Beyond recovery

The broader benefits of Business Continuity Management

A BSI whitepaper for business

bsi.

...making excellence a habit.™

Business Continuity Management (BCM) has become a vital discipline, bringing benefits that go far beyond helping organizations recover from unexpected disruptions. Today, the broader benefits of BCM can best be harnessed through the international management system standard ISO 22301

Executive summary

- BCM is a critical business discipline, helping organizations prepare for, and recover from, a wide range of unexpected incidents and unwelcome interruptions.
- The importance of recovery – the most obvious purpose of BCM – can hardly be overstated. Thousands of businesses have saved time and money by getting back up and running quickly after a disruption – and some even owe their survival to it.
- Despite the 'recovery rationale' for BCM, many business leaders are yet to embrace the discipline – while others are implementing it piecemeal or poorly.
- Organizations are missing out on more – much more – than simply a speedy return to 'business as usual' in the event of disruption. BCM can provide a rich return on investment (ROI) without the occurrence of a disaster.
- A robust BCM process offers many advantages, from lower insurance premiums and process improvements to business expansion and brand enhancement.
- At a strategic level, BCM can play a key part in organizations' risk management processes, answering to the demands of today's onerous regulatory and corporate governance requirements.
- It is time for the 'C-suite' to wake up to the full range of BCM benefits and the true ROI the discipline offers.
- Help is at hand: the management system standard ISO 22301 provides the ideal framework for implementing a BCM system.
- Many organizations, both large and small, have already implemented ISO 22301, harnessing a host of benefits from this multi-faceted standard.
- Some have maximized the benefits by achieving independent third party certification to ISO 22301, enabling them to demonstrate 'badge on the wall' best practice in this vital area.
- There is a growing trend for companies to be required to hold certification to ISO 22301 by powerful private and public sector customers – or risk losing business.

First, stay in business

First and foremost, Business Continuity Management (BCM) 'does what it says on the tin'. BCM helps organizations to prepare for, and recover from, a wide range of unexpected incidents and unwelcome interruptions. In times of crisis, it is crucial in keeping them up and running.

The Business Continuity Institute (BCI) puts it like this: "Business Continuity is about taking responsibility for your business and enabling it to stay on course whatever storms it is forced to weather. It is about 'keeping calm and carrying on'."

It continues, "Building and improving resilience in your business is a critical aspect of BCM. It's about identifying your key products and services and the most urgent activities that underpin them. Then, once that analysis is complete, it is about devising plans and strategies that will enable you to continue your business operations and enable you to recover quickly and effectively from any type of disruption, whatever its size or cause. It gives you a solid framework to lean on in times of crisis and provides stability and security."

The importance of business recovery, the most obvious purpose of BCM, can hardly be overstated. Take the case of Vodafone UK, a major technology-dependent company with millions of personal customers and thousands of business and public sector clients. The company says business continuity is of triple importance to it: firstly, it must ensure it carries on its own business; secondly, it is an integral part of its customers' BCM because its services are vital to them; and thirdly, its network is part of the UK's critical national infrastructure – so there would be damage to the UK as a whole if it went down.

Blind to the benefits?

Thousands of businesses, both large and small, have saved time and money because their BCM system has proved effective in getting them back up and running quickly after a disruption. Some even owe their survival to it.

But despite the powerful 'recovery rationale' for BCM, many business leaders are yet to embrace the discipline – while others are implementing it piecemeal or poorly. As Lyndon Bird, the BCI's Technical Director explains, "The obvious benefit of BCM doesn't always convince the C-suite. It's not that they're stupid – far from it – these are intelligent people or they wouldn't be leading organizations in the first place. They can see the dangers of a flood, cyber attack or terrorism, for example, but they may not think it's likely to happen to them, nor see BCM as a cost-effective measure if it does."

Repeatedly reminding business leaders about how risky the world is can be counter-productive, argues Bird. "They already know this and they're accustomed to accepting a degree of risk."

