BUSINESS CONTINUITY MANAGEMENT

Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOREWORD</td>
<td>5</td>
</tr>
<tr>
<td>1 INTRODUCTION TO BUSINESS CONTINUITY MANAGEMENT</td>
<td>6</td>
</tr>
<tr>
<td>2 THE THREATS TO BUSINESS OPERATIONS</td>
<td>11</td>
</tr>
<tr>
<td>3 THE KEY STAGES OF BUSINESS CONTINUITY MANAGEMENT</td>
<td>13</td>
</tr>
<tr>
<td>4 DEVELOPING A PLAN</td>
<td>16</td>
</tr>
<tr>
<td>5 WHAT DOES A GOOD BCM PLAN LOOK LIKE?</td>
<td>18</td>
</tr>
<tr>
<td>6 CONCLUSION</td>
<td>21</td>
</tr>
<tr>
<td>APPENDIX A: FURTHER INFORMATION RESOURCES</td>
<td>22</td>
</tr>
<tr>
<td>APPENDIX B: SUMMARY OF PLANNING FACTORS</td>
<td>24</td>
</tr>
<tr>
<td>APPENDIX C: EXAMPLES OF QUICK WINS</td>
<td>30</td>
</tr>
</tbody>
</table>
"Nearly one in five businesses suffer a major disruption every year. Yours could be next. With no recovery plan, you have less chance of survival."

Source: Expecting the unexpected. www.london-first.co.uk

It is in the nature of busy people running small to medium sized enterprises to focus much, if not all, of their effort in generating sales and serving customers. Building a successful business demands it, while the administrative functions of the ‘back-office’ in support of this effort tend to follow in their wake as the enterprise matures. Traditionally Business Continuity Management (BCM) is not considered ‘core business’; yet there has never been a more pressing need to demonstrate good governance and resilience across the spectrum of all business activities.

In our wildest moments of optimism, which typically underpin the culture of business, we never plan for when things go wrong; when they do, small businesses tend to feel the ill wind first and often buckle under the strain, never to return. In 1996, following a bomb in Manchester, 750 businesses were directly affected and 250 closed down – the task of recovery being just too great. Absorbing the crisis and continuing in business after the major disruption this caused was well beyond the ability of those business owners. And yet small business is vital to a vibrant and balanced economy – as many as 70% of all working people in the UK are in businesses which employ 10 people or less.

The question is how can you plan for the unexpected and take advantage of the many benefits which accrue as a result of a Business Continuity Plan? It is often the case that those who run small business believe BCM to be ‘a big-ticket item’ and out of their reach. On the face of it this seems unduly harsh. Why is it that simple, cost-effective and common sense measures are out of reach of decision-makers responsible for running small businesses? After all, large businesses are comprised of many small business units and administrative functions joined together in a common purpose. What attributes do these have which enable them to absorb crises and return to normal after major disruption. Is their size and scale alone, the answer?

This guide will offer tools, tips and techniques for businesses of any size but importantly it is to readers in the small business community that it will hopefully resonate most. No business plans to fail, whatever its size, but without a strong sense of ‘the show must go on’ in the face of adversity small businesses often fail to plan for a worst case scenario. The ‘spectaculars’ seldom happen, so why bother planning? Well, the simple truth is that it is the mundane which commonly trip up smaller businesses: the loss of key customers, the loss of information, the sudden break up of a senior management team, or a new and dynamic market entrant.

Business Continuity Management provides a proven corporate discipline which helps small businesses to plan for, respond to, cope with and recover from sudden, unexpected and often traumatic events. Permanent closure is no longer the default setting in the wake of disruption. By following the steps in this guide and focusing on the consequences of disruption, asking yourselves ‘what if’ more often than ‘how much’ you can reap significant benefits.
1. INTRODUCTION TO BUSINESS CONTINUITY MANAGEMENT

‘Prejudice against Business Continuity Management is a typical characteristic of decision makers who have grown up in well-oiled, proven business environments where nothing ever goes wrong…’

anon

BACKGROUND

Business Continuity Management has always been regarded as a ‘big business discipline’ out of reach of the SME community. The truth is that business continuity is for all businesses regardless of their size. Building in resilience to all operations and making continuity part of the way normal business is carried out will ensure you adopt the right ‘posture’. The key is business as usual – all the time. This approach will reassure your supply chain and give confidence to all stakeholders with an interest in ensuring your success.

WHAT IS BUSINESS CONTINUITY MANAGEMENT?

BCM is a management discipline which extends well beyond the IT function. It is the means by which organisations design, develop, implement and maintain response and recovery measures in order to identify threats and vulnerabilities, while mitigating and managing the risks to services and operations, and the effects or consequences of disruption.

BCM is about creating, sustaining and improving organisational resilience – the ability to absorb disruption however caused – and ‘bounce back’ without the disruption damaging customer service or business reputation.

While there is a clear need for those responsible for IT to have credible disaster recovery plans in place (known more commonly as IT Continuity Plans) such as offsite data storage and ‘always on IT’, it is no longer the IT department which is most at risk. An entire organisation – regardless of its size – is ‘at risk’ if it does not have a Business Continuity Plan.

BCM DEFINED

BCM is an ‘holistic management process that identifies potential impacts that threaten an organisation and provides a framework for building resilience and the capability for an effective response that safeguards the interest of its key stakeholders, reputation, brand and value-creating activities’.

The process ensures that businesses are capable of planning for, responding to, coping with and recovering from any incidents and the consequences of disruption on service delivery. When simple BCM measures are implemented correctly they become an integral part of the way in which ‘normal’ business is carried out.

A Business Continuity Plan therefore ensures that when ‘things go wrong’ – which they do with increasing regularity – response and recovery plans are aligned with business objectives and service priorities.

THE CONTEXT FOR BCM

The loss or unavailability for more than a few hours of any critical business process, IT system or information can have a significant impact on any business, in many cases threatening its survival. While bombs, fires and floods capture the headlines, 90% of serious disruptions to business services are caused by mundane events such as road-works, emergency service cordons, damaged power cables, user error, procedural failure, temporary loss of power, data loss etc.

1 The quote above is taken from the British Standard (Code of Practice) for BCM (BS 25999-1:2006).
The ability to identify risks to operations and put in place a capability to mitigate and manage those risks;

The ability to manage uninsurable risk, such as risk to reputation;

Effective response to major disruptions;

The ability to demonstrate that the process is credible and consistent via exercising and auditing (BS 25999);

Competitive advantages conferred by the ability to maintain customer service, staff employment and stakeholder confidence.

