VALIDATING YOUR BUSINESS CONTINUITY PLAN

Ensuring your BCP actually works

Robert A. Clark

itgp™

Validating Your Business Continuity Plan

Ensuring your BCP really works

ROBERT A. CLARK

IT Governance Publishing

IT Governance Publishing
IT Governance Limited
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely, Cambridgeshire
CB7 4EA
United Kingdom

www.itgovernance.co.uk

First published in the United Kingdom in 2015
by IT Governance Publishing.

ISBN 978-1-84928-773-9

ABOUT THE AUTHOR

In addition to being a Fellow of the Institute of Business Continuity Management, a Member of the Business Continuity Institute and an Approved BCI Instructor, Robert Clark is also a Fellow of the British Computer Society and a Member of the Security Institute. In 1973 he joined IBM as a trainee computer operator. Big Blue was one of those forward thinking organisations that practised business continuity management (BCM) long before the expression had even been coined. But back then, in the 1970s, with the exception of periodic fire evacuation drills, BCM was simply referred to as disaster recovery and was entirely focused on protecting the IT environment, along with the associated electronic data.

It was less than 12 months into his 15 year IBM career that Robert first became exposed to BCM. Both local and overseas disaster fall-back trials were regular features in the IBM calendar and often involved testing recovery capability by transferring UK operations to Germany or the Netherlands. During his time with the corporation, the closest the operation came to a real disaster fall-back was in 1974, during the UK miners' strike, when power interruptions became common place.

Robert's 15 years with IBM were followed by a variety of positions including 11 years with Fujitsu Services (formerly ICL), working with clients on BCM related assignments. In 2005 he was tasked with validating Fujitsu's own BCM state of readiness across Europe. He is now a freelance business continuity consultant and has spent much of the last four years in Malta, where he has promoted BCM both through consultancy assignments and BCI licensed training.

In 2014 Robert became a part-time associate lecturer at Manchester Metropolitan University, where he has been delivering BCM to both undergraduate and postgraduate students, alongside his consultancy commitments. As a member of ‘Toastmasters International’, he is no stranger to public speaking. An experienced keynote speaker, he often makes use of platforms to promote BCM whenever the opportunities present themselves.

For more information about the author please refer to his website at: *www.bcm-consultancy.com*.

Other publications by the author

Validating Your Business Continuity Plan is Robert Clark’s second book. His first, *In Hindsight – A compendium of Business Continuity case studies*, also published by ITGP, went to number one on the Amazon bestseller’s lists shortly after its publication in 2014.

He has also had a chapter published in the book: *International Case Studies for Hospitality, Tourism and Event Management Students and Trainees* in 2015 which was entitled: *easyJet Leads the Way on Safer European Air Travel Initiative.*

FOREWORD

If there exists a warm, friendly book about business continuity, then this is it. Reading this book is like having an elderly but very experienced uncle teaching you about the subject, sharing their experience, the lessons they have learned and (business continuity) war stories. It is an easy read, not overly complex, and is sprinkled with anecdotes and lessons learned from Bob's long career in IT and business continuity.

I first met Bob when I was teaching the Business Continuity Institute's (BCI) good practice guidelines in Belfast in 2010. When I think about the course, I am reminded of three events. Firstly, there were only two people on the course, which made the teaching of a four-day course very intense and break-out group work rather difficult! Secondly, the volcanic ash cloud was at its height, so how we all got there I am not too sure. Thirdly, I remember Bob being on the course and I wondered why someone of his experience was on a training course. I think I learned as much from Bob sharing his experiences as he learned from me!

One of the aspects I have enjoyed about *Validating Your Business Continuity Plan* is that it is up to date. This is not some tired old soak in their twilight years writing a book as a vanity project and peddling obsolete business continuity practices. Bob, as shown by coming on the BCI course, keeps himself up to date with the latest business continuity thinking. The book uses all the latest terms, mentions current standards and is just, well, contemporary!

The book is all about validating your business continuity plan, which is part of the business continuity management lifecycle concerned with the practices of exercising, maintaining and reviewing your business continuity programme. As this book states, this is one of the most important parts of business continuity. Without a practiced and tested plan, the rest is worthless. Bob could have just gone for a book on exercising, but I think he makes the subject more complete by talking about the maintenance and review elements as well.

The book covers the need for validating business continuity plans and talks through some of the standards and guidance associated with the subject. It very quickly gets to the meat of the subject by looking at developing exercise programmes. What makes Bob's book slightly different from others is that he comes at exercising from a technical angle as well as from the more standard incident management path that others take. He covers all aspects of exercising and goes into some depth on a number of scenarios, concentrating on media, ICT and terrorism. I thought the information provided in the pandemic case studies was especially interesting and there are a number of other equally insightful case studies. Although the bulk of the book is about exercising, there is a chapter each on maintaining and reviewing a business continuity management system.