Bird believes that excessive scaremongering can obscure the fact that BCM offers more – much more – than simply a speedy return to 'business as usual' in the event of disruption. By embedding BCM, organizations can unlock a host of additional business benefits and bring a healthy boost to their 'bottom line'. "The C-suite is much more interested in these tangible business benefits – carrots are more effective than sticks," he says.

Continuity concerns

- 77% of organizations are "extremely concerned" or "concerned" about unplanned IT and telecom outages
- 73% are concerned about data breaches
- 73% are concerned about cyber attacks
- Use of the Internet for malicious attacks is again number one with 73% of respondents seeing it as a major trend that requires a business continuity response
- 63% of respondents see the influence of social media as a major trend affecting reputation management and crisis communications
- Supply chain disruption and the underlying trend of increasing supply chain complexity are lead concerns in manufacturing and retail sectors.

Source: The Horizon Scan 2014 by the BCI, in association with BSI, which surveyed 690 organizations in 82 countries.

Payback time

Investments in BCM can more than pay for themselves even without the occurrence of a major disaster. Rainer Hübert, Managing Consultant at HiSolutions, a Berlin-based consultancy specializing in IT governance and risk management, lists a number of ways in which BCM can provide a healthy return on investment (ROI), including reduced insurance premiums, lower interest rates on loans, greater process efficiency and, in particular, an increase in contracts won or retained.

In a powerful paper, first presented at the 2013 BCM World Conference, Hübert argues that insurers can be persuaded to take account of a company having a BCM programme in place, calculating that, in the event of an incident, damage will be contained and the company's revenues will recover much more quickly. "This could result in a lower insurance premium," he says.

A similar argument applies to the interest rate charged on bank loans. The rate reflects, among other things, the risk of the borrower defaulting on the loan through bankruptcy or delaying repayments because of a major crisis. If the company has an effective BCM programme in place, it stands a better chance of avoiding such a crisis, or at least surviving it and recovering more quickly, resulting in a lower risk of credit default. "This can be presented to the bank and become part of negotiations regarding interest rates. If successful, the negotiated rates may be lower than without the BCM programme," says Hübert.

On process efficiency, he continues, "When discussing BCM, you consider contingency plans and processes, and how to work without urgently needed resources after a catastrophic event. This can lead to the creation of new ideas, not only to implement a workaround process in case of a disaster, but also to improve day-to-day processes in normal situations." He says the cumulative effect of small improvements can easily repay the total yearly running costs of a BCM programme.

Best practice

Lorna Anderson, Business Continuity Technical Expert at BSI, agrees. "A lot of organizations rumble along by doing things 'the same old way', but implementing BCM gets them to examine the whole lifecycle of the business and look at themselves with a fresh pair of eyes. It forces them to create process maps, to identify areas of confusion and overlap and to ask themselves 'why are we doing things this way?'" she says.

If cost-savings are on one side of the ROI 'coin', the ability to drive revenue growth is on the other. "In some cases, having a robust BCM process in place is mandated by customers, so without it, you're not in the game," says Anderson. This is particularly likely in highly-regulated industries such as banking and financial services, and in public sector organizations that are subject to the Civil Contingencies Act 2004, which requires them to adhere to a coherent framework for emergency planning and response.

In many cases, the main driver for BCM is an entirely voluntary desire to achieve and demonstrate best practice, reassuring customers and other stakeholders. "This is the key for business decision-makers," says BCI's Bird. "Where BCM really scores is in helping to retain existing customers and win new ones."

Most important is reassuring customers regarding security of supply. Without BCM in place, asks Bird, how can customers be sure that their suppliers will still be able to fulfil contracts in the event of a business interruption? "The word 'reliability' is one we don't use enough," he says. "If your company is reliable, it will go a long way to inspiring confidence in customers and become a trusted brand."

Manufacturing icon, Vauxhall: Decisive drivers for BCM

Vauxhall UK's journey to BCM certification began in 2011 when John Jack, manager responsible for business continuity planning across the whole of GM UK, was tasked with creating a BCM system for the firm's four key sites at Luton and Ellesmere Port. In May 2012, it achieved certification to the British standard for BCM BS 25999, before successfully transitioning a year later to the new international standard, ISO 22301.

