# Implementing Business Continuity Management – Sharing Good Practice from an Irish Context

MONICA KELLY, DR. CAROLINE MCMULLAN,
DCU Business School
Dublin 9
Ireland

## ABSTRACT

Never has the need for robust, resilient organizations been so evident as in recent times with more and more well-established, respected organizations becoming unstable or even perishing as a result of the global recession. Added to these challenging economic times we have the demands of managing increasingly complex organizations, which are often highly dependent on sophisticated Information Systems and technology. Perrow's Normal Accident Theory (1994) points to the fact that "no matter how hard we try there will be serious accidents because of the interactive complexity"[1] of the organizations in which we work.

The introduction of BS25999, the British Standard for business continuity management, draws on international good practice in this field and brings together a clear view of what should constitute effective business continuity management for organizations across all sectors. This has provided Business Continuity Managers with a benchmark against which this aspect of their organization can be measured.

This paper provides an overview of the Business Continuity Management Lifecycle. It discusses the key steps which must be taken in order to establish a Business Continuity Management Programme. It then explores the various approaches and methods which may be employed to gain a greater understanding of the organization. The paper highlights how organizations need to determine the BCM strategy which should be implemented and how to plan for delivery of an effective response in the event of a disruption to normal business. This will involve giving appropriate consideration to key resources such as: People; Premises; Technology; Information; and Supplies.

The paper includes a discussion on ensuring all arrangements are fit for purpose, and outlines the importance of high quality exercising and training initiatives. Finally the paper determines how Business Continuity Management can be embedded into the culture of organizations so that they continue to grow in terms of resilience and maintain key functions and outputs in times of crisis.

The research for this paper involved the completion of a number of case studies which investigated how BCM is implemented in a range of organizations. As each phase of the BCM Lifecycle is discussed an example of good practice, drawn from these cases, will be outlined in order to illustrate how the various elements of the BCM lifecycle may be implemented within organizations across the public, private and voluntary sectors.

Effective BCM should reap significant rewards. It should improve resilience against disruption to mission critical activities, will provide a proven/rehearsed method of restoring the organization's ability to supply its key products and services to an agreed level within an agreed time after disruption and helps to safeguard an organization's reputation, brand and value-creating activities

**KEYWORDS: BUSINESS CONTINUITY MANAGEMENT; RESILIENCE; CASE STUDIES**

## INTRODUCTION

The operating environment for organizations throughout the world has been particularly turbulent over the past year. The economic downturn, threat of influenza pandemic, severe weather conditions, the earthquakes in Pakistan, New Zealand and Japan, have combined to produce many challenges for business. This complex and very challenging environment greatly impacts organizations' performance and their ability to achieve their business objectives.

Perrow's Normal Accident Theory (1994) points to the fact that "no matter how hard we try, there will be serious accidents because of the interactive complexity of the organizations in which we work"[1]. This complexity, when combined with the volatile operating environment, points to the need for increased resilience within organizations.

Many decision makers still believe that disasters only happen to others and that the probability of disaster is low, hence the investment in areas such as risk, crisis or business continuity management is not justified. Disaster however, "can strike in any form, at any time and no organization is immune from a disaster- not even the best-run ones" [2] and the chaos created across Europe by the Icelandic volcanic ash cloud at the end of 2010, seemed to validate this thought.

While organizations cannot control the national or global economic environment, they can however shield themselves from the "storm" by increasing resilience and managing the recovery of core elements of their business during a crisis. In these difficult economic times, a solid risk management strategy and robust business continuity management could be the key factors in winning major contracts and keeping a business afloat.

Added to the challenges of the present economic environment, we have the demands of managing increasingly complex organizations, which are often highly dependent on sophisticated information systems and technology. As businesses increasingly rely on data, information and technology, new threats are constantly emerging that affect all corporations. Authors such as Hawkins et al., 2000 [3]; Elliott et al., 2010 [4]; and Botha and Von Solms, 2004 [5] agree that it is imperative for organizations to recognize that having a solid business continuity plan in place is no longer a luxury – it is now a business necessity.

Organizational resilience, has been described as "the capability of an organization to minimize the impact of severe disruption events on its objectives" [6] and also as the ability of an organization to "survive, and potentially even thrive, in times of crisis [7]. Therefore we argue that improving organizational resilience must become a priority for management. To achieve resilience it is vital that organization build effective risk, crisis and business continuity management.

It was once said: "it is not the strongest of the species that survives, nor the most intelligent … it is the one that is the most adaptable to change"[8]. Organizations will have to adapt to the increasingly demanding and changing environment. They must become flexible and creative; new fresh thinking about managing modern organizations may be required.

In recent years there has been some evidence to suggest that organizations have "increasingly focused on their ability to respond to crisis"[9]. However organizations often find it difficult to measure their level of preparedness and to evaluate the progress made toward becoming truly resilient. It can also prove difficult to “demonstrate the value-added by business continuity”[10] and to justify the investment. For managers to secure investment in resilience there must be “an evidenced way of measuring it” [11] that would enable them to make a business case for the necessary investment.

