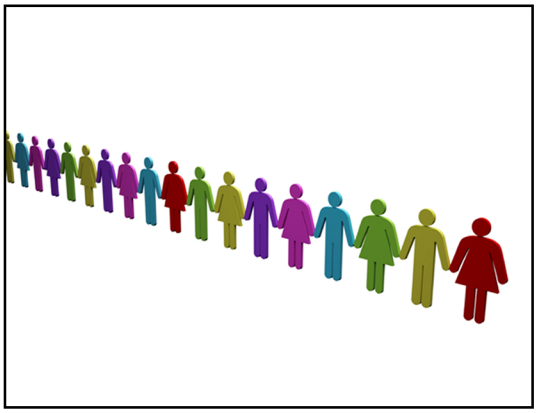
the business continuity
JOURNAL
Volume Three, Issue Three



the business continuity JOURNAL

Welcome

WELCOME to the Business Continuity Journal, the peer reviewed journal for the business continuity profession worldwide.

We would appreciate your continued feedback on the publication in general, or on any specific paper. Send this via e-mail to editor@businesscontinuityjournal.com

Call for papers

The next issue of the Business Continuity Journal will be published in May 2008. Authors are invited to submit papers on any subject related to business continuity management by 31st March 2009.

Send either the completed paper, or a synopsis, to the journal's editor, David Honour, at editor@businesscontinuityjournal.com Papers must not have been previously published elsewhere.

Papers will be assessed by the Business Continuity Journal's peer review panel as to suitability for publication.

Business Continuity Journal website

As well as receiving the Business Continuity Journal four times a year, subscribers gain access to a subscriber-only website which provides an archive of all issues of the journal as well as access to other editions (for example UK subscribers can read and download the North American and International versions). To access the subscriber website visit http://www.businesscontinuityjournal. com

If this is not your copy of the Business Continuity Journal you can subscribe at the above website or simply email subs@businesscontinuityjournal.com for more details. The journal is available at the following rates depending on your preferred delivery method:

Delivery by e-mail (PDF): £95 / $US 180 / 140 euro
CD via postal service: £145 / $US 275 / 210 euro
Printed copy via postal service: £195 / $US 370 / 285 euro

Copyright

ISSN

ISSN 1752-4539

The Business Continuity Journal peer review panel

The current peer review panel is as follows:

Publisher and other contacts

Publisher
Portal Publishing Ltd,
PO Box 1393,
Huddersfield,
HD1 9TN
England

Telephone: +44 1484 300750

Editor
David Honour
editor@businesscontinuityjournal.com

Subscriptions
subs@businesscontinuityjournal.com

Future publication dates

Volume Three Issue Four: May 2009

Volume Four Issue One: September 2009
Volume Four Issue Two: December 2009
Volume Four Issue Three: March 2010
Volume Four Issue Four: June 2010

Contents

As a result of all these activities, BS 25999-2 is coming under the close scrutiny of organizations being certified, the certification bodies and UKAS. The overall consensus is that BS 25999-2 has been constructed to a very high standard and has generally been very well received by these three groups. As with any new standard, there are inevitably some areas of confusion and misunderstanding and there are aspects of the standard that are more difficult to comply with than others. In this paper, the author will address the following:

- Management system requirements

- Business impact analysis.

THE COMPONENTS OF A RESILIENCE CAPABILITY

Pages: 33-41

Author: Alan Elwood

Abstract: Resilience is defined as the 'ability of an organization to resist being affected by an incident' (1) and ultimately may be said to be the aim of business continuity management. Why else spend the time and resources implementing BCM within an organization if it is not going to help that organization overcome adversity? True some pain will be felt. There will be some disruption, and not everything will go to plan but if resilience is demonstrated then 'victory' will surely follow. Clearly within BCM talk is of resilient businesses but in the wider context, resilience is used in more nebulous terms such as labelling social groups as resilient communities. What is interesting about this is that we routinely use the word resilience in many contexts but do we truly understanding what it comprises of? Defining the component parts of resilience, the benchmark of BCM success, is therefore an important issue. This paper defines the components of resilience. It develops a framework used by the military to define fighting power (2) and applies it to resilience. In so doing it explores how, if any of the three component parts is missing or ineffective, no organization can claim to have true resilience.

DELIVERING IT SERVICE CONTINUITY MANAGEMENT - A CASE STUDY

Pages: 42-48

Author: Stephen Nuttall and Mark Moody

Abstract: The Department for Work and Pensions (DWP - the largest government department in the UK) and EDS, one of its key IT service providers have, together with other suppliers, transformed the delivery of IT services into the world class IT Infrastructure Library (ITIL) model. This has required a move from a traditional business continuity and disaster recovery deployment, into an IT service continuity management (ITSCM) model – effectively embedding business continuity for IT services into an end to end IT service approach.

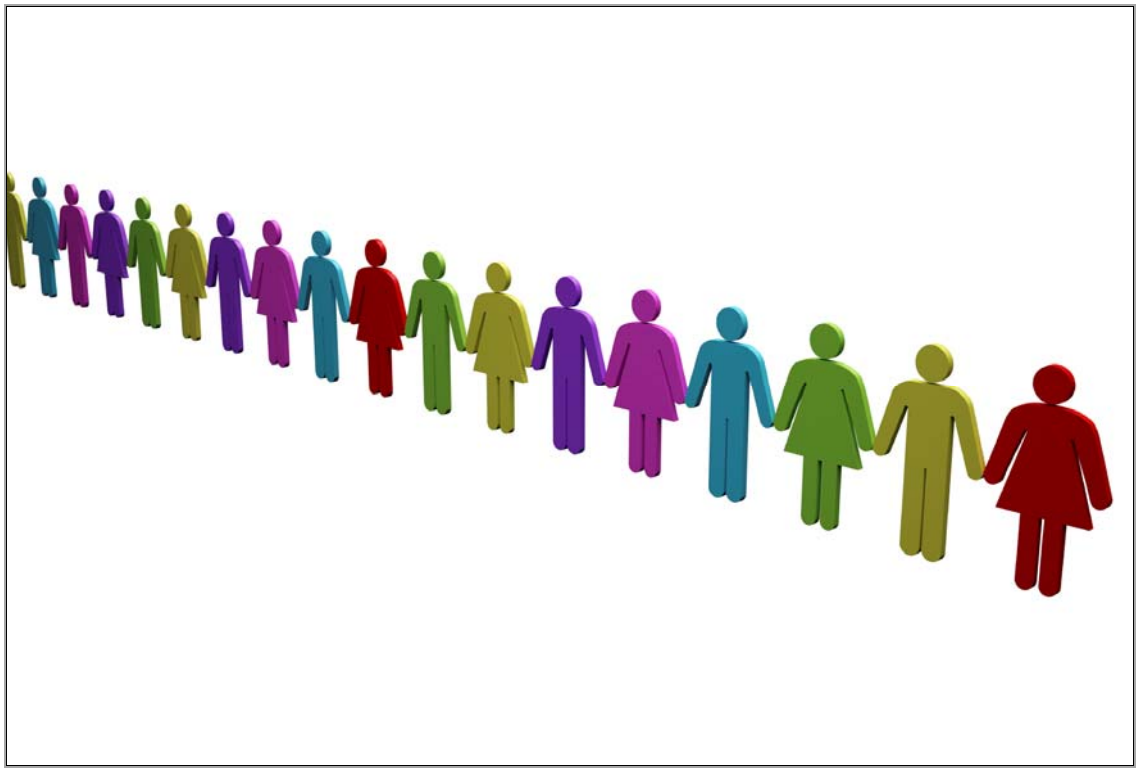
This paper is about how EDS and the DWP worked together to develop and deliver a new model and how we met and overcame the challenges in order to do it.

RESEARCH ROUNDUP

Pages: 49-60

Abstract: A brief summary of commercial and academic business continuity research which has been published between September 2008 and January 2009

EMBEDDING BCM IN THE ORGANIZATION'S CULTURE



AUTHOR: Andy Mason, BSc, MBCS, CITP, MBCI, Head of Business Continuity, PricewaterhouseCoopers LLP

ABSTRACT: The concept of embedding business continuity in an organization's culture is not new. Over the years it has developed through the various iterations of the BCI's Good Practice Guidelines, was then taken up by PAS 56, and featured in the original Business Continuity Management Lifecycle diagram.

With the onset of BS 25999, embedding BC into an organization's culture has undergone a change in its positioning in the BCM Lifecycle, both within the Code of Practice in Part 1 and as a measurable component of the Specification in Part 2. But what does 'embedding in the culture' mean, what do you need to do, and how do you know you have achieved it? And, most importantly for certification purposes, how can you measure such a potential intangible?

This paper seeks to explore the requirements of BS 25999, and discusses various ways to 'embed BCM within your organization's culture'.

BS 25999 – a catalyst for change

In the development of BS 25999, one of the early discussions revolved around the long-established BCM Lifecycle and whether it should be changed. As a testament to its creators, there actually was very little that could or needed to be changed, and the key components maintained their position. However, it was recognised that all elements of the Lifecycle had a place in embedding business continuity, and as such 'embedding' should move from being a 'spoke' in the old BCM Lifecycle 'wheel' to the 'tyre' wrapped around it, recognising that everything we do within our business continuity management programmes can, and should, be used to embed BC into our organizations' cultures. Consequently, the BCM Lifecycle diagram was changed and forms an essential role in the framework of the Code of Practice.

One of the greatest challenges in developing the new standard was that the target audience was potentially vast and that the language used had to be both inclusive and scalable. This was recognised in the preamble at the head of section 10 on page 40 of the Code of Practice where it says: "To be successful, business continuity has to become part of the way that an organization is managed, regardless of size or sector." It matters not whether your organization is public or private sector, finance, retail, manufacturing or charity, small medium or large, business continuity should be seen as a valid and valued management discipline.

The Code of Practice sets out what organizations should be doing within their BCM programme, and hints at what they 'may' do. Whilst there are a number of commentaries, it does not explain in great detail why or how. So how can we go about embedding business continuity into our organization's culture?

BCM Lifecycle – 'embedding' in all stages

The preamble continues: "*At each stage of the BCM process, opportunities exist to introduce and enhance an organization's BCM culture*." The key message here is that each element of the BCM Lifecycle is two-way in terms of both gathering and sharing information. Each component of the Lifecycle contributes to a different level of understanding and awareness, bringing in differing and disparate audiences from all levels across the organization. By inputting to the deliverables as well as gaining deeper insight into the components of the programme, they should gain a deeper level of understanding than that achieved by broader and more generic campaigns across the whole organization. This should assist in managing expectations both in the capability of your BCM programme, what is important and achievable, and in the organizations ability to respond to a disruptive event.

Understanding the organization

The discussions held and the questions asked during the BIA process should enable the targeted audience to see what they are inputting to and the benefits that the BCM programme should bring to the organization. The discussion around the impacts of disruptive events should not only provide the information required for the wider BC programme, it could and should act as a catalyst for change required in the organization when issues around resilience and recovery capabilities are highlighted. The risk analysis, by its very name, will enable you to engage with another audience within your organization. Identifying and highlighting the risks to the organization should enable the engagement of the risk management community and into top management through groups such as risk and audit committees. If these two groups begin to ask the 'what if?' questions as a matter of course, then you have moved a long way in terms of embedding BCM into the culture.

Determining BCM strategy

Once the analysis of risk and business impact has been completed, you should have the opportunity to engage in various forums with other parts of your organization's top management, including up to board level, agreeing and developing the appropriate continuity strategies. Whilst the analysis phase interfaces with the management levels responsible for the delivery aspects of the organization's key products and services, and the supporting critical activities and associated risks, the BCM strategy discussions are likely to take place with those who are responsible for the organization's wider objectives and budget. Strategy and steering groups are useful to provide the business viewpoint and necessary support for any programme activity, particularly if there is any cost involved. It is important that once these strategies have been agreed, awareness of the strategies, the potential impacts of events and understanding why they are appropriate, is taken to the top management and wider organization.

Developing and implementing a BCM response
Depending on the size of your organization, yet another audience could be engaged during the development and delivery of your incident management and business continuity plans. The identification of appropriate incident management teams across your organization is likely to include some people who have not yet been directly involved in any of the preceding components of the Lifecycle and, again, when continuity plans are developed for more granular business or service teams and units. Those with specific BCM roles and responsibilities may require more in the way of specialist skills training, and the Code of Practice reflects this in section 10.3 where it states "Response skills and competence throughout the organization should be developed by practical training, including active participation in exercises."

Exercising, maintaining and reviewing
Exercising, rehearsing and testing your teams and plans are by far the best way of directly embedding business continuity in the culture, taking the dry paper and turning it into a more realistic experience. Making these events visible increases awareness and understanding of those not directly involved and shows that business continuity is taken seriously within your organization.

