Director
BUSINESS WISDOM MAKING EXCELLENCE A HABIT

Achieving resilience

How to mitigate risk and protect your business

In association with bsi.

Group Editor Lysanne Currie
Writer Tom Nash
Chief Sub Editor Robert Sly
Art Director Chris Rowe
Commercial Director Sarah Ready
Advertising Director Jo McGraw
Client Sales Manager Fiona O'Mahony
Head of Commercial Relations Nicola Morris
Production Manager Lisa Robertson
Chief Operating Officer Andrew Main Wilson

Editorial 020 7766 8950
director-ed@iod.com
Advertising 020 7766 8900
director-ads@iod.com
Production 020 7766 8960
production@iod.com
Institute of Directors 020 7839 1233
www.iod.com

How to manage risk in your business

Every organisation faces different risks throughout their lifetime. These can range from minor threats to large crises that can threaten your reputation and ultimately your business.

By being prepared you can mitigate risk, assure stakeholders you can continue to operate following an incident, and fulfil your regulatory and statutory obligations – helping you to minimise the impact on your reputation, business and brand. In fact, having a comprehensive risk management system in place can help you acquire new customers, attract staff and/or obtain external funding.

For more than a century we have been challenging complacency to help our clients perform better, reduce risk and achieve sustainable growth. BSI pioneered standards to support better risk management including information security (ISO/IEC 27001) and business continuity management (ISO 22301).

This booklet, the third in a series, explains how BSI helps organisations to anticipate and review potential risks that business both can and cannot influence. Whether the challenge lies in protecting information, ensuring you understand legislation such as anti-bribery law or you just want your business to survive in the face of adversity, BSI can help. Please take advantage of our exclusive offers for IoD members on the back cover.

Howard Kerr *Chief executive, BSI*

recycle

Published by Director Publications Ltd for the Institute of Directors, 116 Pall Mall, London, SW1Y 5ED. Opinions expressed do not necessarily reflect IoD policy. The IoD accepts no responsibility for views expressed by contributors.

In search of security

Effective processes can help organisations maintain sound corporate governance, manage risks and give them a competitive edge

Corporate governance is under intense scrutiny, with the UK – traditionally seen as a leader in this field – persistently seeing trouble on its own watch. In the last few months alone, shareholder revolts over executive pay and a spate of corporate scandals have shaken public confidence in the system by which British business operates.

Governance, as defined by Sir Adrian Cadbury's corporate governance code in the 1990s, is "the system by which companies are directed and controlled". Good governance requires rigorous supervision of the management of a company, ensuring that business is done competently, with integrity, and with due regard for the interests of stakeholders.

Good governance for listed companies is laid down by the latest UK corporate governance code. But having a "highway code" does not necessarily make people good drivers. That's where standards come in, helping businesses of all sizes to achieve and maintain best practice.

Anne Hayes, head of market development at BSI, says a central standard demonstrating best practice in governance is being developed by BSI and is scheduled to launch early next year (see p10). "But there are already many standards in related fields, including risk management, business continuity and information security," she explains.

- 85% of BSI clients who adopted information security built stakeholder confidence
- 79% experienced faster recovery speed from incidents having implemented BCM
- 83% of BSI business continuity clients cited enhanced reputation as the key benefit
- 64% of BSI health and safety clients reduced incidents while 49% made cost savings
- 99% of organisations meet information security targets after they have implemented ISO/IEC 27001

