

The Business Continuity Management Toolkit

GARY HIBBERD



PUBLISHED BY **ark** GROUP G R O U P IN ASSOCIATION WITH **InsideKnowledge** **Managing**PARTNER

Contents

Executive summary.....	IX
About the author.....	XI
Dedication	XIII
Acknowledgements	XV
PART ONE – Introduction	
Chapter 1: Why does an organisation need a BCM framework?	1
The role of the business continuity manager	1
Should your organisation employ a full-time BCM practitioner?.....	1
What makes a good BCM practitioner?.....	1
The vital ingredient for success in BCM	3
Reasons for implementing a BCM framework	3
It could be you.....	7
Chapter 2: The definition of BCM.....	9
What is BCM?	9
The components of BCM.....	9
Where is BCM’s place in an organisation?	10
Budgeting for BCM	11
The BCM project cycle	11
Project timeline	11
Do I need special software to implement a BCM strategy?	11
Chapter 3: The BCM standards	13
Which Standards should I follow – BS25999-2 or BCI GPG?.....	13
The life cycle of BCM.....	14
Chapter 4: The BCMS framework	17
Creating your BCMS	18
Policy, strategies, Terms of Reference (ToR), procedures and guidelines.....	18

PART TWO – The Five Key Phases of Implementing a BCM Strategy

Phase 1: Project and Initiation

Chapter 1: The project management process 25
 Communication – integral to effective BCM 25
 Tips for gaining support for your BCM project..... 25

Chapter 2: Project definition..... 29
 Scope and objective..... 29
 Critical Success Factors 30
 Resource requirements 30
 Timelines..... 30
 Major milestones 31
 Deliverables 31

Chapter 3: Organisational buy in..... 33
 BCM steering committee 33
 Selling BCM to stakeholders 33
 Selling business continuity to senior managers..... 34
 Stakeholder analysis..... 35
 Your vision 37
 Establish why you’re doing this..... 38
 Establish the goals of your line manager, your function and your business..... 38
 Write your own ‘Mission Statement’ 38

Chapter 4: The BCM policy..... 41
 What should the policy contain? 41
 Policy development 42
 Policy example..... 42
 Step one – What the policy should state 42
 Step two – BCM steering group review 43
 Step three – Publish..... 44

Chapter 5: The BCM strategy 45
 Strategy development 46
 Understanding the customer 46

Chapter 6: The BCM charter 47
 What the charter should contain 47
 Roles and responsibilities of the EMT 47
 Taking the business with you on the BCM journey..... 48

Phase 2: Understanding the Organisation

Chapter 1: The BIA and RA – Critical components of a BCP	51
The BIA and RA	51
The BIA.....	51
Components of the BIA	55
Dependencies.....	57
Recovery requirements.....	58
What’s next?	61
RA	61
What is risk?	61
The final analysis	65
Chapter 2: The development of recovery strategies	67
What is a fit-for-purpose incident response structure?	67
What is the ICS?.....	68
What should my ICS look like?	69
Who should be part of the team and the structure?	70
Reaction experiment – The Smoke Filled Room.....	72
How do I determine how we will recover each critical activity within its RTO?	72
What do I do with this information?	73

Phase 3: Practical Implementation Begins

Chapter 1: Implementing your BCM strategy	79
Crisis management, BCP and DR.....	79
What makes a good plan?	80
One plan or more?.....	81
Chapter 2: Crisis management plans	83
What does a CMP look like?	83
Reaching the CMT	84
How is the CMT invoked?	84
Invoking the CMT in practice	86
Command centres	87
The author’s experience	88
Management of the crisis	89
An example of a CMP.....	90
Management of the incident	91
Chapter 3: Responsibilities and actions	93
Recovery focus.....	94
Contacting people	95
Invoking DR.....	97
Recovery sites	98

Chapter 4: Other CMPs	99
Media CMPs	99
Reputational risk	99
The Lockerbie disaster	101
Chapter 5: Business continuity plans	103
How many plans do I need and what size should they be?	103
Creation of the BCP	103
Invoking the BCP	104
Plan scenarios	105
The detail	105
Business Recovery Team (BRT)	106
Loss of people	107
Loss of site (also known as denial of access)	107
Loss of systems/technology	112
Loss of providers	115
Returning to BAU	115
Useful information (also known as the 'Appendix')	117
Pandemic plans	119
Chapter 6: Disaster recovery plans	125
Mission-critical and/or business critical services.....	125
Meeting with IT	127
Who should complete the DR plans?.....	129
What does the DR plan look like?	130
The disaster recovery strategy.....	132
Post-disaster recovery	135
Post incident review	135
Crisis management, business continuity and disaster plan sign off	136
Post Incident Reviews (PIR) and Root Cause Analysis (RCA)	136
BCPs and incident management plans.....	138
Phase 4: Maintaining your BCP	
Chapter 1: Exercising your BCP	143
How do we exercise BCPs?	143
Where do we begin?.....	143
The scope	144
The types of exercises.....	145
The story of a hero.....	160
Chapter 2: Maintaining and reviewing your BCM processes	161
The reviewing of BCM arrangements.....	161

Auditing	162
Example of an index in the annual report.....	163
Phase 5: Embedding BCM in the Organisation	
Chapter 1: Achieving organisational buy in	167
Preventative and corrective actions	167
The BCM awareness strategy	169
What do people know about BCM currently?	169
How do I deliver my awareness?	171
Tools.....	172
Afterword.....	175
Appendix	177
Index	179

Executive summary

FLOODS, TERRORISM, war, global economic crisis, pandemics, plane crashes and severe weather – you would think that this is a list from the Bible, yet all of these events have occurred in the past 12 months, affecting people and businesses in the UK. Some of them occurred quite literally ‘out of the blue’, whilst others were disasters in slow motion.