Even regular and ongoing maintenance has the potential to influence culture, either driven by cyclical review-and-amend, or by post-incident or rehearsal learning being implemented to enhance both plans and teams.

Internal or independent auditors are another group that should be actively engaged to assist in the delivery of your BCM programme. They are capable of bringing different viewpoints and weight to the issues you may be facing, can be used to raise awareness of BC to others within the organization and ultimately can raise issues up to the highest levels.

BCM programme management
Steering groups have already been mentioned, but they are useful to ensure that programmes are on track in terms of what the business actually requires and also the objectives and deliverables. By engaging adequate levels of support from the business, you are ensuring that they have recognised responsibilities and are bought into the BCM programme.

Who should you target?

Awareness is for everyone! Business continuity, like health and safety, requires everyone to play their part, and awareness and education is relevant from the board room to the mail room and all points between. The commentary note on section 10.1 in the Code of Practice says "*All staff have to understand that BCM is a serious issue for the organization and that they have an important role to play in maintaining the delivery of products and services to their clients and customers*". Whilst some of your organization requires detailed and specific knowledge, the majority only needs enough knowledge to understand what they should do *now* to make their own business operation resilient before an event takes place, and then what they should do in the event of an incident happening.

The basic rule is to talk to as many people as possible, whoever will listen, and at every opportunity, whether by invitation or creation on your part. You may wish to target specific groups – board members, audit committee, risk managers, regional managers, various leadership teams, etc. You should also look to cover 'everyone' – all staff within your organization, your customers and clients, your third party suppliers, your insurers, etc.

What you say and how you say it?

The Code of Practice states that "*The organization should have a process for identifying and delivering the BCM awareness requirements of the organization and evaluating the effectiveness of its delivery*". What you say is dependent on your organization's own communication style and methods, and the Code of Practice says "*An understanding of the existing culture within the organization will assist in the development of an appropriate BCM culture programme*".

What you say also depends on who you are targeting and communicating with, and what element of business continuity you are raising awareness about. All staff require a general level of awareness on what their roles and responsibilities are in terms of what they should do prior to an incident and what is expected of them during and after an incident. Those directly involved in managing incidents and ensuring continuity of business and services require more in the way of education and in depth training.

Again, how you put over your message will depend on your organization and what is available to you. The Code of Practice gives a number of examples of what an organization may consider doing to raise awareness of business continuity:

- A consultation process with staff throughout the organization concerning the implementation of the BCM programme;
- Discussion of BCM in the organization's newsletters, briefings, induction programme or journals;
- Inclusion of BCM on relevant web pages or intranets;
- Learning from internal and external incidents;
- BCM as an item at team meetings;
- Exercising continuity plans at an alternative location (e.g. a recovery site); and
- Visits to any designated alternative location (e.g. a recovery site).

Each organization should look for both 'push' and 'pull' opportunities, pushing business continuity information out to staff, as well as giving opportunities for staff to explore more in-

depth topics. A multi-channel approach, using all the communications channels your organization has, should greatly improve the chance of getting your message across. However, there is a fine balance between enough awareness and overkill. It must be recognised that other parts of the organization will be trying to achieve the same aims, so it is vital that a joined-up and coordinated approach is adopted, where the business continuity message is pushed out via the risk, health and safety, security, information security and other business messages.

Will anyone listen?

In the commentary on section 10.1 in the Code of Practice, it recognises that "*Creating and embedding a BCM culture within an organization can be a lengthy and difficult process which might encounter a level of resistance that was not anticipated*". However good and creative your awareness and education campaigns may be, it is almost inevitable that you will experience everything from opposition to denial, claims of information overload to just plain ignoring the message. Not everyone in an organization, however much we BC professionals jump up and down, will want to read, understand or take any actions. People will focus on doing their job today and all the problems that they may face, so they may not be interested in the ifs, buts and wherefores of tomorrow. Unless they can see a real reason why they should do something now, then expect resistance, and even if they see the reason for doing it – still expect some resistance.

BS 25999:2 – How do you measure it?

Part 2 of the British Standard focuses on the 'shall haves' of your BC management system, and as such is more concise in its requirements, with the purpose of "To ensure that the organization embeds business continuity into its routine operations and management processes, regardless of its size or the sector in which it operates". In turn, it lists three areas of activity:

a) Raise, enhance and maintain awareness through an ongoing education and information programme for all employees and establishing a process for evaluating the effectiveness of the BCM awareness delivery; and

b) Communicate to all employees the importance of:

- meeting business continuity management objectives;
- conforming to the business continuity policy; and
- continual improvement; and

c) Ensure that all employees are aware of how they contribute to the achievement of the organization's business continuity objectives

Measuring success, particularly in something as intangible as 'culture', is the challenge, not only for those who are trying to implement programmes, but also for those who are reviewing the programmes for return on investment, internal audit, quality and certification. Various measures could be adopted that assist in showing continual improvement and evaluating effectiveness, including:

- Repeated questionnaires and surveys, with measured responses and analysis
- Attendance at awareness raising, governance and rehearsal events, measured feedback scores
- Number of requests for wider assistance to the business e.g. client proposals or supplier due diligence
- Other parts of the organization asking for assistance in developing their own plans and programmes.

Despite all of this, embedding into the culture is reliant on the actions and activities of people. Measuring the breadth and depth of your impact on the organization's culture through these same people is likely to be subjective at the very best, and the capability to measure with any degree of 'accuracy' is likely to diminish as the size of an organization gets bigger.

Conclusion

Educating, awareness-raising, training, whatever you like to call it, is a vital and ongoing part of any BCM programme. I believe that 'embedding' is now accurately reflected in the BCM Lifecycle diagram, showing that all we seek to deliver should have a wider impact on the culture of our organizations. By utilising every opportunity within each component of the Lifecycle to spread the word, you should be able to provide deeper levels of understanding that broad and generic campaigns could never achieve.

While we will always have different depths of knowledge as to what business continuity means to each individual and business unit, and support for the BCM programme, 'embedding into the culture' is truly where the BCM programme meets with the people who make up your business, this is where the rubber hits the road! Awareness equals understanding, and understanding leads to a greater chance of success in what you are trying to achieve.

Author

Andy Mason, BSc, MBCS, CITP, MBCI, Head of Business Continuity, PricewaterhouseCoopers LLP

Andy started his working life in 1985 in computer operations at the University of London's LSE and King's College. He then moved to Pickfords Ltd in 1990 and in 1995, became an IT Auditor for Hertfordshire County Council. 1997 saw a move back to the private sector, when Andy joined the IT Audit team at Sainsbury's. In 2002 he was invited to join the Business Continuity Group on secondment, becoming permanent in 2003. In April 2006, Andy joined PricewaterhouseCoopers LLP as the Head of Business Continuity, responsible for the internal-facing BC programme for the UK Firm's offices and c16000 staff.

Andy is a serving member of the British Standards Institute Committee that developed the British Standard for Business Continuity, BS 25999 Parts 1 and 2.

Authors note

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

MANAGING CROWDS IN EMERGENCIES: PSYCHOLOGY FOR BUSINESS CONTINUITY

AUTHOR: Dr John Drury, senior lecturer in social psychology, University of Sussex

ABSTRACT: Business continuity managers operate with theories of crowd behaviour – whether they realise it or not! These theories have practical implications for the management of emergencies in any business environment. Some of these effects may be good, others less so.

This paper describes some of the latest ideas in the field of mass emergency psychology, and how they can inform best practice in business continuity. These ideas have been informed by recent research carried out in the Department of Psychology at the University of Sussex, in collaboration with colleagues from the Universities of St Andrews and Nottingham. This work also builds upon and integrates existing trends in the wider fields of disaster research and social psychology. It is based on a presentation given by the author at the Canary Wharf Group annual estate-wide business continuity exercise 2008 ('Tiger 2'). The research referred to was made possible by a grant from the Economic and Social Research Council (Ref. no: RES-000-23-0446).

Images of mass emergency behaviour

Popular culture contains a readily recognizable image that comes to mind whenever we refer to mass emergencies, disasters or evacuations. That image is '*mass panic*'. Mass panic refers to a number of psychological features. These include exaggerated perceptions of danger, and instincts for personal survival overwhelming civilized behaviours. Both of these features are exacerbated by the crowd itself, which is a medium for the 'contagion' of irrational sentiments. The behavioural effects of mass panic are said to include disorder and a lack of co-ordination. The crowd might have been able to escape the fire if people had filed out in an orderly fashion. Instead, they jammed a limited exit, fighting with each other and even trampling their own grandmothers, in their desperation to escape!

Yet we can also easily bring to mind popular representations of collective responses to emergencies that are quite the reverse of this negative image. Clichés like the 'spirit of the Blitz' and the 'British Bulldog spirit' evoke an enhanced sense of community, solidarity and strength in adversity: people coming together, talking to their neighbours, offering mutual support, taking responsibility for others, remaining in control of their emotions, and so on.

It is much more than an academic matter which of these representations we choose to believe. Each has very specific and quite different implications for practice – for the emergency services, for event organizers, for health and safety officers, for those who design public spaces, and for business continuity. We shall draw out each of these implications in the course of this article. First however, let us ask what the research evidence tells us about which is correct.

Mass panic or collective resilience?

Despite its common-sense appeal, reviews of the literature on mass emergency events find little evidence for the existence of mass panic. Whether it is fires, floods, bombings or other types of emergency and disaster, researchers have found little support for the view that the crowd as a whole exaggerates the perceived threat, loses control emotionally and behaves selfishly (1). Thus a lack of mass panic has been noted at events as diverse as the atomic bombing of Japan in World War II (2), the Kings Cross Underground fire of 1987 (3), and the 2001 World Trade Center evacuation (4).

Rather than mass panic, it is much more common to find survivors helping the vulnerable, orienting to friends and relatives, being generally co-operative, using their knowledge of building layout and exits, thinking critically about public address information, drawing upon social rules to guide their behaviour, communicating and discussing strategies of escape with each other. It has been pointed out, in fact, that people are more likely to be killed in an emergency such as a fire not through 'panic' but through the opposite – i.e. not taking the emergency seriously enough!

Our own recent studies illustrate some of these points. For example, when we spoke to survivors from the London bombings of 2005 we found widespread agreement that mutual helping was common and that levels of courtesy and co-operation were higher than on a normal day on the London Underground. And our studies of survivors of the sinking of the Jupiter in 1988 and the Hillsborough stadium crush of 1989 found numerous references to emotional self-control, orderly queuing, self-sacrifice and strangers 'pulling together'.

Importantly, therefore, in line with current research in the field, our studies suggest that mass emergency behaviour is (a) often *social* rather than individualistic or anti-social, and (b) typically *cognitive* (i.e. knowledge-driven) rather than unthinking or irrational.

Put together, these ingredients of social behaviour and cognition in the evacuating crowd add up to a model not of panic but of *collective resilience*. Resilience is something we all clearly hope for and seek to build upon, in case of emergency. Unlike the notion of mass panic, with its implication that there is something brutal under the veneer of civilized behaviour, the concept of resilience implies enduring and inherent integrity in human nature. The model of evacuation behaviour we have developed suggests some new ideas about the causes and consequences of this collective resilience.

Thus, our collective resilience model, in bringing together strands from the existing research with our own recent findings, suggests how business continuity managers can have an important role to play in *facilitating* such resilience. In terms of practical implications for managing crowds in emergencies, we present the implications of the model in six areas:

- preparation,

- information,
- trust,
- the wording of warnings,
- enhancing cohesion, and
- accommodating the public urge to help.

Preparation

The literature comparing emergencies that have been managed well versus those that have been managed badly makes very clear that two standard procedures can be crucial. These are, first, fire wardens who know the building and, second, regular practice drills (5).

The rationale for these practices is as we have just outlined. If we regard the emergency crowd as prone to panic, then there is no point arming people with the training and knowledge of what to do in the worst case scenario, for they will simply forget all about it and run around like headless chickens. If, on the other hand, crowds are cognitive, then survivors will be able to make good use of information.

It may seem like a banality to recommend practice drills. But in fact many organizations and building managers are reluctant to implement them on a regular basis, if at all, because of the 'inconvenience' they cause to the building and other estate users.

Against this argument of 'inconvenience' it only needs to be pointed out that there is little greater 'inconvenience' than death! And the difference between life and death could be the few seconds gained through a well-practiced drill. When the World Trade Center was evacuated in 1993 in response to a car bomb in the basement, it took people an average of two and a half hours to exit. When the plane hit Tower 1 in 2001, people had only one hour 42 minutes to get out before the building collapsed. Almost everyone below the floor hit by the plane survived. Their evacuation rate was in fact considerably faster than in 1993; indeed, if they had evacuated at the same rate as in 1993, many more would have perished (6).