Benefits of Business Continuity Management

BCM enables organisations of all sizes, from all sectors, to fully realise the potential of their managers and leaders; significantly increase their employees’ impact in the workplace and deliver the kind of measurable benefits that will drive the business forward. This is because it provides:

A PLAN FOR ALL SEASONS

‘Black swan events’ – those rare events, which rarely happen, often provide the justification for developing business continuity plans and there is disappointment when the major event doesn’t occur! This was often reported to be the case in the wake of Y2K and Avian bird flu.

The fact is that most events for which business continuity can provide effective work-arounds are disruptions ‘when your business cannot function on an as-intended basis’; affected by events which disrupt the normal flow of activities which you engage in to satisfy the growing needs of all your stakeholders.

It is more likely the case that business services will be affected more directly by these mundane events, rather than the ‘spectaculars’. Since so many services are delivered online and supported by remote call centres, shared services, and innovative ICT, the ability to respond and continue delivering ‘as normal’ is compromised if plans are ineffective or non-existent.

Research by the Chartered Management Institute (March 2010) summarises the types of disruptions, as can be seen on the adjacent page.

An effective, flexible and simple plan will cope with all these scenarios and more, as long as it considers the consequences rather than focusing exclusively on the causes.

BCM is related to a number of complementary risk management disciplines and should be undertaken with a complete and thorough understanding of a business’s policies, standards, processes and supporting services for:

- IT Continuity Management;
- Crisis Management;
- Corporate Governance and Risk Management;
- Information Security and Data Protection.

BCM AND BUSINESS STRATEGY

BCM has a significant influence on business strategy. High-availability services should be supported by simple plans for when service disruption occurs. BCM addresses the risks to those business services that could cause a sudden and serious impact, such as the loss of a website. Critical incidents include (but are not restricted to):

- Loss, damage or denial of access to key IT services;
- Failure or non-performance of critical service providers, distributors or commercial third parties e.g. trading partners;
- Loss or corruption of information;
- Sabotage or commercial espionage;
- Deliberate infiltration or attack on IT systems.
Any disruption, however caused, constitutes a strategic risk and may damage your ability to operate, thereby undermining the good reputation you have worked so tirelessly to create. BCM is integral, therefore, to business strategy and ideally the two should be aligned.

It is axiomatic of delivering effective services to your customers that this should continue in the wake of disruption however it is caused: your customers expect it and you should demand it.

### Range of disruptions encountered by UK companies

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of IT</td>
<td>82</td>
<td>46</td>
<td>58</td>
<td>60</td>
<td>70</td>
<td>67</td>
<td>73</td>
<td>73</td>
<td>71</td>
<td>69</td>
</tr>
<tr>
<td>Loss of telecoms</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>62</td>
<td>64</td>
<td>56</td>
<td>63</td>
<td>68</td>
<td>59</td>
<td>62</td>
</tr>
<tr>
<td>Loss of people</td>
<td>–</td>
<td>–</td>
<td>54</td>
<td>48</td>
<td>55</td>
<td>56</td>
<td>57</td>
<td>59</td>
<td>54</td>
<td>52</td>
</tr>
<tr>
<td>Loss of skills</td>
<td>59</td>
<td>43</td>
<td>51</td>
<td>48</td>
<td>56</td>
<td>49</td>
<td>59</td>
<td>62</td>
<td>52</td>
<td>55</td>
</tr>
<tr>
<td>Damage to brand/reputation</td>
<td>50</td>
<td>40</td>
<td>46</td>
<td>48</td>
<td>48</td>
<td>39</td>
<td>49</td>
<td>55</td>
<td>52</td>
<td>51</td>
</tr>
<tr>
<td>Premises denial</td>
<td>55</td>
<td>32</td>
<td>54</td>
<td>51</td>
<td>53</td>
<td>54</td>
<td>60</td>
<td>63</td>
<td>55</td>
<td>56</td>
</tr>
<tr>
<td>Fire</td>
<td>62</td>
<td>32</td>
<td>51</td>
<td>53</td>
<td>56</td>
<td>44</td>
<td>53</td>
<td>58</td>
<td>48</td>
<td>55</td>
</tr>
<tr>
<td>Extreme weather</td>
<td>29</td>
<td>9</td>
<td>24</td>
<td>25</td>
<td>29</td>
<td>26</td>
<td>43</td>
<td>46</td>
<td>44</td>
<td>48</td>
</tr>
<tr>
<td>Terrorist damage</td>
<td>30</td>
<td>23</td>
<td>47</td>
<td>48</td>
<td>53</td>
<td>44</td>
<td>46</td>
<td>53</td>
<td>42</td>
<td>46</td>
</tr>
<tr>
<td>Negative publicity</td>
<td>43</td>
<td>37</td>
<td>45</td>
<td>46</td>
<td>44</td>
<td>34</td>
<td>43</td>
<td>51</td>
<td>41</td>
<td>41</td>
</tr>
<tr>
<td>Employee health and safety</td>
<td>30</td>
<td>22</td>
<td>35</td>
<td>34</td>
<td>35</td>
<td>30</td>
<td>38</td>
<td>44</td>
<td>40</td>
<td>38</td>
</tr>
<tr>
<td>Environmental incident</td>
<td>19</td>
<td>19</td>
<td>26</td>
<td>23</td>
<td>35</td>
<td>27</td>
<td>30</td>
<td>36</td>
<td>31</td>
<td>29</td>
</tr>
<tr>
<td>Supply chain disruption</td>
<td>–</td>
<td>25</td>
<td>34</td>
<td>32</td>
<td>35</td>
<td>28</td>
<td>34</td>
<td>37</td>
<td>28</td>
<td>36</td>
</tr>
<tr>
<td>Customer health/product safety</td>
<td>21</td>
<td>22</td>
<td>25</td>
<td>26</td>
<td>27</td>
<td>26</td>
<td>31</td>
<td>35</td>
<td>28</td>
<td>29</td>
</tr>
<tr>
<td>Pressure group protest</td>
<td>14</td>
<td>9</td>
<td>14</td>
<td>27</td>
<td>20</td>
<td>16</td>
<td>18</td>
<td>27</td>
<td>21</td>
<td>19</td>
</tr>
<tr>
<td>Loss of water/sewage</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>41</td>
</tr>
<tr>
<td>Transport disruption</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>37</td>
</tr>
</tbody>
</table>

Source: Chartered Management Institute
BUSINESS CONTINUITY AND DISASTER RECOVERY

What is the difference? Put simply business continuity involves the whole business, while disaster recovery traditionally only covers the recovery process from disruption to IT systems and services. A business continuity plan will include requirements to keep all critical services running while a disaster recovery plan only considers the effects on IT. There is little purpose in having an IT system up and running if access to premises is denied and people are unavailable. Business continuity is proactive and includes risk mitigation before an incident occurs, while disaster recovery is reactive and takes place after an incident occurs.