Jack explains that there were three decisive drivers for the company's decision to strive for certification to ISO 22301.

Firstly, GM has a global corporate policy that requires Vauxhall to have BCM plans in place. "Whist it doesn't specifically require ISO 22301, we knew that by achieving certification we would fully comply with GM's policy," says Jack.

Secondly, Vauxhall supplies fleet organizations that are covered by the Civil Contingencies Act 2004. "These customers are obliged to ask us about our BCM provisions and they must have assurance that we are certified," he says.

Thirdly, Vauxhall believes that achieving certification to ISO 22301 is simply the right thing to do, helping to create a 'thinking culture' at the company, where risks are identified and preventative measures taken: "We don't just respond to business interruptions, but question things that might occur before they actually happen."

Vauxhall has found that certification to ISO 22301 has fully addressed its three specific business needs. Jack explains: "If the business went down there would be severe financial and reputational costs, so certification enables our GM parent company to be satisfied that we've got a BCM mentality."

"We're also able to demonstrate to our fleet customers that we've got a robust BCM process in place – and that it has been validated by an independent third party in BSI. We can use this in our non-fleet business too – it's a reassurance to all our customers that we're serious about always being 'open for business'."

In addition, Vauxhall has used certification to reinforce its culture of continual improvement. "The whole concept of BCM is based on prevention as well as response," says Jack. "So, whilst we have a structure to be able to respond effectively to a business interruption, we also have a built-in mentality of risk awareness. ISO 22301 isn't just a nice certificate on a desk – our folks really live this."

Phil Millward, GMUK HR Director with overall responsibility to the board for the BCM system, concludes, "A disaster can strike any organization, big or small, at any time. And it can arrive in a variety of ways, from a utility failure or a parts shortage to terrorist bomb or flood. But when it does, you need to have a process in place to mitigate the impact and return to 'business as usual' as quickly and as painlessly as possible. For us at Vauxhall ISO 22301 fulfils this critical business need."

Service sector leader, Scottish Friendly Assurance Society Ltd: Assured best practice

Scottish Friendly Assurance Society Limited is the largest mutual life society in Scotland.

In October 2013, Scottish Friendly achieved certification to ISO 22301, after smoothly transitioning from its predecessor, BS 25999, and following its 2012 certification to ISO/IEC 27001, the international standard for Information Security (IS).

The motivation for many organizations in acquiring certification to ISO/IEC 27001 or ISO 22301 is often externally driven, for example, being mandated by a key client as part of contract negotiations. But this was not the case for Scottish Friendly, where the main driver was its own desire to adopt best practice, continually improve its IS and BCM systems and protect the interests of its members.

A key issue was the need to maintain the availability of its IT systems. The organization has moved from a direct selling model to direct marketing and, more recently, e-commerce, increasing its reliance on its IT infrastructure.

Given the objective of adopting best practice across the Society, Scottish Friendly believed its scope for certification should cover the whole organization. As Jeff Wilson, Head of IT, explains, "It was important that an all-inclusive approach was taken, where all staff felt engaged in the process. We have a lot of highly capable people and were determined to own the development of our management systems."

Wilson continues, "We also saw information security and business continuity as mutually dependent activities with considerable overlap."

From day one, there was total commitment from the Executive Management Team to both certification projects. They also benefited from the "gentle steering" of consultant Ultima Risk Management, while further support came from BSI, which was selected as the certification body.

Whilst there was already a strong IS and BCM culture among staff, the projects have brought greater consistency and involvement across all parts of the organization, embedding both disciplines and clarifying staff responsibilities.

