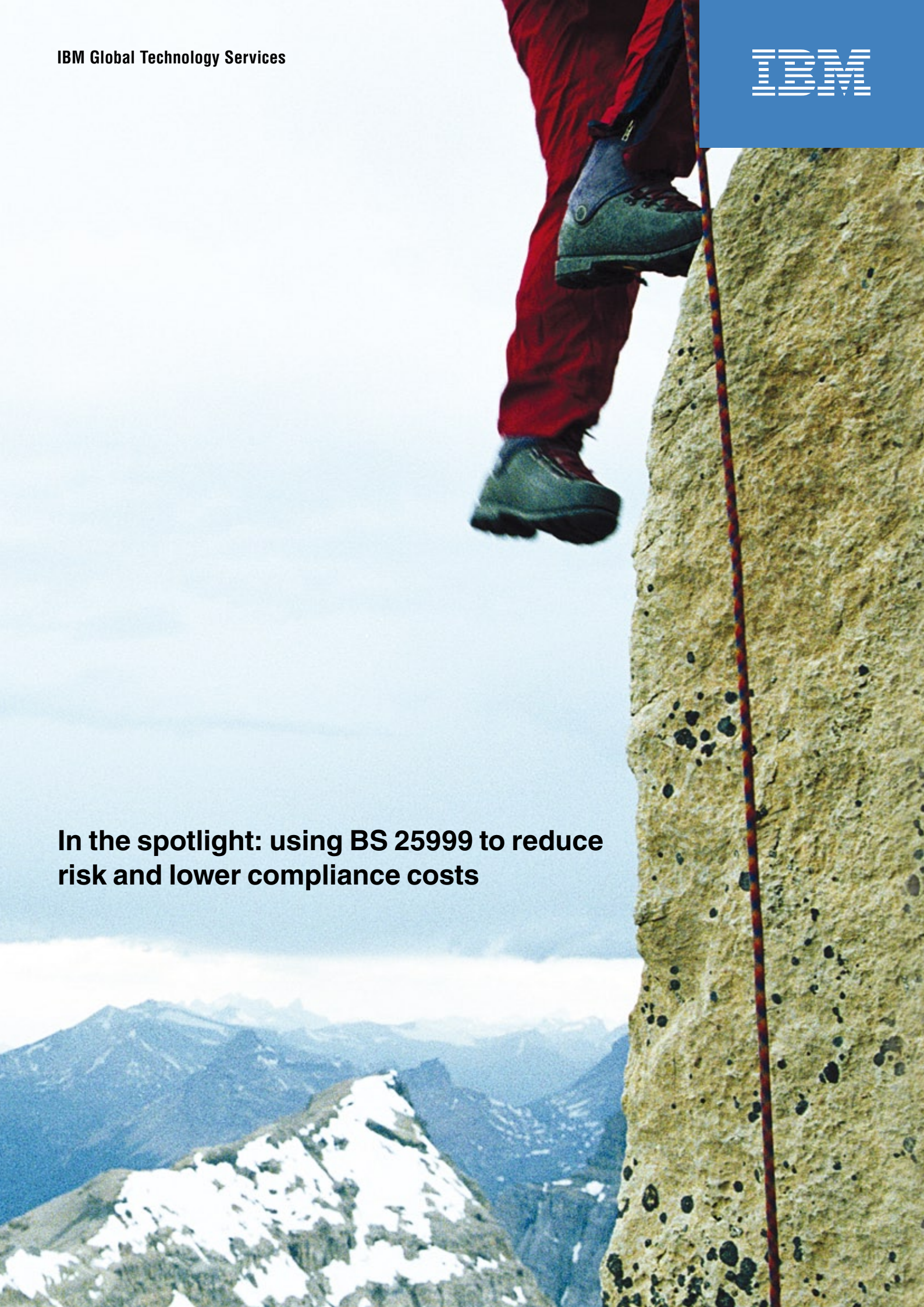
IBM Global Technology Services



In the spotlight: using BS 25999 to reduce risk and lower compliance costs

Synopsis

Organisations today have to comply with an ever-increasing number of regulations and legislation, a subset of which imply a requirement for effective business continuity and risk management. Adopting the new British Standard BS 25999, arguably the most comprehensive benchmark against business continuity good practice available, could reduce compliance costs by providing a single independently accredited certification that satisfies the business continuity requirements of most regulations and legislation.