Why was the 2001 evacuation so much more efficient than in 1993? One reason was that new technologies were introduced to facilitate the exit, such as photo-luminescent signs pointing the way down the fire exits. But, on top of that, after 1993, six-monthly fire drills were introduced. Survivors were armed with knowledge.

Information

There is a common practice amongst those 'in the know' in emergency situations to try to withhold and restrict information about the nature of the danger. Event security teams communicate in code-words if there is a fire. The authorities debate amongst themselves how much the public really need to know. 'Information' that there is a fire or other emergency takes the form of a simple alarm. And architectural 'solutions' the problem of evacuation (e.g. width of exits) are prioritised over enhanced technologies of communication (7).

All this makes sense if we believe that crowds are prone to over-react. But if, as we have argued, *under*-reaction is more likely, then it is the assumption of mass panic itself that is the real problem! It is crucial, therefore, that survivors are able to recognize an emergency for what it is as soon as possible. Why doesn't this always happen? Why, when an alarm goes off, do people continue to sit at their desks and ignore it? Too often, they think it is just a test, a false alarm or a drill. These reactions are understandable, because a simple alarm carries very little information.

The logic of our argument that the emergency crowd is thinking rather than irrational is that more rather than less information should be conveyed, and that the traditional alarm is something of an anachronism. Our society is replete with the most advanced digital technologies of surveillance: Britain is the most observed nation in the world! But our systems for *giving* rather than *taking* information by contrast rely largely on primitive analogue equipment! It is time to go beyond megaphones and alarms and make use of new technologies, such as giant LED screens, use of mobile phone systems and so on.

After 1993, the World Trade Center introduced voice communication on each floor (8). As we have already seen, the evacuees of 2001 did not succumb to panic. And, in systematic demonstration of the utility of enhanced provision of information, an experiment carried out on the Newcastle Metro (UK) found that the most efficient emergency egress took place when passengers were told via a public address system that there was a fire and where in the complex it was located. The least efficient egress took place when the alarm took the form of a simple siren or bell. Responses to the order simply to 'evacuate immediately' fell between these extremes (9).

Some psychologists argue that we process information less efficiently under conditions of stress. On the other hand, one of the reasons that we are recommending here that those affected by an emergency are kept informed is in fact to *reduce* their stress and anxiety. Uncertainty itself is stressful. Evacuees need just the right amount of information to (a) understand the seriousness of the situation (b) locate the appropriate and safest exits. In summary, therefore, armed with *practical information* during the event, collective behaviour will be more adaptive and efficient.

Trust

The presumption that there will be mass panic leads to a lack of trust in the responsible behaviour in the crowd and the public. It justifies the withholding of information, as we have seen.

But the withholding of information can itself produce a lack of trust on the part of the public and the crowd. Public address announcements that are deliberately vague and wilfully uncommunicative police officers serve to create hostility and suspicion, and hence sour the relationship between the public and those in authority. Perceived lack of openness by those in-the-know risks producing what we have called 'reverse crying-wolf syndrome'. The authorities obfuscate so many times that, when they do actually tell the truth and give out some valuable practical advice, it may not be believed by the sceptical public!

The nature of modern hazards means that the need to foster trust between the authorities and the public is greater than ever. One of the greatest man-made threats today is that of chemical, biological, radiological and nuclear (CBRN) attack. Chemical attack is perhaps the most likely of the four. Emergency services personnel may find themselves stretched to breaking point in such an event. Here, instead of the usual strategy of dispersing a crowd away from an emergency area, the crowd may need to be quarantined so decontamination can take place.

Unless there is a relationship of mutual trust, these policies of containment and decontamination could be perceived as infringements of civil liberties rather than public health measures. If they are to be complied with, for the safety of the wider population, the reasons for these policies therefore need to be clearly communicated by a trusted source. Put slightly differently, in many cases the authorities *need* the public to take *ownership* of their own civil defence procedures. This is a key point we shall return to again later.

The wording of warnings

What do we imagine when someone advises us 'don't panic' (10)? When there is already a relationship of mistrust and suspicion, such advice only indicates to us that there is indeed something to panic about!

Mass panic is not only an image in popular culture, but a discourse with pernicious consequences for what we expect of and perceive in other people. If we are told that others are panicking, this undermines our trust in their commitment to act in a socially responsible way. In leading us to expect selfish, individualized behaviour from others, references to their panic provide a rationale for selfish behaviour on our part. This was well illustrated when mass media reports of motorists panic buying petrol during a time of fuel protests only encouraged more such so-called panic buying!

As we have argued, information needs to be made available: *practical* information. In the case of an evacuation, the nature and location of the threat needs to be communicated. But the advice 'don't panic' is neither informative nor practical!

Enhancing cohesion

In rejecting mass panic as a model of behaviour in emergencies, social scientists have sought instead to explain the cohesion - togetherness, social behaviour, support - observed in mass emergency crowds. Research has suggested that everyday rules of behaviour and social roles continue to influence people in emergencies (11). Also, there is support for the idea that people try to stay with friends and family members, and indeed would rather die with them than escape alone (12). Our own research has sought to complement these accounts by explaining solidarity and self-sacrifice amongst strangers. Our theory is that shared identity is the basis of such widespread cohesion.

In order to test this idea we first developed a method for simulating aspects of mass emergency evacuation in a laboratory (13). Based on computer game techniques, we produced a virtual reality simulation of a crowd escaping a fire in an underground railway station. We then looked at the relationship between the shared identity our research participants felt with other crowd members in the simulation and their behaviour towards them. As expected, high-identification participants – i.e. those who felt a greater sense of togetherness with others – helped more and pushed less than did low-identification participants.

We were able to replicate this experimental finding, which was in line with research in other areas of social psychology, such as helping behaviour and collective action (14). But we also sought to look at how this process of shared identity might come about.

While we were exhibiting the virtual reality simulation at the Royal Society in 2005, the London bombings took place. The availability of so many accounts of the events encouraged us to move from the laboratory to collecting archive and interview data (15). As is well known, co-operation and orderly behaviour were common and selfish behaviours infrequent amongst survivors. Yet few people were with friends and relatives. We developed a hypothesis that the shared fate of the emergency itself can bring people together and create a sense of *shared* identity. In line with this, most of those that we interviewed described in rich and detailed terms the sense of unity they felt with other survivors, even though they didn't know them personally.

A third study tested systematically this idea of shared fate and shared identity as the basis of cohesion (16). We interviewed 21 survivors from 11 different emergency events, including the Hillsborough crush (1989), the Bradford fire (1985), a Canary Wharf evacuation (2001), and the Harrods bomb (1983). On the basis of their interview accounts, we divided people into high- versus low-identifiers. As expected, high-identifiers were more likely than low-identifiers to

perceived ‘shared fate’ in the crowd; to give help and receive help; and to perceive calm, order, social rules and courtesy. They were also less likely to experience selfishness from others.

Based on these findings, and together with the existing literature, we therefore explained cohesion in mass emergencies in terms of a social identity model of collective resilience. Resilience refers to the ability of individuals, groups and organizations to resist attack and recover from adverse conditions. We suggest that shared identity is the key to such resilience. Shared identity allows people to see themselves and act as part of a collective (even if they don’t know each other). The collective is an adaptive mechanism: feeling part of a collective enables survivors to express and expect solidarity, and thereby to co-ordinate and draw upon collective sources of support and other practical resources, to deal with adversity.

Collective resilience as shared identity makes sense of some of the practical recommendations we have been describing. Thus we treat information as veridical knowledge when we trust its source, and we trust its source when we categorize that source as one of ‘us’. We feel less anxiety and stress when we perceive those around us as ‘us’ rather than ‘them’; we then expect fellow survivors to be supportive not competitive; and we believe their reassurances. And since we share their perspective, we feel ownership of the plans and goals we seek to realise.

In practical terms, therefore, the natural human cohesion that arises in a mass emergency can be facilitated (rather than inhibited) by business continuity managers in the following ways:

- First: use of any strategies which promote, build upon and refer to unity. This could be as subtle as the type of language used. For example, the contemporary reference to rail users as ‘customers’ positions them in an individualizing cash nexus, whereas the more old-fashioned term ‘passengers’ evokes their (common) relationship to the train.

- Second: *including* employees and the public – whether in the planning and preparedness stages or during the event – rather than excluding them. Inclusion refers not only to sharing information but also to sharing control. The crowd and the public often need to take greater ownership of their own civil defence.

This takes us to our final practical recommendation:

Accommodating the public urge to help

Whenever there is a major incident or emergency, one of the first tasks that the emergency services set out to do is to exclude the general public from the scene by throwing a cordon around it. While there are indeed people who just come to gawp, many who come to the scene of an emergency do so because they want to offer help.

The same is true for survivors themselves. The urge to help by the public, whether directly or indirectly affected by the emergency themselves, is inevitable. We are therefore arguing that this urge needs to be harnessed, rather than suppressed.

There are several reasons for this. First, as discussed, enabling survivors to get involved and take ownership, rather than being excluded by the 'experts', can serve to build unity and cohesion. Second, if people feel that they are doing something constructive rather than standing idly by, then it can actually make them feel better. The counter-argument to these points is that well-meaning members of the public can get in the way of those who do actually know best. Third, however, and most importantly, the emergency services sometimes have no choice but to rely on members of the crowd.

This is well illustrated in our study of the experiences of those on the bombed London underground trains in July 2005. Many of those caught up were not reached by the emergency services for a considerable period of time. In the absence of fire and ambulance crews, it was their fellow passengers who administered first aid, tore up clothing for make-shift bandages and attempted to rescue each other in various ways. In events like this, in other words, the crowd becomes the fourth emergency service.

Conclusions

If there is one claim which sums up the argument of this article it is that the crowd can operate as a *psychological resource* in times of emergency.

This is not to say of course that crowds do not present problems of various practical kinds for those whose job it is to manage large buildings or public spaces. There are obvious *logistical* problems, for example, in managing the most effective use of fire assembly points if large numbers of people evacuate severable buildings simultaneously: where does one put all these people?

But such logistical problems of the crowd are quite different than the psychological problems implicit in the notion of mass panic. Mass panic is just one theory that business continuity managers can adopt to inform their practices in preparing for and reacting to a mass emergency. We have argued here that, as a theory, mass panic is part of the problem not part of the solution. It rationalizes practices which exclude, deny, divide, disenfranchise and disempower the crowd. By contrast, we suggest, crowd behaviour in emergencies should be seen as both social and knowledge-driven. This kind of perspective provides the rationale for practices which enhance and facilitate the tendency toward collective resilience which naturally arises in emergency crowds.

Author

Dr John Drury, Department of Psychology, University of Sussex
j.drury@sussex.ac.uk

For the last five years Dr. Drury has been working on the psychology of emergency mass evacuation. Further information on his research, consultancy and CPD training can be found at his website: http://www.sussex.ac.uk/affiliates/panic/

References

(1) Quarantelli, E.L. (2001). *Panic, sociology of*. In N. J. Smelser & P. B. Baltes (Eds.), International encyclopedia of the social and behavioural sciences (pp. 11020-11023). New York: Pergamon Press.

(2) Janis, I. L. (1951). *Air war and emotional stress*: Psychological studies of bombing and civilian defense. New York: McGraw-Hill.

(3) Donald, I. & Canter, D. (1992). *Intentionality and fatality during the King's Cross underground fire*. European Journal of Social Psychology, 22, 203-218.

(4) Blake, S. J., Galea, E. R., Westeng, H., & Dixon, A. J. P. (2004). *An analysis of human behaviour during the World Trade Center disaster of 11 September 2001 based on published survivor accounts.* Proceedings of Third International Symposium on Human Behaviour in Fire, Belfast, September.

(5) Chertkoff, J. M., & Kushigian, R. H. (1999). *Don't panic: The psychology of emergency egress and ingress*. Westport, CT: Praeger.

(6) Proulx, G., & Fahy, R.F. (2003). *Evacuation of the World Trade Center: What went right?* Proceedings of the CIB-CTBUH International Conference on Tall Buildings, Oct. 20-23, Malaysia, pp. 27-34.

(7) Sime, J. D. (1995). *Crowd psychology and engineering*. Safety Science, 21, 1-14.

(8) Proulx, G. & Fahy, R.F. (op. cit.)

(9) Proulx, G. & Sime, J.D. (1991). *To prevent 'panic' in an underground emergency: Why not tell people the truth?* In G. Cox & B. Langford (eds.), Fire Safety Science:

Proceedings of the Third International Symposium, (pp. 843-852), London: Elsevier Applied Science.

(10) Wessely, S. (2005). *Don't panic! Short and long term psychological reactions to the new terrorism: The role of information and the authorities.* Journal of Mental Health, 14, 1-6.