Sources: BSI Excellerator Research 2011 and Erasmus University study

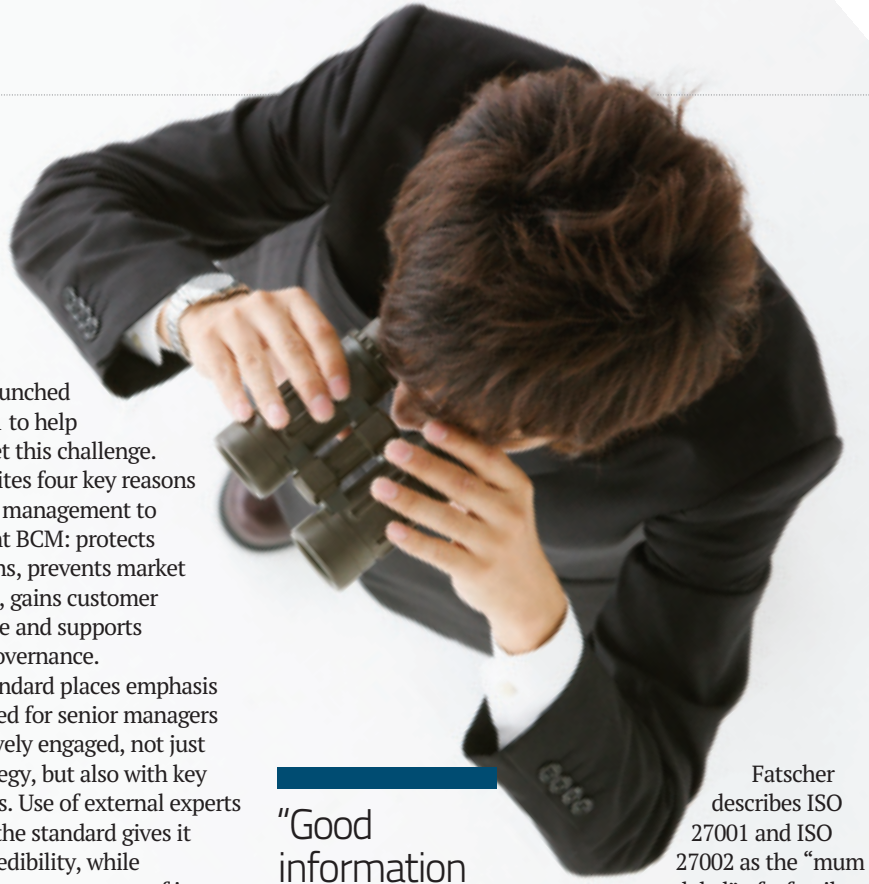
Hayes counters the impression that such standards are adopted solely by large companies as defensive measures, to help avoid disasters and reputational damage: "They're equally applicable to SMEs and should be implemented in a way that suits an organisation. They shouldn't be seen as negative. They can encourage customers to seek opportunities to do business with you."

MANAGING RISK

"A key risk management standard is ISO 31000, which enables organisations to 'establish the context' of their risk in order to reveal and assess the nature, complexity and diversity of the risks across business disciplines," explains Hayes.

BUSINESS CONTINUITY

Dr David Hitchen, global scheme manager for business continuity management (BCM) at BSI, says: "Organisations need a BCM system that meets the highest standards."



BSI has launched ISO 22301 to help them meet this challenge. Hitchen cites four key reasons for senior management to implement BCM: protects reputations, prevents market share loss, gains customer confidence and supports general governance.

The standard places emphasis on the need for senior managers to be actively engaged, not just with strategy, but also with key operations. Use of external experts to create the standard gives it market credibility, while independent assessment of it shows good practice in BCM to stakeholders.

"The BCM standard is flexible, so SMEs can implement it to the areas of their business where it is needed," says Hitchen. "It can give a competitive edge to those providing critical services."

PROTECTING INFORMATION

Information is key to the operation of most businesses. The discipline of information security has evolved to contribute to the wider goal of good governance, says David Fatscher, BSI's sector development manager for ICT. In fact, he prefers the term information governance.

> "Good information governance must stretch from the boardroom to the switchboard"

Fatscher describes ISO 27001 and ISO 27002 as the "mum and dad" of a family of standards designed to help businesses manage and protect valuable information assets, giving confidence to stakeholders.

The former is the only certifiable international standard to define the requirements for an information security management system (ISMS). It adopts a method for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an ISMS. "This standard is applicable to businesses of any size or sector," says Fatscher.

"Good information governance must stretch from the boardroom to the switchboard."

CASE STUDY 1

Business as usual

Vodafone has adopted a business continuity management standard to cope with any disruption to its activities

Vodafone UK is part of a global communications business with more than 370 million customers. The group operates in more than 30 countries and has partner networks in many more. As a major, technology-dependent company, with millions of personal customers and thousands of business and public sector clients, it is vital for it to carry on business as usual regardless of any disruption, large or small.

"Business continuity is of triple importance to us," says Roger McLoughlin, business continuity manager for Vodafone UK (pictured). "First, we must ensure we carry on our own business; second, we're an integral part of our customers' business continuity plans because our products and services are vital to them being able to carry on if they suffer an incident; and third, our network is part of the UK's critical national infrastructure – there would be damage to the country as a whole if we go down."

Vodafone has long taken the issue of business interruption seriously. Twenty years ago its emphasis was on disaster recovery, but it has since broadened its approach to adopt the discipline of business continuity management (BCM). In 2008, it became the world's first mobile telecommunications operator to achieve BSI's breakthrough standard for BCM, an internally recognised management framework that added consistency and credibility to Vodafone's BCM programme.