Having recently read a couple of other books on business continuity and crisis management, I found Bob's book very different in style. The other recent books were very much textbook-orientated, with lots of 'how to', checklists of considerations, and well-researched, sharp case studies, with every detail double-checked. Bob's is an altogether more approachable style; the case studies' details may not be as sharp but it is easy to dip in and out of the book.

It is very much written in the style of teaching the BCI good practice guidelines. It gives the hard facts of how to validate your business continuity plan but also some context in which to place the work and good relevant examples. For those more experienced business continuity professionals, it may not give you any radical new ways of carrying out validation but it will give you reassurance that you are on the right lines and doing the right thing. I would, personally, rather read this type of book on business continuity than others I have tried to read, which were so horribly complex that I didn't get beyond page five. I once met the author of one of the horribly complex business continuity books and immediately asked him to explain what his book was all about. He couldn't make me understand what the book was about either and he looked slightly worried when I suggested he might like to refund me the price of the book!

So, who should read this book? I think it is really aimed at those starting in business continuity and those who have some experience but are looking to gain more. I would also recommend it to those who are taking the good practice guidelines exam and also those who are perhaps carrying out their first few exercises and are looking for reassurance or guidance that they are carrying out best practice. Lastly, I recommend it to anyone who just wants a good read about business continuity – perhaps learn a fact or two, and enjoy the experience of someone who has been doing this since 1974!

Charlie Maclean-Bristol FBCI FEPS
Director
PlanB Consulting
CIR Awards - Business Continuity Consultant of the Year 2011

PREFACE

Validating your business continuity plan (BCP) can be broken down into three component parts – exercising, maintenance and review. In considering each of these three components, this book also takes account of industry standards and guidelines to help steer the reader through the validation process.

> *"A classic failing of a great many business continuity plans, is that they are written and then left on the shelf."* (Drewitt, 2013)

Too many organisations complete their BCPs and then just put them on the shelf to gather dust, without a thought about verifying that the plans actually work. They seem to miss the point that business continuity management is a process of continuous improvement and that the validation phase is a vital constituent part. Moreover, despite the advances that BCM has made in recent years, I still find there are organisations that firmly believe that business continuity is just a computer problem. Consequently, if they do undertake any business continuity planning and validation, it is invariably ICT focused and little else. There is no question that ICT is where business continuity has its roots but organisations that have not recognised that the world has moved on are still living back in the 1970s.

For me, it was in 1974 that I had my first experience, in what was termed a disaster recovery fall-back trial. My IBM colleagues and I had the task of transferring a mission critical IT operation from the UK and proving that it could be successfully recovered and run at an IBM location in Germany. This was intended to assure the continuity of this vital operation should IBM UK's ability to meet its obligations be compromised in any way. The exercise involved hand carrying several boxes of 9-Track 2,400 foot magnetic tapes which even the most advanced only had a capacity of less than 200 megabytes. It is amazing to think that 40 years on the external hard drive that I use for my home computing can comfortably slip into a jacket pocket and has a one terabyte data capacity. The 9-Track tapes contained the vital records that we needed to restore the UK environment for the test at the German host site. These exercises were the only occasions in my life that I can recall ever walking through the red channel at customs, as it was obligatory to declare that we were transporting what was referred to as 'merchandise in baggage'.

I must confess that for someone who has enjoyed a life-long penchant for travel, the prospect of having to spend a long weekend in Germany on expenses was more exciting than the justification for the trip itself. But like so many subsequent business trips I have undertaken, the professional demands took precedence and I never really got the chance to explore the locality. Consequently, I have long since come to regard business travel as an occupational hazard rather than a personal pleasure. One airport departure lounge is much like any other, as have been the hotels that I have stayed in along the way. However, in Germany I did get my first taste of something for which the novelty has never faded and what we now know as business continuity.

If nothing else, my 15 years with IBM emphasised the importance of not only exercising your business continuity plans but ensuring that every employee knew instinctively what part they would have to play in a crisis, even if it was simply 'go home until you are contacted'. Whether the exercise was a simple and inexpensive desk check involving two or three people, or a full blown live rehearsal, it was always taken seriously.

Since that weekend back in 1974, I have literally lost count of the number of BCM exercises and tests that I have been involved with. Some have been straightforward, low cost/low risk exercises, while others have been expensive and risky rehearsals which had the potential of creating a high profile disaster had they gone wrong. And yet, I cannot recall a single test that did not reveal something that needed to be reflected in the business continuity plan under scrutiny. Sometimes all that was necessary was just the dotting of an 'I' or the crossing of a 'T'. In other instances, BCPs have been proved to be inadequate, with substantial rework being needed. It is always better to discover that your plan has flaws during a test, rather than after you have experienced a genuine disaster. It is certainly worth remembering that there are always lessons to be learned and let us not forget that BCM is a process of continuous improvement.