(11) Johnson, N. R. (1988). *Fire in a crowded theatre: A descriptive investigation of the emergence of panic.* International Journal of Mass Emergencies and Disasters, 6, 7-26.

(12) Sime, J. D. (1983). *Affiliative behaviour during escape to building exits.* Journal of Environmental Psychology, 3, 21-41.

(13) Cocking, C., & Drury, J. (2008). *The mass psychology of disasters and emergency evacuations: A research report and implications for the Fire and Rescue Service.* Fire Safety, Technology and Management, 10, 13-19.

(14) Levine, M., Prosser, A., Evans, D. & Reicher, S. (2005). *Identity and emergency intervention. How social group membership and inclusiveness of group boundaries shape helping behaviour.* Personality and Social Psychology Bulletin, 31, 443-453.

(15) Cocking, C., Drury, J., & Reicher, S. (In press, 2009). *The psychology of crowd behaviour in emergency evacuations: Results from two interview studies and implications for the Fire & Rescue Services. I*rish Journal of Psychology.

(16) Drury, J., Cocking, C., & Reicher, S. (in press, 2009). *Everyone for themselves? A comparative study of crowd solidarity among emergency survivors.* British Journal of Social Psychology.

the business continuity JOURNAL

BS 25999: KEY ISSUES TO ADDRESS FOR CERTIFICATION

AUTHOR: Malcolm Cornish, FCA, FBCI, operations director Continuity[2]

ABSTRACT: BS 25999-2 (Part 2 - the Specification) was issued in November 2007. Since that time many organizations have been certified and UKAS (the United Kingdom Accreditation Service) has been assessing the audits undertaken by certification bodies as part of its process towards accrediting these bodies in respect of BS 25999.

As a result of all these activities, BS 25999-2 is coming under the close scrutiny of organizations being certified, the certification bodies and UKAS. The overall consensus is that BS 25999-2 has been constructed to a very high standard and has generally been very well received by these three groups. As with any new standard, there are inevitably some areas of confusion and misunderstanding and there are aspects of the standard that are more difficult to comply with than others. In this paper, the author will address the following:

- Management system requirements

- Business impact analysis.

Detailed considerations

Management system requirements

There is a big difference between implementing business continuity management (BCM) and establishing a fully effective business continuity management system (BCMS). This became clear to BCM Committee Panel 2, which had been given the responsibility by the British Standards Institution to create BS 25999-2. As one of the ten or so actively involved in the panel, I quickly learnt that there were many aspects of a management system that are quite onerous and demand disciplines beyond the normal approach of BCM practitioners.

In particular, the aspects that seem to have caused the most difficulty relate to:

- Competency of personnel (BS 25999-2: Clause 3.2.4)
- Documentation and records (BS 25999-2: Clause 3.4)

Thankfully, we had experts in management systems who were able to combine and improve on the text from other management systems standards in order to set out precisely in BS 25999-2 what is needed. Close reading of the text is all that is required.

Competency of personnel

3.2.4 The organization shall ensure that all personnel who are assigned business continuity responsibilities are competent to perform the required tasks by:

- *determining the necessary competencies for such personnel;*
- *conducting training needs analysis on personnel being assigned BCM roles and responsibilities;*
- *providing training;*
- *ensuring that the necessary competence has been achieved; and*
- *maintaining records of education, training, skills, experience and qualifications.*

Documentation and records

There are a number of facets that need to be addressed. As well as identifying all the different documents that are required in respect of the work undertaken (all have a reference to relevant clauses) the standard also requires that:

3.4.1.2 Records be established, maintained and controlled to provide evidence of the effective operation of the BCMS

3.4.1.2 Documented procedures be established in order to identify the controls over BCMS documentation and records

For records:

3.4.2.1 Controls shall be established over BCMS records in order to:

- *ensure that they remain legible, readily identifiable and retrievable; and*
- *provide for their identification, storage, protection and retrieval.*

For documentation:

Controls shall be established over BCMS documentation to ensure that:

- documents are approved for adequacy prior to issue;
- documents are reviewed and updated as necessary and re-approved;
- changes and the current revision status of documents are identified;
- relevant versions of applicable documents are available at points of use;

- documents of external origin are identified and their distribution controlled; and
- the unintended use of obsolete documents is prevented and that such documents are suitably identified if they are retained for any purpose.

Business impact analysis

Before BS 25999-2 arrived, you could talk to thirty business continuity practitioners and get forty different explanations of what is meant by the term 'business impact analysis' (BIA). Thankfully BS 25999 (identically in both parts 1 and 2) sets out the definition of a BIA and identifies its fundamental requirements. However, there still appears to be confusion surrounding the BIA and it is rare to find examples of BIAs that have been conducted in full compliance with BS 25999-2.

Understanding of the terms MTPoD and RTO

There appears to be a great deal of confusion surrounding the newly introduced term 'maximum tolerable period of disruption (MTPoD)' as defined by the standard and its relationship to the term recovery time objective (RTO). Part of the confusion is of the standard's own making. In the terms and definitions, maximum tolerable period of disruption is defined as:

Duration after which an organization's viability will be irrevocably threatened if product and service delivery cannot be resumed.

This suggests that MTPoD is attributable to the organization as a whole. In the body of the standard, there is, however, no reference to MTPoD in relation to the organization as a whole or individual products and services.

The next reference to MTPoD is in the definition of recovery time objective, which BS 25999 defines as:

Target time set for resumption of product, service or activity delivery after an incident

NOTE The recovery time objective has to be less than the maximum tolerable period of disruption.

This suggests that MTPoDs are applicable to products, services and activities. There is, however, no further reference in the standard to MTPoDs in respect of products and services.

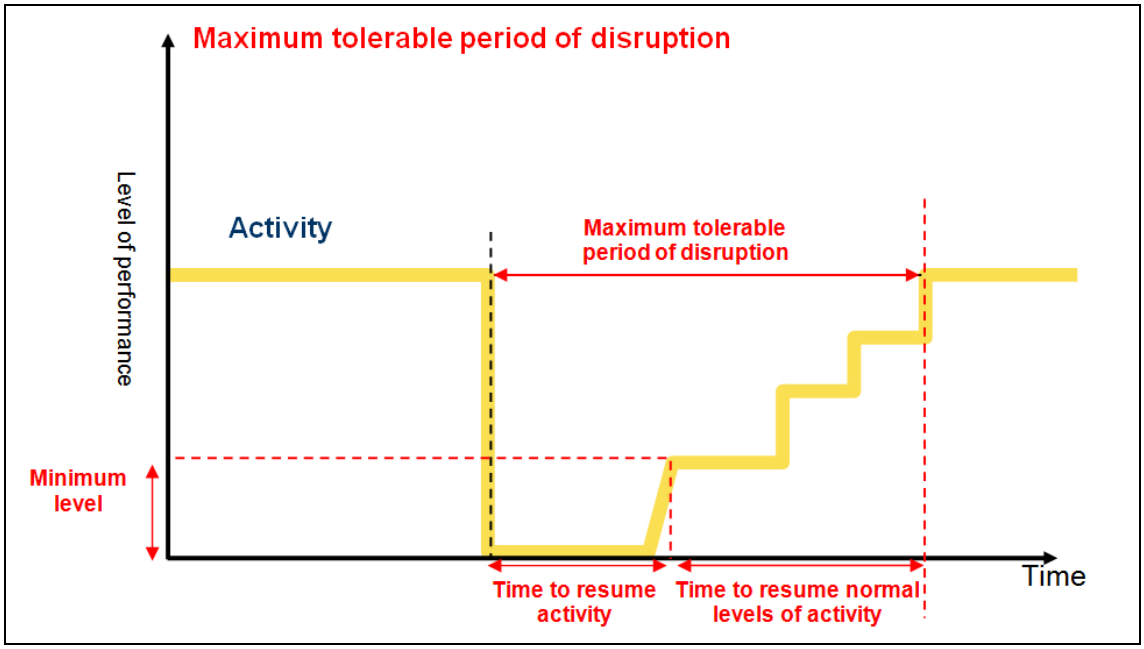
The only other reference to MTPoD is in relation to individual activities under the heading business impact analysis (clause 4.1.1), where the requirement is for the organization in relation to ALL activities to:

Establish the maximum tolerable period of disruption for each activity by identifying:

- *the maximum time period after the start of a disruption within which each activity needs to be resumed;*
- *the minimum level at which each activity needs to be performed upon resumption; and*
- *the length of time within which normal levels of operation need to be resumed;*

There is also a restatement that RTOs for critical activities must be within their MTPoDs.

The diagram below sets out my interpretation of MTPoD:



In order to determine the 'maximum time period after the start of a disruption within which each activity needs to be resumed', the standard requires the organization to:

Identify impacts resulting from the disruption to these activities, and determine how these vary over time

Based on my experience, it is very common for organizations not to do this. Many fall into the trap of setting a recovery time objective for each activity without full reference to impacts over time, and then call it the MTPoD without considering all the MTPoD components that the standard requires. The training material issued by the Business Continuity Institute in support of its five-day training course compounds the confusion by stating that the MTPoD is the point at which the activity needs to be resumed.

As well as determining the 'time to resume activity', some thought needs to be given to defining the level of performance at resumption (e.g. number of personnel, manufacturing throughput, invoices produced) and determining the time required to return to normal levels

of activity. My belief is that the standard is not looking for a scientific calculation of the latter (BCM is not a science) but is just looking for an indication from someone that understands the activity.

Steps required for full BIA

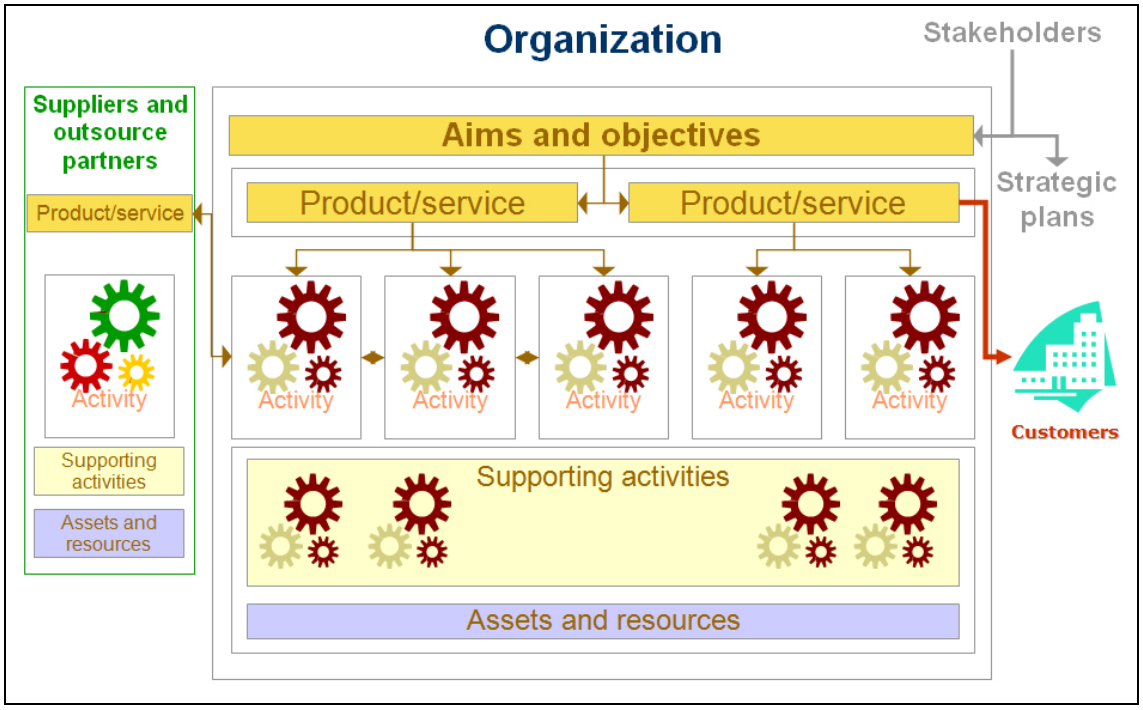
The standard is very specific as to all of the requirements of a BIA because of each requirement's individual significance to the validity of the BIA and consequently, the entire BCM process. As well as identifying critical activities, the BIA enables the organization to obtain consensus as to the order in which activities not identified as critical should be recovered in order to minimise the impact on the business. Failure to establish the MTPoD (including all its components) and use the information to prioritise all activities is likely to result in problems when a major incident occurs.

In essence, all the requirements of the BIA are linked in a chain. Failure of any of the links may jeopardise the validity of the BCM arrangements for critical activities and will almost certainly prevent the appropriate treatment of other activities during a major incident.