These incidents have created a nervous society. Clients and regulatory bodies are looking more closely at an organisation’s ability to not only recover from a disaster, but reduce the chances of a disaster occurring. Over the past ten years, clients and regulators have moved from asking about disaster recovery (what happens after the incident) to business continuity (what happens before, during and after the incident). This process is entitled business continuity management (referred to throughout this report as BCM). BCM – the ability to react to, and recover from any given event – is increasingly becoming a market differentiator and is certainly a matter for regulatory scrutiny. Those businesses which embrace BCM will undoubtedly capitalise on recovering faster than their competitors. Sympathy goes a long way when a business is impacted by a fire, but that sympathy soon runs dry when clients don’t receive the service they want and need within agreed timescales. Effective BCM will help improve a business’ reaction to incidents, ensuring people and/or services are mobilised to fix the issue and

that this is communicated to affected areas of the business. Contingency processes will reduce the impact on the business by deploying work around solutions and, finally if required, disaster recovery (DR) processes can bring the business up and running.

On small mundane incidents, BCM can help identify bottlenecks, single-points-of-failure (SPoFs) and small issues, which could be costing your organisation money everyday of the year. On larger events, BCM can help identify where your recovery efforts should be focused so that you can recover the business according to what is most vital to your survival.

Without an effective BCM in place, the decision-making process is made ‘on the fly’ and prone to mistakes, leading to delays in bringing back your business. But there is a general problem in implementing an effective BCM framework. Few people understand exactly what is required, it takes a long time to implement, tools and approaches are different (depending on the level of experience of the practitioner) and there is a perception that there has to be large costs in its development. While no two organisations are the same, the problems they face are similar and, therefore, the tools and methodology for implementation should be built on best practice and/or on proven techniques.

This report is a comprehensive step-by-step guide on implementing a successful BCM framework and discusses Business Impact Analysis (BIA), risk assessment (RA), who should be involved in the strategy and

process, what tools are needed and how they should be deployed, how to sell your business continuity strategy to decision makers, and how an effective BCM structure not only improves your performance in a crisis, but satisfies regulatory requirements, clients' needs and drives down operational losses. A business continuity strategy cannot work without strong project management and communication skills, and these often-neglected aspects of the BCM process are examined in this report.

This report covers the complete life cycle of BCM as outlined in the industry standards for business continuity – BS25999-2 and the BCI 'Good Practice Guide' (BCI GPG). It is divided into five phases which represent the key stages of a BCM strategy and framework implementation:

- Phase 1: Project management and initiation;
- Phase 2: Understanding the organisation;
- Phase 3: Developing and implementing a BCM strategy;
- Phase 4: Maintaining your BCP; and
- Phase 5: Embedding BCM in the organisation.

Each phase includes practical examples – both fictional and real-life – and templates to support the points discussed, so that the reader can immediately put the guidance into practice.

This report intends to be accessible to both the practitioner new to BCM as well as the more seasoned practitioner. When writing, I challenged myself to make this topic come to life as much as possible as compared to what a lot of people in the industry think, there is an exciting side to BCM, as the reader will discover.

About the author

GARY HIBBERD has been working as the risk and business continuity manager for Irwin Mitchell Solicitors LLP, a top 20 law firm in the UK, for the past 18 months, but has over ten years' experience in business continuity management. Prior to joining Irwin Mitchell, he held the position of UK business continuity manager and European crisis management leader for GE Money, Europe. He helped to develop global strategies on business continuity, often travelling throughout Europe, America and Australia to demonstrate how to implement tools used to embed business continuity management in the organisation. With a background in IT and information security, Gary's experience is derived from practical application of the strategies he helps organisations develop. With a keen eye for what works and what does not, he approaches every new challenge with enthusiasm and a belief that a single positive act can make a difference.

Dedication

THIS REPORT is dedicated to those individuals who are not afraid to ask the difficult questions and to speak up whilst others remain silent. These are the people who embrace change and see change as a challenge and an opportunity to improve and grow – the optimistic pessimist who understands that sometimes things go wrong but feels that there are actions we can take to change the outcome.

More personally, I would like to dedicate this report to my wife Sue whose love, support, encouragement and good humour have enabled me to accomplish more than I thought possible. Also to Luke and Jessica who I am continually proud of and love – thank you for making me smile every day. To my family for all their encouragement and support and to my mother Von, whose strength and personality are truly an inspiration. Finally, this report is dedicated to the memory of my father Ray Hibberd who I miss more than I thought possible, and who showed us what love, strength, hard work and endurance can achieve. For this, I am eternally grateful.

Acknowledgements

THE AUTHOR would like to acknowledge the professional and eloquent editing of this report undertaken by Ark Group editor Stephanie Ramasamy, who ensured the right words fell into the right places and offered gentle encouragement where needed.

Thanks also to the Business Continuity Institute for allowing me to include the 'Good Practice Guide' (BCI GPG) within this report and to the British Standards Institute who also gave permission to include extracts from the British Standard for Business Continuity Management (BS25999-2).