Some will argue that in order to better understand resilience one will have to move away from “the static concept” to a more dynamic notion, “where an organisation can demonstrate different stages of resilience over time” [12]. For example an organization can be resilient to fire or flooding but not a flu pandemic. Business Continuity Management may provide the structure, tools and techniques needed to ensure resilience in all critical aspects of an organization.

Business Continuity Management is a relatively new discipline, often regarded as a “diverse, rapidly evolving and at times controversial subject” [13]. Its origins are firmly rooted in Information Technology Disaster Recovery. In the early 1970s the focus was largely limited to technology, the failure and recovery of computers and information systems. This focus on technology was visible throughout the 1980s and 1990s [14] however, in early 1990s the emphasis shifted from a functional to a more organization-wide approach to continuity planning. This important element of strategic and operations management has slowly made its way into many private sector organizations, particularly those with high levels of regulations, such as finance and banking. Alongside these developments within sectors of industry, professional bodies and national policy makers have developed business continuity standards. Formal standards have been introduced in the US, Australia, Singapore and UK. Such standards provide business continuity managers with a benchmark against which resilience and good practice in this aspect of their organisation can be measured.

The introduction of BS25999, the British Standard for business continuity management, draws on international good practice in this field and brings together a clear view of what should constitute effective business continuity management for organizations across all sectors. The standard formally defines Business Continuity Management as:

> “holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.” [15]

This paper provides an overview of the Business Continuity Management Lifecycle (the Lifecycle) that lies at the heart of BS25999. It discusses the key steps which must be taken in order to establish a Business Continuity Management Programme. It then explores the various approaches and methods which may be employed to gain a greater understanding of the organization. Next the paper highlights how organizations need to determine the BCM strategy which should be implemented and how to plan for delivery of an effective response in the event of a disruption to normal operations. This will involve giving appropriate consideration to key resources such as: People; Premises; Technology; Information; and Supplies. The paper includes a discussion on ensuring all arrangements are fit for purpose, and outlines the importance of high quality exercising and training initiatives. Next the paper determines how Business Continuity Management can be embedded into the culture of Irish organizations so that they continue to grow in terms of resilience and maintain key functions and outputs in times of crisis.

The research for this paper involved the completion of a number of case studies which investigated how BCM is implemented in a range of organizations. As each of these elements are discussed an example of good practice, drawn from these cases will be described in order to illustrate how the various elements of the BCM lifecycle may be implemented within organizations across the public, private and voluntary sectors.

Effective BCM will reap significant rewards. It should improve resilience against disruption to mission critical activities, will provide a proven/rehearsed method of restoring the organization's ability to supply its key products and services to an agreed level within an agreed time after disruption and helps to safeguard an organization's reputation, brand and value-creating activities.

## METHODOLOGY

This paper involved two key tasks. The first involved undertaking a thorough review of BS25999 with a view to evaluating the Standard and identifying the key elements which should be adopted by organizations wishing to implement good practice in BCM.

The second step involved the identification of examples of good practice. It was decided that a case study methodology was best suited to this study. The aim of each case study was to determine how organizations deal with each of the six phases in the BCM Lifecycle and then to identify elements which may be judged as qualifying as good practice - this judgement was made by using the Standard as the Benchmark of quality.

Yin [16] outlines case study research as:

> "an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident."

Given the dearth of research into how organizations implement BCM, a case study methodology seems an appropriate starting point. The results will provide an insight into how the BCM Lifecycle has been operationalised and how other organizations can learn from the success stories which exist across a wide range of sectors.

## INTRODUCING THE BCM LIFECYCLE

The BCM Lifecycle (see Fig. 1) is an ongoing, interactive process that will aid organizations in effectively implementing BCM.  In practice the Lifecycle involves four stages (Understanding the Organization - Business Impact Analysis; Determining BCM Strategy, Developing and Implementing a BCM response; and Exercising, maintaining and reviewing) supported by two ongoing processes (BCM Programme Management and Embedding BCM in the Organization's Culture).

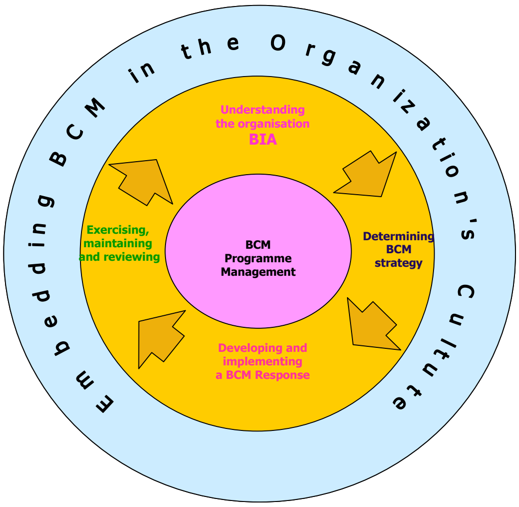
Embedding BCM in the Organization's Culture
Understanding the organisation BIA
Determining BCM strategy
Developing and implementing a BCM Response
Exercising, maintaining and reviewing
BCM Programme Management

**Fig.1 – The BCM Lifecycle** [17]

### (1) BCM Programme Management

The standard recognizes the strategic importance of BCM programme management that:

> "enables the business continuity capability to be both established and maintained in a manner appropriate to the size and complexity of the organization". [18]

The first step in implementing effective BCM involves top level commitment within the organization. The engagement of top management is essential when introducing BCM in an organization as adequate resources and support are required. A strategic decision must be made regarding how the organization is going to structure the BC function. This will involve determining a system of governance, identifying who will be responsible for BCM, planning where Business Continuity will sit within the organization structure and agreeing how the function will be managed.