The essence of business continuity is to keep vital business operations running in the event of disruption while disaster recovery specifically and historically refers to disruption to the IT infrastructure resulting in the unavailability of IT services. The relationship between the two is defined by either an internal Service Level Agreement (SLA) if IT is delivered in-house, or an external SLA if IT is outsourced to a third party supplier.

Since the publication of BS 25777 in November 2008, the language of disaster recovery is being replaced by IT Continuity Management.

CLOUD COMPUTING

There is much talk about ‘cloud computing’, and continuity of service ‘in the cloud’ is beginning to offer many innovative ways of ensuring Business and IT Continuity Management for small businesses, including backing-up in the cloud.

Whether you opt for Software-as-a-Service, Platform-as-a-Service, Infrastructure-as-a-Service, (or a combination of all three); the key requirements of managing effective business continuity can be achieved by suppliers in the ‘cloud’. As application or platform services are outsourced it means you will have to define clearly your return to normal service levels such as Recovery Time and Recovery Point Objectives (RTO and RPOs) and include your desired availability targets in any Service Level Agreement between you and your cloud suppliers. In turn, this means that carrying out a Business Impact Analysis becomes vital.

It also means that risk and continuity are shared. As the commissioner of services to support your BCM programme, it will remain your responsibility to understand your supplier’s continuity capabilities in the cloud and this can be achieved by designing solutions which meet your RTO while remaining compliant with BS 25999 and BS 25777.

Put simply, the RTO (or the target time set for resumption of product, service or activity delivery after an incident) drives the service and availability levels that you need to achieve and which your supplier delivers against. Similarly, the RPO refers to the point in time to which data should be restored following a disruptive incident.

Whichever technical path you decide to take, an effective Business Continuity Plan is increasingly used to manage relationships in the supply chain. Since the availability of the cloud provider’s infrastructure or applications is critical to your ability to deliver and maintain services to your customers, the key is to collaborate and understand what each other’s abilities are and use British Standards and Service Level Agreements to govern the relationship.

More information on choosing and doing business with a cloud computing provider can be found in the IT Faculty publication *Cloud Computing – A Guide for Business Managers*.
KEY CHARACTERISTICS OF BCM
The primary characteristics of BCM can be summarised as follows:

- A planning process driven by risk and threat assessment;
- A focus on consequences not causes;
- Physical asset dispersion;
- A focus on critical capabilities and information;
- Teamwork and mutual support;
- Training, regular exercises and rehearsals;
- Flexible and co-ordinated response measures.
2. THE THREATS TO BUSINESS OPERATIONS

INTRODUCTION

‘80% of businesses affected by a major incident close within 18 months.
90% of businesses that lose data from a disaster are forced to shut within two years.’

Source: Federation of Small Businesses http://www.fsb.org.uk

An effective Business Continuity Plan will ensure that you are capable of planning for, responding to, coping with and recovering from, major disruptions to ‘normal’ operations from events across the risk and threat spectrum.

WHAT CAN GO WRONG

These are examples of some of the events from across the ‘threat spectrum’ which Business Continuity Planning is designed to cope with:

- Fire;
- Floods;
- Snow;
- Hackers;
- Sabotage;
- Fraud;
- Terrorism;
- Loss of reputation;
- Supply chain failure;
- Computer virus;
- Water leaks;
- Equipment failure;
- Vandalism;
- Theft;
- Human error;
- Power failure;
- Computer hardware failure;
- Software failure;
- Telecommunications failure;
- Civil disturbance;
- Explosion;
- Storm damage;
- Extreme weather;
- Pollution.

SURELY OUR INSURANCE WILL COVER US!

Sadly not for every eventuality. In particular, insurance does not cover for loss of customers or reputation. In the event of a fire an insurance company will not manage your immediate crisis. They are not responsible for your decision-making. And while they may pay out – eventually – there is often a long gap between the crisis and financial settlement. Insurance and outsourcing of the risk to a third party is important but it is only part of the answer. An insurance policy on its own is simply not enough to manage a crisis.

INCREASE IN THREATS

Threats are on the increase from a growing range of sources, for example: viruses, hackers, fraud and espionage. Exposure and dependency is on the increase: the growing use of IT, networks, communications and technology enablers, often with less central control, means that there are new entry points for intruders. At the same time stakeholders, managers, business partners, auditors and regulators are all demanding more protective risk management measures.
WHY DO WE NEED TO PLAN?

‘If you have a plan, and you operate that plan to the best of your ability – even if you may get something wrong on the day, at least you are defendable at a tribunal, a public enquiry or in court. But: if you have NO plans made, then you are not defendable, and you are on your own…’

Source: Legal counsel in the wake of the Canary Wharf Bomb, 1996

Planning is necessary in order to:

• Protect and ensure safety of all personnel;
• Limit collateral damage;
• Shutdown essential services in an ordered fashion;
• Preserve vital data/records;
• Recover ‘central services’ in priority order;
• Reduce financial loss/market share;
• Avoid financial penalties and fines;
• Avoid loss of client goodwill and negative PR.

CONSEQUENCES

The key to effective BCM planning is to consider the consequences rather than the causes of disruption, because it is possible to develop a single process which can respond to a range of incidents however they are caused. If you spend too much time trying to think of all the possible causes of disruption there would be an endless list of possibilities and planning for them all would be impossible. It is essential to consider consequences during working hours, at night, at weekends and during any annual shut-down periods.

So concentrate on the consequences not the causes and ask ‘what if’ questions, such as:

• What if we lose customer demand?
• What if customers cannot contact us?
• What if we lose access to our premises: for a day, a week, a month?
• What if the power goes down?
• What if we lose ICT and networks (especially access to fast, reliable broadband)?
• What if we lose utilities: e.g. gas and water?
• What if we lose information (digital and hard copy) in a fire/flood/or from theft?
• What if staff cannot arrive for work?
• What if we suffer staff casualties?
• What if we lose transport links?
• What if we lose a supplier?

Business continuity solutions can be implemented to protect from a variety of natural and man-made events. One key business decision to be taken is the type of incidents and risks that need to be protected against. Risk management and BCM plans can be developed for each of these consequences before disruption occurs.