Furthermore, an effective business continuity management system can deliver other benefits. For example: through organisational improvements identified and enacted through its implementation, reduction of operational risk and a competitive advantage in the future, where BS 25999 certification may be sought by customers as some assurance of supply chain continuity.

Risk? What risk?

IBM has published the findings of a major new study, 'Balancing risk and performance with an Integrated Finance Organization', of over 1,200 chief financial officers (CFOs) and senior finance executives from 79 countries worldwide, which concludes that a surprising number of enterprises are not well prepared to handle the impact of a major risk event to their organisation.

The study indicates that in the past three years 62% of enterprises with over $5 billion in revenue encountered a major risk event. When a major risk event did occur (such as strategic, operational or geopolitical) 42% of these enterprises were not well prepared for the event.

> *"The failure of suppliers and supply continuity is the number one risk factor of 28% of organisations."*
>
> "Managing Risk in the Supply Chain: A Qualitative Study," AMR, January 2007

Who owns risk?

CFOs are increasingly becoming 'owners' of risk management within their enterprise and sharing ownership with the CEO. The same study found 61% of CFOs are expected to lead risk management within their organisation, followed by CEOs (50%), chief technology officers (27%) and chief risk officers (19%). A 2007 Economist Intelligence Unit Business Resiliency Survey highlighted that "76% of respondents agreed that operational risk should be an issue that involves all business units and 69% took a similar view about business continuity planning".

> *"43% of CFOs think that improving governance, controls and risk management is their top challenge."*
>
> CFO Survey, IBM Business Consulting Survey

Regulation, regulation everywhere…

Organisations today sometimes see themselves as drowning in a sea of regulations and legislation, perhaps with good cause. Businesses today are arguably navigating the most intense period of regulatory change in history. Under such relentless tidal pressure, the next new wave of legislation or regulation can make it seem like a fight to keep a head above water, making it hard to view this onslaught in a positive light. But of course legislation and regulations can be a good thing. They should offer a framework in which society and free markets can thrive by establishing a clear set of rules that bring stability and reduce risk. We have a history of regulation and legislation aimed at improving corporate governance and risk management, for example with the Sarbanes Oxley Act (2002, USA) and its equivalents in other jurisdictions (such as Canada, Japan and the European Union), but why so much regulation now and will it never cease?

> *"58% of organisations say that regulators have significant influence over their business continuity planning."*
>
> "Business Resilience: Ensuring Continuity in a Volatile Environment," Economist Intelligence Unit, March 2007

We've never had it so good…

We are fortunate to live in a period of unprecedented global growth and prosperity, which owes much of its success to the phenomenon of globalisation. Globalisation has been driven over decades by a number of forces, each of which has been more important than other forces at different points in time:

- *The first major driver for globalisation was the free flow of trade goods, and progress continues as new trade agreements are brokered between nations, and internationally, at each round of talks at the World Trade Organisation.*
- *The second driver was the free flow of capital, and today vast sums move between financial markets, and barriers to international investment and foreign ownership of firms are much reduced.*
- *The Internet has also played a part, enabling the free flow of information globally, although some nations, Canute-like, still seek to deny the inevitability of this particular rising tide.*
- *Finally, today we are struggling to come to terms with the globalisation of labour markets and the free 'flow' of labour, either in terms of people moving across national borders to find work or the work moving to where there is a lower cost supply of skilled workers. The International Monetary Fund estimates that the collapse of the Iron Curtain and the opening of India and China (together with population growth in these areas) have delivered a fourfold increase in global labour supply in the last 25 years[1] – a powerful force for globalisation indeed.*

…Or so risky?