Under BS25999 it is suggested that management should:

> "Appoint or nominate a person with appropriate seniority and authority to be accountable for BCM policy and implementation; and
> Appoint or nominate one or more individuals to implement and maintain the BCM programme". [19]

In larger, more complex organizations management may "nominate representatives across the business by function or location to assist in the implementation of BCM programme" [20]. Traditionally it has been the case that BCM responsibilities have been viewed as an 'add-on' to an individuals 'normal job'. This is no longer acceptable. Instead it is recommended that:

> "The roles, accountabilities, responsibilities and authorities should be integrated into job descriptions and skill sets and reinforced in appraisal, reward and recognition policy". [21]

Once these elements are in place it is important to 'design build and implement' a BC Programme which must be communicated to all stakeholders [22]. The various elements of the programme, which will be discussed later in the paper, must be managed through the person/people who have been given overall responsibility for BCM within the organization. This group will have overall responsibility for:

> "Maintaining documents appropriate to size and complexity of organization;
> Monitoring performance of BC capability;
> Managing costs associated with BC;
> Establishing and monitoring change management and succession management regimes". [23]

**Example of Good Practice – Electricity Supply Board (ESB)**

The effective management of a BCM Programme is particularly challenging in large, complex organizations. However, ESB have invested huge time and expertise in devising a system which ensure that all elements of BCM operate effectively and efficiently across the organization.

ESB's Business Continuity (BC) policy decrees that all key plans are to be updated and exercised at least once per annum. An annual schedule is published at the start of the year, incorporating plan updates, exercises and quality assurance arrangements. This schedule is reviewed monthly with Business Continuity Co-ordinators at the Corporate BC Forum.

A central, secure managed inventory of plans and significant plan-related data is maintained by the BC Programme Manager. This forms a basis for monthly assessment and reporting of "Plan Status" to management. All significant actions from quality assurance and from exercises are collated into "Action Logs", one per business unit. The Action Logs are used for progress tracking, and for escalation as required to senior management. Regular reporting takes place to various BC Steering Committees and to the Group Risk Committee. The Board Audit Committee also receives progress updates on a number of occasions throughout the year.

### (2) Understanding the Organization – Business Impact Analysis (BIA)

BIA has arguably been regarded as "the most fundamental and important product of the lifecycle" [24]. The aim of this phase of the BCM Lifecycle is:

> "to assist the understanding of the organization through the identification of its key products and services and the critical activities and resources that support them. This element ensures that the BCM programme is aligned to the organization's objectives, obligations and statutory duties".[25]

Under BS25999 it is suggested that this understanding can be achieved by clearly identifying the objectives of the organization, clarifying any stakeholder obligations which may exist, recognising all statutory duties placed on the organization and gaining a clear understanding of the operating environment of the organization. Once the strategic direction and responsibilities of the organization are clear, the next step involves "identifying the activities, assets and resources that support delivery of products and services" and then "assessing the impact and consequences over time of the failure of these activities, assets and resources" [26]. It is not sufficient to think of these components in isolation. Instead cognizance must be taken of the interdependencies which exist within the organization and the reliance placed on third parties.

In order to gain a complete understanding of the organization and how key products and services are delivered, BS25999 advocates the use of a Business Impact Analysis:

> "For each activity supporting the delivery of key products and services the organization should:
>
> a) Assess over time the impacts that would occur if the activity was disrupted;
>
> b) Establish the **maximum tolerable period of disruption** of each activity by identifying:
>
> The maximum time period after the start of a disruption within which the activity needs to be resumed,
>
> The minimum level at which the activity needs to be performed on its resumption,
>
> The length of time within which normal levels of operation need to be resumed;
>
> c) Identify any inter-dependent activities, assets, supporting infrastructure or resources that have also to be maintained continuously or recovered over time." [27]

This often time consuming and complex element of the Business Continuity Lifecycle is vital to the success of BCM in any organization. So important is this to effective BCM, that Von Rössing (2011) [28] referred to the BIA as the "backbone of the entire business continuity exercise". Barnes (2011) [29] regards BIA as the "basis for decision-making and strategic planning upon which the whole BCM framework resides" and argues that the BIA has an essential role when justifying the investment in business continuity.

The output from the BIA will allow organizations to identify critical activities:

> "Those activities whose loss, as identified during the BIA, would have greatest impact in the shortest time and which need to be recovered most rapidly may be termed 'critical activities'. Each critical activity support one or more key products or services". [30]

Once these critical activities have been determined the next step involves a risk assessment of these activities.

> "Critical activities are underpinned by resources such as people, premises, technology, information, supplies and stakeholders. The organization should understand threats to these resources, the vulnerabilities of each resource and the impact that would arise if a threat became an incident and caused a business disruption". [31]

A variety of qualitative and/or quantitative risk assessment tools may be used to complete this assessment. As a result of the BIA and the risk assessment, the organization should identify mitigation and risk treatment measures (Treat, Tolerate, Transfer or Terminate) which will "reduce the likelihood of a disruption"; "shorten the period of disruption"; and/or "limit the impact of a disruption on the organization's key products and services" [32].