Case study: Company A, an IT consulting company, issued a warning to all members of staff in the wake of Met Office reports warning of significant snow storms in January 2010 to work from home and only make essential travel journeys for clients who required consultants on-site. All clients were phoned to explain the situation and given an option. All were happy to allow consultants to work from home. The internet replaced the road network, physical travel was minimised and business continued. Not ‘like normal’ but ‘as normal’ as it could be.
BCM is dependent on a range of business variables, assets or components such as: people, information, business processes and service capabilities, physical premises, ICT infrastructure, management support and financial commitment. The impact of a major incident may be a loss of access to a site or office, a severe and prolonged shortage of staff, a loss of IT or telecommunications, fuel shortages or transport network disruption. It may even be the loss of a key business partner or failure in the supply chain.

The Six Stage Approach to BCM

There is a six stage approach which has been endorsed by both the Business Continuity and British Standards Institutes:

- Stage 1 – Programme management;
- Stage 2 – Understanding the organisation;
- Stage 3 – Determining the BCM strategy;
- Stage 4 – Developing and implementing a BCM response;
- Stage 5 – Exercising, maintaining and reviewing;
- Stage 6 – Embedding BCM in the business.

Figure 1   Relationship between ICT continuity management and business continuity management

Source: British Standards Institute
Another useful way to think about BCM is to consider the seven Ps of Business Continuity, as can be seen from the list below:

Programme management: Proactive management of the Business Continuity Management process (as distinct from plans development). The purpose is to run a BCM system.

People: Response, recovery and return-to-normal roles and responsibilities (together with BC training, education and awareness).

Processes: Making sure that all business processes which support delivery of services are included in plans, (including ICT).

Premises: Ensuring that infrastructure requirements (e.g. options for alternate buildings and facilities) are included in plans.

Providers: Supply chain, including outsourcing (critical 3rd parties with whom your business has a ‘transactional’ relationship).

Profile: Brand, image and reputation (the sum of activities for which value and reputation are key to survivability).

Performance: Benchmarking, evaluation and audit (measurement against key performance indicators, British Standards, good practice guidelines and industry best practice).

ARE THERE ANY HARD MONEY BENEFITS?
Some organisations have looked to their insurance companies for a reduced premium through adopting BCM practices. While it would be fair to say that the response is not universally positive, it does put businesses in a stronger position to assess risk if BCM practices are used. Other organisations are seeing an advantage in marketing their ‘resilience’ to potential customers and are winning new business as a result. In a downturn, this may be a timely and reassuring message to customers.

TIPS AND TECHNIQUES
This section includes a range of tips and techniques, all gained from the practical experience in the implementation of BCM, that can assist in the development of an effective BCM plan. It is based upon the seven Ps of Business Continuity mentioned previously.

Programme management:
• Get endorsement from the senior management team/business owners;
• Develop a policy statement;
• Implement a Business Continuity Management System (BCMS).

People:
• Know your staff and their immediate family members;
• Know their skills and capabilities;
• Instil an awareness of potential threats and train people what to do in a major incident.

Processes:
• Understand and document critical business processes;
• Understand the dependencies between business processes;
• Maintain an asset register of skills, capabilities and vulnerabilities;
• Design resilient procedures;
• Carry out exercises on the incident management process.

Premises:
• Be creative and flexible about where people work;
• Have recovery options considered BEFORE an incident occurs (hot, warm, cold sites, home etc);
• ‘Network-enable’ these options.

Providers (specifically of ICT resources):
• Explain the purpose and highlight the need within your supply team(s) of effective BCM;
• Liaise with all your suppliers and ensure they have a plan to maintain continuity of service to you;
• Make sure that your suppliers understand that your business reputation depends on their ability to deliver effective services;
• Design in redundancy, disperse your technology assets and information resources securely.

Profile:
• Ensure that any external links with media are managed effectively;
• Create positive conditions and perceptions.

Performance:
• Measure and draw evidence to support your process from:
  - BS 25999-1:2008 – Business Continuity Management;
  - BS 25777-1:2008 – IT Continuity Management;

Collectively these are Codes of Practice that take the form of guidance and recommendations. You may decide to opt for self certification or formal accreditation.

Understand that information is the critical resource:

‘Whether enterprise is for profit or not for profit, protecting information is an essential part of managing information and information systems. Modern companies, corporations and governments, for their success and survival, are dependent upon information – information that is created, processed, stored and shared. Yet the act of creating, processing, storing and sharing information makes it vulnerable to loss, manipulation, theft or destruction’.

Source: Edward Halibozek
Corporate Vice President of Security, Fortune 100 company

• Know what you know;
• Know what you need to know;
• Know what you don’t know!
• Know your critical information requirements;
• Understand the value of your information and the risks to it;
• Protect information resources.
4. DEVELOPING A PLAN

“We don’t have a plan, so nothing can go wrong”

Source: Spike Milligan

The Business Continuity Institute (www.thebci.org) publishes a set of Good Practice Guidelines. The following stages within this section summarise the main points contained in these guidelines.

STAGE 1 – BUSINESS CONTINUITY MANAGEMENT SYSTEM
When organisations embark on a BCM programme they are unlikely to have a Business Continuity Management System (BCMS) in place, nor probably understand the decisions needed to create one. A series of steps are required to work towards a formulation of this system. The most important of these are:

• Ensuring that the BCM programme supports the strategy, objectives and culture of the business;
• Deciding on the scope of the BCMS and formulating a policy;
• Acceptance of the need to have a business continuity plan.

STAGE 2 – UNDERSTANDING YOUR BUSINESS
The Business Impact Analysis (BIA) is the foundation upon which the process is built. It identifies, quantifies and qualifies the impacts of loss or disruption.

Outputs from the BIA include: Recovery Time (RTO) and Recovery Point Objectives (RPO), together with estimates of recovery requirements (resources, facilities, equipment etc). It also assists in evaluating the threats to business operations, and the likelihood and impact on specific functions. Measures can be identified to help reduce the probability of occurrence or reduce the impacts under ‘business as usual’ decision-making.

STAGE 3 – DEFINING A BCM STRATEGY
In essence, this stage identifies the alternative strategies that are available to mitigate, for example, loss of critical assets such as personnel, premises and ICT. It also assesses the potential effectiveness of these strategies in maintaining your ability to safeguard critical functions. This includes services which might be outsourced, such as ICT.

In the context of BCM, the ‘strategy’ is concerned with identifying and selecting the alternative operating methods that might be used to maintain critical services to an acceptable minimum level following a disruption. For each product and service businesses should ask a simple question ‘what if this service (or function) is disrupted?’, and make a strategic decision on how best to protect its delivery.