The BCI GPG can be downloaded free of charge from: <http://www.thebci.org/gpg.htm>. This is a useful resource which supports this report.

The BS25999-1 and BS25999-2 publications can be purchased from the BSI website at: <http://www.bsigroup.com>. BS25999-1 is a Code of Practice whilst BS25999-2 is the Standard against which your business can be accredited. Both publications are useful in the further development of the BCM framework.

Disclaimer

This report and the CD-ROM are provided by way of a self-help manual and not a formal advice note. They must not be construed as providing specific advice for any given organisation. No guarantee is given as to the effectiveness of any of the recommended procedures, or the accuracy of these materials, and it is for each organisation to consider its own approach to BCM, having regard to all the information sources that are open to it. To the extent permitted by law, Gary Hibberd and Ark Conferences Ltd and/or their servants and agents will accept no liability for any action taken or not taken, or the consequence of any action taken or not taken, as a result of these notes, or any training session or general consultation on this topic.

PART ONE

Introduction

Chapter 1: Why does an organisation need a BCM framework?

The role of the business continuity manager

Managing business continuity is one of the more unique roles within an organisation. Rarely does a discipline give you an access-to-all-areas status. You have before you the opportunity to raise your profile, be noticed, talk to the decision makers, influence strategic decisions, have input and impact on projects, help reduce cost and possibly be a key player during major events affecting your business.

A key success factor in BCM is being able to develop a BCM culture (see Phase 5 in this report). But in order to create a cultural change, we have to change behaviour. You have to change how people think, feel and react to what you're giving or saying to them. What may not be obvious to you now is that, to be truly successful in BCM, you're going to have to work on your skills as a salesperson. If you have a background in this area, you'll understand the importance of getting people to believe in the product, and in order to make them believe, you have to believe first.

If you are interested in making your business more resilient, productive and reliable, then you need every skill and trick available to help others see just how BCM impacts them and how they have a part to play.

BCM is unlike the vast majority of disciplines in that it does not deal in absolutes or certainties – it deals in possibilities and uncertainties. It is our role to ask the questions that others either don't

think of or ignore, because the truth is too ugly to consider. I call this the 'Ostrich Syndrome'. Our role is to ask: 'what if that part fails or how long can we manage without the component of that product?' Essentially, we ask the difficult questions, the ones others may be thinking, but are afraid of voicing. My opening line in these situations is, 'I'm going to ask you some dumb questions, because I'm good at them...'

Should your organisation employ a full-time BCM practitioner?

The answer to this is dependent upon the size and complexity of your business. If you are a practice with two or three other partners all operating from a small office in a city centre, then the answer is mostly likely that one person can be assigned the responsibility for managing associated documentation and the BCM framework.

However, if your business employs a larger group of people, disbursed over different geographical locations (and possibly even time zones) then there is a justification for assigning this task to a single individual to work on full time. It is unquestionable that auditors and clients alike will be unimpressed if you've simply given the task of putting together your BCM framework to an overworked member of the business, who already has too much to do on a daily basis.

What makes a good BCM practitioner?

To succeed in BCM requires a set of qualities, which are just as important

as the set of skills required. Mike Hager, CEO at Business Risk Management Group coined the term 'Optimistic Pessimist' in an internet article:¹

"I often tell a joke about a little boy who gets thrown into a room with a 10-foot-high pile of horse manure, and he comes out saying, 'Hey, where there's this stuff, there's gotta be a pony, right?'

"Pessimists believe that there are all kinds of threats out there, but there's no way to keep them out. Optimists say, 'Yeah, I know there's an opportunity for people to attack, but we haven't been attacked in 20 years, so why worry about it?' I'm the optimistic pessimist, I actually believe something is going to happen, but I'm crazy enough to believe that I can do something about it."

This identifies the outlook one must have to not only participate in this area, but to maintain a sense of perspective.

As any BCM practitioner will testify, the only certainty in BCM is that you will experience negativity and apathy for what you are endeavouring to deliver. If you're new to BCM, the following are some universal truths, and if you've been involved in this area for a while, you'll recognise the prevailing perceptions:

- You're going to help people put plans in place which you hope will never be used;
- You're implementing something which few see the value of, until it happens;
- You'll never be finished – a little like painting the Golden Gate Bridge, once you get to the end it's time to start over;
- It's unlikely that people are going to be pleased to see you; and

- You're probably going to be accused of being a 'voice of doom'.

If you're the type of personality that thrives on pleasing people and delivering an end-product, then unless you can adapt (and quickly), you'll find yourself struggling to cope with some of the negative attitudes that you'll likely experience in this area.

When we think of skills, we traditionally think of project management or experience in the chosen profession, and whilst these are certainly important and advantageous, having good communication skills is of vital importance in BCM. When I say communication skills, I'm also referring to negotiation and influencing skills.

Communication is a two-way exchange, and one of the most valuable skills you should possess (or should look to improve) is the ability to communicate effectively, taking notice of what is said – both verbal and non-verbal – and reacting accordingly.

I believe the most important, traditional skills a BCM practitioner should possess are:

- Project management;
- Leadership;
- Organisational;
- Facilitation and presentation;
- Verbal and written communication (this is not to be underestimated); and
- Understanding of a variety of IT technology (from networks and telephony, to infrastructure).