### Example of Good Practice – Allied Irish Banks (AIB)

Without a sound BIA it is unlikely that BCM will be effective. AIB, with the assistance of Renaissance Contingency Services Ltd., have devised a BIA which epitomizes good practice, as defined under BS25999.

Within AIB, the BIAs are completed at Business Unit (BU) level. The first step involves undertaking an analysis of the business processes for the BU. For each mission critical business process staff must identify: (1) the resources needed to deliver the process (including staff, technology etc); (2) How long the Business Unit can function without this process (Recovery Time Objective); (3) the Recovery Point objective – when must the process be restored; (4) the business process dependencies; (5) the volume of work which must be handled; (6) critical work periods during the day/week/month; (7) the Revenue/Cost Impact of the Business Unit being unavailable; (8) the business impact of loss of process; and finally (9) any third party dependencies. Completion of all nine steps of the BIA results in a comprehensive picture of what is happening in each unit and the priority for recovery in the event of a disruption to core business activities.

### (3) Determining BCM Strategy

Once recovery priorities have been identified, based on the output from the BIA, strategies may be devised for the following resources: People, Premises, Technology, Information, Supplies and Stakeholders.

The selected strategy will be influenced by a number of factors such as the length of time the organization can tolerate a disruption of the critical activity; the finance available to implement the chosen strategy and the impact which will result if no strategy is put in place. Strategy decisions may also be influenced by the current economic environment. In challenging economic times organizations will be under severe pressure to justify investment in business continuity measures. The sector in which the organization operates and its regulatory and legal requirements will also influence the type of strategy selected and how resources are allocated.

#### (a) People

The organization should identify a strategy for maintaining core skills and knowledge. BS25999 proposes that a range of strategies may be employed in order to ensure the correct number and mix of personnel is maintained.

The first step involves documenting how critical activities are performed. The presence of such documentation will allow for more seamless handover to staff who do not normally complete these activities and will also facilitate knowledge retention and management within the organization.

Multi-skilling of staff, including contract staff, can reap significant benefits in the event of staff shortages. In addition, it is advised that core skills are separated out across a range of staff in order to “reduce the concentration of risk” and that succession planning is undertaken [33].

**Example of Good Practice – Dublin City University**

Education institutions such as schools, colleges and universities are not "immune from the risks, impacts and aftermath of various types of emergencies, both small and large scale. A major incident can have a destabilising effect on both students and staff" [34]. Apart from the financial consequences, the University's reputation is at stake and the risk of litigation may lead to loss of business.

As a leading university in Ireland, Dublin City University (DCU) is committed to providing and maintaining, a safe and healthy environment for its students and staff. A campus crisis management team and business continuity plans are in place in order to ensure this is achieved. Maintaining critical activities in case of an incident is essential and the university believes the better prepared it is for dealing with emergencies, the more effective and efficient its response is likely to be. "Robust emergency planning and response arrangements need to be coupled with appropriate Business Continuity Planning (BCP) to ensure overall organizational resilience"[35].

The University's Flu Pandemic Contingency Plan, an integral part of their Business Continuity Strategy, aims to provide "a framework for the co-ordination of the University's response to a flu pandemic or significant outbreak of disease" The plan is designed to help ensure the university can respond to and recover effectively from a "widespread outbreak of flu resulting in absenteeism rates of 20% or greater, affecting the normal operation of the university and its campus"[36].

As part of the "Business Continuity 5 Step Planning Process", the university identified core/critical activities and the core elements (internal and external) which must be maintained even with limited staff or if the university is required to close down by national health authorities. Examples of these critical activities include teaching, research, administration, and the provision of services such as security.

In case of a pandemic, alternative arrangements were considered. These include home working, reallocation of healthy staff, implementation, if possible, of alternative teaching/evaluation models that do not require class attendance. Staff and students would be able to log in to the DCU network from home and access securely a variety of online tools such as personal portal pages, emails, and online registration systems.

In addition key personnel (and alternates) with responsibility of maintaining critical activities and resources, security, technology, etc have been identified. A skills matrix has also been compiled in order to facilitate the efficient identification of the skills which exist within DCU staff – this may save vital time during a crisis.

A DCU Flu Pandemic Response Team (FPRT) is in place. This team is responsible for managing and monitoring the university's response to a pandemic. Additionally, provision has been made for staff from various units and specialists from external agencies to join the response team as necessary.

### (b) Premises

The impact of losing all or part of the normal place of work may be reduced by having alternative arrangements agreed in advance. A number of options may be considered:

> "Alternative premises within the organization;
> Alternative premises provided by other organization;
> Alternative premises provided by 3rd party;

> Working from home or at remote sites;
> Other agreed suitable premises;
> Use of an alternative workforce in an established site". [37]

It is important to remember that a smooth switch to these sites requires significant planning and testing prior to invocation.