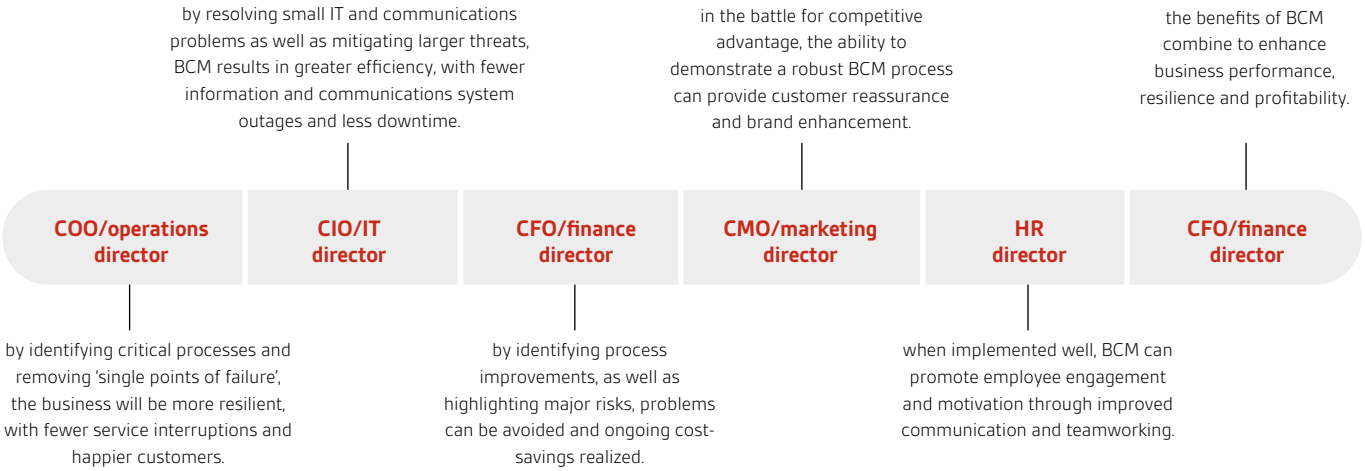
The Society has been able to reduce audit preparation time, as many of the processes established to meet the requirements of the two standards are easily recognizable to auditors.

Another benefit has been the introduction of an online tool for incident reporting, which has helped to streamline corrective and preventive actions.

Overall, its certifications to ISO/IEC 27001 and ISO 22301 has made Scottish Friendly more resilient – and demonstrated this to stakeholders. Fiona McBain, Chief Executive, concludes, "Scottish Friendly attaches great importance to ensuring the confidentiality, integrity and availability of customer information. Providing first class customer service is at the heart of what we do and building upon best practice in all our business operations helps us achieve this."

Benefits across the board

Gary Hibberd, Managing Director of management consultancy Agenci Information Security, describes how BCM can offer solutions to various directors around the boardroom table, in both large and small companies:



Company directors and officers can also reduce the legal and regulatory risks and liabilities they face in a personal capacity through the added protection that BCM can provide.

Governance and risk

At a strategic level, BCM has grown in stature and sophistication, playing a key part in organizations' risk management processes, answering to the demands of today's onerous regulatory and corporate governance requirements – for example at engineering and construction group Costain.

Good governance for listed companies is laid down by the UK Corporate Governance Code, which states: "The board is responsible for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives. The board should maintain sound risk management and internal control systems".

But having a 'highway code' does not, in itself, make people good drivers. Julian Thrussell, Senior Consultant at Ultima Risk Management (URM), a consultancy specializing in business resilience standards, says few organizations have a truly rounded understanding of risk across business continuity, information security, physical security, financial risks such as interest rates, exchange rates, and product risk like e-commerce or launching products. "Risks are often calculated in silos, slewed to reflect department goals and as such are very difficult to compare," he says.

Thrussell continues: "Supply chains are poorly understood, creating single points of failure that can be catastrophic, while IT outsourcing and online hosting is often undertaken in blind faith."

Simple measures – such as agreements with partners to share facilities in the event of a disruption – are often overlooked in favour of expensive options. "Why do so many people think they need a 'dark site' when serviced-office suppliers such as Regus are available?" questions Thrussell

He adds, "Business continuity exercises are often inappropriate to risks faced, with the highest risks often neglected because they are perceived as dull, compared to the more dramatic, but less likely to occur, earthquakes and plane crashes."