These skills will be put to the test in all the five phases of implementing a BCM strategy – project initiation, analysis of data/information, development and implementation of strategies, presenting to board-level teams and interviewing managers at all levels of the business. It is also important to consider the value of softer qualities. In my view, a good

BCM practitioner needs to be tenacious, hard-working, interested in the discipline, organised, creative, have a good sense of humour and have a keen eye for detail, whilst being able to step back and see the bigger picture. If you're a BCM practitioner already, ask yourself if you possess these skills. I don't imagine this is an all-inclusive list, but it's not far off.

The vital ingredient for success in BCM

The holy grail of BCM is to implement an infrastructure which impacts upon the culture – to make it risk aware and risk enabled. In order for this to happen, people must change their attitude to risk and towards BCM. BCM needs to be seen as an enabler and a tool to reduce loss. For this to happen, there must be leadership commitment and buy in from the top of the organisation, which will then feed down into the board and further into the business. If senior management pay lip-service to BCM, it quickly becomes evident and others will follow their example. Senior managers must be seen to promote and support BCM in a public and visible fashion, because without this effort, the BCM programme will quickly stall and fail.

Working example

Working in a call centre, John, BCM manager was sat in a meeting with a number of senior IT managers, including the IT director. The meeting was to discuss the movement of the IT communication centre from the third to the sixth floor.

The meeting was going well, with everyone discussing the phased approach to moving the most important

systems first and ensuring engineers were onsite to support the move. How could the move fail?

John: "When was the last time we shut down the mainframe in that room?"

Silence fell on the meeting.

IT manager: "Not while I've worked here. So, at a guess, about eight years."

John: "So, do we know it'll come back online?"

Discussions then turned to the possibility of the critical server not coming back online. An engineer was secured to be onsite at the time of the planned shutdown, which turned out to be a good thing. During the move, the server had several problems and the engineer was able to recover the service in a matter of a few hours rather than a couple of days.

Reasons for implementing a BCM framework

There is a common trap which business continuity practitioners fall into when thinking about risk and the reasons why a business must adopt a BCM framework. They focus on negative events, such as what happens if the business is hit by a hurricane, how should it react in a fire or where should staff go if the office is flooded. While these are important questions, there are other reasons for implementing a BCM framework.

A business imperative

From a business perspective, there are a number of very good reasons to ensure you

consider what can go wrong and build in contingency into your processes. It reduces waste, problems are identified sooner, work-around solutions can be developed, the impact felt by an event can be identified early on and decisions on how to deal with the event can be made. Having a well-understood and considered continuity process in place can improve your speed to respond, which enables you to return to normal services faster.

In today's marketplace, reputation and reputational risk are of key concern to any business wishing to secure a long-lasting future. An effective response to an incident can quickly establish your business as one which is able to control its risks and meet them head-on. The importance of this should not be understated.

In the past, BCM and its core components have suffered greatly because there hasn't been any real impetus to undergo the growing pain that comes from proper contingency planning. It is true to say almost all businesses have some element of contingency plans or disaster recovery measures. It seems then that most businesses both in the public and private sector have got along just fine without a true BCM framework in place, leading to the question – why bother? The simple answer to this is the increasing level of scrutiny both from clients and regulatory bodies. They need to see that a business is managing its risks in an effective manner, and typically this means having a BCM structure.

Further in this chapter, risks associated with critical third parties and establishing the level of contingency in place for them are discussed. It is true to say that individual clients may not ask too many questions about your ability to recover from, or react to, a major incident, but if you deal with corporate entities (particularly financial services), you

will undoubtedly need to have a response to questions surrounding your capability to recover from an incident. However, if (and when) an incident occurs, corporate and individual clients will both want to know why they were affected and what you're doing to recover from the incident.

Regulatory imperative

I hinted at the importance corporate bodies are placing on BCM and this scrutiny is largely a result of increased regulatory requirements placed upon organisations in various industries – both directly and indirectly.

The Financial Services Authority (FSA) has, for a number of years, required organisations to understand their risk profile and to evidence that they are taking appropriate actions to manage those risks. This is due, in part, to a number of high-profile events in the financial world, such as the Barings Bank collapse and the Enron collapse. Both of these events were largely caused by inadequate controls surrounding risk or loop-holes, which allowed individuals to commit fraud resulting in the loss and misappropriation of millions of pounds and dollars.

Increased risk controls were needed and quickly introduced, with Sarbanes Oxley (SOX) in the US and BASEL I and later BASEL II in order to regulate the banking industry, ensuring shareholders and investors would not be exposed in the future. Banks and financial institutions are now required to understand and manage their risks at a granular level, assessing both internal and external threats/risks.

Therefore, one of the many risks identified by financial businesses is the risk of failure or loss of a critical provider or supplier. It is no longer acceptable to merely ensure that your organisation has plans and

processes in place to manage an incident, but that you have considered the possibility and impact upon your own business should a key provider also incur a disaster. It is for this reason that corporate bodies (regulated by the FSA) will need evidence of your ability and that of your providers and suppliers to recover from a crisis. If you or your clients are regulated by the FSA, then there is a need to identify, manage and mitigate risks to your business in a structured and controlled manner.