Over the four decades since my initial foray into disaster recovery, I have seen the testing scene maturing in line with the evolution of business continuity. One important point that has long since been apparent to me is that it is virtually impossible to validate every aspect of your plan. To attempt to do so, particularly in a live rehearsal situation, could be creating a disaster of your own making. An exercise programme that defines a controlled and systematic approach, and also one which staggers the activities over a period of time, should be adopted. For some organisations, their exercise programme could extend over several years. Indeed, it is not uncommon for organisations to be regularly rehearsing their BCP, after all, practice does make perfect.

Conversely, you will almost certainly come across those individuals who 'do not have time' to support testing initiatives, or whatever other excuses they choose to present. I have generally found that the inclusion of business continuity as a part of someone's performance objectives, supported by clearly defined and measurable deliverables, will usually do the trick.

In retrospect, I believe it would be true to say that back in the 70s with so much focus on IT disaster recovery, although we did not appreciate it at the time, it was really the tail that was wagging the dog. In fact, some of my IT colleagues even seemed to believe that IT was more important than the business it was intended to support. Such arrogance, or perhaps it was simply naivety? Now, with us well into the 21st century, non-IT based scenarios have long since become a major feature of exercising, as the world has woken up to realise that there is much more to business continuity than just worrying about information technology. Moreover, business continuity has matured into an international standard – ISO22301, although other standards, such as PAS 56 and BS 25999 have played their part along the way in the evolution of the discipline. During that time I have enjoyed working on every phase of the BCM lifecycle and, for some clients, working with them to facilitate the development of their end-to-end business continuity programmes.

Business continuity has no doubt finally come of age with the launching of ISO22301 in 2012 and this book pays due deference to the ISO's criterion. However, in writing the content, it would have been remiss of me to overlook the many years of experience I have gained along the way, coupled with the lessons learned, much of which predates the launching of ISO22301.

CONTENT

CHAPTER 1: INTRODUCTION

> *"One of the oldest axioms within the field of disaster recovery or business continuity planning is that a plan that is not tested or maintained is of little value, or in some cases worse than no plan at all."* – (Armit, 2007, p. 323).

The intermittent fire alarm warning sounded. It was not the routine weekly test of the system, scheduled for every Tuesday morning at 10 am. The multi-storey building housed around 500 occupants who instinctively followed standard procedure, cleared their desks, powered off their PCs and prepared to evacuate. Fire wardens donned their high visibility jackets and took up position at their designated stations, including those detailed to assist both pregnant and disabled staff evacuate, should the need arise. Lift vestibules were also manned by wardens to prevent any attempt to use the lifts.

Within two minutes, the fire alarm had changed from an intermittent to a continuous warning signal, thereby heralding an immediate evacuation of the building. Supervised by fire wardens and in an orderly fashion, staff moved promptly to the clearly marked emergency exits. Security personnel manned the exit doors to prevent any unauthorised re-entry, while fire wardens checked that offices, meeting rooms and toilets, etc. were clear.

Staff congregated at their pre-assigned fire assembly points and head count checks were performed, with department managers or their deputies responsible for reporting back to the incident manager. The building reception area staff were responsible for safeguarding the visitor's book during evacuations, to establish each visitor's whereabouts. Any missing members of staff had to be accounted for (e.g. vacation, sick leave, working away from the office, etc.). Had this not been possible, it would be assumed that they were still in the building. As the last report was received, the incident manager checked his stopwatch. Everyone accounted for, including visitors to the building. The evacuation had been completed in nine minutes and 34 seconds – almost one minute inside the target evacuation time. Apart from completing the mandatory post exercise report, along with any recommended actions, the exercise seems to have been successfully concluded – or was it?

Apart from testing how quickly the building could be evacuated, let us also consider what else this exercise may have been trying to achieve. As a bare minimum, an evacuation drill should look to:

- identify any flaws that exist in the evacuation strategy.
- use the opportunity as an awareness exercise for employees who are new, or just unfamiliar with the building selected for the evacuation.
- ensure that the arrangements for any disabled employees or visitors, including any expectant mothers, are properly managed. Remember that the actual number needing assistance may well fluctuate from exercise to exercise.
- monitor the effectiveness of the evacuation from any new building extensions, or from existing areas that may have been subjected to internal structural alterations.

- ensure that any areas with a secure access designation do not in any way compromise the safety of employees, solely in the interest of security[1].
- gauge the effectiveness of communications throughout the building. For example, a public address system announcement may be better heard in some areas than in others.
- consider whether employees' behaviour and attitudes are appropriate. For example:
  - ○ Did everyone take the drill seriously and follow instructions?
  - ○ Did anyone try and use the lifts during the evacuation?
  - ○ Were there any attempts at unauthorised building re-entry?
- solicit both positive and negative feedback from employees, both in terms of the smoothness of the evacuation, as well as the effectiveness of the officials, such as the security personnel and fire wardens. Keep in mind that officials may be negotiating their own learning curve. Also consider whether there were enough officials on duty to carry out the tasks required, especially where evacuating the disabled is concerned.