"The aim is that when we have any sort of incident, our customers won't notice a thing"

The company is being audited for the successor standard, ISO 22301, which updates and builds on its predecessor, providing a framework for continual improvement and the ability to demonstrate to stakeholders that its BCM programme meets international best practice.

"Our interest has been in achieving best practice," says McLoughlin. "We've found that moving towards certification has helped in this, so the process makes good business sense for us." He says that BSI certification also carries great weight in the eyes of customers, "which is of great value to us", giving them assurance that Vodafone is operating to the highest BCM standards, constantly monitoring and reviewing its procedures, and being independently audited.

He is acutely aware that assurance about BCM forms a key part of most bids and contract renewals. "We're aware of what our competitors are doing in this area and of customer requirements – and we are also asking it of our own suppliers."

McLoughlin says the new standard has helped Vodafone to achieve clarity about who its key stakeholders are and to communicate with them more effectively. "It pushes you to take an integrated and thorough approach, with proper KPIs [key performance indicators], audits and reviews to ensure that you are measuring up."

Vodafone's BCM has had huge support from senior management, ensuring it is now fully integrated within wider governance and risk management strategies. It is also aligned with the compliance function, recognising that increasingly onerous legal and regulatory requirements have to be fulfilled. "One of the things that has helped us has been to rationalise our business policies into two categories – 'may need to know' and 'need to know'," continues McLoughlin. "BCM is one of a handful of policies that is in the 'need to know' group, so all employees have to build awareness of it."

"Moving towards certification makes good business sense for us"

The company surveys staff every two years to see how well they understand BCM and their role if any disruption to normal activities occurs, whether a major disaster or a minor setback. It has also developed an online training module for everyone, helping them view BCM as integral to their job. It is now piloting new software to make the interface with staff more user-friendly.

"We want to ensure we're at the leading edge of BCM, using it to manage everyday incidents, not just disaster recovery, and to embed best practice into every part of our business," says McLoughlin. "The aim is that when we have any sort of incident, our customers won't notice a thing."

CASE STUDY 2

Secure in the knowledge

Capgemini uses an information security standard to boost its resilience, reassure clients and outperform competitors

Capgemini is a global leader in consulting, technology, outsourcing and local professional services. It operates in 40 countries, 100 languages and employs 120,000 people worldwide.

Security is a key building block upon which the group depends, protecting its assets, resources and people – and those of its clients – and ultimately providing it with a competitive edge.

With this in mind, Capgemini has adopted a comprehensive approach to information security, introducing measures to address the confidentiality, integrity and availability of information it needs to hold to carry out its business operations effectively.

Important security drivers include traditional threats such as accidents, natural disasters and deliberate attacks, but also new challenges such as increased government regulation and tougher requirements from the payment card industry.

"If we fail to comply we risk heavy fines and severe damage to our reputation," says Bill Millar, head of security for Capgemini's information outsourcing services business in the UK.

Security is also a major concern for clients. "Without robust systems in place, we could lose business," continues Millar. "ISO 27001 enabled us to focus on our customers' security requirements rather than simply complying with commercial practices. That's why we went down the standards route. We wanted to achieve best practice and be able to prove that to ourselves, but we also wanted to demonstrate it to both commercial and government clients who are insisting on it."

Capgemini's Dutch and Indian operations had been the first to adopt the information security standard ISO 27001 and "they were clearly getting benefit from it", says Millar. For example, in putting together bids and tenders the company "was producing reams of paper on each occasion, spending huge amounts of time and money proving our infosec (information security) credentials. We thought, 'let's just get certification' and release staff to do other jobs."

By early 2008, Millar had created a business case to justify the required investment and won the approval of his board. "It wasn't difficult. In fact, the board asked: Why aren't we doing this already?" he says. He used Capgemini's own UK Security Forum as the control structure for the project and recruited a dedicated two-person team.

BSI was identified as the preferred external auditor, and began by defining the parameters of the project. "BSI advised us to reduce our scope and approach the task in bite-sized chunks, which made it much more manageable."

First, the company's risk approach was clarified; then it started to communicate with staff and gain buy-in from account leads; next, it brought its security documentation up to date, adding new areas such as mobile security; and finally it began a cycle of thorough security audits, systematically covering the areas initially listed.

In November 2008, Capgemini's UK outsourcing business achieved its goal of having an information security management system certified to ISO 27001. It has since gone on to recertify itself in 2011, with 10 of its 14 UK sites now covered.