**Example of Good Practice – Dublin Fire Brigade**

Dublin Fire Brigade (DFB), like all emergency services, operates in a particularly time-sensitive environment. For this reason it is imperative that it has robust Business Continuity arrangements in place if one of the stations across the city should become compromised. DFB operate a BC arrangement where a neighbouring fire station will take over all emergency calls until the station has appliances which are Mobile and Available (MAV). If possible, the crew and appliances will be moved to the neighbouring station so that the appropriate level of cover is maintained. The most regular occurrence of appliances being moved to cover different areas is when an appliance is unavailable due to maintenance or technical/mechanical failure.

This good practice is also invoked when DFB experiences a peak in demand for services. When a station is stripped of appliances and crew the Mobilisation Officer (the highest ranking operational officer on duty) is notified and he/she may then make a decision to move one appliance from the next nearest station to cover the depleted area.

It takes considerable effort to ensure BC across the city of Dublin – even during a 'normal' working day. DFB operate a sophisticated, well designed system to ensure they can cope with each call appropriately. In order to achieve this, most addresses in the Dublin area (about 75%) have a Pre-Determined Attendance (PDA). This means that when the Emergency Dispatcher (ED) takes a 999 call the computer will offer a set number of fire appliances, specials i.e. turntable ladder, foam unit, chemical incident unit etc to that particular incident. This PDA is based on pre-fire plans and experiences from fire crews that have dealt with similar incidences. The ED can then choose to accept the PDA or change it, depending on the circumstances and information received from the call. If there is no PDA given, the ED will then rely on Standard Operational Procedures i.e. three fire appliances, ambulance and a District Officer to every domestic fire.

### (c) Technology

The importance of maintaining and restoring technology during an incident will vary depending on the type of organization and the sector in which it operates. BS25999 proposes a range of strategies such as:

> "geographical spread of technology i.e. maintaining the same technology at different locations;
> holding older equipment as emergency replacements; and additional risk mitigation for unique or long lead time equipment".[38]

The organization must have a clear understanding of the systems and applications which underpin all mission critical activities. Once these critical systems and applications have been identified a recovery time objective (RTO) must be established for each. The RTO will guide the continuity arrangements put in place. These arrangements may range from duplication of all technology at a different site, to entering into a contract for seats at a Business Continuity/Data Recovery centre. The strategy will be guided by the RTO and the cost of various solutions.

**Example of Good Practice – AIB**

AIB's business is critically dependent on IT services and many of their services are now available 24 hours a day, 7 days per week. Operating within a highly regulated industry has put additional pressures on the organization in terms of high levels of service quality, availability and security. Also in line with regulatory requirements, AIB has "to demonstrate recovery times of two hours or less in respect of many key services. Loss of data or transactions due to a service disruption is also unacceptable"[39]. As a result, in 2005 the organization undertook a major project to relocate two of its data centres in Dublin as the old premises were no longer considered adequate from a security and business continuity perspective. This project was regarded as the largest IT project undertaken by AIB and the largest of its kind ever in Ireland. In terms of supporting strategy the main driver was enhancing business continuity as no financial returns were expected from this project.

**(d) Information**

The BCM Strategy for information protection and recovery must encompass information stored in both hardcopy and electronic format. The selected strategy must ensure that:

> "Any information required for enabling the delivery of the organization's critical activities should have appropriate: confidentiality; integrity; availability; and currency". [40]

**Example of Good Practice – SAP**

Day-to-day information continuity is essential. Loss of data availability for any reasons could have serious implications for most organizations. It is also very important for organizations to strike the right balance between data availability and data storage security and reliability.

As the world's leading provider of business software SAP understands the importance of having a solid BCM strategy and reliable data centres. In line with the group attitude towards business continuity, the Irish organization is resolute in being a 'risk-intelligent', 'risk-agile' organization. Therefore comprehensive measures are in place to ensure data availability, security and integrity. Traditional offside storage is complemented by centralised backup solutions such as 'data replication'. Solutions such as Double-Take® Software enable continuous full-server backup, hardware-independent on-demand restoration and any-point-in-time recovery options, facilitating the organization to protect and recover its business-critical data and applications.

**(e) Supplies**

An inventory of all the supplies need to support critical activities should be maintained at all times. The strategy for maintaining these supplies may include:

- additional supplies at another location;
- arrangements for deliveries at short notice;

- diversion of just-in-time deliveries to other locations;
- holding of materials at warehouses or shipping sites;
- transfer of sub-assembly operations to a location which has supplies; and
- identification of alternative/substitute supplies. [41]

In general it is suggested that, where possible, organizations should avoid being dependent on one supplier, ensure suppliers have appropriate BCM in place and build up a record of "alternative, capable suppliers" [42].

**Example of Good Practice – Intel**

In many organizations BCM has matured over time. One example is the Materials Division within Intel Corporation, the group in charge of the sourcing and procurement of the goods and services needed for the manufacturing and operations process.

For an organization like Intel, having a robust flexible supply chain, resistant to interruptions is crucial, therefore Intel has identified as imperative for its successful manufacturing building a robust BC planning for their Materials organization. A number of practices have been put in place in order to reduce the risk of loosing a critical supplier and/ or material: "stockpiling inventory, switching to alternative sources of supply and/ or alternative locations"[43].