The legal industry, for example, is regulated by the Solicitors Regulation Authority (SRA), which introduced the Solicitors' Code of Conduct 2007. This states that a law firm needs to manage its risks and minimise disruption to its clients. On business continuity, Rule 5 of the Code outlines:

"5.01 Supervision and Management responsibilities

(1) If you are a principal in a firm, a director of a recognised body which is a company, or a member of a recognised body which is an LLP, you must make arrangements for the effective management of the firm as a whole, and in particular provide for:

- a. The continuation of the practice of the firm in the event of absences and emergencies, with the minimum interruption to clients' business; and
- b. The management of risk."

Interestingly the model employed to develop the Code of Conduct is based upon the FSA's own model and, therefore, it is envisaged that the focus on effective risk management will continue to increase in the legal industry.

Accreditation against the Standards

In 2006 the British Standards Institute (BSI) introduced its Code of Practice for BCM –

BS25999-1 (Part 1) and in 2007 this was recognised as the standard by which a company could be assessed – BS25999-2 (Part 2). The Code of Practice (Part 1) outlines the approach a business should take to implement BCM whilst Part 2 details what must be in place in order to be accredited.

Much of this report focuses on this Standard as it is becoming increasingly recognised as the *de facto* standard and companies which operate in accordance with it can offer assurances to clients and regulators that they are in control of the disaster recovery risk.

There is also the Law Society's Lexcel Standard which was introduced in 2004. Section 4 of the guidance on the Lexcel Practice Management standard states:

"4.3 There should be a business continuity plan envisaging the nature of catastrophic events that could beset the practice and the contingency plans that should be put into effect should they become necessary."²

In the Law Society's guidance, the term "business continuity plan" is stated as a singular entity, yet further into the extract it states "...put into effect should they become necessary". So this now implies that there are multiple entities that must be in place. This may sound like a trivial observation but it does highlight the confusion surrounding business continuity and what constitutes a plan. This report aims to get to the heart of this problem and provides some solutions.

One may already be asking whether this standard should be followed. The answer is no. A standard is something by which you can and will be measured. There are no rules under any current regulatory body stating you must comply with one standard or another (in relation to BCM), but it is true to say that by working towards

formal accreditation, or by adhering to certain principals as outlined within the BCM standard, you will be positioning your business for when the time comes to provide formal evidence of your risk management capabilities. It is almost inevitable that this time will come.

It's a dangerous world out there...

Is the world we live in today more risky than it was ten years ago? Probably not, but what has changed over the last ten years is that the world is more risk-aware than it ever was. This is due, in part, to the speed of communication which is now possible. Events, anywhere in the world are instantly communicated via myriad communication mediums – Twitter, Facebook, e-mail, BlackBerries, news channels (traditional and online), radio and finally print.

Passer-by gets scoop

On Thursday 15 January 2009, Captain Chesley Sullenberger was forced to carry out a manoeuvre he had been trained for but never envisaged he would have to use.

US Airways flight 1549 was only three minutes into the flight from LaGuardia, New York when a flock of birds flew into its twin jet engines causing a mechanical failure.

The Captain calmly informed the passengers to prepare for impact, knowing that he had to land the plane. One hundred and fifty people onboard braced themselves for a watery landing as Hudson river loomed closer with each passing second.

On impact, the plane moved rapidly down the river and, at one point, looked as if it might sink. Rescue boats

were on the scene in minutes. It was a miracle that no one was killed with only two people experiencing broken legs and others suffering from shock. The Captain was hailed a hero.

As the scene played out in front of stunned onlookers, one witness to the dramatic landing was Jim Hanrahan. Using his mobile phone, he quickly took a couple of pictures and uploaded them to Flickr, a popular site for managing photographs. He then followed this by updating his Twitter status with the following message: "I just watched a plane crash in the Hudson river in Manhattan," adding a link to the pictures he had just taken.

Jim witnessed the landing, took the pictures and reported this on the internet within four minutes of the incident. This took place a full 15 minutes before the mainstream media were onsite to take pictures.³

While the headline-grabbing events are high impact, low probability, there are many more mundane incidents that can quite easily impact your business and for which we should be prepared, such as:

- Swine flu;
- Postal strikes;
- Power cuts;
- Petrol crisis;
- Bad weather;
- Virus infecting your computers; and
- Loss of a critical member of staff (due to illness, death, injury or lottery win).

These are just a few of the everyday events which will, in some cases, hit the headlines whilst others do not. But headliners or not,

your business needs to understand how to react to them and protect the interest of stakeholders (i.e. employees, shareholders, clients, etc.).

The world we operate in today and the clients we serve are different to how they were many years ago. Our customers have developed and evolved just as technology has. The customer is not just 'King' anymore, he/she is an impatient 'King' too. Your response, when trying to access a company website and speed slows to a crawl or a page takes a few seconds to load, may be:

- Ten seconds – 'I'll wait';
- Twenty seconds – 'This is frustrating'; and
- Thirty seconds – [Click] 'Lets search again'.

If your business relies on the internet as a major source of revenue to sell its services, then you'll be very aware of the need to build a web presence that not only looks good but is quick to load. But what happens if your page doesn't load at all because the server is down or your building has been hit by fire or flood? As the customer, I wouldn't know why your website is no longer available. I'd just know I can't get to it. As a customer, I'll try once or twice, but very quickly, my loyalty will falter and I'll be looking for another provider of services if that service isn't available when I want or need it.

It could be you...