> *"77% of CEOs say the level of complexity in their business is higher than it was three years ago."*
>
> "Globalization and Complexity: Inevitable Forces in a Changing Economy", PriceWaterhouseCoopers, 2006

Globalisation is a good thing; however it creates an increasingly complex set of interrelationships, be they economic, political, social, technological or trade-based, and with this increasing complexity comes a new fragility or sensitivity to disruption that has potentially unforeseen and far-reaching consequences if not properly addressed.

> *"Complexities in supply chain management are dramatically increased by today's shift toward emerging global markets for material sourcing, manufacturing, distribution and product development."*
>
> Source: 2006 Value Chain Study, SCM Institute for Business Value in conjunction with AC Nielsen, Economic Times of India and IBM Global Benchmarking

The International Monetary Fund stresses the growing economic interdependence of countries worldwide through increasing volume and variety of cross-border transactions in goods and services, free international capital flows, and more rapid and widespread diffusion of technology. But globalisation is not just increasing economic interdependence. For virtually every organisation, globalisation is increasing the interdependence, integration and interaction between people and organisations in disparate parts of the world. Even if you believe that your own organisation controls its own destiny, the chances are that you are wrong. For example, your organisation probably relies on another company for cleaning, guarding, catering, mechanical facilities and electrical maintenance, and so on, even if your own operations, customers and first tier suppliers are entirely based in your home country, which is an increasingly rare situation even for small businesses.

> *"It does not matter who or what caused the disruption – you still pay."*
>
> Source: Supply Chain Disruptions and Corporate Performance, Vinod R. Singhal, College of Management, Georgia Institute of Technology, June 2005

[1] "The Globalisation of Labour", Chapter 5, IMF World Economic Outlook, April 2007

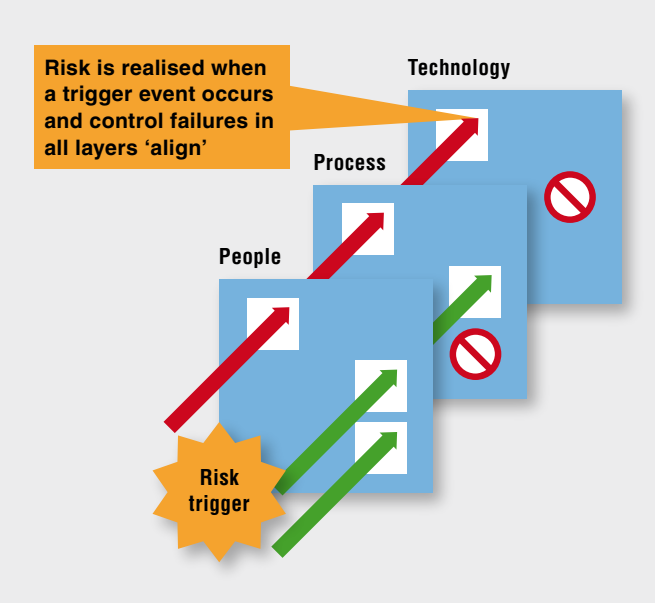
Accidents are inevitable (?)

In 1984 Charles Perrow published a paper entitled "Normal Accidents, Living With High Risk Technologies", which led to something called Normal Accident Theory, also referred to as System Accidents. The theory postulates that failure in one part of a system (material, human, or organisation) may coincide with the failure of an entirely different part of the system and that in complex systems these possible combinations are practically limitless. An unforeseeable combination can cause cascading failures of other parts of the system and where the complex system is also tightly coupled then these cascading failures can accelerate out of control, confounding attempts to regain control and recover the situation. The conclusion of Normal Accident Theory is that accidents are inevitable in complex and tightly coupled systems – "normal". Whilst this theory was focussed upon the safety of industrial processes, such as the production of chemicals or nuclear power, it has some relevance to any highly complex and closely coupled system and we can postulate that this is what organisations today and their global supply chains are increasingly becoming. In other words, we had better be prepared to handle disruption and not just within operations under our own direct control but also in our supply chains.