Intel's BC plans been developed over a number of years going through different maturity phases and they were actively tested in 2006 during hurricane Katrina and Level 4 Typhoon Milengo. The live tests of the BC plans confirmed the importance of accurate risk assessment, identification of critical materials and suppliers and the need for a proactive response to major events.

### (f) Stakeholders

BS25999 stresses that it is important to "consider and protect interests of stakeholders" and that strategies should be put in place to "manage key relationships with stakeholders, business or service partners and contractors"[44]. The Standard places particular significance on the wellbeing of stakeholders with specific needs and on building a sound relationship with the local responders who will assist with civil emergencies, the Fire Brigade, An Garda Síochána etc.

**Example of Good Practice – Ireland's International Financial Services Centre/Emergency Planning Society (IFSC/EPS) Local Interest Group**

The Irish Branch of the EPS and organizations based in the IFSC, plus adjacent sites in Dublin city centre, have organised a Local Interest Group (LIG) to promote sharing of good practice in Emergency Management and BCM. This group meets on the third Thursday of each month. The group have established a strong network of stakeholders, including local representatives of An Garda Síochána. To date the LIG have identified key risks in the operating environment, become engaged in actively influencing projects such as the LUAS Docklands Line and worked to build resilience within this area of the city and undertaken desk-top and live exercises to test Emergency Plans and BC arrangements.

### (4) Developing and Implementing a BCM response

Stage four of the BCM Lifecycle involves developing plans which will allow the organization to implement an effective BCM response. The first step involves putting in place an incident response structure/team which will allow the organization to:

1. Confirm the nature and extent of the incident
2. Take control of the situation
3. Contain the incident
4. Communicate with stakeholders. [45]

This Incident or Crisis Management Team will also activate the BC response. According to the Standard:

> "The team should have plans, processes and procedures to manage the incident and these should be supported by BC tools to enable continuity and recovery of critical activities.
> The team should have plans for activation, operation, coordination and communication of the incident response.
> Organizations may develop plans to recover or resume normal operations – sometimes this may not be possible hence may wish to ensure BC plans are capable of extended operation to give time for development of recovery (back to normal) plans." [46]

BS25999 sets out detailed guidance on what the Incident Management Plan and the Business Continuity Plan should contain.

### Example of Good Practice - Irish Rail "The Malahide Incident"

Irish Rail, the sole railway operator in Ireland, was faced with a major incident in 2010 when part of the Malahide Rail Viaduct on the Dublin to Belfast line collapsed into the sea. A train carrying approximately 70 passengers had just cleared the viaduct before the incident. A second train, with approximately 400 passengers on board, was scheduled to traverse the Viaduct some four minutes later.

In line with good practice, as outlined in BS25999, Irish Rail immediately confirmed the nature and extent of the incident. Even as the incident was unfolding, pre-planning and the resulting standard operating procedures designed by Irish Rail meant that the situation was brought under control and contained immediately. The driver of the train cleared the viaduct, contacted the Central Traffic Control Centre to report what had happened and to request "Emergency Signal Protection" which would ensure that the railway line was closed in both directions. He then put a Track Circuit Operating Device (TCOD) on the line – which provided further assurance that the line could not be travelled. The actions of the train driver have received official commendation [47].

Irish Rail's communication in the immediate aftermath focused on four key tenets.

(1) Time - They ensured all "known details" of the incident were in the public domain as soon as possible.

(2) Emphasis - They did not try to down play the incident, or the potentially disastrous outcomes that might have resulted from the collapse.

(3) Truth - Although the cause of the incident was not immediately known they did not attempt to deflect attention away from the company.

(4) Access – As the incident occurred on a Friday evening Irish Rail made it known to all media sources that relevant personnel would be made available immediately and continuously over the weekend.

From a Business Continuity perspective, Irish Rail immediately commenced planning for continuity of service for what they described as "critical processes" – in this context the focus was delivery of an efficient commuter service by rush hour on Monday morning. Management decided on a strategy which involved "Saturation of Resources" – the number of coaches provided to transfer commuters exceeded what they could possible require. This strategy allowed Irish Rail to exceeded customer expectations. Once they had dealt with commuters on Monday they were in a better position to review what was needed on an ongoing basis - with a view to a more realistic match between supply and demand. Media coverage at this time included interviews with very satisfied commuters who were unequivocal in their praise for Irish Rail.

Alongside these business continuity arrangements, the organisation was working hard to ensure they could repair the viaduct as quickly as possible:

> "The line was immediately closed after the incident and following the reconstruction of Pier 4, strengthening of all the other piers, replacement of the pre-cast beams and reinstatement of the weir, it was re-opened to traffic on 16th November 2009".[48]

Irish Rail exceeded expectations by completing this engineering project in less than three months.

### (5) Exercising, Maintaining and Reviewing BCM Arrangements

BCM arrangements, including plans, cannot be considered resilient until they have been tested in a realistic, comprehensive forum. "Maintaining plans, which although notoriously difficult, is essential, if plans are to retain credibility and support" [49]. Even when detailed plans have been prepared, these arrangements "cannot be considered reliable until exercised and unless currency is maintained" [50]. An exercise programme is 'essential to develop teamwork, competence, confidence and knowledge' and all BCM arrangements should be "verified through exercising, audit and self-assessment processes to ensure they are fit for purpose" [51].