Strategic options for products and services include:

• Do nothing;
• Adopt an approach that mitigates the loss or addresses the risk;
• Change, suspend or terminate the use of the product or service;
• Incorporate the requirements in the business continuity plan.

If the last option is selected then there are a number of tactical choices to be made based on the resumption timescales determined from the Business Impact Analysis.

STAGE 4 – DEVELOPING AND IMPLEMENTING A BCM RESPONSE
This stage delivers an actual plan – how long it takes to develop will depend on the complexity of your business. Every business is different in this regard.

The aim of the plan is to identify the actions that are necessary and the resources which may be required to
enable your business to manage the consequences of disruption. It should be simple and flexible.

The requirements for an effective response are:

- A clear procedure for escalation and control of an incident;
- Communication with stakeholders – staff, customers, shareholders;
- Plans to resume after disruptions to activities – cross-skilling for staff, alternate premises, off-site data, re-routing of telecoms, etc.

STAGE 5 – EXERCISING, MAINTAINING AND AUDITING BCM

This stage sets out the steps to ensure that the BCM plans are fit for purpose, kept up-to-date and quality assured.

Plans cannot be considered reliable until they have been rehearsed and the systems tested. This rehearsal can take various forms (technical tests, desktop walk-throughs and full live exercises). Workshop time spent discussing plans is a vital part of the process as this develops competence, instils confidence and transfers knowledge.

STAGE 6 – DEVELOPING A BCM CULTURE

Finally, ensuring that a continuity culture is embedded in your business will make the difference between success and failure if you ever need to rely on the plans in a real situation. Establishing a culture of continuity takes time and is dependent upon the integration of individual aspirations with business objectives and priorities.
5. WHAT DOES A GOOD BCM PLAN LOOK LIKE?

‘The superior man, when resting in safety, does not forget that danger may come. When in a state of security, he does not forget the possibility of ruin. When all is orderly, he does not forget that disorder may come. Thus his person is not endangered, and his States and all their clans are preserved’

Source: Confucius

THE GOLDEN RULES FOR A BUSINESS CONTINUITY PLAN

When developing a Business Continuity Plan it will help to bear in mind the following recommendations, all of which are designed to ensure that it is as effective as possible:

- Keep it simple;
- Recognise that there is no single answer for all events;
- Weigh up all of the options and make the plan(s) appropriate;
- Ensure you can manage during a crisis;
- Know what is needed to manage resources;
- Make departments or services own their plans;
- Exercise, maintain, audit and review;
- Control the distribution of the plan and ensure that version control is also addressed;
- Make plans easily accessible.

THE CONTENTS OF A BUSINESS CONTINUITY PLAN

Plans will differ between businesses but there are some components that are common to all plans. The following list is by no means exhaustive but it gives a good indication of some of the major elements that you should be looking to incorporate into your plan:
<table>
<thead>
<tr>
<th>SECTION</th>
<th>PARAGRAPH TITLE</th>
<th>CONTENTS</th>
</tr>
</thead>
</table>
| 1       | Plan and control information | Ownership  
Distribution  
Maintenance cycle and change control |
| 2       | Introduction | Scope  
Context  
Purpose  
Plan structure  
Emergency response  
Crisis management  
Business recovery plans  
IT recovery plans |
| 3       | Emergency response | High level process overview  
Emergency response team  
Emergency response objectives  
Emergency response tasks  
Initial assessment  
Assigning an Emergency Level (1,2,3,4) |
| 4       | Crisis management | Crisis management structure (one or more teams)  
Crisis management team responsibilities  
Service operations responsibilities (front of house)  
HR, Facilities, ICT responsibilities (back office/corporate support services)  
Details: team members, evacuation, authority to invoke, BC invocation, notifications, assessments, tasks, internal/external communications, critical contacts, locations of alternate premises, confirmation of recovery strategy |
| 5       | Individual recovery plans | HR, Facilities, ICT, business units/departments etc |
| 6       | Appendices | Change control  
Assessment checklists  
Severity index  
Objectives, tasks  
Actions taken and decision log  
CMT/SMT agenda\(^2\)  
Scenario flow charts etc |

\(^2\) CMT = Crisis Management Team. SMT = Senior Management Team. In a small business it is likely these teams would be one and the same.
## A SEVERITY MATRIX

A severity matrix is a useful tool for clearly highlighting to your staff what constitutes a minor incident through to what you define as a major incident. The matrix should specify the actions to be taken in the event of any of the different levels of incident or disruption actually occurring.

An example of a simple severity matrix is included below.

<table>
<thead>
<tr>
<th>SEVERITY LEVEL</th>
<th>CRITERIA</th>
<th>ACTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Minor Incident</td>
<td>The incident is unlikely to affect business operations.</td>
<td>SMT: inform</td>
</tr>
<tr>
<td></td>
<td>No staff casualties.</td>
<td>CMT: involvement not required</td>
</tr>
<tr>
<td></td>
<td>The incident can be dealt with and closed by the regular site staff and/or the emergency services.</td>
<td></td>
</tr>
<tr>
<td>2. Minor Disruption to Business Unit</td>
<td>Impact to business operations expected to be of limited severity.</td>
<td>SMT: inform</td>
</tr>
<tr>
<td></td>
<td>Minor short-term disruption to ICT.</td>
<td>CMT: notified and placed on standby</td>
</tr>
<tr>
<td></td>
<td>Incident expected to be dealt with inside 24 hours.</td>
<td></td>
</tr>
<tr>
<td>3. Significant Disruption</td>
<td>Loss of ICT.</td>
<td>SMT: involvement mandatory</td>
</tr>
<tr>
<td></td>
<td>Staff hospitalisations (no fatalities).</td>
<td>CMT: involvement mandatory/invoke BCP</td>
</tr>
<tr>
<td></td>
<td>Incident expected to require more than 24 hours to resolve.</td>
<td>Board/owners: involvement mandatory</td>
</tr>
<tr>
<td></td>
<td>Access denied for more than 24 hours.</td>
<td>Key customers: informed</td>
</tr>
<tr>
<td>4. Major/Catastrophic Incident</td>
<td>Loss of ICT.</td>
<td>SMT: involvement mandatory</td>
</tr>
<tr>
<td></td>
<td>Major widespread incident in the geographic area.</td>
<td>CMT: involvement mandatory</td>
</tr>
<tr>
<td></td>
<td>Significant disruption to business activities.</td>
<td>Board/owners: involvement mandatory</td>
</tr>
<tr>
<td></td>
<td>Staff fatalities.</td>
<td>Key customers: informed and kept in close contact</td>
</tr>
</tbody>
</table>
BCM helps to identify what your business critical functions and outputs are and the threats to them. It provides you with a proven planning framework to design effective measures to deal with these threats and, if risk mitigation is not possible, then workable contingency plans are also provided to manage the consequences of disruption when it occurs.