> *"It is that supply chain issue that scares us most, if I am blunt. Just do the probabilities. If only 50% of companies have a business continuity plan at all[2] (further statistics lead to some doubt as to whether it is a good continuity plan), that means by the time you have gone three links down the supply chain there will be roughly a 90% probability of failure. And if that failure is on a critical supplier that means that entire supply chain is prejudiced because of one link inside the chain."*
>
> Bruce Mann, Director of Civil Contingencies, Cabinet Office, speaking at the BSI Business Continuity Global Launch in London on 30 October 2007

In particular, the rising threat of an influenza pandemic has raised supply chain continuity concerns in many industries, including retail, industrial and distribution. However, evaluating end-to-end supply chain continuity can be a mammoth task. Wal-Mart reportedly has in excess of 60,000 organisations in its global supply chain, for example.[3]

Risk controls are applied in layers and it's only when control failures align and a trigger event occurs that disasters happen



[2] Business Continuity Management Survey Report, Chartered Management Institute, March 2007

[3] Various sources including "The Greening of Wal-Mart's Supply Chain", Supply Chain Management Review, 2007

Regulations and legislation can be a good thing

Regulation and legislation can be good; they establish a framework within which society and free trade can thrive based upon the ground rules laid out, which should offer stakeholders a margin of stability and reasonable levels of risk. A nation state without the effective rule of law is almost certainly not a good place to invest or indeed to live. As the business environment changes in response to all sorts of drivers, new risks arise and one route to mitigation at national and international level is through new legislation and regulation.

The global financial market is a good example of an increasingly complex and tightly coupled system where vast sums of money move from organisation to organisation and country to country in the blink of an eye. As technology is leveraged to allow money to move quickly and electronically between organisations like some sort of massively complicated and fast game of musical chairs, institutions can remove slack (we are equating money with chairs in this analogy) from the system because they can transact secure in the knowledge that necessary money will arrive from another counterparty just in time, which is great right up until the music stops and there are not enough chairs to go around.

This is a form of systemic risk, arising where financial institutions rely upon other institutions in the supply chain to deliver the money needed in time to meet their commitments – but what if someone does not deliver that money on time? Central banks used to step in and provide liquidity but the amounts that could be needed are increasingly eye-watering. As the system becomes more integrated and interrelated between different organisations it becomes more complex and more closely coupled. The risk of an unforeseen combination of events resulting in a failure that cannot be corrected in time to avoid a serious problem rises. In short, the risk increases and regulation is needed to mitigate it.

Basel II is an international banking accord that seeks to manage this risk by ensuring that financial institutions hold reserves that are appropriate to the level of risk taken, including the IT and infrastructure operational risk that underlies all banking processes. More reserves (money or liquidity) in individual institutions help maintain a systemic capacity to allow correction without cascading consequences, limiting the systemic risk. Basel II is enacted in national regulations for banks by each participating national regulatory body. These regulations require both bank risk management processes and risk outcomes to be evaluated.

However, each national regulator might interpret Basel II slightly differently and take the opportunity to apply additional regulation appropriate to their own situation, and this is where compliance gets challenging for organisations operating under different regulatory regimes in different countries around the world, as many financial institutions do today. A typical large financial institution might find itself complying with the same Basel II base requirement modified by the national regulator in the UK, USA, Hong Kong, Singapore, Germany, Japan, and so on, with the possibility that one or more of these jurisdictions might just choose to go a little further than was set out in Basel II.

The European Union Data Protection Directive (concerned with privacy) is another example that is not specific to the finance sector, where the initial EU Directive has been enacted in some countries in significantly different ways, complicating operational decision-making and compliance for organisations operating across national boundaries.

The compliance challenge

The compliance challenge is twofold. First one of scale; there is an enormous and ever-increasing amount of legislation and regulation, both nationally and internationally. Secondly, each piece of legislation / regulation requires careful interpretation to understand its implications, some of which might require material changes to your organisation's governance, processes and reporting in any number of areas.