Whilst a genuine emergency evacuation would give no consideration to the prevailing weather conditions, some leeway can be demonstrated in the case of an exercise. Should the prevailing conditions threaten to be inclement at the time of the proposed exercise, continuing regardless

[1] During an evacuation drill, quite by chance, I once found myself trapped in a corridor linking two buildings. The electronic swipe card security system was designed to prevent re-entry after the fire alarm had activated, so I was stopped from entering either building.

may well add an avoidable element of extra risk to the proceedings. Snow and ice, or torrential rain, would not make for ideal conditions and postponing the exercise until conditions are less hazardous may be the most prudent option.

It is perhaps also worth pointing out that this exercise was conducted without any prior warning being given to employees. I have come across business continuity practitioners who argue that you should always provide notice of an intended test. This raises an interesting discussion point, but more about that later in the book.

For other examples of emergency evacuation procedures, anyone who has flown in a commercial aircraft needs only consider the pre-flight safety instruction from the cabin crew. It does not matter whether individuals are experiencing their very first flight, or they have flown hundreds of times, they are still requested to listen and observe while the safety announcements and demonstrations are being carried out. In the event of an emergency, passengers need to know how to behave and how to exit the aircraft as expediently as possible. Cabin crew also need to assess whether the passengers sitting in seats next to emergency exits are, in their opinion, physically capable of opening the exit should the need arise.

As someone who enjoys cruising on a regular basis, I know that one of the first obligatory activities for passengers after embarking is to attend an emergency evacuation drill, which in a live situation could result in the need to abandon ship. Ocean going cruise ships are getting larger and larger, and in some cases the passenger numbers can amount to several thousand. All passengers must report to their pre-allocated muster station, and as part of this rehearsal they need to demonstrate to the safety crew that they can quickly and correctly put on their life jackets before they are dismissed. Practising this ‘abandon ship’ routine is a massive logistical exercise for the crew. They need to ensure that all passengers are accounted for, and any that fail to appear will be expected to attend a follow up exercise.

Both aircraft and ship’s crews will also be directed to engage in regular mandatory training, to ensure that they are capable and competent in dealing with just about any emergency that they are called upon to cope with. In fact, on one recent cruise, I opted to remain on-board while in port and actually observed, first-hand, some of the ship’s crew training for a fire scenario – one of the most dangerous threats that ships face.

> *“Around 80 died in the accommodation block from carbon monoxide poisoning while waiting for direction from management.”* (Dakin & Jacobsen, 2014, p. 106)

The world is full of tragedies where people have been injured or killed because they did not know what to do when faced with life threatening incidents. Alternatively, they may have found their emergency exit routes blocked, or totally inadequate to deal with the numbers trying to use them. In many instances these tragedies could have been prevented had evacuation procedures been regularly tested, so staff knew what they had to do instinctively.

I personally have been evacuated from two burning offices and from a third office due to the serious risk of an explosion at a neighbouring chemical company’s premises. Moreover, I have been evacuated from four hotels in the dead of night when the fire alarm unexpectedly sprang into life. On three occasions it was a false alarm but one was a genuine fire. I don't know about you, but I am never at my best when I am woken up, and it takes a few moments to get my brain into gear. But whenever I check-in to a hotel, I always take the time to find out what and where my emergency evacuation options are before I go to bed. If the lights fail and there is smoke outside your room, knowing which way to go could make the difference between surviving or not.

In 2013, I organised a business continuity and security conference in Malta. One of the case studies was presented by Mario Lentini and concerned an industrial fire that culminated in the creation of an exclusion zone by the Maltese Civil Protection Department (CPD) and which subsequently disrupted those businesses caught within that zone. Lentini was, at the time, responsible for incident management at the Bank of Valletta which had a small self-contained back office business unit based at the site of the fire. The building in question was a multi-occupancy affair which had to be quickly evacuated, especially when smoke started to penetrate their offices through the air conditioning system. Moreover, with the CPD concerned that the smoke was potentially toxic, the evacuation was so rapid that some employees had no opportunity to collect their personal effects resulting in keys, wallets and mobile phones being left in the building. Once outside they were also understandably prevented from recovering their cars from the basement car park beneath the burning building.

During the Q&A session that followed Lentini's presentation, a rather animated debate broke out, as it transpired that a few conference attendees had actually found themselves 'trapped' in an adjacent section of the building from where the fire started. Their designated emergency exit route took them through the premises of other organisations and they discovered their exit route had been obstructed. Fortunately, they found an alternative means of escape. Had an emergency evacuation exercise ever been conducted – apparently not! It also raised the issue of who should actually own a multi-occupancy building evacuation plan, along with the responsibility to periodically exercise the plan.

One final word I would like on this subject is not so much about an evacuation but a lockdown. A situation may transpire that means it may not be safe to actually leave the building you are in. There may, for example, be a shooter on the prowl, or an imminent terrorist threat, in which case you will probably be instructed to lock the doors and keep away from the windows. If there has been a chemical, biological or radiological release in the vicinity, you may be instructed to close all doors and windows and switch off any systems that draw air into the building, while awaiting further instructions.