Future goals for Capgemini include certifying the final four sites to the standard, as well as spreading the word about its benefits to other parts of the group – Polish and German arms of the firm have already signed up.

Millar lists a host of benefits (see box, left). But above all, he says: "It's not just about looking after data; it's about caring for people and physical security, too."

> "It's not just about looking after data – it's about caring for people and physical security, too"

THE REWARDS

Bill Millar lists eight benefits of using ISO 27001:

- Improved security for Capgemini UK and its clients
- Assurance to new and current clients
- Demonstrable best practice
- Enhanced security awareness and enthusiasm among staff
- Better security documentation
- Security now seen as an integral part of Capgemini's UK outsourcing business
- Upgraded security reporting process
- Board-level value, creating operational buy-in and financial backing

Future perfect?

A new standard is being developed to help businesses demonstrate best practice in governance

The word governance is bandied about by businesses of all sizes and in all industries, in the public sector and in the media, but who knows what it really means?"

So asks Michael Faber, BSI governance committee chair and a member of the executive committee at the Institute of Operational Risk.

Helpfully Faber, with reference to the BSI committee work, builds on Sir Adrian Cadbury's definition (see p4), to come up with: "The system by which a whole organisation is directed, controlled and held accountable." He and the committee add: "Governance is not an ivory tower issue for the board, but must be delivered throughout the whole organisation. Take ethics… if they are held at board level, they must also be practised by all staff."

Faber and the committee have added the words "and held accountable" to Cadbury's mantra. "Responsibilities can be spread, but accountability should be clear, and often it isn't," he says, noting that it should be measurable and demonstrable both internally, "to benchmark yourself", and externally so that external regulators, shareholders and other stakeholders "can see you are exercising good governance".

A new standard to help businesses show best practice in governance is being developed by BSI through its consensus process, and is due to be launched in 2013. BS 13500 will enable organisations to understand what they need to do to ensure good governance. It will tell those external to any organisation what they can expect to see in place to ensure effective governance is operating. Faber says the framework represents "a defining moment" in response to governance issues. It will be an independent standard for UK organisations developed through work with professional bodies, government and business.

"The challenge is for it to be applicable to organisations of all sizes and sectors," he says. "Our aim is to provide succinct best-practice guidance and signposts to other good work."

Faber says good governance helps to protect organisations and allows them to take advantage of opportunities. Business is about taking risks, he says. But there is a difference between measured risks and taking them carelessly. "If they manage risk well, they'll be more successful. Their biggest risk is to take no risks," he says.

"If companies manage risk well, they will be more successful. Their biggest risk is to take no risks"

HAVE YOUR SAY

● As with all our standards, a draft of the new BSI governance standard will be available to the public during September to allow an opportunity to influence its content. Give your views at… **www.bsigroup.com/drafts**

BEATING BRIBERY

The UK Bribery Act came into force in July 2011, making it an offence for commercial organisations to fail to prevent people associated with them from committing bribery on their behalf.

BSI published BS 10500 to help organisations implement an anti-bribery management system. It takes into account both UK law and internationally recognised good practice, and it can be used both in the UK and overseas.

To comply with the standard, an organisation must apply a series of measures, including the adoption and communication of an anti-bribery policy, training and guidance for employees, appointing a compliance manager, undertaking risk assessment and due diligence, controlling gifts and hospitality, implementing procurement, commercial and financial controls, and instituting reporting and investigation procedures.

Compliance can help establish that a business has introduced reasonable and proportionate measures designed to prevent bribery from happening.

Managing risk isn't about a policy in a desk drawer...

1. You have robust plans in place
   But do you test **ALL** of them regularly?
2. You evaluate your supply chain risks
   But are **ALL** your suppliers as prepared as you?
3. You have written policies and procedures
   But do **ALL** your staff know what's expected of them?

It's essential to establish the foundations, whatever the risk. But to achieve real stakeholder confidence and maximize reward make sure your organization embeds its risk management thoroughly.

For a few more critical questions to help understand how effective your organization is in managing risk, visit www.bsigroup.com/iod

Exclusive offers for IoD members*

FREE TRIAL for business continuity assessment tool	£100 risk management training voucher	20% saving on a BSI risk assessment	20% saving on BSI's risk management guides

*Terms and conditions apply, visit www.bsigroup.com/iod

Find out more:
Visit **www.bsigroup.com/iod**
Phone **0845 080 9000**

bsi.

...making excellence a habit.™