BCM copes with small-scale as well as headline incidents and is not a one-off planning exercise but a genuine business process – for all SMEs. For its maximum effectiveness it should be woven into the fabric of normal business planning and decision-making.

Through asking the question ‘what if...’ your business can define its approach to BCM by considering the consequences (and not just the causes of disruption) while applying the key principles such as asset dispersion – storing data, electronically, and off site in a digital archive; cross-training and cross-skilling members of staff in essential tasks and ensuring a steady pulse of awareness throughout the trading cycle.

‘Better to have the business continuity plan and not need it, than to need the plan and not have it’

Source: Anon (Australia)
# APPENDIX A: FURTHER INFORMATION RESOURCES

## USEFUL WEBSITES

<table>
<thead>
<tr>
<th>ORGANISATION</th>
<th>WEBSITE</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cabinet Office</td>
<td><a href="http://www.cabinetoffice.gov.uk">http://www.cabinetoffice.gov.uk</a></td>
<td>Leads on emergency planning and training to ensure the resilience of the UK at every level, central, regional and local, against disruptive challenges.</td>
</tr>
<tr>
<td>UK Resilience</td>
<td><a href="http://www.ukresilience.info">www.ukresilience.info</a></td>
<td>This website exists to provide a resource for civil protection practitioners, supporting the work which goes on across the United Kingdom to improve emergency preparedness.</td>
</tr>
<tr>
<td>MI5</td>
<td><a href="http://www.mi5.gov.uk">www.mi5.gov.uk</a></td>
<td>The Security Service (MI5) is responsible for protecting the United Kingdom against threats to national security. This website provides information about the Security Service, the threats it counters, links to sources of security advice.</td>
</tr>
<tr>
<td>Business Continuity Institute</td>
<td><a href="http://www.thebci.org">www.thebci.org</a></td>
<td>The Business Continuity Institute (BCI) was established in 1994 to enable individual members to obtain guidance and support from fellow business continuity practitioners. The BCI currently has over 5000 members in 90 countries.</td>
</tr>
<tr>
<td>London Prepared</td>
<td><a href="http://www.londonprepared.gov.uk/businesscontinuity/">http://www.londonprepared.gov.uk/businesscontinuity/</a></td>
<td>Business Continuity Management (BCM) is planning to ensure that your organisation has a relatively quick and painless return to ‘business as usual’ in the event of a major disruption.</td>
</tr>
<tr>
<td>Continuity Advice</td>
<td><a href="http://www.continuitycentral.com">www.continuitycentral.com</a></td>
<td>Continuity Central provides a constantly updated one-stop resource of business continuity news, jobs and information.</td>
</tr>
<tr>
<td>The British Standards Institution</td>
<td><a href="http://www.bsi-global.com">http://www.bsi-global.com</a></td>
<td>The BSI Group:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Develops private, national and international standards;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Certifies management systems and products;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Provides testing and certification of products and services;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Provides training and information on standards and international trade;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Provides performance management and supply chain management software solutions.</td>
</tr>
<tr>
<td>Global Continuity</td>
<td><a href="http://www.globalcontinuity.com">http://www.globalcontinuity.com</a></td>
<td>Global Continuity ‘reduces the risk of business interruption’ and perhaps more importantly, it reduces losses and thereby the impact of a disaster by providing a range of recovery services aimed at small and medium sized companies.</td>
</tr>
</tbody>
</table>
FURTHER READING
British and other Standards:

• BS 25999-1 Business Continuity Management Code of Practice (BSI);
• BS 25999-2 Business Continuity Management Specification (BSI);
• BS 25777:2008 IT Continuity Management Code of Practice (BSI);

METHODOLOGIES AND OTHER PUBLICATIONS
These include:

• Managing Successful Projects with PRINCE2 (Office of Government Commerce);
• Managing Successful Programmes (Office of Government Commerce);
• Management of Risk (Office of Government Commerce);
• Project Management Body of Knowledge (Project Management Institute);
• The Risk Management Standard (Institute of Risk Management);
• IT Infrastructure Library, (Office of Government Commerce).
APPENDIX B: SUMMARY OF PLANNING FACTORS

Some of the key planning factors to consider at the outset of your Business Continuity Planning exercise are included in this appendix as an aide memoire.

<table>
<thead>
<tr>
<th>FACTOR/CONSIDERATION</th>
<th>OBSERVATIONS</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  Understand the drivers</td>
<td>Why are you introducing BCM?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Internal or external drivers?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>How quickly must it be introduced?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>What will be covered?</td>
<td></td>
</tr>
<tr>
<td>2  Current drivers</td>
<td>Regulation/Legislation: Civil Contingencies Act 2004</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Government</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Auditors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Corporate Governance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Insurers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Customers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Supply chain</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Protection of brand/reputation</td>
<td></td>
</tr>
<tr>
<td>3  Scope</td>
<td>Will your BCM cover:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The entire organisation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• By division</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• By location</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• By service</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• By customer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• By regulatory/statutory requirement</td>
<td></td>
</tr>
<tr>
<td>4  Programme management</td>
<td>BCM policy statement</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ongoing support from the Board/Executive and Senior Management Team</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BCM structure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Adequate resources to deliver BCM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>An assurance process (KPIs)</td>
<td></td>
</tr>
<tr>
<td>FACTOR/CONSIDERATION</td>
<td>OBSERVATIONS</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------</td>
<td>----------</td>
</tr>
<tr>
<td>5 Responsibility</td>
<td>Where will ultimate responsibility lie?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Board</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Senior Management Team</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Risk/compliance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Finance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Facilities</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Quality</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Health and safety</td>
<td></td>
</tr>
<tr>
<td>6 Understanding the Organisation</td>
<td>Who are the key stakeholders?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>What are the key services?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>What are the supporting critical services?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>What processes are used to deliver critical activities?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Who and what is used in these processes? Internally, externally</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The impact over time if critical activities are interrupted – for whatever reason</td>
<td></td>
</tr>
<tr>
<td>7 Business Impact Analysis (BIA)</td>
<td>What is it</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Why is it important</td>
<td></td>
</tr>
<tr>
<td></td>
<td>How is it done</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Key terms: Recovery Time Objectives (RTO), Recovery Point Objectives (RPO), Maximum Tolerable Period of Disruption (MTPD)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Key themes: qualitative and quantitative impacts</td>
<td></td>
</tr>
<tr>
<td>8 BIA Questions</td>
<td>Describe your business</td>
<td></td>
</tr>
<tr>
<td></td>
<td>What are your main service activities?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>With whom do you need to be in contact (internal)?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>With whom do you need to be in contact (external)?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>What are your most critical times in the day/week/month/year?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>What are your qualitative impacts?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>What are your financial impacts?</td>
<td></td>
</tr>
</tbody>
</table>