The only building lockdown I have ever personally experienced was in the UK in 1991 which was necessitated by hurricane force winds. The 14 floor Portsmouth based building was at the time occupied by Zurich Insurance and it literally swayed in the breeze. From my vantage point on the 12th floor, I could see the destruction, particularly to the roofs of other buildings in the area, with the resultant airborne debris making the street a very dangerous place to be. The ground floor reception area had also been hastily turned into a refuge for members of the public caught out in the open, as the conditions had rapidly deteriorated. Fortunately these events are rare in the UK but alas other parts of the world regularly suffer the grief and destruction caused by the adverse weather conditions synonymous with the likes of hurricanes, cyclones and typhoons.

1.1 Unconscious incompetence to unconscious competence

> *"Business continuity is not so much an add-on or an after-thought, it needs to be a way of life."*

So what does all this building evacuation and lockdown stuff have to do with business continuity? Firstly, in my experience, building evacuation rehearsals are probably practiced as much, if not more than, any other situation. Secondly, in the initial building evacuation example on page 21, the organisation in question was rehearsing its emergency evacuation procedure and its effective execution in a genuine situation could literally make the difference between life and death. Probably with the exception of new employees, the staff just reacted to the well-rehearsed exercise in an '*unconscious competence*' state of mind. They did not need to think about what they had to do, they just did it. However, had this evacuation been caused by an incident that left the building unusable (e.g. fire, flood, explosion, toxic chemical release, etc.), thereby creating what is known as a denial of access situation, business continuity plans will be expected to dictate what happens next and how the business will manage the incident.

It is also entirely possible that you could be reacting to instructions from the police. For example, bomb threats are definitely not uncommon, although the ratio of hoaxes to genuine threats seems weighted heavily in favour of the hoax. That said, you cannot afford to ignore these threats and in effect engage in a game equivalent to playing Russian roulette with the health and safety of your employees.

However, the types of incident that can occur are diverse, as are the impacts they can cause an organisation, and many of them are covered later in this book. Moreover, while high profile incidents, such as burning buildings, tend to attract the attention of the media, many of the incidents that organisations may find themselves dealing with will not necessarily be 'headline making' material but could still threaten the survival of unprepared organisations. A business continuity plan will also often be expected to be capable of interfacing with other plans, such as emergency evacuation plans or pandemic plans. If an organisation has already created these plans when it develops its BCP, there is no point in re-inventing the wheel and duplicating what already exists. But the organisation needs to ensure that these plans are joined up and will work alongside each other. This is where validation can certainly help.

The 2010 edition of the Business Continuity Institute's Good Practice Guideline (BCI, 2010, p. 41) identifies four levels of staff awareness which can be defined as:

1. '*Unconscious Incompetence*' where staff are unaware of BCM issues and they do not know what they do not know.
2. '*Conscious Incompetence*' where staff are aware of BCM generally, but know little about its detailed requirements.
3. '*Conscious Competence*' where staff are cognisant of the BCM issue and are proficient (e.g. in following documented procedures) in supporting BCM.
4. '*Unconscious Competence*' where staff are instinctively fully competent in applying BCM in a variety of circumstances.

Most organisations will first engage with business continuity when their staff are at the lowest level of awareness – '*Unconscious Incompetence*'. Their objective should be to attain the highest level through a variety of methods, such as exercising their BCP, training, awareness campaigns and rehearsals. Exercising fosters teamwork and collaboration between diverse areas of an organisation, while developing proficiency, confidence and knowledge as it levitates the overall level of competence. Moreover, the organisation's confidence in its own ability to manage incidents will profit too.

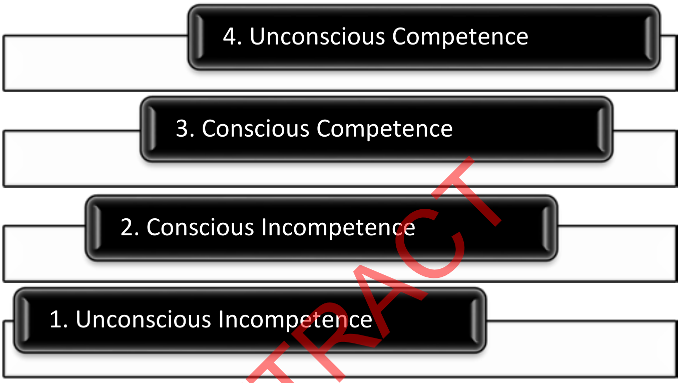

4. Unconscious Competence
3. Conscious Competence
2. Conscious Incompetence
1. Unconscious Incompetence

Figure 1: The four BCM 'levels of competence'

In fact, testing, validation, exercising or rehearsals are all variations of a common theme and, in addition to proving that a business continuity plan works as intended, they would certainly be expected to play an important part of its development towards that desired level of '*Unconscious Competence*'.