The exercise programme should give "objective assurance" that BCM arrangements will be effective and that plans will deliver the desired outcome. The programme should exercise the:

> "Technical, logistical, administrative, procedural and operational systems of the BCP;
> BCM arrangements and infrastructure – including roles, responsibilities, incident management locations etc;
> Validate the technology and telecommunications recovery including the availability and relocation of staff". [52]

An effective exercise programme may improve capability by:

- practising the organization’s ability to recover from an incident;
- verifying that the BCP incorporates all organizational critical activities and their dependencies and priorities;
- highlighting assumptions which need to be questioned;
- instilling confidence amongst exercise participants;
- raising awareness of business continuity throughout the organization by publicizing the exercise;
- validating the effectiveness and timeliness of restoration of critical activities; and
- demonstrating competence of the primary response teams and their alternatives [53]

It is vital that all elements of the BCM Lifecycle are maintained in a timely and structured manner. Such maintenance must ensure that BCM is not viewed as a one-off task but rather an iterative process which takes account of all changes in the operating environment and takes account of new products, services etc.

The outcomes of the BCM maintenance programme should include:

- “Documented evidence of the proactive management and governance of the organization’s BC programme;
- Verification that key people who are to implement the BCM strategy and plans are trained and competent;
- Verification of the monitoring and control of the BCM risks faced by the organization; and
- Documented evidence that changes have been incorporated into BCM”. [54]

Review of BCM Arrangements should be undertaken by top management within an organization and may take the form of a self assessment or audit, an independent audit completed by competent person(s) from within the organization or from an external body.

**Example of Good Practice – Allied Irish Banks**

Once again AIB may be introduced as an example of good practice in BCM. Within AIB all Business Continuity plans are tested at least annually. These tests include the testing of all key functions and, where feasible, include some actual transaction processing. Business Units work with IT providers to ensure IT Service Continuity Management processes are aligned with their business continuity needs.

Where multiple Business Units share a building, simultaneous BCM testing is conducted, where feasible. On a rotation basis, the staffs supporting key processes are involved in tests (including senior management). ‘Out-of-hours Call Tree’ contact tests, for priority business units, are also undertaken on an annual basis. All test and exercise results are documented and evaluated to ensure performance has reached a suitable standard.

### (6) Embedding BCM in the Organization’s Culture

> “Building, promoting and embedding a BCM culture within an organization ensures that it becomes part of the organization’s core values and effective management”. [55]

The quote above describes the ultimate aim of the BCM Lifecycle. Embedding BCM in an organization’s culture will result in a “more effective BCM programme, increased confidence in ability to manage incidents, increased resilience and reduction in the likelihood and impact of disruptions” [56]. If BCM is to become embedded in the culture of the organization it must be supported by:

> “leadership from senior personnel in the organization;
> assignment of responsibilities;
> awareness raising;
> skills training; and
> exercising plans”. [57]

It is really only when an organization has all elements of the BCM Lifecycle in place that it can be regarded as embedding BCM in the organization’s culture. Some organizations, such as JP Morgan Chase, ESB, SAP and AIB, have gone some way towards making BC part of the organization’s core values. As BS25999 becomes more widely used and organizations are audited against the Standard, it will be possible to make a more valid assessment as to how good practice in this element of the Lifecycle may be achieved.

## CONCLUSION

Business Continuity Management has its roots in data recovery and was therefore viewed as being firmly under the control of the IS/IT specialists within an organization. There has been a growing awareness that all mission critical elements of an organization need to be afforded the same level of attention as IS/IT if there is to be continuity of all critical functions during and after a major incident. Even with this growing awareness, Business Continuity was often driven/managed within each business unit and data/systems recovery was addressed by IS/IT staff. In recent years, this division is beginning to disappear as both groups begin to see the value of working together on what are clearly inter-related issues. IS/IT and business strategy are becoming more integrated as organizations increasingly understand the business value of alignment. Additionally there is evidence of a convergence with risk and health and safety management strategies. Managers throughout the organization need to work together to identify and protect the systems most critical for the company. The BIA and the BCP will help keep critical functions running during a crisis or, if this is not possible, it will guide the recovery priorities after an incident.

The introduction of BS25999, and most especially the development of the BCM Lifecycle, may be viewed as a watershed in the evolution of BCM. For the first time organizations have a standard against which BCM may be measured. The Lifecycle also encourages the building of resilience across all mission critical elements of the business.

This research points to clear evidence that many organizations are implementing elements of good practice within BCM. Although few are using the BCM Lifecycle to inform how they approach BCM, there are elements which can be mapped back to the Lifecycle. There is much to be gained from sharing this experience with academics and practitioners working in the field of BCM. The value of this research which identifies and disseminates examples of good practice in BCM is three-fold: it may help guide those responsible for implementing effective BCM in organizations across the public, private and voluntary sectors; the research will allow policy makers and professional bodies to see how this relatively new standard may be implemented in practice; and it adds to the body of research in a relatively new academic area.