This is where BCM comes in – to support the business in properly assessing the potential impact of a variety of risk outcomes, including 'black swan' events that are not widely anticipated. In practice, the board must ensure that a company's major risks are identified, and build appropriate resilience into its business model and operational processes.

Engineering exemplar, Costain: Building resilience

Costain is a long-established British engineering and construction group, today employing around 4,000 people.

Through its ISO 22301 certification, the company demonstrates to both internal and external stakeholders that it has a robust management system in place to cope with a business disruption.

Costain is a powerful advocate for management system standards in general. As well as ISO 22301, it holds multiple certifications, including: ISO 9001 (Quality), ISO 14001 (Environment), BS OHSAS 18001 (health and safety), BS 11000 (Collaborative Business Relationships) and ISO/IEC 27001 (Information Security).

Tony Blanch, Costain's Business Improvement Director, says the reasons for adopting each standard have varied. While many have been partly client-driven, the decision to adopt the BCM standard ISO 22301 was "totally internal", he says. "The question of how robust we were was being raised regularly at board level, and we needed more tests to find out. It took us about two minutes to decide to go for it – it was a 'no brainer'."

Costain has consistently harmonized standards implementation with its broader business strategy. For example, its implementation of ISO/IEC 27001 and ISO 22301 has fitted perfectly with the group's wider risk-based strategy to increase resilience and boost performance. "The standards have given us a structure to identify risks to our business and manage these, rather than try to defend ourselves against every theoretical threat," explains Blanch. "The process has become more thorough, systematic and easier to maintain.

The company has found that the vital ingredient is not financial, but harnessing the commitment of management and staff. "There's no need for standards to cost a lot of money," says Blanch. "The biggest investment is in people's time – the more effort you put in as a company, the more you get back."

BSI has played a key role in supporting Costain's success. In the case of several standards, BSI carried out a pre-audit inspection "to make sure we were heading in the right direction," says Blanch. "They've always been readily available to give us help whenever we've needed it."

Costain is justifiably proud of the wide range of management certifications and the tangible benefits that the standards help deliver as a result of independent assessment by BSI. As for the future, while the global construction industry continues to change rapidly, the company can demonstrate that it has robust management frameworks in place to drive business performance, reduce risk and achieve sustainable growth.

"We have definitely used standards effectively to differentiate ourselves from the competition," says Blanch.

Raising the standard: ISO 22301

It is time for 'the C-suite' to wake up to the full range of benefits that BCM offers. BSI has pioneered the international BCM system standard ISO 22301 to help them address this challenge by creating a BCM system that meets the highest standards.

ISO 22301 provides a framework for continual improvement and the ability to demonstrate to stakeholders that a BCM programme meets international best practice. It puts great emphasis on the need for senior management to be actively engaged, not just with strategy, but also with key operations.

Implementation of the standard also requires the whole organization to become involved, improving communication, clarifying employee roles and generating greater engagement and enthusiasm among employees.

Many organizations have already implemented ISO 22301, harnessing the benefits of operating a robust BCM system.

The requirements of the standard are fully scalable, making it just as easy for SME's, as for large organizations, to implement a BCM system that conforms to it, as the experience of Lettergold Plastics highlights.

Organizations can maximize the benefits of BCM by achieving independent third party certification to ISO 22301, enabling them to demonstrate 'badge on the wall' best practice to internal and external audiences. BSI's Anderson says many companies have found certification has helped them achieve best practice, as well as carrying great weight in the eyes of customers. "It gives them assurance that they operating to the highest BCM standards, constantly monitoring and reviewing procedures, and being independently audited."

Lettergold Plastics, the growing enterprise: Not just a 'tick in the box'

Newmarket-based Lettergold Plastics Ltd is a typical dynamo of the UK economy, a growing SME that currently employs around 25 staff. The engineering company specializes in injection moulding, contract packaging and, in particular, domestic water treatment products.