> *"An untested plan is only a strategy."* Richard Gagnon, 2007

Organisations that choose not to validate their BCP will not only miss the opportunity to improve the organisation's level of BCM competence, but arguably, the BCP itself will be worthless. It does not matter how much it cost you to develop, or how much attention to detail you pay in preparing your BCP, if it is not validated, it will simply not be worth the paper it is printed on.

1.2 The benefits of effective validation

For some organisations, the investment required in developing its business continuity response will have been substantial. Once a BCP has been produced, unless a good understanding and appreciation exists amongst its sponsors for the need for validation, along with a commitment to continuous improvement, a BCM programme can stall.

> *"A continuity plan without realistic testing is not only useless – it is also a complete waste of money."*
> Herve Riou

From a validation perspective, it is perhaps a good moment to remind ourselves of its importance. But before focusing specifically on validation, I would like to share something that I was reminded of recently. It relates to a survey conducted by the Chartered Management Institute amongst its membership. Entitled 'Planning for the worst', it quizzed members on their business continuity management. Two of the findings particularly stood out for me:

> *"The most compelling finding in this year's survey is that 81% of managers whose organisations activated their business continuity arrangements in the last 12 months say that it was effective in reducing disruption.*
>
> *The same number agree that the cost of developing BCM is justified by the benefits it brings their organisation."* (Pearson & Woodman, 2012, p. 14)

With such a large percentage of the participants believing that the benefits derived justify the cost, one significant interpretation from the second paragraph is that, if properly applied, BCM can be cost neutral.

Whether your organisation is a large multinational corporation or a SME, validation is still a critical component of the BCM process. So what exactly are we trying to achieve by applying validation? From a high-level perspective, we should be looking to demonstrate that all information in the plan(s) has been confirmed, the plan(s) has been fully rehearsed, and all appropriate employees and their nominated deputies have also been involved in the exercises. With every exercise undertaken, the workforce should be moving closer to that goal of reaching 'Unconscious Competence', while instilling a greater level of confidence in both management and workforce alike. It will also serve to raise the level of awareness across the organisation.

Validation will be broken down into more detail later in the book, as it takes the reader through a logical approach to exercising business continuity plans from a simple desk check, through to a live rehearsal. It will consider the standards and guidelines that are available, while providing examples of actual testing – some of which worked well and some of which did not. Case studies have also been included that look at how organisations have dealt with exercising their BCPs to address a variety of threats, such as:

- Civil unrest
- Cyber attacks
- Denial of access
- Discovery of white powder in a mail delivery
- Exclusion zones

- Explosion
- IT/telco failure
- Loss of staff/expertise
- Pandemics
- Power failure
- Terrorism (including 9/11 type scenario, bomb threats, WMD threat, plus a college campus gunman threat).

Examples are also given in section 5.1, where reputational damage was caused by atrocious media communication in three actual live situations. However, before getting into the 'nuts and bolts' of BCP validation, the book will consider the argument that business continuity should actually start at home in *Chapter 3*. Many of us, even those individuals who perhaps do not consider themselves to be well versed in its methods, conceivably already practice BCM without actually realising it.

1.3 Why do we need to exercise our BCP?

> *"Validation is the Professional Practice within the BCM Lifecycle that confirms that the BCM Programme meets the objectives set in the BC Policy and that the organisation's BCP is fit for purpose."* (BCI, 2013, p. 94).

Once a BCP has been developed, it still remains theoretical until such times as it can be proved that it works, by subjecting it to an effective validation programme. Unfortunately, this will be considered by some ill-informed executives as an unnecessary overhead that is rarely of the highest priority, and it will invariably take its place behind whatever happens to be considered as the issue of the day. I am constantly amazed by executives who dismiss the inherent dangers associated with not validating their BCPs as being irrelevant. Back in the late 1990s, I witnessed this happen with monotonous regularity with the various Year 2000 programmes I worked on. With the benefit of hindsight, we can argue that the Y2K threat was grossly overrated hype. Even so, we did not necessarily know that at the time, and with the immoveable deadline getting ever closer, I found some executives still reluctant to engage with the process. To save time, one executive I had the dubious pleasure of working for, even wanted the team to modify suspect computer software and reinstall it into the live environment without testing it first. This was not a shrewd plan and had we concurred he would have undoubtedly been the first to complain should we have ended up creating more problems than we fixed.

But to not validate your BCP, not only serves to devalue its currency, but it also creates the very serious and avoidable risk that it will not perform if and when called upon to do so. This begs the question – *'Is your BCP really worth the paper it's printed on?'* If you have not validated the plan, there can only be one answer – 'No'.