On top of these external challenges, most organisations are still organisationally, functionally and technically disaggregated, which can make it harder and more costly to comply with regulations. Compliance would therefore benefit from becoming part of a holistic or enterprise risk management and governance approach that ensures consistency and avoids unnecessary duplication of effort. Clearly, business continuity management is a subset of risk management and should integrate with your organisation's larger risk governance arrangements.

> *"Firms with above average… governance… Had more than 20% higher profits than firms with poor governance following the same strategy."*
>
> Source: Peter Weill and Jeanne W. Ross, Harvard Business School Press, 2004

Standards can help keep compliance costs down through simplification

> *"Businesses put separate and typically manual processes and controls in place to monitor and report on compliance. This leads to large amounts of duplication causing high admin overhead costs (up to 30% according to Towergroup)."*
>
> Dr. Jürg von Känel, IBM T.J. Watson Research Center, 2005

Occasionally, a new standard comes along that meets a need in the marketplace, is comprehensive, thoughtfully constructed and just makes sense. Such a standard can add real benefit by providing a common language with which to talk about a particular topic and a clear benchmark against which adopters can achieve and maintain an independently accredited certification.

In the area of information security, the British Standard BS 7799, which subsequently transformed into ISO 17799 and continues to develop with the ISO 27000 series of standards, is one such example. From an early point in the standard's history its compliance benefit was clear. The Department of Trade and Industry (now the Department for Business Enterprise & Regulatory Reform) has stated that "The use of ISO/IEC 17799 and BS 7799 can help businesses to meet the information security requirements of the Data Protection Act."[4] The UK Financial Service Authority's Systems and Controls Handbook section on Information Security also offers an example of how this standard aids compliance:

> *"A firm should ensure the adequacy of the systems and controls used to protect the processing and security of its information, and should have regard to established security standards such as ISO17799 (Information Security Management)."*
>
> FSA Handbook, SYSC 13.7.8, November 2007

The new standard BS 25999 should be similarly effective in the area of business continuity management in offering legislators, regulators, insurers, external auditors, customers and other influential stakeholders a much simpler assurance in the area of an organisation's business continuity management capability and operational risk readiness. In other words, BS 25999 certification may increasingly been seen as an acceptable demonstration of compliance with the business continuity requirements and expectations of regulations and legislation, thereby potentially lowering compliance costs.

BS 25999 is set to take off

The British Standards Institution (BSI) reported that, whilst most draft British Standards draw and average of 250 downloads, BS 25999-1 logged some 5,000 downloads following its publication in November 2006; 20 times more than normal[5]. When BS 25999-2 was released in draft for public consultation (August 2007), over 13,000 responses were received.[6]

BS 25999 has not simply been created overnight, having developed from the Business Continuity Institute's Good Practice Guidelines (first created in 2002) into the BSI's Publicly Available Specification (PAS) 56 (2003). The standard has been supported over the years of its development by a number of influential stakeholders including the UK government (Cabinet Office, Department for Business, Enterprise and Regulatory Reform, FSA), the Association of British Insurers, the Institute of Directors, the Institute of Internal Auditors, the Institute of Risk Management and the Business Continuity Institute, to name but a few. So there is wide backing for what is a well thought out standard and evidence of intense market interest and need. The UK government hopes that adoption of BS 25999 will improve the UK's resilience through increasing the percentage of organisations with effective business continuity arrangements and therefore lowering the supply chain risk. For large organisations with extended supply chains BS 25999 can also offer reassurance and help ease the burden of assessing supplier resilience. The stage is set for rapid uptake of BS 25999 and progression to international standard.