Some of you may recall the UK National Lottery slogan: 'It could be you', with adverts showing the heavenly hand pointing at unsuspecting individuals, inferring that if only they buy a ticket, 'It could be them'. Well, it's quite possible the same fickle finger of fate is looking down at your business and is poised ready to strike in a rather less attractive way. Yet, it seems that human nature favours

downgrading negative risk (like floods, illness, etc.) and upgrading positive risks or outcome of an event, like the Lottery. There is a whole field dedicated to the study of risk perception and whilst we will touch upon this in places, the subject is so vast that it is beyond the scope of this report. However, I would like to quote psychologist Mark Griffiths:

"If you were told that you have a one in fourteen million chance of getting cancer in the next seven days people will say 'Oh well it is obviously not going to happen to me it is so infinitesimal' but the fact that there is a one in fourteen million chance of winning the lottery people think 'Yes, it's got to be someone why can't it be me.'"⁴

The adage, 'Treat your customers well... or your competitors will' sits neatly with BCM, because if your systems or processes fail, and you don't respond effectively, then your customers will almost certainly go elsewhere. After all, wouldn't you?

References

1. 'The optimistic pessimist', CSO Online, February 2004; can be found at: http://books.google.co.uk/books?id=F2AEAAAAMBAJ&pg=PA47&lpg=PA47&dq=Mike+Hager+optimistic&source=bl&ots=ao8W6Bs_XL&sig=WCBOwP38xgioclCgNAwYpwanvM&hl=en&ei=jeEMS7yqF5KJ4Qbi24SCBA&sa=X&oi=book_result&ct=result&resnum=4&ved=0CByQ6AEwAw#v=onepage&q=Mike%20Hager%20optimistic&f=false
2. See: <http://www.lawsociety.org.uk/documents/downloads/lexcelguidanceFeb05.pdf>
3. See: <http://news.bbc.co.uk/1/hi/7832642.stm>
4. See: http://www.bbc.co.uk/worldservice/sci_tech/features/figure_it_out/lottery.shtml

Chapter 2: The definition of BCM

THE BUSINESS Continuity Institute (BCI) is an organisation dedicated to the development of best-practice guidance for businesses wishing to implement BCM. It has been in place for a number of years and has helped to shape the industry in the UK and internationally. It was the main body of professionals who were consulted in developing the British Standard for business continuity (BS25999-1 and BS25999-2). I will, therefore, refer to the BCI on a number of occasions in this report, and indeed, it is their 'Good Practice Guide' which will be used as a framework to implement BCM.

What is BCM?

"Business Continuity Management is a holistic management process that identifies potential impacts that threaten an organisation and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities."¹

This definition is provided by the BCI and it captures the essence of BCM and its significance to an organisation. The following unpicks this definition.

Holistic management process

This is looking at the whole system rather than just concentrating on individual components. Holistic in this context not only refers to the focus on more than one area of the business (for example, IT or operations), but it also refers to BCM being made up of crisis management, business continuity

planning and disaster recovery (DR). In addition, holistic means looking at not only the big events (for example, fires, floods or terrorism), but also the more common, almost mundane events (for example, system outages, telephony problems, etc.).

Potential impacts

BCM has much to do with risk management and the consideration of potential events that may impact upon your business.

Stakeholders

This refers to any organisation or individual that has a direct interest in actions or decisions of your organisation. This point is important as everyone is a stakeholder in BCM. Everyone has a vested interest in seeing the business continue – from the people at the bottom of the organisation to those at the top.

Reputation

This refers to the general estimation that the public has for a person or entity.

When I'm asked what I do for a living and I tell people that I'm a business continuity manager, the next question I'm typically asked is, 'So what does that mean?' My stock response is simply, 'I'm there to help protect the reputation of our business and ensure it's still around tomorrow.'

The components of BCM

While we have a useful definition of BCM, it is also important to outline what it is ultimately made up of.

Crisis management planning

Crisis management planning is the first step to achieving a robust response to an emerging threat. Essentially a Crisis Management Plan (CMP) deals with the framework of incident management and the command and control of any given event which, due to the size and speed of the incident, can't be managed as part of day-to-day operations.

Business continuity planning

"A Business Continuity Plan is a documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable an organisation to continue to deliver its critical activities at an acceptable predefined level."²

Disaster recovery

This is the process for recovering the business to an acceptable level of service by following agreed, documented and maintained processes. Typically DR refers to technology recovery, however it also relates to site and people recovery.

There is much we must do to get to a point where we have documented procedures in place (the project management phase), but our aim is to provide evidence of these BCM components, so that we can be truly effective when an incident occurs.

Where is BCM's place in an organisation?

This may sound like a simple question, but placing BCM in the wrong place in your business could determine how successful you are in its implementation. In my experience, BCM struggles most when it is aligned to IT or operational areas. The reason for this is simple – when BCM sits in IT, everyone assumes that

this is an IT issue and therefore concentration seems to be focused on technical DR. When BCM sits in operations, the operations leader, quite understandably, wants to ensure that operational areas are considered first and, therefore, support areas are often neglected (for example, HR, sales and marketing, accounts, etc.). To ensure the holistic approach is undertaken, all areas of the business must be addressed. In the organisational structure, BCM is best placed in a department which has a cross-functional remit such as compliance/legal, internal audit or risk.

Working example

While visiting a financial institution, John wanted to understand the level and breadth of the plans in place. Initially asking the IT manager how many CMPs were in place, '100' came the response.

John: "How many BCPs?"

IT manager: "200"

John: "How many DR plans?"

IT manager: "200"

While the number of plans seemed excessive for the size of the business, the answers to the next questions were more worrying.