The Business Impact Analysis is the foundation work from which the whole BCM process is built. It identifies, quantifies and qualifies the business impacts of a loss, interruption or disruption of business processes on an organisation and provides the data from which appropriate continuity strategies can be determined.
<table>
<thead>
<tr>
<th>FACTOR/CONSIDERATION</th>
<th>OBSERVATIONS</th>
<th>COMMENTS</th>
</tr>
</thead>
</table>
| 8 BIA Questions (continued) | On which IT systems/applications is your service dependent?  
What manual fallback/reversionary modes does your business have in place?  
Who are your key service suppliers?  
What are your business’s Recovery Time Objectives (RTO)?  
What alternate working locations are available for your business?  
What are your business’s Recovery Point Objectives (RPO)?  
What is your business’s Maximum Tolerable Period of Disruption (MTPD)?  
On what vital records does your business depend? |                                                                                                     |
| 9 Risk Assessment     | Identify single points of failure:  
• People  
• Premises  
• Processes  
• Information and systems  
• Facilities  
• Suppliers | Consider vulnerability of critical resources  
Consider security of these resources  
Can you reduce the vulnerabilities and improve resilience?                                         |
| 10 Strategic Options   | • Do nothing (accept risk)  
• Change, transfer, end business process/service (avoid risk)  
• Insure (transfer risk)  
• Loss mitigation (reduce impact)  
• Plan for continuity | Risk strategy would probably be a blend of two or more of these options                              |
| 11 Sign Off            | Board/SMT should sign off:  
• The documented list of key products and services  
• The Business Impact Analysis  
• The risk assessment | To ensure the work has been appropriate and is a true reflection of the organisation                 |
| 12 Delivering Critical Services | Understanding of:  
• Key services  
• Supporting critical activities and resources  
• Threats/risk to these  
• Recovery time and levels at which services will be required following disruption | At a strategic level: what options are available?                                                     |
<table>
<thead>
<tr>
<th>FACTOR/CONSIDERATION</th>
<th>OBSERVATIONS</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>13 Delivering BCM Strategies</td>
<td>What do we mean by strategy?</td>
<td>In the context of BCM, ‘strategy’ concerns the determination and selection of alternative operating methods to be used to maintain critical services following disruption, to an acceptable minimum level.</td>
</tr>
<tr>
<td>14 Strategic Approach</td>
<td>Implement appropriate measures to reduce likelihood of incidents occurring and/or reduce impacts if they do Provide continuity for key services and supporting activities during and following disruption Take account of these services and their supporting activities that have not been identified as critical</td>
<td></td>
</tr>
<tr>
<td>15 Determining BCM Strategies</td>
<td>Ideally these should cover: • People (HR) • Premises (facilities) • Information &amp; Communication Technologies (ICT) • Suppliers • Stakeholders</td>
<td></td>
</tr>
<tr>
<td>16 Appropriate Strategy</td>
<td>Will depend on the Maximum Tolerable Period of Disruption (MTPD) The cost of implementing the mix of strategies The consequences of inaction</td>
<td></td>
</tr>
<tr>
<td>17 BCM Options</td>
<td>‘Budge up’ Displace Remote/home working Reciprocal arrangements High availability systems Hot/warm alternatives Alternate routing for telecoms</td>
<td>‘Workarounds’ Storage and salvage Succession planning Cross-training Quick response contracts Suppliers of BCM + many more</td>
</tr>
<tr>
<td>18 Sign Off</td>
<td>Board/SMT should: - Determine continuity strategies have been properly undertaken - Consider and cater for likely cause and effect (consequences) - Ensure chosen strategies are appropriate to meet the business’s risk appetite and business objectives</td>
<td></td>
</tr>
<tr>
<td>FACTOR/CONSIDERATION</td>
<td>OBSERVATIONS</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| 19 Developing a Response | Plans should be developed to cover key services and their supporting activities and might include:  
- High level plans  
- Departmental plans  
- Incident management plans  
- Full recovery plans | | |
| 20 Plans should contain | Scope of plan  
Roles and responsibilities  
Plan invocation  
Contact details  
Task and action lists  
Resource requirements  
Forms and annexes | | |
| 21 Test, Review and Maintain | Test systems  
Exercise plans  
Rehearse people  
Keep plan(s) current and up-to-date  
Determine measures for assurance  
Internal, external audit or self assessment  
BS 25999-1:2006, BS 25777:2008  
External benchmarks | | |
| 22 Establish BCM Culture | Raise awareness across organisation  
Train appropriate staff  
Inform stakeholders  
Ongoing support from Board/SMT  
Executive sponsor  
Communicate to all | | |
<table>
<thead>
<tr>
<th>FACTOR/CONSIDERATION</th>
<th>OBSERVATIONS</th>
<th>COMMENTS</th>
</tr>
</thead>
</table>
| 23 Communications    | Consult with staff concerning the implementation of the BCM programme  
Discuss BCM in newsletters, briefings, team meetings, induction training, internal communications etc  
Include BCM on web and intranet  
Incorporate lessons learned from internal/external incidents  
Exercise continuity plans  
Arrange visits to designated alternate locations for relevant members of staff |          |
| 24 Source            | Continuity Forum | http://www.continuityforum.org/ |
## APPENDIX C: EXAMPLES OF QUICK WINS