In May 2008, Lettergold became only the third company in the UK to become certified to the BCM standard BS 25999, and it has since transitioned to ISO 22301.

Andy Drummond, Lettergold's Managing Director, explains that the catalyst for certification to the BCM standard came from prospective customers. "We originally sought certification to fulfil a tender requirement and that's happened several more times since," says Drummond.

But building a management system based on the standard has turned out to be much more than just a 'tick in the box' on tender forms. It has provided Lettergold with tried and tested methods of minimizing the adverse impact of an incident on its operations, as well as protecting the interests of its customers and other stakeholders.

Above all, it has reinforced the confidence of customers seeking certainty of supply from Lettergold. "The BCM system is a great reassurance to them and to ourselves. Previously, recovery plans probably only existed in my head. Like many small firms, we were over-reliant on a few individuals, especially the business owner," says Drummond.

Lettergold has used its BCM system to ensure access to key utilities, as well as for testing the strength of its supply chain for more specialized materials. For example, it has tested alternative sources for industrial chemicals normally imported from Belgium. "We ran a real exercise, acting as if our Belgian supplier's factory had burned down," explains Drummond.

Lettergold engaged a specialist consultant, Adrian Austin of Hereford-based Atlantic Consultants, to help it implement ISO 22301. "It's all too easy to create a big, fat BCM manual for a small firm, which then gets left on the shelf because it's not relevant to day-to-day activities," says Austin. "What's needed are simple mechanisms and paperwork that captures the key points – a 'what do we do when something goes wrong' manual."

"BSI was extremely helpful too," says Drummond. "They carried out a pre-audit inspection to give us some additional guidance, clarifying issues we might have misinterpreted and giving us feedback on changes we needed to make to meet the requirements of the actual audit."

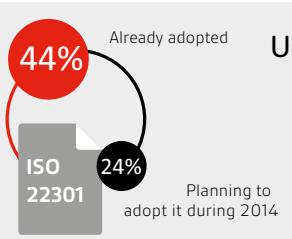
"Now, whenever we introduce something new into our processes, we consider the implications for business continuity – we ask ourselves 'what can go wrong?' It can be very helpful to have this risk management mindset," concludes Drummond.

Prepare for take-off

Companies are increasingly being required by powerful private and public sector customers to have BCM in place – or risk being refused new contracts and excluded from tenders. HiSolutions' Hübert expects that companies delivering products or services on time-critical terms will, "sooner or later, become part of a supply chain protected by ISO 22301 certification. They will only remain part of the supply chain if they can prove the existence of a working BCM programme – ideally with an ISO 22301 certificate."

Hübert, predicts a "snowball effect" for ISO 22301 within global supply chains, with more companies becoming required to hold certification and also mandating it for their own suppliers. "This will lead to an avalanche of ISO 22301 certifications," he predicts. "Without it companies will lose bids and even lose existing contracts because of failed compliance with their customers' purchase regulations."

URM's Thrussell observes that while at present the take-up of BCM is "reasonable", it is lower than that of information security management, due to fewer customers currently mandating it.



Use of the international standard for business continuity management (ISO 22301)

"This is not particularly logical given the considerable risks attached to business continuity – I can really see the demand for ISO 22301 building," he says.

Reiterating four key drivers for business leaders to implement ISO 22301 – customer confidence, reputational risk, market share loss, and governance expectations – BCI's Lyndon Bird urges companies to make the most of ISO 22301 and steal a competitive advantage. "It makes sense to have a robust BCM system, get it certified and give confidence to your stakeholders," he concludes.

Find out more about ISO 22301 with BSI

Call: **0845 080 9000** or visit:

www.bsigroup.com/bcm

bsi.

BSI UK
Kitemark Court
Davy Avenue, Knowlhill
Milton Keynes, MK5 8PP
United Kingdom

T: +44 845 080 9000
E: certification.sales@bsigroup.com
bsigroup.com