John: "How many of those plans focus on support areas, such as accounts, payroll, HR and marketing?"

IT manager: "None. They're all focused on our operational areas because that's what the clients see first, particularly the client-facing teams."

John: "But wouldn't the loss of the accounts system impact on other areas?"

IT manager: "Oh yes, but we have a full technical recovery plan for the accounts system."

John: "Great... so does your accounts department know where to go and what to do if the site isn't accessible?"

IT manager: "Erm... no. We don't have any site recovery for them. They'd work from home."

John: "Can they access their accounts systems from home?"

IT manager: "Not sure to be honest. We've never checked."

Budgeting for BCM

This is an almost impossible question to address at the outset. But no matter what it costs, two points are worthy of mentioning here – it should be seen as an investment in the future of your business and it doesn't have to cost the earth. The cost of time and effort of people should be approached in a systematic and planned way to ensure that this cost is not wasted.

There will also be a budgetary requirement for BCM, but placing this in the organisational structure of a cross-functional team (such as risk or internal audit) will ensure that each business stream pays its part in the investment as an overhead to the business.

The cost of BCM can only be reviewed on an ongoing basis using tools such as risk assessments and BIA. These are discussed further in Phase 2 Chapter 1.

The BCM project cycle

Approaching BCM in a systematic and methodical manner will ensure a better chance of success. In truth, BCM is a programme, much like a change control programme. There is no end to the implementation of BCM because things change too often – both in business and in the regulatory landscape.

BCM isn't a one-off event, with a beginning, middle and an end. There's no such thing as a finished BCP. While it can be signed-off as complete, the document will change if a person's role changes or telephone numbers change. It is an evolving process that will grow and increase in strength over time as it matures. So, while there is an element of project management to BCM, the most important point to remember is that BCM is a programme of work which requires time and commitment.

Project timeline

While there is an element of project management throughout the whole BCM life cycle, it's almost impossible to put a timeline on the whole programme. However, it is possible to estimate how long individual components of the initial project may take, so that you have a guide as to the length of time it will take to complete these steps. This estimation will be dealt with further in Phase 1 Chapter 1, but for now, it's important to note that there is no quick fix to implementation of BCM and therefore each programme will have its own timeline, dependent upon the size and complexity of the business in question.

Do I need special software to implement a BCM strategy?

The short answer to this question is no. Although there are countless tools on the

market to help with the management and creation of BCM documentation (including plans), I firmly believe that the simpler the solution, the easier the implementation. All the plans and processes described in this report are built using Microsoft Word, Excel and PowerPoint which are generally used by most business these days. I have seen some very clever tools used in the past which have included miniature CDs containing all copies of BCPs and contact details small enough to fit into a wallet. Yet, the obvious point is that in the initial hour(s) of an incident, there is a strong likelihood that a computer will be unavailable. Therefore, a simple wallet card which contains key information would be much easier to create and use. Of course, this does require additional work and it is not easy to ensure everyone is holding the correct version of a plan; but I have yet to see any software tool (large or small) which can remedy this.

There are tools which will help improve your capabilities in a crisis, but these are largely communication tools which enable a large number of people to contact your business to receive updates, or enable your business to contact large numbers or people to tell them of your issues. These will be discussed further in Phase 4 Chapter 1. Of all the tools that could be investigated, I believe it is the communications tool which will be of most use to your business.

References

1. Business Continuity Institute definition
can be found at: <http://www.thebci.org/certificationstandards.htm>
2. BS25999 – Specification for business continuity management; can be purchased at:
<http://shop.bsigroup.com/en/ProductDetail/?pid=00000000030169700>

Chapter 3: The BCM Standards

Which Standards should I follow – BS25999-2 or the Business Continuity Institute’s Good Practice Guide (BCI GPG)?

When implementing a BCM framework, the two main bodies which direct our efforts tend to be either BS25999 or the BCI GPG. Yet, the BCI GPG is aligned very much to the British Standard for BCM – BS25999-2:2007. So where there may have been some confusion a while ago about where to start with the implementation of BCM, this is no longer the case. Furthermore, the BCI GPG is a well-structured document which provides a great framework to follow if you’re already comfortable with BCM and have experience in the field.

However, the intention is to offer practical advice and steps to follow for the implementation of a BCM strategy. Figure 1 includes elements a BCM practitioner requires to be successful – standards, the framework and practical advice.

The approach we take when implementing a BCM strategy should be based on a solid foundation and, in my opinion, the BCI GPG and the BS25999-2 Standard are effective tools to help us get to where we need to be.

The GPG (which is available free of charge at: <http://www.thebci.org>) is a useful guide and I and many others have used this structure to great effect over the years. The framework covers the following topics (which we will discuss at length in this report):

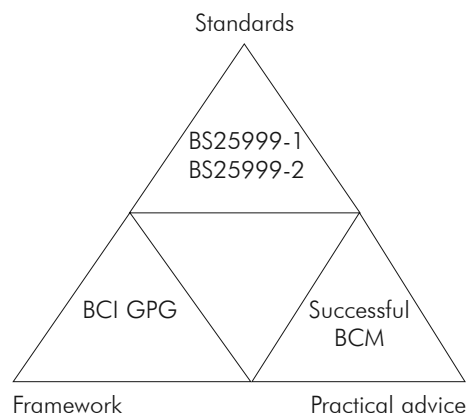


Figure 1: The elements for a successful BCM strategy

- BCM policy and programme management;
- Understanding the business;
- Determining business continuity strategies;
- Developing and implementing a BCM response;
- Exercise, maintaining and reviewing BCM arrangements; and
- Embedding BCM in the organisation’s culture.