## ABBREVIATIONS AND ACRONYMS

AIB (Allied Irish Bank)
BCL (Business Continuity Lifecycle)
BCM (Business Continuity Management)
BCP (Business Continuity Plan)
BIA (Business Impact Analysis)
BU (Business Unit)
DCU (Dublin City University)
EPS (Emergency Planning Society)
ESB (Electricity Supply Board)
IFSC (Ireland’s International Financial Services Centre)

## REFERENCES

[1] Perrow, C. (1994) “The Limits of Safety: The Enhancement of a Theory of Accidents”, Journal of Contingencies and Crisis Management, Vol. 2, No.4, pp 212-220.

[2] Hiles A., “The Definitive Handbook of BCM”, 2nd Edition. Chester: Wiley, p.11. 2007

[3] Hawkins, S. M., Yen, D.C., & Chou, D.C., “Disaster Recovery Planning: A Strategy for Data Security”, Information Management and Computer Security, Volume 8, Issue. 5; pp. 222-229, 2000

[4] Elliott, D., Swartz, E., & Herbane, B., “Business Continuity Management: A Crisis Management Approach”, 2nd edition, Routledge, 2010

[5] Botha, J. & Von Solms, R, “A Cyclic Approach to Business Continuity Planning”, Inf. Manag. Comput. Security 12(4): 328-337, 2004

[6] Parsons, 2010, “Organisational Resilience”, The Australian Journal of Emergency Management, Vol. 25, No. 02, April 2010

[7] Seville E, Brunsdon D, Dantas A, Le Masurier J, Wilkinson S, Vargo J., “Organisational resilience: Researching the reality of New Zealand organisations”, Journal of Business Continuity & Emergency Planning, 2008 04;2(3):258-266.

[8] Megginson, L. C., “Lessons from Europe for American Business”, Southwestern Social Science Quarterly, 44(1): 3-13, at p. 4, 1963

[9] Stephenson, Vargo and Seville, “Measuring and Comparing Organisational Resilience In Auckland”, The Australian Journal of Emergency Management, Vol. 25, No. 02, April 2010

[10] Stephenson, Vargo and Seville, “Measuring and Comparing Organisational Resilience In Auckland”, The Australian Journal of Emergency Management, Vol. 25, No. 02, April 2010

[11] Stephenson, Vargo and Seville, “Measuring and Comparing Organisational Resilience in Auckland”, The Australian Journal of Emergency Management, Vol. 25, No. 02, April 2010

[12] Gibson, CA. “An integrated approach to managing disruption-related risk: Life and death in a model community”, Journal of Business Continuity & Emergency Planning, 2010 07; 4(3):246-261.

[13] Bird, L, “Foreword” in Hiles, A., The Definitive Handbook of BCM, Wiley, 2007

[14] Elliott, D., Swartz, E., & Herbane, B, “Business Continuity Management: A Crisis Management Approach”, 2nd edition, Routledge, 2010

[15] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S2.3.

[16] Yin, R.K, “Case Study Research Design and Methods”. Thousand Oaks, Sage Publications, 2003

[17] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S.3.7.

[18] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S.3.7.

[19] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S5.2.

[20] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S5.2.

[21] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S5.2.

[22] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S5.3.

[23] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S5.4.

[24] Barnes, P. “Business Impact Analysis”. In: Hiles A. (2011) The Definitive Handbook of BCM, 3rd Edition. Chester: Wiley p.166.

[25] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S6.

[26] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S6.1.

[27] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S6.2.2.

[28] Von Rössing, R. “BCM Audit”. In: Hiles A., The Definitive Handbook of BCM, 3rd Edition. Chester: Wiley p.477, 2011

[29] Barnes, P. “Business Impact Analysis”. In: Hiles A. (2011) The Definitive Handbook of BCM, 3rd Edition. Chester: Wiley p.181.

[30] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S6.3.

[31] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S6.5

[32] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S6.6.1

[33] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S7.3

[34] Association for University Chief Security Officers (AUCSO), **“**Planning for and Managing Emergencies: A Good Practice Guide for Higher Education Institutions, 2008

[35] Association for University Chief Security Officers (AUCSO), **“**Planning for and Managing Emergencies: A Good Practice Guide for Higher Education Institutions, p.137, 2008

[36] Dublin City University, “Framework Flu Pandemic Contingency Plan”, 2009

[37] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S7.4

[38] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S7.5

[39] Hanson, K., "Relocation of AIB's Main Data Centres", available

at http://www.continuitycentral.com/feature0488.htm

[40] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S7.6

[41] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S7.7

[42] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S7.7

[43] Hepenstal, A. & Campbell, B., "Maturation of Business Continuity Practice in the Intel Supply Chain", Intel® Technology Journal, Vol. 11, issue 02, May 2007

[44] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S7.8

[45] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S8.2

[46] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S8.2

[47] http://www.irishrail.ie/news_centre/news.asp?action=view&news_id=668

[48] http://www.irishrail.ie/upload/malahideviaduct.pdf

[49] Hiles A "The Definitive Handbook of BCM", 3rd Edition. Chester: Wiley, p.443, 2011

[50] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S9.2

[51] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S.9.1

[52] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S.9.2

[53] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S.9.2

[54] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S.9.4)

[55] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S.10.1

[56] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S.10.1

[57] BSi. (2006) British Standard: Business continuity management – Part 1: Code of Practice (BS25999-1), S.10.1