Because BCM arrangements and plans have to be put in place for critical activities, they come under closer scrutiny as the BCM process continues. The Standard does not, however, require further examination of the remaining activities, some of which may become 'critical' surprisingly quickly during an incident. If an organization does not use the BIA to gather key information, agree the impact implications and document them in an appropriate manner, the next opportunity will be when an incident occurs and there is not enough time to get it right.

Definition of RTO

In the terms and definitions of BS 25999-1 (which were intended to be identical in Part 2, apart from terms not used), the definition of RTOs extends to IT systems and applications. I would also contend that RTOs are required for all supporting elements required for the resumption of activities (supporting activities, products and services supplied by suppliers and outsource partners, assets and resources) as shown in the diagram below:



Conclusions

Management system requirements

The standard is very explicit and clear as to additional requirements of a management system. There is additional cost and effort involved in creating a BCMS and obtaining certification as opposed to just implementing effective BCM. Organizations should therefore make sure that there are sufficient benefits in achieving certification before embarking on that course of action.

Business impact analysis

The BIA requirements set out in BS 25999-2 are to my mind extremely sound and workable. There is considerable confusion surrounding the *maximum tolerable period of disruption* (MTPoD), so something needs to be done about it.

MTPoD could be retained as a term that relates to the organization as a whole or individual products and services. It is for example useful for management to express a view as to how sensitive the organization is to disruption and use this as an indicator of the level and extent of planning that would be expected. The difficulty is that I do not have a clear idea as to how it could reasonably be determined.

The 'activity' MTPoD (using my interpretation) is unnecessary. Its components are defined, so the requirement for a name is superfluous. Some may chose (as does the BCI) to use the term to describe the 'time to resume activity' in the MTPoD diagram above. The only other references to MTPoD are in relation to RTOs, which must be within it. If you go along with my explanation of MTPoD, this requirement is only saying that you must recover the activity within the time that you have determined it must be back to normal! All practitioners would I am sure agree that once you have determined on an 'impact over time' basis the latest time at which an activity must be resumed in order to avoid unacceptable impacts, you must set its RTO within that. The RTO will be influenced by other factors (e.g. dependencies, lead times for essential equipment, backlog issues) so could be significantly sooner that the time determined based on impacts.

The obvious conclusion is to define a new term TWWAMBRAULI being 'Time Within Which Activity Must Be Resumed to Avoid Unacceptable Levels of Impact'…..unless of course someone can come up with something snappier!

Author

Malcolm Cornish, FCA, FBCI, operations director , Continuity²
malcolm.cornish@continuity2.com

Malcolm has specialised in business continuity management for the past nineteen years dealing with all aspects of business continuity management in most business sectors. He is a Fellow of the Business Continuity Institute (FBCI) and has played an active role in the development of the institute from its inception. He is currently a member of the BCI Audit Committee and on the BCM committee of the BSI that is responsible for BS 25999. Malcolm develops and leads Continuity² training courses, is a regular conference presenter and has published many articles and papers to promote awareness and understanding of business continuity.

THE COMPONENTS OF A RESILIENCE CAPABILITY

AUTHOR: Alan Elwood, MSc, MBCI, Emergency Planning Solutions Ltd.

ABSTRACT: Resilience is defined as the 'ability of an organization to resist being affected by an incident' (1) and ultimately may be said to be the aim of business continuity management. Why else spend the time and resources implementing BCM within an organization if it is not going to help that organization overcome adversity? True some pain will be felt. There will be some disruption, and not everything will go to plan but if resilience is demonstrated then 'victory' will surely follow. Clearly within BCM talk is of resilient businesses but in the wider context, resilience is used in more nebulous terms such as labelling social groups as resilient communities. What is interesting about this is that we routinely use the word resilience in many contexts but do we truly understanding what it comprises of? Defining the component parts of resilience, the benchmark of BCM success, is therefore an important issue. This paper defines the components of resilience. It develops a framework used by the military to define fighting power (2) and applies it to resilience. In so doing it explores how, if any of the three component parts is missing or ineffective, no organization can claim to have true resilience.

Components of resilience

The resilience model as defined by the author is as per figure one. It consists of three components which will be discussed in detail in the following sections.

Figure one: the resilience model.

The tangible component

The tangible component of resilience is the most straightforward aspect to consider and comprehend. The current British Standard (BS 25999-1), complimented through risk management techniques, majors upon this facet of resilience. The tangible component provides for those aspects of resilience that equate to the physical world. Risk management talks about introducing mitigating measures, transferring risk, changing what is done and introducing BCM strategies. In turn BCM highlights the need for tactical options for such concerns as people, premises, suppliers, stakeholders, technology and information (3). In these cases it is easy to see, if not a little bit more difficult to implement (4), the need for physical interventions that are aimed at increasing resilience. So it is that organizations diversify staff, employ knowledge networks, build redundancy into technology and develop communications plans with stakeholders. The ultimate expression of the tangible component perhaps lies within the production of the business continuity plan itself. Here, within one document, lies the answer to our resilience needs, or does it? Whilst it is clear that we cannot simply hypothesise about resilience it is also true that physical interventions alone are not enough, something, in a way, alluded to through the concept of a BCM culture (5). General Dwight D. Eisenhower famously said: "*In war, before the battle is joined, plans are everything, but once the shooting begins, plans are worthless*". Perhaps what he meant is that there is more to capability than plans, and the tangible outworking of them, alone.

The intangible component

The intangible component is a fundamental pillar of a resilience capability. It accounts for the principles and doctrine engaged to develop that capability in the first place. The intangible component may be considered to be the conceptual framework around which the resilience development takes place. In essence such doctrine may be thought of as 'what we do' rather than 'how we do it', the latter being akin to the tangible component. Here again the current British Standard provides a useful backdrop in that it prescribes a methodology for the conduct of resilience development through achieving a BCM capability. The key advantage of such a methodology is not that it tells practitioners how to do things but that it provides a common framework of understanding. This enables practitioners from different, but interdependent, organizations to have clarity about resilience and BCM. However, despite the vital nature of this component, organizations are failing to fully exploit it (6). Certainly current guidance covers the 'what' in terms of broad BCM capability development and maintenance. True resilience, however, requires something greater than a borrowed generic doctrine that perhaps stops short of what the organization needs to achieve whilst in the teeth of a disaster. The effective implementation of the capability in time of crisis requires a fully integrated 'what' that is bespoke to the organization. Just as a common understanding is crucial across the BCM field so it is vital within the structures and people of any organization faced with having to respond to an interruption. For this to be achieved organizations need to develop their own BCM doctrine. The purpose of such a doctrine is to enable a coherent and focused

response through guiding behaviour. After all the BCM capability resides not in the plan but in the organization's ability to implement the plan. A suggested model, see figure two, for such doctrinal capability in terms of BCM must start with an organization's philosophy towards resilience. This in turn will be defined by clearly identifiable principles, enacted freely through universally understood and accepted cultural practices and underpinned by the techniques and procedures employed in day to day work. An organizational policy is the starting point for the development of such a philosophy but not enough in itself.

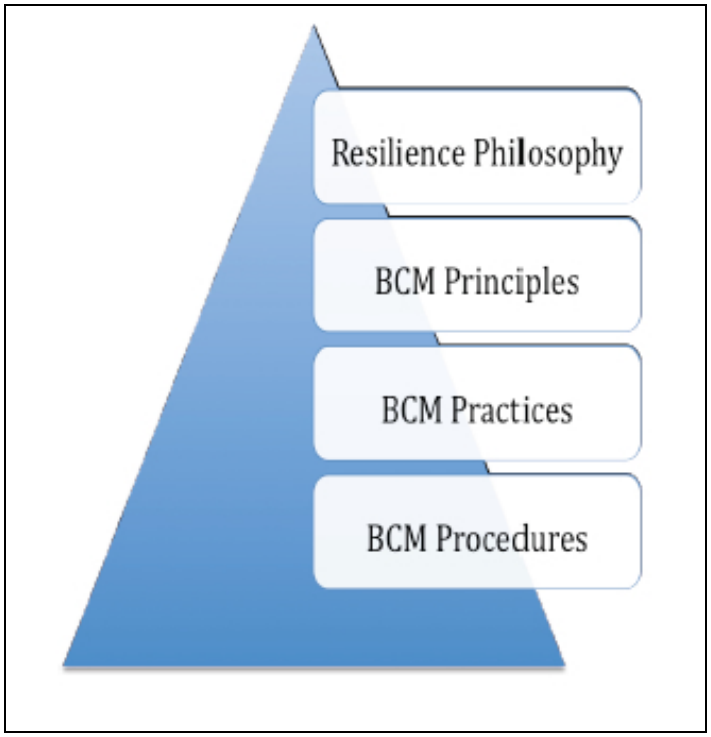


Figure two: organizational resilience philosophy.

The cohesive component

For the tangible component to become reality and to achieve what it is designed to achieve in resilience terms, requires that the intangible component is fully inculcated into how people think and act in relation to resilience. No amount of planning, expenditure, use of resources or ingenious mitigation measures will ever guarantee triumph if the espoused BCM culture is only visible within the readily accessible corporate values. Rather it must be worked down into the taken for granted assumptions of the workforce, see figure three. Thus it is required that an organization develops a sound moral and ethical base for resilience. Such a cohesive force establishes an understanding in all to act within the bounds of what is generally thought to be right in resilience terms. This moral responsibility, which through BCM extends beyond the

corporation to the network of clients, staff, shareholders and others, is the essential driving force of resilience. The real value adding nature of BCM resides within this self imposed moral strength to seek to ensure that the organization can survive and prosper despite interruptions and to be able to demonstrate this to others. Such moral capability requires that leadership is demonstrated by those charged with promoting BCM and resilience. The word leadership is used, as distinct from management, for this is about changing and altering perceptions and ideals, not about accounts, production or HR. Realising that success is not based upon individual actions alone the leader must be able to build moral cohesion. The cohesive component is the sole factor likely to result in strong individual motivation, team commitment and task goal orientation. Without all three characteristics in place someone may only be motivated to serve themselves, the team may seek to protect itself at the expense of the organization and the organization may not be fully focused on the task in hand. This would be bad enough in terms of normal routine but could prove fatal in the event of an interruption. No amount of doctrine or mitigation measures will overcome such a weakness in resilience and as such it is important that the nature of the cohesive component is understood. It comprises, amongst other things, of continuity through individual bonds, shared experiences, clear understanding of the task, the anticipation of friction points and shared values. Unfortunately it is all too readily undermined by corporate actions unrelated to resilience such as the recent trends in downsizing and redundancy (7). For people and teams to display such traits requires leaders who understand their people, make the right decisions in times of crisis, communicate openly and empower staff to act on their initiative. They often inspire people to achieve the seemingly impossible and ultimately sustain the team in doing so. The classic example of such leadership failure can be found within the 1987 Challenger Shuttle disaster were in reality poor leadership, and not engineering or systems failures, derailed the space programme for years. Leadership development, and in particular crisis leadership skills, and the development of cohesive teams are essential to the establishment of a true resilience capability.

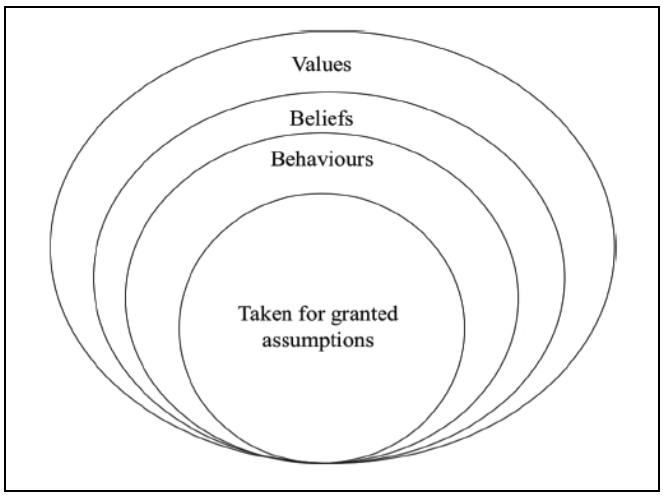


Figure three: the cultural model. Source – Schien, E. H., organizational Culture and Leadership: A Dynamic View, Jassey-Bass,1985, p 14.

The levers of change

If leadership is a fundamental tenant of a successful resilience capability and if the leader is seeking to embed within individuals and teams a form of BCM glue to hold them together in times of trouble, then he or she needs the tools to do so. In turn these tools must reflect the tangible, intangible and cohesive aspects that have been outlined as the key component parts of any resilience capability. This is because at the heart of the issue lies the notion of the paradigm, that is the actual resilience of an organization, as opposed to the aspired to state. This paradigm is in itself a function of the interworking of the tangible, intangible and cohesive components. This would be of little use, beyond academic study, if the leader were unable to, in some fashion, alter that paradigm. Fortunately there exist 'levers' that can be used by the leader to adjust the paradigm and in so doing fine tune resilience. To alter the resilience paradigm means that the leader has to be able to influence the tangible, intangible and cohesive forces that create that paradigm and so the levers must allow these areas to be adjusted individually. This concept is outlined in figure four.