In addition to these stages, the new Standard for BCM – BS25999-2 details components, which should¹ exist if BCM is to be successful. These components are:

- A policy;
- People with defined responsibilities;
- Management processes related to:
 - Policy;
 - Planning;
 - Implementation and operation;

- Performance assessment;
- Management review; and
- Improvement.
- A set of documentation providing auditable evidence; and
- Topic-specific processes relating to the subject, such as BIA and BCP development.

These components are known as the Business Continuity Management System (BCMS), a term you will come across many times whilst discussing BCM; but please be aware of the important difference between BCM and BCMS:

- BCM = Business Continuity Management – the holistic process that identifies potential impacts; and
- BCMS = Business Continuity Management System – the documentation and processes used to evidence a robust BCM framework and infrastructure.

In addition to these components, it is declared in the BS25999 Standard that the following documents should be in place too:

- Scope and objectives of the BCM strategy;
- The BCM policy;
- The provision of resources;
- The competence of BCM personnel and associated training records;
- The BIA;
- The risk assessment;
- The BCM strategy;
- The incident response structure;
- BCPs and incident management plans;
- BCM exercising;
- Maintenance and review of BCM arrangements;
- Internal audit;
- Management review of the BCMS;

- Preventative and corrective actions; and
- Continual improvement.

People are often confused by BCM when looking at this list of requirements. This report will aim to help you get to where you need to be as quickly and as painlessly as possible by showing you what to focus on and when. The components, along with standard project management tools, will be described in detail with practical examples of how to develop and implement your BCM strategy. In this report, we will cover all the requirements of the BCI and the BS25999-2 by building our BCM framework using the following five phases:

- Phase one – project management and initiation;
- Phase two – understanding the organisation;
- Phase three – developing and implementing a BCM strategy;
- Phase four – maintaining your BCP; and
- Phase five – embedding BCM in the organisation.

These five key phases discussed in Part 2 of this report will take us to where we need to be, in a structured and orderly fashion, ensuring that we link each phase to the BS25999-2 Standard and the BCI GPG.

The life cycle of BCM

If you have been exposed to any development or programme management processes in the past, you may have come up against something termed 'PDCA', which stands for 'Plan-Do-Check-Act'. This approach is used in many other quality-assurance programmes such as:

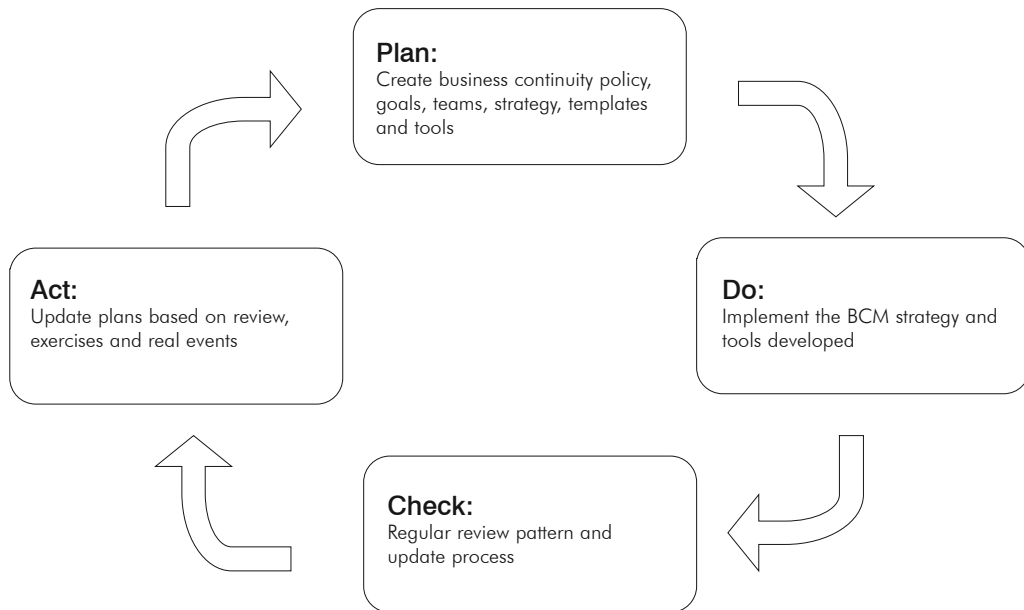


Figure 2: BCM life cycle

- ISO9001 – quality management;
- ISO 14001 – environmental standards; and
- ISO 27001 – information security.

Essentially, the stages of implementing a BCM framework include the setting of policies, objectives, processes and procedures (plan), then moving to implement the processes (do), after which they must be monitored for their effectiveness (check) and finally acting upon the findings of the previous stage (act), which leads us back to the beginning by adapting our policies and processes to ensure they are appropriate. The phases examined in this report follow this typical life cycle.

While BCM has a life cycle, the process is one of continual improvement. Now that we have laid the ground work, we are better prepared to begin building our BCM framework by starting to develop our BCMS.

Reference

1. I write “should exist if BCM is to be successful”. Please be aware that if you would like to be accredited against this Standard, you must have these components in place as it is against these which you will be audited.