<table>
<thead>
<tr>
<th>CATEGORIES</th>
<th>TRIGGER (CAUSE OF INCIDENT) OR KEY ISSUE</th>
<th>CONSEQUENCE/IMPACT</th>
<th>QUICK WIN/LOW COST (SOLUTIONS)</th>
<th>COST</th>
<th>BENEFIT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BCM PROGRAMME MANAGEMENT</strong></td>
<td>No senior champion for BCM and executive support highlighting policy and strategy etc</td>
<td>BCM programme and planning will fail</td>
<td>Appoint Management Team/Board-level champion</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>No budget for BCM</td>
<td>BCM planning will fail</td>
<td>Set budget</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>No organisational acceptance of reality: rising expectations, threats, vulnerabilities and dependencies</td>
<td>BCM adoption will fail</td>
<td>CMT/Board endorses/drives the programme accepting the need for change</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>No staff training programme</td>
<td>BCM planning and maintenance will fail</td>
<td>Training and awareness campaign</td>
<td>Low – Med</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>No knowledge of BCM – Project Team</td>
<td>BCM delivery and implementation will fail</td>
<td>Train BCM Project Team in BCM process</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>No plans or process ownership</td>
<td>BCM process will fail</td>
<td>Appoint Heads of Departments as plan owners</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>No Crisis/Incident Management Team</td>
<td>BCM response and recovery will fail</td>
<td>Appoint and train Crisis/Incident Management Team</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>No knowledge transfer or sharing of ideas</td>
<td>Key benefit of this process is lost</td>
<td>Collaboration across business</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td><strong>PEOPLE</strong></td>
<td>Staff holidays, career development etc</td>
<td>Loss of key staff – planned</td>
<td>Multi-tasking Cover for essential services</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Staff illness/industrial action</td>
<td>Loss of staff – unplanned</td>
<td>Health and Safety HR and Industrial Relations</td>
<td>Low – High</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Lack of training in BCM/failure to invest in people</td>
<td>Critical skills fade</td>
<td>Individual and collective training</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td><strong>PROCESSES</strong></td>
<td>Data unavailability, modification malware, virus etc</td>
<td>Loss of data/critical information (hard/digital copy)</td>
<td>Off-site storage, backup, resilient platform architecture, dual applications/suppliers</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Technical ICT failure, however caused</td>
<td>Long term loss/failure of all ICT operations</td>
<td>ICT disaster recovery plan(s)</td>
<td>Low – High</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Technical ICT failure, however caused</td>
<td>Short term disruption to ICT service</td>
<td>ICT disaster recovery plan(s)</td>
<td>Low – High</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Human error</td>
<td>Short term failure of process</td>
<td>Training in BCM Documented processes/procedures – BCM</td>
<td>Low – High</td>
<td>High</td>
</tr>
<tr>
<td>CATEGORIES</td>
<td>TRIGGER (CAUSE OF INCIDENT) OR KEY ISSUE</td>
<td>CONSEQUENCE/IMPACT</td>
<td>QUICK WIN/LOW COST (SOLUTIONS)</td>
<td>COST</td>
<td>BENEFIT</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------</td>
<td>--------------------</td>
<td>--------------------------------</td>
<td>--------</td>
<td>--------</td>
</tr>
<tr>
<td><strong>PREMISES</strong></td>
<td>Fire, flood, arson, terrorist attack</td>
<td>Long term (six months) structural damage to business</td>
<td>Asset dispersion. Telephony resiliency options</td>
<td>Low – High</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Fire, flood, arson, terrorist attack</td>
<td>Short term denial of access to business</td>
<td>Asset dispersion. Telephony resiliency options</td>
<td>Low – High</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Fire, flood, arson, terrorist attack</td>
<td>Total loss of business</td>
<td>Asset dispersion Alternate site</td>
<td>Low – High</td>
<td>High</td>
</tr>
<tr>
<td><strong>PROVIDERS</strong></td>
<td>Power: sub-station flooding</td>
<td>Total loss/failure of power (UPS)</td>
<td>Alternate supply, generator(s) Supply chain BCP audit</td>
<td>Low – High</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Power: deliberate/accidental damage to grid</td>
<td>Disruption to power</td>
<td>Dual suppliers Service Level Agreements Supply chain BCP audit</td>
<td>Low – High</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Power: unavailability of service provider’s staff</td>
<td>Loss of other non-power utilities (e.g. gas and water)</td>
<td>Dual suppliers Service Level Agreements Supply chain BCP audit</td>
<td>Low – High</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Telephony</td>
<td>Disruption/loss of telephony</td>
<td>Dual suppliers Service Level Agreements Supply chain BCP audit</td>
<td>Low – High</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Other utilities/suppliers</td>
<td>Loss/failure of other key 3rd party suppliers (non ICT)</td>
<td>Identify/source alternate suppliers Supply chain BCP audit</td>
<td>Low – High</td>
<td>High</td>
</tr>
<tr>
<td><strong>PROFILE</strong></td>
<td>Breach of statutory obligations/duties</td>
<td>Loss of reputation and credibility Legal action</td>
<td>Audit against relevant statutes</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td><strong>PERFORMANCE</strong></td>
<td>Poor audit report</td>
<td>Failure to benchmark against or adopt best practice</td>
<td>BS 25999-1:2006 GPG 2010</td>
<td>Low</td>
<td>High</td>
</tr>
</tbody>
</table>
James Royds has worked extensively in the risk, governance and compliance sector since 1996 delivering solutions and services to clients in the private and public sectors. He is currently the Chairman of the Business Continuity Institute (BCI) and a Fellow of both the BCI and the Chartered Management Institute. He is also the Director of Resilience for Steelhenge, responsible for leading their consultancy practice in the United Kingdom and the Middle East (www.steelhenge.co.uk).

James specialises in meeting the growing demand for integrated risk, business continuity, crisis management and information security solutions and is regularly invited to speak at major conferences and symposia.

He has recently qualified as a Lead Auditor for BS 25999 and was one of a handful of trusted experts co-opted by the BSI to tour the UK raising awareness of the British Standard for Business Continuity Management when it was first published in 2006.
IT FACULTY BENEFITS

• Keep on top of important developments with e-bulletins, bi-monthly magazine and technical reports.

• Access information on demand via the faculty’s exclusive website and the IT Counts community.

• Advance your career and business with practical help and resources – from online tools to free member events.

• Exchange ideas and make useful contacts through our networking facilities.

• Have your say and contribute to the faculty’s reputation for engaging with the important issues and the key players in IT.

The IT Faculty exists to help accountants make better use of IT and to further the study of information technology in all its forms, including the development of thought leadership and research. Membership is open to anyone, not just Chartered Accountants, for an annual subscription of £99.

Visit us and join online at icaew.com/itfac.

As a world-class professional accountancy body, The Institute of Chartered Accountants in England and Wales (ICAEW) provides leadership and practical support to over 132,000 members in more than 160 countries, working with governments, regulators and industry to maintain the highest standards.

Our members provide financial knowledge and guidance based on the highest technical and ethical standards. They are trained to challenge people and organisations to think and act differently, to provide clarity and rigour, and so help create and sustain prosperity. The ICAEW ensures these skills are constantly developed, recognised and valued.

Because of us, people can do business with confidence.

Information Technology Faculty
ICAEW T +44 (0)20 7920 8481
Chartered Accountants’ Hall F +44 (0)20 7920 8657
Moorgate Place E itfac@icaew.com London icaew.com/itfac
EC2R 6EA UK

£17.50