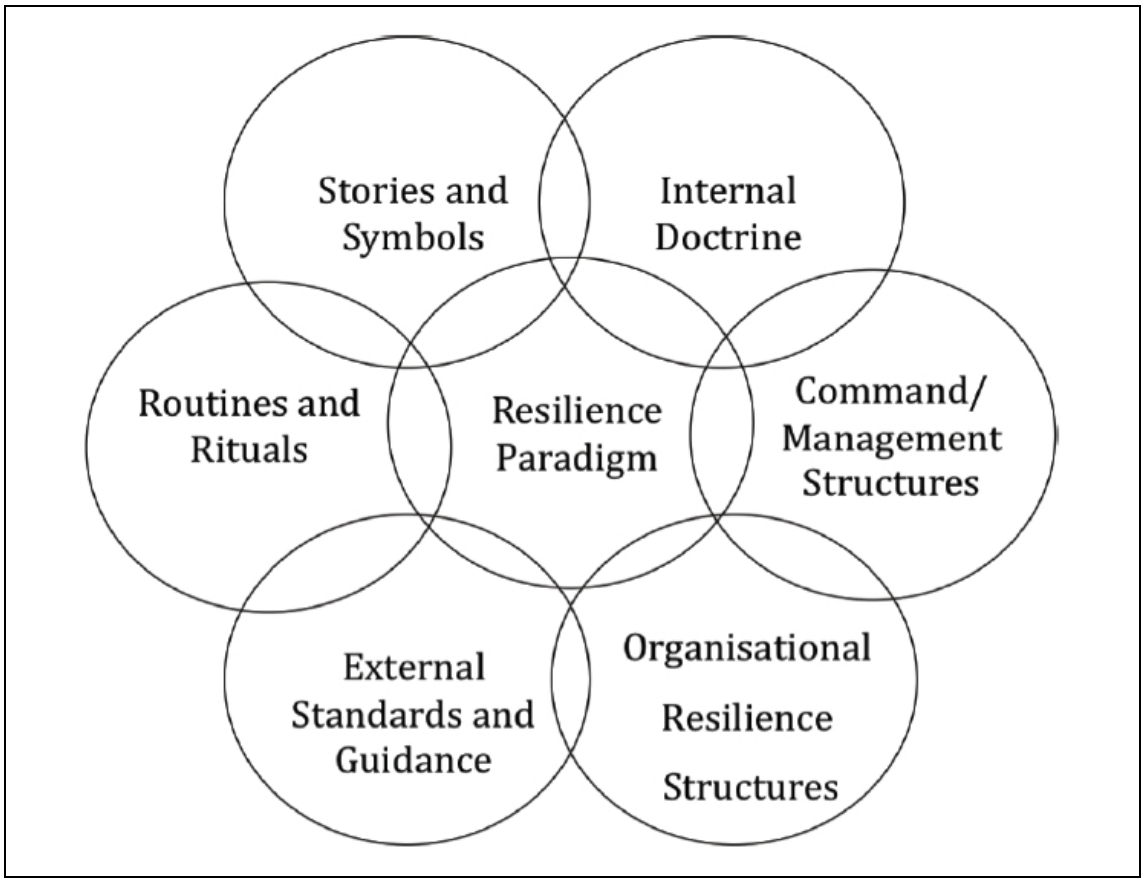


Figure four: the resilience levers. Source: adapted by the author from Johnson, G., Scholes, K., and Whittington, R., Exploring Corporate Strategy, 7th ed, Harlow, Prentice Hall, 2006.

The individual resilience levers may be summarised, or defined, as follows:

Levers for the tangible component

- Organizational resilience structures – this includes the establishment of the BCM related mitigation measures and the structures put in place as a result of planning.

- Command and management structures – this includes the development of plans themselves, for response, continuity and recovery. It also includes the creation of command and control arrangements designed to implement plans, such as crisis management structures.

Levers for the intangible component

- External standards and guidance – this includes the adherence to benchmarked best practice and guidance, such as BS 25999, in developing BCM capabilities.

- Internal doctrine – this includes the development of organizational specific BCM doctrine, taking account of External Standards and Guidance, which reflects the culture and nature of the user and the contextual situation they are in.

Levers for the cohesive component

- Stories and symbols – this includes stories told by members to each other and to new members. They embed the resilience paradigm by presenting history and flagging up important events and personalities normally in relation to success or failure and heroes or villains. It also encompasses the symbolic affects of language, boardroom engagement, titles and other aspects that express more about the actual value placed on resilience by the organization than their intrinsic content alone.

- Routines and rituals – this includes the way things are done and that have persisted over time. They often encourage behaviour, for example through the ritual of induction training, and at the same time reflect core beliefs and as such are a useful guide to actual behaviour in a crisis. They are visible within and outside of the organization but can hinder the adoption of resilience measures. For example is it routine that people are allowed to flag problems to their line manager or are they expected to solve them alone? If the former, great, if the latter then perhaps resilience problems will just get buried, to surface when least wanted.

The resilience levers, which combined form a resilience web, are the accessible ways in which the leader can adjust the resilience paradigm. The resilience web is the tool by which the leader can assess the current paradigm and draw up a vision of the desired future paradigm. By drawing a resilience web for the resilience paradigm as it is and by comparing it to the situation as hoped for it may be possible to identify the mechanism for change required within each lever. That is the steps that must be undergone to move each lever from its current state,

via a transition state, to the future desired state. This provides the practitioner with a useable way in which to approach how the tangible, intangible and cohesive components can be used to influence resilience, whilst taking account of how alterations in one lever may in turn affect other levers. For example steps to promote the importance of organizational resilience structures must be matched by the symbol of board level engagement, which in turn will generate 'stories' about the real value placed on resilience by the organization leading to acceptance of the internal resilience doctrine.

Conclusion

The ultimate objective of BCM is to develop resilience such that an organization is able to weather and recover from any disruption. Critical to the development of resilience are three underpinning component parts. The tangible component, the aspect most readily addressed by those who undertake BCM, caters for the physical and structural BCM measures put in place. The intangible component, covering the philosophy of resilience, is less well addressed. Organizations should seek not only to follow the externally imposed agenda, say from BS 25999-1, but also to develop their own organizational BCM doctrine. Finally, without a moral belief in resilience, demonstrated through strong leadership and the resulting cohesive component acting as the glue within the organization, no amount of physical measures or policy papers will achieve success in time of crisis. Aligning all three of the component parts is vital and if any one area is missing or weak then true resilience cannot be said to exist. To align these component parts the practitioner needs a useful tool that will enable an accurate analysis of the resilience state, or paradigm, to be made through considering those resilience levers that influence its make-up. This may be termed as defining the resilience web and consists of understanding the tangible, intangible and cohesive forces or levers at play. When a comparison is made to the desired end state resilience web then appropriate actions can be selected within each lever to move the organization towards that goal.

Author

Alan Elwood, MSc, MBCI, Emergency Planning Solutions Ltd.
info@emergencyplanningsolutions.com

Alan is a director with Emergency Planning Solutions, an associate course director of the Cabinet Office Emergency Planning College, a lecturer with Queen's University Belfast and consultants with Cranfield University (UK Resilience Cell). Alan's current responsibilities include business continuity and emergency planning training and consultancy for clients within the public and private sectors in the UK, Ireland and globally. Previously he was a commissioned officer within the British Army Alan has considerable training in, and practical experience of, risk management,

emergency planning and business continuity. Alan's experience includes strategic management, project management and detailed operational contingency planning, as well as responsibility for determining the effective allocation of resources for civil protection and business continuity. Previous work has revolved around planning for, mitigating and dealing with major life and business threatening risks requiring a multi-functional approach and robust decision making. Alan holds an MSc in Defence Management and an Honours Degree in Electronic Systems Engineering, both from Cranfield University. He is the secretary of the Northern Ireland forum of the BCI

The New MSc in Resilience

Alan is also currently engaged as a member of a working group who are developing a Masters Degree in the Resilience field. The Resilience Programme (leading to the MSc in Executive Leadership) will be offered by the Ulster University as a two year executive course due to start in the 2009 Academic year. Input into the design and delivery of this innovative academic qualification comes from industry and consultant practitioners as well as leading academics.

The course will cover crisis leadership, transformational leadership, BCM, risk management, reputational and communications management and will provide opportunities to explore the theory through exercises and employment based action learning sets. In addition delegates will receive one to one leadership and personal development mentoring equipping them to better enact what they gain from the course back in their organizations.

If you would like to know more about the Resilience Programme (leading to the MSc in Executive Leadership) please contact Alan via alanelwood@emergencyplanningsolutions.com

References

(1) BS25999-1 page 4

(2)UK MOD AC 71819 Army Doctrine Publication Land Operations

(3) BS25999-1 page 21

(4) Chartered Management Institute BCM 2008, page 3

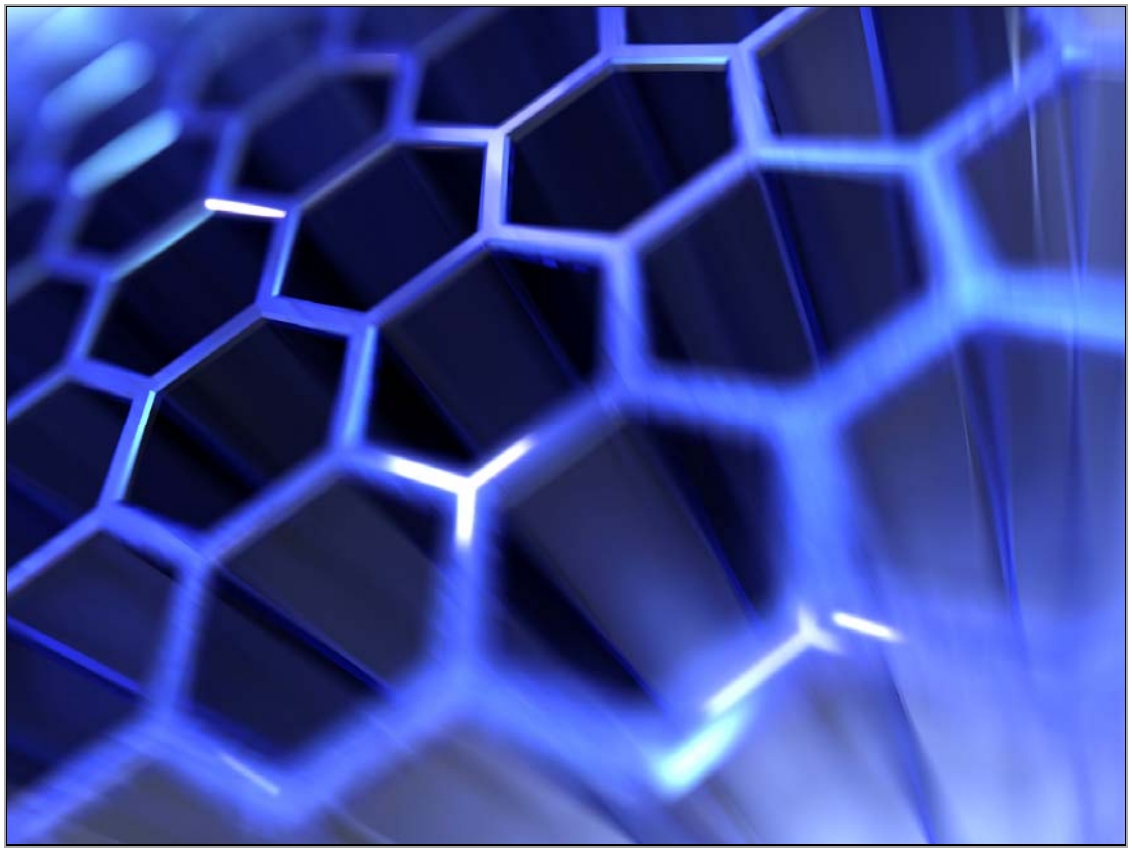
(5) BCI Good Practice Guidelines 2007, Chapter 6

(6) Chartered Management Institute BCM Survey 2008, page 13

(7) Krishnan, R., et al., In Search of Quality Improvement: Problems of Design and Implementation, The Academy of Management Executive, 1993, 7(4), p 7-20.

the business continuity JOURNAL

DELIVERING IT SERVICE CONTINUITY MANAGEMENT - A CASE STUDY



AUTHORS: Stephen Nuttall, MBCI, head of service continuity in Europe, the Middle East and Africa for EDS and Mark Moody IT service continuity manager for the Department for Work and Pensions, UK government.