So apart from recognising that business continuity management is a holistic process, and that validation is an integral part of that process, let us consider some of the benefits derived from exercising your BCP:

- Ensuring that the BCP is fit for purpose, while providing the opportunity to make any amendments or additions to reflect those aspects of the BCP that did not perform as well as expected.
- Authentication of the strategies used to develop the BCP, while verifying that existing business priorities have been acknowledged.
- Confirmation that recovery time objectives can be met, especially in the face of a multiple scenario incident.

- Training employees, including their deputies, in the execution of their respective business continuity roles and responsibilities, by designing realistic scenarios and integrating role playing as part of the exercise.
- Raising the level of awareness of business continuity within the organisation.
- Increasing stakeholder confidence in the organisation's ability to respond to an incident.
- Achieving buy-in and plan ownership from the business areas.
- Assessing whether any organisational changes, including those resulting from acquisitions or mergers, can be accommodated within the constraints of the current business continuity arrangements.
- Testing of those components that require a 'pass' or 'fail' result, such as generators.
- Ensuring that ICT disaster recovery plans can meet recovery time objectives, especially for multiple system failures.

Before your business continuity plans can be signed off as fully operational, along with any associated plans, such as ICT disaster recovery plan, pandemic plan, emergency evacuation plan, etc., it must be demonstrated as being fit for purpose via a structured validation programme.

1.4 Does everyone need to validate their BCP?

The Business Continuity Institute's 2013 Good Practice Guidelines identifies six acceptable strategies that can be adopted as part of your business continuity arrangements:

1. **Diversification:** necessitates identical activities being performed at two or more physically remote locations, such that if work at one location is interrupted, it continues at the other(s).
2. **Replication**: is similar to diversification except that the replicated site is dormant and only becomes operational after an incident. It will generally need staff to be relocated to the replica following an incident.
3. **Standby**: assumes the availability of a facility that can be made ready to recommence business activities within the recovery time objective (RTO) which is assumed to be greater than a day.
4. **Subcontracting**: by using a third party supplier to take over the provision of a service or the manufacture of a product that your organisation offers, or the provision of ICT services, such as disaster recovery facilities.
5. **Post incident acquisition**: assumes the procuring of resources needed to take on activities after an incident. This would usually be driven by pre-prepared lists of requirements and should only be selected as a strategy for RTOs measured in days or weeks.
6. **Do nothing**: implies the luxury of time to decide how to deal with the effects that an incident has caused after the event.

The first three strategies listed and possibly ‘subcontracting’ too, would generally be adopted by organisations with short RTOs that are measured in days or even hours. Number ‘5’ – ‘post incident acquisition’, would be considered an acceptable strategy for organisations with RTOs measured in weeks. Finally, the ‘do nothing’ strategy is what you might expect organisations to select when they really have the luxury of time on their side and RTOs that are measured in months. I have, in fact, from time to time come across a seventh strategy which is a dependency upon what is probably most appropriately referred to as 'divine intervention'. However, in my humble opinion this is analogous to strategy number 6 – i.e. 'Do nothing'.

The BCI good practice guidelines (GPG) also point out that the sixth strategy is the default option for those organisations that are yet to implement business continuity. It implies that organisations electing to opt for this default are assuming that they will have months to respond to an incident. The truth may be that they really do not know how much time they have, particularly if they have not completed a business impact analysis. Given these circumstances, this makes option '6' a potentially dangerous option, especially if you do not know how much time you have to recover your organisation before it could find its very survival placed in serious jeopardy.

So let us consider the question of 'Do we really need to validate our BCP?'. To my mind, if any of the first four strategy options are used as input to your BCP development, the answer is a no-brainer – 'Yes', you must validate your plan. As for the post incident acquisition, while it may not be possible to perform any live exercises due to the very nature of the strategy, all other types of exercise (see Section 4.2.1) should be considered. Finally, I have to admit that undertaking any kind of exercise would be very difficult for the 'Do nothing' strategy, particularly if you intend to wait until after an incident to decide what to do. How can you define an exercise based upon key decisions that you are yet to make?

> *"As a simple rule, if it has not been tested it does not work."* (Armit, 2007, p. 324)

I hope you have already got the message that a business continuity plan that has not been validated should be considered as nothing more than a strategy. So you can only really say you have a BCP in place once it has been validated. Moreover, the BCI provide us with some rather alarming company failure statistics:

- **25% of companies never reopen following a disaster**
- **80% of companies that have not recovered within one month are likely to go out of business**
- **75% of companies without a business continuity plan in place are likely to fail within three years**

Figure 2: Percentage of companies that go out of business
Source (The BCI Video – The Time is Now)

Effectively validating your BCP can only enhance the likelihood of successfully dealing with an incident and improve your organisation's chances of not becoming just a 'statistic'. Like fire drills, practice makes perfect, and ensures the ongoing development of employee awareness and organisational readiness. This is complemented by the flexibility to try out multiple scenarios, providing ample opportunities for dress-rehearsals – particularly if they are performed unannounced. Any flaws in the BCP will be detected, and rest assured that validation affords us a far less risky approach than waiting to exercise the plans with a real incident!