[4] Information Security: BS 7799 and the Data Protection Act, Achieving Best Practice in Your Business, DTI, 2004

[5] Avaluation Consulting, LLC and BSI Management Systems America, 2007

[6] Neil MacArthur, Director of Strategy, IDL Worldwide, 2007

Business benefits can flow from BS 25999

Organisations may realise benefits from adopting BS 25999 in a number of different ways:

- *Potential competitive advantage through demonstrated ability to continue product or service delivery*
- *Reduction of risk to revenue flows*
- *Reduction of costs associated with recovery from unplanned business interruptions*
- *Better positioned to require BS 25999 certification of critical suppliers and consequent cost savings and risk reduction in supply chain continuity assurance*
- *Reduction in business continuity compliance costs associated with a fragmented response to regulatory and legislative requirements*
- *Performance improvements and cost savings identified and realised as an indirect consequence of implementing an effective business continuity management system.*

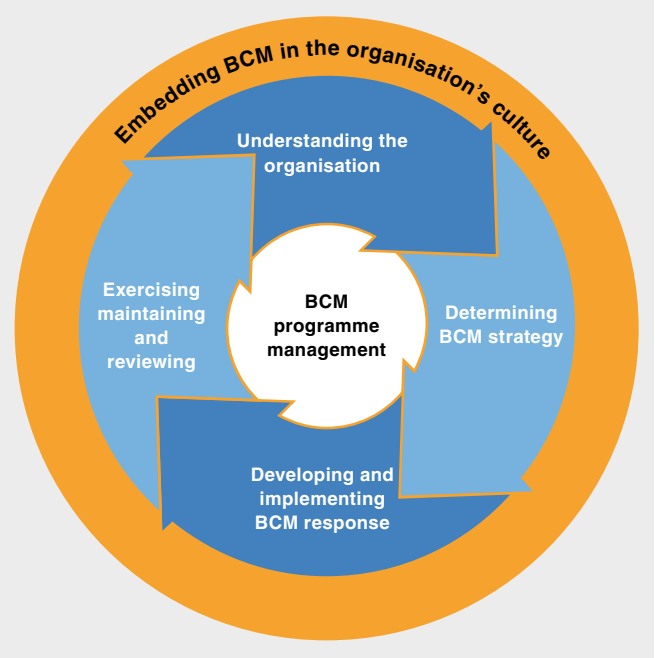
It may be better to proactively adopt BS 25999 rather than wait until your organisation is required to do so by your customers or other stakeholders.

IBM can help

IBM Business Continuity and Resiliency Services has over 40 years of experience in the business continuity and disaster recovery industry and extensive global coverage with over 150 global resiliency centres in 55 countries offering in excess of five million square feet of disaster recovery space and over 40,000 work area recovery positions. In addition to helping customers recover during service invocations, our crisis response team has accumulated onsite crisis management experience at over 70 major crisis events in more than 40 countries over the last decade, responding to events such as the tsunami, hurricanes, volcanoes, World Trade Center and other disasters where the scale of the event threatens communities and extraordinary support and assistance is required.

We have a large international team of dedicated business continuity consulting professionals and, as you might expect, have a well-established business continuity and risk management methodology backed by years of experience in helping organisations of all types and sizes to overcome their business continuity challenges and drive positive change in their businesses. Our methodology is constantly updated to reflect IBM's thought leadership and changing marketplace requirements such as BS 25999, NFPA 1600, APS 232, PAS 77 and other relevant standards and regulations worldwide. Our people undertake a rigorous internal programme to certify as IBM consultants, which helps us to ensure consistency and quality of service delivery anywhere in the world and each person signs up to an ethical code of conduct because we value the trust you place in us and will always seek to act in your best interests.

The business continuity management lifecycle[7]



We can apply our consulting expertise to support the development and implementation of a business continuity management system for your organisation, regardless of its size, complexity and international footprint. Whether you just need help in structuring or performing a business impact analysis, defining and integrating business continuity risk governance, delivering awareness training, facilitating exercises, or any other single aspect of business continuity, we can help. We pride ourselves on our innovative and pragmatic approach to understanding and meeting your requirements and our ability to act as agents for positive change.

Case Study – Risk Quantification

Working with a global bank, IBM determined that three business continuity risks accounted for 80% of the client's operational risk for information security. The findings had a 99.97% confidence level, which satisfied Basel II requirements under the AMA approach.