ABSTRACT: The Department for Work and Pensions (DWP - the largest government department in the UK) and EDS, one of its key IT service providers have, together with other suppliers, transformed the delivery of IT services into the world class IT Infrastructure Library (ITIL) model. This has required a move from a traditional business continuity and disaster recovery deployment, into an IT service continuity management (ITSCM) model – effectively embedding business continuity for IT services into an end to end IT service approach.

This paper is about how EDS and the DWP worked together to develop and deliver a new model and how we met and overcame the challenges in order to do it.

The context

EDS: As a major provider of IT services to many clients, business continuity has been an essential, indeed critical, part of EDS' services for many years. EDS works closely with its clients and suppliers to ensure that services can be maintained to agreed levels in the event of disruption. However, understandably, clients have become ever more demanding about the standards of service and availability they need to maintain their business and this has meant a fundamentally different cultural approach to how they specify, manage and audit the services they receive.

The DWP plays a key role in supporting the social and economic well-being of the UK. With a turnover of over £100 billion a year and processing 10 million financial transactions a night, it employs over 100,000 staff and has in excess of 100 departmental contact centres. DWP has 20 million customers and helps people to find jobs, supports those out of work, provides security in retirement, strives to advance the rights of disabled people and improve health and safety in the workplace. The UK public relies on these services and rightly expects them to be there when needed. Of equal importance is the ability for DWP to maintain its services to the public in the event of incidents or even disasters. This is where ITSCM has a vital and unique role to play.

The DWP mission and vision for ITSCM

Mission
*"*To ensure DWP IT is resilient and DWP has the capability to withstand an IT disaster and maintain its reputation."

Vision
"To build world-class resilience, crisis management and disaster recovery for DWP IT."

The transformation goal
To move from a mature and well understood business continuity and IT disaster recovery service to a fully integrated, business focussed IT service continuity management service. This would involve confirming where we wanted to get to; where we currently were; and deciding the best way to get from one to the other.

The ITSCM Challenge

ITIL is a very mature and well understood set of principles and high-level processes. Indeed, many organizations, large and small, have been using ITIL, or parts of it, for many years. However, these processes must be tailored for use within the organization – they are principles rather than detailed work instructions.

The ITIL model depends on a number of core services such as change management, release management and configuration management to name but a few; yet as we began to develop the ITSCM processes, none of these were in place in a detailed form – they were being developed in parallel with the other ITIL process. Like many large projects, we have to start before all the details are finalised: apart from anything else, many of the details would be driven out by the earlier stages, so at times, it was as if we were in the middle of a building site with a critical deadline and we had to start building AND finalising the plans at the same time. We were nothing if not busy!

We had had a long and mature business relationship between the DWP and EDS BC teams, yet our relationship was to be tested on many occasions over the coming years as we strove to build a new model that worked for the DWP, the suppliers and which we could both demonstrate as 'delivering the goods' for our various stakeholders.

To start with, we set out a basic visualization of how this might work. This is shown in figure one:

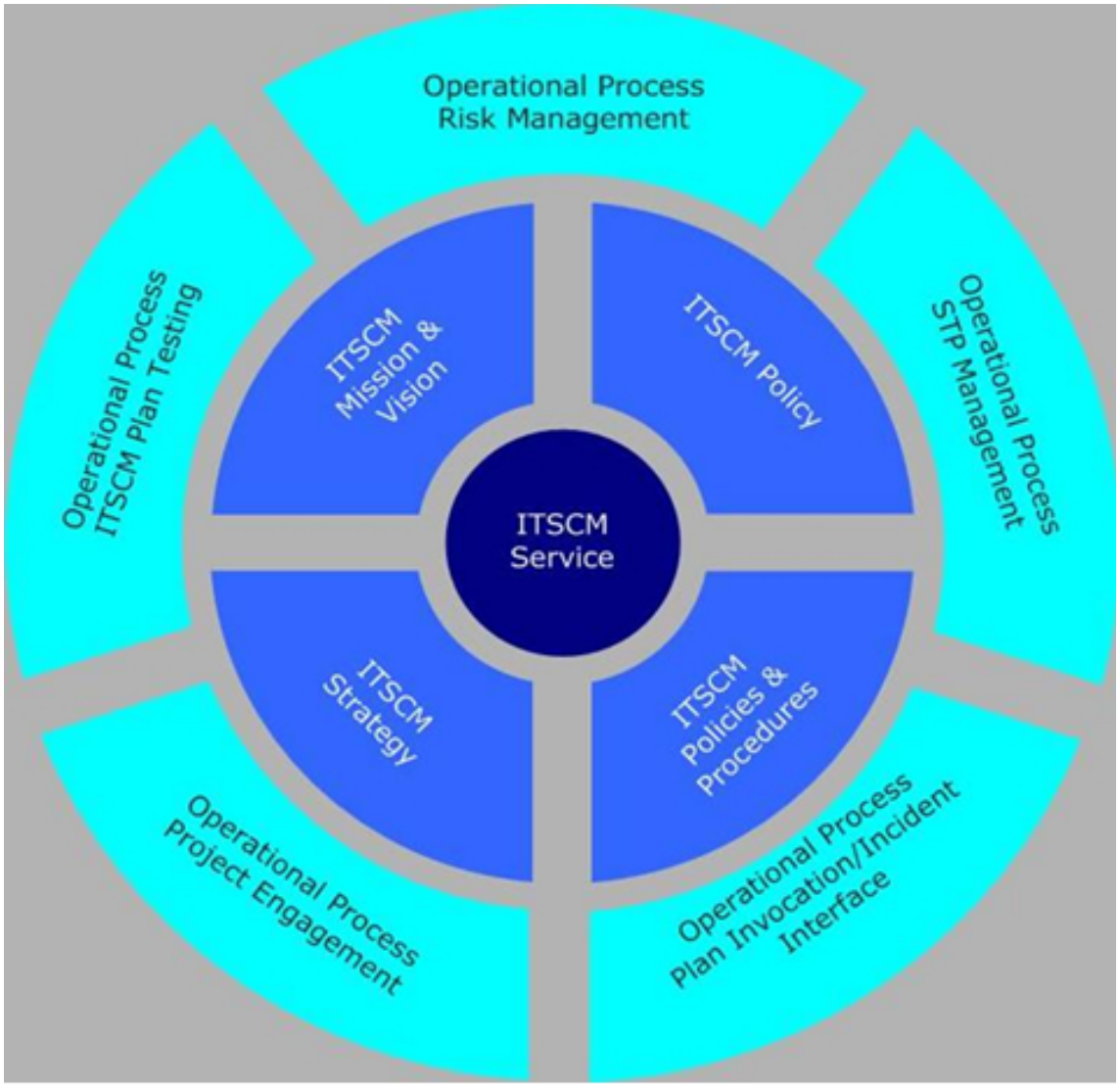


Figure one: Basic visualization

- Over the months and years, this model was shown in many different ways and developed in granularity and depth, yet the basic principles remained the same:
- Ensure that everyone knows what the policies and strategies are;
- Give the key stakeholders the opportunity to clearly state their requirements based on BIA results (and, if necessary, justify their requirement);
- Set an optimal level of service and make sure that every stakeholder knows what THEY need to do and what they should expect
- Decide how the standard will be managed for all the business units and suppliers

- Agree how the service requirements will be validated
- Keep the principles SIMPLE!

The journey – challenge and opportunity

The first thing we found out was that (almost) everyone could see the benefits of implementing ITSCM. The second thing we learned was that (almost) everyone had a slightly different view of how this should be done!

One interesting aspect of the programme was that some areas which we assumed would be a great strength (and indeed, mostly were), also caused some minor difficulties. For example, the fact that the various groups had worked together over many years was a benefit, surely? In fact, at times, it caused us some difficulties. Because we had been involved in delivering a highly effective and mature BC/DR model, we didn't always quite realise just how much of a cultural and operational change was needed in order to transform into the very broad and business-focussed service we needed to provide with ITSCM. (Probably one of the main features of a truly integrated ITSCM service is that it focuses on what the business needs to achieve and demonstrates that it can actually do this. The old, although it has to be said, reliable, IT-DR model focussed more on proving that we could recover the technology components – a quite different matter).

However, there is nothing quite like a deadline to focus the attention and we set up a programme to address these issues and focus on the culture we needed to adopt (focus on business outcomes at least as much as individual deliverables); understand what we needed to achieve and demonstrate, (prove to DWP stakeholders that the solutions put in place would deliver the business outcomes desired); and develop a model that proved this within a multi-supplier environment. (Say what we do, do what we say and prove it matches the strategic and business outcomes required). It wasn't easy, but we got there by working together and being very open and honest with each other.

Quick wins

One of the greatest boosts to any implementation is to get some quick wins: this has benefits both to the stakeholders, who can actually see meaningful progress; and for the teams delivering ITSCM who can begin to see and evaluate what the new services will look like. For us, a great benefit was the experience that many of the team members brought to the programme. We were able to build on this and use it to move forward in a number of areas. The importance of quick wins should not be underestimated: they provide immediate benefits for the organization as well as a psychological boost to the participants.

How do we know when we've 'arrived'?

This is one of those eternally simple questions which seems so easy to answer (we all think we know), but which can occasionally seem like the end of a rainbow! For our programme, the arrival was going to be clearly measured: the programme was run on a formal but adaptable basis. The objectives were broken down into clearly specified deliverables and, most importantly, very specific 'acceptance criteria' were detailed for each of these deliverables. Regular programme meetings took place which ensured that the programme constantly evaluated both progress and, very importantly, the objectives, which often needed to be validated and possibly refined as we got closer to each one. In short, the programme checked that we were still happy that we had a shared understanding of the ultimate programme objectives; that we had a clear statement of the milestones and deliverables to meet those objectives; that we had an agreed schedule for delivery; and, finally, that each deliverable was formally accepted and closed. (This will be no surprise to most project managers, but it is always worth stating the obvious, because what is obvious to one person, is not necessarily obvious to all – as we discovered more than once.)

Key lessons:

Of course, in such a large and diverse programme and organization, there were a lot of lessons: some were new, but others reinforced the need for doing things the way we were, such as the need for clear programme management. Some of the most important lessons included:

- Developing and delivering ITSCM, is not easy – but it is worthwhile.
- ITSCM needed a major change in our working culture compared to our previous BC IT-DR model.
- The culture change was needed in order to help actually deliver the ITSCM model – sounds simple, but it wasn't….!
- A deep understanding of the business needs must be part of the programme development.
- Working together in a constructively critical, but collaborative way was the only way to make sure that this new model worked – but we did have some dark days…
- Share expectations and frustrations – they will cause problems if we don't.
- Manage the risk all the time and minimise the risk exposure.

- Keep business as usual focussed on delivering – it's easy to overlook this in the middle of a major transformation.

- The only 'dumb' questions are the ones we don't ask…!

Benefits

Now that the transformation has been completed and the operational benefits are in place, we can see that getting ITSCM right saves time and money, protecting both the interests of our business(es) and our customers. Most importantly, the senior stakeholders have assurance that whatever happens to the organization, they can be assured of an agreed level of service and priorities which support their business and they can base all their internal BC plans on these assumptions.

Authors

Stephen Nuttall, MBCI

Stephen Nuttall is the head of service continuity in Europe, the Middle East and Africa for EDS, (part of HP), which is one of the world's leading IT Service companies with clients around the world. Stephen has been involved in BC for over 18 years in both the government and public sectors. As well as being a member of the BCI, Stephen has been an ISEB qualified IT Service Manager since 1997, working in a number of ITIL disciplines as well as ITSCM.

Mark Moody, MBCI

Mark Moody is the IT service continuity manager for the Department for Work and Pensions, the largest government department in the UK. For more than 23 years Mark has held a variety of key IT related roles in both the public and private sectors. An ISEB qualified IT Service Manager, for the last 9 years, Mark has specialised in business and service continuity and risk management, more recently implementing the OGC M_o_R approach for DWP ITSCM. In addition to the BCI, Mark is also a Member of the British Computer Society (MBCS).

Research roundup

A brief summary of commercial and academic business continuity research which has been published between September 2008 and January 2009

ENISA survey looks into resilience of communication networks

The EU Agency ENISA (the European Network and Information Security Agency) has published a report on the resilience of communication networks.

The survey found that operators take network resilience seriously:

- It found a better than expected network availability, with only 10 hours downtime a year on average.
- Top network threats are hardware, software and location incidents, but also personnel incidents were also significantly represented.
- Operators describe their network and risk management procedures as 'fairly mature'.
- There is no significant variation by size of operator regarding business continuity procedures.