As a consultant, I have occasionally been asked which industries business continuity applies to. The answer of course is that it is not industry specific. I have personally worked in a variety of industries, plus the public sector. Some exercises would be very similar, such as validating cyber defences, or dealing with a pandemic, regardless of the industry. However, other exercises undertaken will vary from industry to industry, simply because of the very nature of the businesses they operate. For example, retail banks will want to ensure that they can still offer deposit and withdrawal services to customers when there has been an ICT failure. Conversely, a manufacturer may want to validate contingencies that they may have in place that perhaps outsource the manufacture of key products while waiting for damaged plant equipment replacements. The ICT failure may be something that can be resolved relatively quickly, whereas the lead time for replacement plant equipment could take months, as it may need to be built to order, rather than being an off the shelf item. What all these organisations from different industries have in common is the need to validate and maintain their business continuity plans. Despite the inherent differences of their respective end products and services, the validation methods and approach they each use should be comparable.

Since the evolution of business continuity management from its ICT disaster recovery roots, organisations have come to realise that, while their ICT infrastructure remains a vital part of the overall jigsaw, it is only part of what they need to protect. In fact, the entire organisation needs to reach the position where business continuity becomes just a way of life, regardless of their size or raison d'être.

1.5 In the beginning there was a flood

> *"The Founder of Recovery Planning was Noah, but he had good connections and prior warning ... we do not!"* Melvyn Musson (Continuity Central, 2006)

Over the past few years, I have seen some fairly frequent references to Noah and his alleged contribution towards business continuity. Moreover, I have also noted that it has been suggested that Noah should be considered a role model by your average business continuity professional. After all, there are those who would argue that building the Ark and saving the world's animal population from drowning, was indeed the first recorded instance of business continuity in action. It certainly predates the evolution of IT disaster recovery which is the generally accepted origin of what we now acknowledge as modern business continuity. That said, there are accounts that lead us to believe that Noah finished the Ark's construction just before the rains fell, suggesting that perhaps he was working to a plan driven by some sort of sacred deadline.

But let's just take a step back for a moment. Is this role model status really justified when all said and done, until recently, I for one had never actually seen any evidence that he ever exercised his plan? With the rain falling and the flood waters rising, it would not have been a good time to have discovered that the plan had been dangerously flawed in some way. History has since provided examples of ships that were discovered not to be fit for purpose when they capsized and sank. Two cases that come to mind are King Henry VIII's flagship *Mary Rose* that was lost in 1545 and the Swedish ship the *Vasa* which capsized in 1628. In the latter case, the ship sank on its maiden voyage. Let us also not forget the 1912 Titanic catastrophe. Despite being considered by many to be unsinkable, the ship was clearly never stress tested for iceberg collisions.

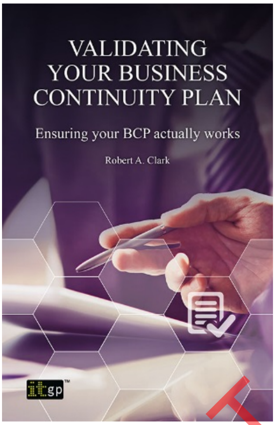
We could of course debate whether the story of Noah and the Ark is actually fact or fiction. However, assuming for a moment that there is some truth in the account, I guess in his defence I should relate to one explanation that I came across while researching for this book. It suggested that when the Ark was constructed, Noah actually had no knowledge of the impending flood.

> *"The Ark was not built as a lifeboat. It was built long before the flood as a commercial river barge for transporting cattle, grain, and other cargo."* (Best, 1999)

Best claims that the Ark had been sailed up and down the River Euphrates, in what is now modern day Iraq, long before the flooding occurred. This being the case, I stand corrected, as Noah did, at the very least, test that the Ark would float and with a host of animals on board too! Of course, this account does challenge the story of Noah building the Ark, by suggesting that it was never built in response to a divine command.

<<< END OF EXTRACT >>>

Validating Your Business Continuity Plan



- examines the three essential components of validating a business continuity plan – exercising, maintenance and review
- outlines a controlled and systematic approach to BCP validation
- covers methods and techniques such as table-top reviews, workshops and live rehearsals

"I found it excellently written and of great value. I guess this was expected based on the qualification and experience level of the author. The premise of the book is excellent as it focuses on the need to actually test a plan rather than just write and store it with no future revisions. The writing style is great and the huge range of examples given will be of great value to anyone purchasing the book. In summary very enjoyable, derived great value from it."
Chris Evans

Buy your copy today

www.itgovernance.co.uk/shop/p-1788-validating-your-business-continuity-plan-ensuring-your-bcp-actually-works.aspx

www.itgovernanceusa.com/shop/p-1524-validating-your-business-continuity-plan-ensuring-your-bcp-actually-works.aspx

www.itgovernance.eu/p-1174-validating-your-business-continuity-plan-ensuring-your-bcp-actually-works.aspx