> *"This research highlights IBM's thought leadership in the operational risk management and risk modelling space."*
>
> Vice President, Information Security Services, large global bank.

The bank wanted to determine which risk areas required prioritisation within its Information Security Services business function. There were 85 separate threats to evaluate. IBM developed an operational risk model by examining business processes, the supporting application and resources, and the 85 risk events that impact the business processes.

For each threat, the data included the probability of occurrence and dollar-range impact based on severity of the event. IBM quantified operational risks for all processes, which included expected and unexpected losses.

According to the bank Vice President of Information Security, "The approach can be used to access the effectiveness of different countermeasures (process countermeasures, technology countermeasures, insurance, etc.) to manage operational risks and optimally allocate investments in countermeasures. This project also identified potential over-allocation of regulatory capital if resource allocation for risk management is based on expected losses, as opposed to estimated loss distribution."

[7] Source: British Standard, business continuity management – Part 1: Code of practice, BS 25999-1:2006, BSI, November 2006

How do I get started?

After reading BS 25999-1 and BS 25999-2 you might be forgiven for feeling a little daunted at the prospect of trying to get your own organisation into shape. But perhaps you are further along the road to certification than you might think.

Start by asking IBM to undertake a quick BS 25999 healthcheck to determine what you have in place already that will support your business continuity management system, what you need to develop and a prioritised roadmap of how to prepare for BS 25999 certification. An IBM BS 25999 healthcheck can help you start your journey to certification – within a couple of weeks you should know where you are now, where you are going and how to get there. It'll give your programme a flying start and IBM can continue to speed your journey to an effective business continuity management system, applying our unmatched experience and expertise, globally and locally, to meet your objectives and transform business continuity and risk management in your organisation.

If BS 25999 isn't on your business continuity radar just yet, IBM has a series of services designed to help formulate and implement business continuity processes and procedures wherever you currently sit in the business continuity lifecycle:

Business continuity expert briefing

IBM offers an initial expert briefing to discuss enhancements to risk management and business continuity policy, potentially by implementing BS 25999-based practices and procedures, with supporting processes and controls, to enable cost reduction and improved responsiveness.

Business continuity stakeholder workshop

An IBM expert facilitated workshop to present and align BS 25999 and business continuity best practice with your stakeholders' priorities. As a result of the workshop, you, your stakeholders and IBM can agree a roadmap of next steps. Whether the priority is evaluating your organisation to identify areas of risk, helping to define a business continuity policy, implementing the policy, or evaluating the effectiveness of an existing business continuity management system, the roadmap will be tailor-made to help meet your organisation's specific challenges and objectives.

If you are concerned about other standards or regulations, we can adapt our Assessment approach to incorporate these for you. For example if you are more interested in the FSA Guidelines on Business Continuity or the BCI Good Practice Guide, or if your business is operating in Australia under APS 232 or one of the other countries with its own national standards or regulations then the chances are that IBM can help.

To arrange for a BS 25999 healthcheck or initial meeting, or simply to discuss your business continuity management challenges with one of our experts, please go to **ibm.com**/services/uk/index.wss/it/igs/a1006911, call +44 870 010 2526 or e-mail govrisk@uk.ibm.com

Author

Robin Gaddum

Robin Gaddum is a managing consultant with IBM and is responsible for leading the UK consulting practice for IBM Business Continuity and Resiliency Services.

IBM United Kingdom Limited
PO Box 41
North Harbour
Portsmouth
Hampshire
PO6 3AU

The IBM home page can be found on the Internet at **ibm.com**

* IBM, the IBM logo and ibm.com are trademarks of International Business Machines Corporation in the United States, other countries, or both.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates. Copying or downloading the images contained in this document is expressly prohibited without the written consent of IBM. All products and/or services are subject to availability.

This publication is for general guidance only.

© Copyright IBM Corporation 2008.
All Rights Reserved.

BUB03001-GBEN-00