The report was Commissioned by ENISA and executed by the IDC.

http://www.enisa.europa.eu/pages/02_01_press_2009_01_22_network_resilience.html

Pandemic planning slips down the UK business agenda

New research, collated by the Continuity Forum and funded by Roche Products Ltd, has found that three quarters of UK bosses (73 percent) are not supportive of pandemic planning activities. This is despite the National Risk Register highlighting influenza pandemic as being the greatest single current threat to Britain.

With experts also agreeing that there is a high probability of an influenza pandemic occurring, the research underlines the vulnerability that businesses are leaving themselves open to, with over a third (36 percent) of companies having no plans to address staff absence, and just 11 percent of businesses establishing stockpiles of antiviral medication to protect their employees.

The research, based on the responses of over 1,500 business leaders, also found that UK businesses are ignoring the likely financial implications of a pandemic, with 91 percent of respondents reporting that they have not assessed the financial impact that a pandemic would have on their business. Furthermore, 88 percent of respondents with a pandemic plan state that their plan takes no account of finances or cash flow.

The research suggests that much of this ill-preparedness stems from a culture of complacency amongst UK business leaders. When asked about the likelihood of a pandemic hitting their organization, 72 percent of businesses reported feeling it was unlikely, and even 61 percent of staff charged with sole responsibility for emergency planning reported a sentiment within their organizations that a pandemic was unlikely.

Worryingly, the research, also uncovers superficial preparation amongst those businesses who claim that they are in a safe position to address the risk and disruption caused by a pandemic. Of the businesses who claim they are prepared, two-thirds (67 percent) admit that their plans will not be complete for at least one year and half (50 percent) report that they have not tested their plans in the last two years.

The impact of the global financial crisis on the business continuity market

The final results of a recent survey by Continuity Central entitled 'The global financial crisis and its impact on the business continuity market' show that the effects of the credit crunch vary markedly from region to region.

212 responses were received in total from all around the world. Regions providing the highest response rates were:

- Australia and New Zealand: 10 percent
- Canada: 4.7 percent
- SE Asia: 4 percent
- UK: 35 percent
- US: 21 percent
- Western Europe (excluding the UK): 11 percent

74 percent of respondents were from large organizations (over 500 employees), 12 percent from medium (100 to 499 employees) and 14 percent from small organizations (less than 100 employees).

Many respondents came from the financial sector and related areas, with respondents by sector including:

- Banking: 13 percent
- Computer hardware, software & services: 5 percent
- Energy and other utilities: 4.7 percent
- Financial services: 30 percent
- Insurance: 5.1 percent
- Public sector 13.6 percent
- Telecommunications 4.2 percent

Responses by question:

1) Has the global financial crisis and the credit crunch had an impact on business continuity planning in your organization?

In total, 57 percent of respondents said that the global financial crisis and the credit crunch had had no impact on business continuity planning in their organization. 33 percent reported that it had had a negative impact and 10 percent said that its impact had been positive in terms of business continuity planning in their organization.

When broken down by organizational size some differences could be seen. Medium sized organizations reported the most impact on business continuity activities, with 38 percent reporting a negative impact. 34 percent of large organizations also reported a negative impact; but only 27 percent of small organizations did.

Large organizations were most likely to state that the global financial crisis and the credit crunch had had a positive impact on business continuity activities; 11 percent stated that this was the case, compared to 6 percent of small organizations and zero medium sized organizations.

67 percent of small organizations said that the global financial crisis and the credit crunch had had no impact at all on business continuity activities. 55 percent of large and 62 percent of medium sized organizations also reported that this was the case.

Regional differences were quite striking, with Western Europe-based organizations apparently being least affected, closely followed by UK organizations. Those located in the United States were the most badly impacted.

The following shows the percentage of regional respondents who said that the global financial crisis and the credit crunch was having a negative impact on business continuity planning in their organization:

- W.Europe: 23 percent
- UK: 33 percent
- SE Asia: 37 percent
- Canada: 40 percent
- Australia and New Zealand: 41 percent
- US: 47 percent

And the following shows the percentage of regional respondents who said that the global financial crisis and the credit crunch was having a positive impact on business continuity planning in their organization:

- Australia and New Zealand : 0 percent
- SE Asia: 0 percent
- W.Europe: 4 percent
- US: 9 percent
- UK: 13 percent
- Canada: 20 percent.

How has spending on business continuity been in 2008 compared to your expectations?

A slim majority (52 percent of respondents) reported that spending on business continuity in 2008 had matched their expectations. However 36 percent said that it had been lower (23 percent) or much lower (13 percent) than expected. Only 12 percent stated that spending was higher (9 percent) or much higher (3 percent).

Regional differences were again apparent. In some regions the majority of respondents reported that business continuity spending was lower than expected. Those based in SE Asia appear to be most affected, with 62.5 percent of respondents reporting that business continuity spending was lower (50 percent) or much lower (12.5 percent). The United States also appears to be badly affected, with 52 percent of respondents reporting that spending was lower (29 percent) or much lower (23 percent).

Spending seems to be holding up best in the United Kingdom, with only 25 percent of respondents saying that it would be lower (20 percent) or much lower (5 percent) than expected.

The full regional breakdown follows:

Australia and New Zealand

Business continuity spending will be:

- Same as expected: 59 percent
- Lower than expected: 19 percent
- Much lower than expected: 22 percent
- Higher than expected: 0 percent
- Much higher than expected: 0 percent

Canada

Business continuity spending will be:

- Same as expected: 50 percent
- Lower than expected: 30 percent
- Much lower than expected: 0 percent
- Higher than expected: 20 percent
- Much higher than expected: 0 percent

SE Asia

Business continuity spending will be:

- Same as expected: 25 percent
- Lower than expected: 50 percent
- Much lower than expected: 12.5 percent
- Higher than expected: 12.5 percent
- Much higher than expected: 0 percent

UK

Business continuity spending will be:

- Same as expected: 61 percent
- Lower than expected: 20 percent
- Much lower than expected: 5 percent
- Higher than expected: 12 percent
- Much higher than expected: 2 percent

US

Business continuity spending will be:

- Same as expected: 39 percent
- Lower than expected: 29 percent
- Much lower than expected: 23 percent
- Higher than expected: 4.5 percent:
- Much higher than expected: 4.5 percent

W.Europe

Business continuity spending will be:

- Same as expected: 54 percent
- Lower than expected: 21 percent
- Much lower than expected: 17 percent
- Higher than expected: 4 percent
- Much higher than expected: 4 percent.

How will spending on business continuity in 2009 compare to spending in 2008?

Overall, the majority of organizations expect business continuity spending to hold up in 2009, with 42.5 percent stating that it would be the same in 2009 as it was in 2008 and 20.5 percent expecting it to be higher (19 percent) or much higher (1.5 percent) in 2009. 37 percent anticipate that business continuity spending will fall: 20 percent say that spending will be lower in 2009 compared to 2008 and 17 percent state that it will be much lower.

Organizations based in the United Kingdom were the most positive. Only 24 percent thought that spending would be lower (16 percent) or much lower (8 percent) in 2009. This was followed by Western Europe-based organizations, where only 30.5 percent thought that business continuity spending would be lower (13 percent) or much lower (17.5 percent) in 2009 compared to 2008.

The most pessimistic respondents were based in the United States. Here, 51 percent thought that business continuity spending would be lower (29 percent) or much lower (22 percent). SE Asia followed closely behind, with 50 percent of respondents believing that spending would be lower (25 percent) or much lower (25 percent).

The full regional breakdown follows:

Australia and New Zealand

Compared to 2008, business continuity spending in 2009 will be:

- Much lower: 24 percent
- Lower: 19 percent
- Same as 2008: 38 percent
- Higher: 19 percent
- Much higher: 0 percent

Canada

Compared to 2008, business continuity spending in 2009 will be:

- Much lower: 10 percent
- Lower: 30 percent
- Same as 2008: 40 percent
- Higher: 20 percent
- Much higher: 0 percent

SE Asia

Compared to 2008, business continuity spending in 2009 will be:

- Much lower: 25 percent
- Lower: 25 percent
- Same as 2008: 50 percent
- Higher: 0 percent
- Much higher: 0 percent

UK

Compared to 2008, business continuity spending in 2009 will be:

- Much lower: 8 percent
- Lower: 16 percent
- Same as 2008: 57 percent
- Higher: 17.5 percent
- Much higher: 1.5 percent

US

Compared to 2008, business continuity spending in 2009 will be:

- Much lower: 22 percent
- Lower: 29 percent
- Same as 2008: 29 percent
- Higher: 18 percent
- Much higher: 2 percent

W.Europe

Compared to 2008, business continuity spending in 2009 will be:

- Much lower: 17.5 percent
- Lower: 13 percent
- Same as 2008: 52 percent
- Higher: 17.5 percent
- Much higher: 0 percent.

Thinking of staffing requirements in the business continuity team in your organization, how has this changed recently?

The majority of organizations seem to be maintaining business continuity teams at their current levels. 64 percent of total respondents said that this was the case. 22 percent of organizations reported that they had a reduced requirement for business continuity staff and 14 percent said that they had recently taken on more team members.

Job losses appear to be highest in the Australia and New Zealand region, with 40 percent of respondents stating that staffing requirements were reduced. Western Europe organizations also reported high numbers of staff reductions (30.5 percent of organizations had a reduced requirement) but this region also reported the highest growth, with 17.5 percent of organizations saying that they had recently taken on extra business continuity team members.

The full regional breakdown follows:

Australia and New Zealand

Business continuity staff numbers have recently been:

- Reduced 40 percent
- Increased 10 percent

Canada

Business continuity staff numbers have recently been:

- Reduced 10 percent
- Increased 10 percent

SE Asia

Business continuity staff numbers have recently been:

- Reduced 12.5 percent
- Increased 12.5 percent

UK

Business continuity staff numbers have recently been:

- Reduced 17.5 percent
- Increased 9.5 percent

US

Business continuity staff numbers have recently been:

- Reduced 24 percent

- Increased 9 percent

W.Europe

Business continuity staff numbers have recently been:

- Reduced 30.5 percent
- Increased 17.5 percent.

Will the financial crisis result in more regulations related to business continuity?

The final question in the survey looked at the issue of regulation and asked whether respondents thought that regulations relating to business continuity would increase as a result of the global financial crisis and the credit crunch.

Overall, 44 percent of respondents expect more business continuity related regulations and 56 percent do not. No respondents expected less regulation in future.

Respondents from the financial services and the banking sector were the most expectant of new business continuity regulations (62 percent and 61 percent, respectively, anticipate more regulations in future as a result of the global financial crisis and the credit crunch). However, only 27 percent of those from the insurance industry expect to see increased regulation. 40 percent of telecommunications sector respondents expect more business continuity regulations, which is the highest level outside financial sectors. This was followed by energy and other utilities (30 percent), the public sector (24 percent) and computer hardware, software & services (23 percent).

When looked at regionally, Western Europe was the only area where the majority of respondents expect to see more regulations relating to business continuity as a result of the financial crisis and credit crunch. The United States was the region with the least expectation of this, with only 34 percent of respondents anticipating more regulation. The full list follows:

Percentage expecting more business continuity regulations as a result of the financial crisis and credit crunch:

- W.Europe: 56 percent
- SE Asia: 50 percent
- Canada: 40 percent
- UK: 39 percent

- Australia and New Zealand: 36 percent
- US: 34 percent.

Survey finds that business continuity information is not being disseminated in many UK organizations

Less than 50 percent of UK workers have been advised what to do in the event of their workplace becoming inaccessible.

New research by YouGov on behalf of the BCI Partnership reveals that less than 50 percent of UK workers have been advised what to do in the event of their workplace becoming inaccessible following an incident such as a fire or flood.

Key results from the October poll also show that less than 30 percent of workers thought their employer could survive a continued disruption for over six months with nearly 20 percent fearing their employer would be out of business within one month.

On a personal level 44 percent of respondents felt their families would start to suffer after just four weeks if continued disruption at work meant the loss of the family's main income.

The poll, which covered 2000 UK adults, also explored workers' understanding of the term 'business continuity management' showing a generally poor level of knowledge of the discipline with marked regional variations indicating that workers in London had a better understanding.

Stratus survey provides US business continuity snapshot

A survey by Stratus Technologies has sought to capture an overview of the current state of business continuity planning in the US.

Stratus asked whether business continuity is a priority at respondents' companies; whether they actively follow a plan to ensure business continuity; if they believe that implementing a business continuity plan provides a significant competitive advantage; and how often they test their business continuity plan.

Business continuity was a strategic priority for 76 percent of the companies surveyed, 69 percent said they followed a business continuity plan; and 86 percent believe that a business continuity plan is a significant strategic advantage. However, only 45 percent of companies following business continuity plans tested them more than once a year. Of the remaining companies, 35 percent tested yearly, and 20 percent not at all.