 *Guide to business continuity management* and the Business Continuity Institute’s *Good Practice Guidelines*.

On the international front, there are also a range of business continuity-related standards and guidelines available. In Australia, for example, the HB 221 *Business Continuity Guidelines* were drawn up in 2004, becoming HB 292 *A Practitioners Guide to Business Continuity Management* following a review in 2006. In Singapore, TR 19 *Technical Reference for Business Continuity Management* is a well-used best-practice mechanism for BCM managers, while in the United States NFPA 1600 *Standard on Disaster/Emergency Management and Business Continuity Programs* has been in existence for a number of years.

The publication of BS 25999 was in response to a market-wide demand from both public and private sectors for a formal standard that would introduce a level of consistency to the discipline, provide clarity as to what constituted BCM, establish accepted terminology and definitions, and create a means of benchmarking between companies, industries and regions.

The market demands clarity and consistency, accepted terminology and a means of benchmarking on BCM.

A proactive, non-prescriptive approach to business continuity encourages organizations to find the solutions that best meet their own needs.

In November 2006, BSI published BS 25999 Part 1, which provided a guide to business continuity best practice. Kevin Brear, business continuity manager on the information and security group, practice protection, at Deloitte & Touche, described it as “a paradigm shift for the business continuity industry in the UK”. While there are a number of organizations and societies with an interest in business continuity, he believes that “by placing it under the stewardship of BSI, the standard is, and can clearly be seen to be, an independent document”.

The standard provides guidance and recommendations on business continuity best practice. “The goal is to enable organizations operating in any sector, including industrial, commercial, public and voluntary, to understand, develop and implement business continuity within their operations,” says Mike Low, director of BSI British Standards.

“Rather than a prescriptive document, BS 25999 seeks to encourage organizations themselves to find the solutions that best meet the demands of their own risk framework. By facilitating a more proactive approach to business continuity, the standard places the control firmly in their hands.”

BS 25999 has introduced a consistent approach to business continuity best practice founded upon proven methodologies. It enables organizations to clearly demonstrate to the markets they serve that they have a robust BCM strategy in place which can now be measured and also benchmarked against the strategies of competitors. “As a benchmark to set UK plc, I think it is excellent,” says Mr Caddick at Marsh.

As the standard becomes more established, companies are increasingly able to use BS 25999 as a marketing tool as it provides a mechanism for evidencing competitive advantage and a means of enhancing their reputation and brand perception as a secure supplier or provider of goods or services. “With BCM also now playing an increasingly prominent role in the tender process,” says Mr Low, “companies can provide, by adopting a British Standard, measurable evidence of the existence not only of a plan, but also an effective, robust strategy which is embedded into the culture of their organization.”

Reassuring the market

“The arrival of the British Standard for BCM has marked a significant milestone in establishing business continuity as a basic commonsense approach to managing a business – and managing it responsibly,” says Mr Mellish at Sainsbury’s. “In my view, the British Standard has provided the credibility and gravitas to make it a standard requirement in future corporate governance legislation. The sooner senior executives recognize this and address it then greater assurance can be provided to all of their stakeholders.

“The standard will also ensure a more consistent approach is applied,” he continues, “and this will in turn assist in benchmarking and provide insurance companies with a more effective way of measuring the effectiveness of a company’s ability to minimize the impact of any major incident.”

The universality of BS 25999 also provides international appeal for the standard. Mr Sierwald of Phoenix Continuity Services in Sydney believes that the very fact that BS 25999 is a good fit with most BCM approaches in Australia makes it of real interest. Commenting on its potential impact on the wider Asian market, he adds: “My experience with organizations in India is that those which act as service providers to ‘Western’ companies are keen to have a certifiable standard as extra assurance for clients who choose to outsource business processes.”

“BSI has seen a lot of interest from Asia and other areas around the world,” concurs Mr Crask, “which suggests to me that countries outside of the EU wish to comply with the standard to demonstrate their reliability and security to foreign investors.”

“We are seeing a growing awareness of business continuity, and BS 25999 has played a part in this,” believes Mr Beesley at TDG. “My view is that over the next few years, particularly in the industry in which I operate, business continuity will become increasingly important because of the influence of BS 25999 and the focus that this has given people.”

If this proves to be the case, then the question every company must ask itself is: What does not having adopted the standard say to the market about how we run our business?

The standard will provide a more effective way of measuring the effectiveness of a company’s ability to minimize the impact of major incidents.

The role of standards

A standard provides a mechanism for facilitating the proactive implementation of best practice. The principles of any British Standard are based upon good management practice, and set out clear and unambiguous provisions and performance objectives.

A proactive, non-prescriptive approach to business continuity encourages organizations to find the solutions that best meet their own needs.

“There are no rules laid down,” explains Mike Low, director of BSI British Standards, “but rather a series of recommendations and guidelines which provide an organization with the flexibility to hand-pick those elements and procedures which best fit their specific requirements.”

In the development of any formal standard, a national committee is established which includes representatives from government, business, consumer groups, manufacturers, suppliers, academic institutions, trade associations, regulators and societal interest groups.

“Only by achieving consensus across such a diverse range of practitioners,” believes Mr Low, “can a standard successfully embody what is considered best practice for that particular sector.” A draft of the standard is then placed into the public domain for consultation. All comments and responses are reviewed by the committee and the standard is amended where necessary. Only then, when approved, will the standard be published.

In order to ensure that each standard continues to remain current, it undergoes a process of maintenance and review whereby it is updated, revised or, if necessary, withdrawn.

“BSI is not seeking to create an array of stand-alone standards,” says Mr Low, “but rather a family of interrelated standards.” In compiling each standard, the process takes into consideration other related standards. Effort is made to provide a level of uniformity across the documents, which enables organizations to implement additional complementary standards more easily.

How BSI can help

Standards matter. They contribute at least £2.5bn each year to the UK economy and play a key role in enabling innovation, improving competitiveness, increasing reliability, ensuring safety, improving accessibility, controlling quality, managing risk and improving business performance.

As the world's first national standards body, BSI British Standards has a globally recognized reputation for independence, integrity and innovation. Part of the BSI Group operating in 86 markets worldwide, BSI British Standards serves the interests of a wide range of industry sectors, as well as government, consumers, employees and society overall, to make sure not just British but European and international standards are useful, relevant and authoritative.

BSI champions UK interests at home and abroad and is an incubator of many of the world's leading standards. It is the national gateway to all the European and worldwide standards bodies promoting fair trade, technology transfer, economic prosperity and security.

Several publications describe the benefits of using standardization to achieve broader organizational and national strategic objectives. Information about these is available from BSI British Standards.

To find out more about how BSI can help you, visit the website at www.bsigroup.com or email britishstandards@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001

Fax +44 (0)20 8996 7001

www.bsigroup.com

© The British Standards Institution

raising standards worldwide™

