Organisation Resilience: Business Continuity, Incident and Corporate Crisis Management.

Introduction

Despite their best endeavours no organisation can have complete control over its business environment especially its supply chain. It is therefore essential for both public and private sector organisations to have an effective and appropriate business continuity management (BCM), incident and corporate crisis management capability.

This paper is by Dr David J. Smith MBA LL.B(Hons) FIBCM BCCE who is the Chairperson of the Institute of Business Continuity Management. He is also a practicing business continuity professional and Director of several companies that provide business continuity consultancy and training. David is also the Business Continuity lead, author and principle trainer of the accredited BCM Diploma at the Hatfield Tuition College of the HTC Further Education Training Colleges in Pretoria, Johannesburg and Cape Town.

The paper outlines various considerations, issues and approaches that can help organisations prepare for business continuity, incident and corporate crisis management within the context of the BCM life cycle (see Figure 3) and are aligned to BS25999 and ISO22301. In particular the paper addresses the following issues within the context of business continuity:

- Business Continuity Management (BCM);
- Corporate Governance and other key drivers;
- BCM standards;
- A BCM System (BCMS);
- Building and embedding BCM within the organisation;
- Avoiding the planning bureaucracy
- Using accepted standards;
- The BCMS framework and workflow:
- Incident and Corporate Crisis Management;
- A three tier response and governance structure;
- Categories of incident and corporate crisis;
- Incident and corporate crisis management implementation programme;
- Review and evaluating performance;
- Summary;
- The fatal price of failure;
- Suggested further reading and references

So what is the difference between what is already in place and why is it so important?

Both national and international events of recent years has led Governments, regulators, insurers and other public and private sector bodies to emphasise and actively promote the view that a robust, proactive, effective and appropriate level of organisation resilience and proven BCM preparedness is essential. As part of the overall risk management of an organisation and in the face of the challenges and threats that inevitably arise in today's national and global business and public sector service environment complacency is wholly unacceptable.

Reg. No. 2012/004736/08

This warning is reinforced by historical research and the issues are further highlighted and reinforced in the findings and conclusions of recently published research conducted by the Institute of Risk Management (UK).[1] The summary of the conclusions of that research are that ...'Many of the risks we have highlighted are inherent in every organisation. Unrecognised and unmanaged, these underlying risks pose a potentially lethal threat to the future of even the largest and most successful businesses. Boards, particularly chairmen and NEDs (non-executive directors), have a large, important blind spot in this dangerous area. Without board leadership, these risks will remain hidden because only boards can ensure that enough light shines on these hard to see risks'.[2]

In respect of the research and its findings Mark Taylorson considers, 'The case studies outlined in Roads to Ruin consist of some of the world's biggest organisations, with the risk events having considerable, often catastrophic, impacts on these organisations. In seven cases the companies faced bankruptcy. In eleven cases the Chairman and/or CEO lost their roles and a huge number of executive and non-executive directors lost their jobs... it identifies key flaws within these organisations' risk management that significantly contributed to these events... Directors have to make crucial risk-related decisions impacting the future of their companies and Roads to Ruin provides them with important lessons in the flow of information, communication and corporate governance that were found lacking in the case studies investigated'.[3]

Whilst many commentators within the public sector describe the differences between the public and private sector I firmly believe the management discipline of BCM, incident and corporate crisis management is common to both. This is reinforced by King III and its associated guidelines. However, in recognising the differences in the raison d'etre of both the public and private sectors it is perhaps helpful to consider BCM as Service Continuity Management in respect of the public sector. Within this context it is recognised that both sectors are producing either a service or product for consumption by an internal or external customer or client and have various stakeholders. As a consequence, 'reference to **"business"** ...is intended to be interpreted broadly to mean those activities that are core to the purposes of an organisation's existence'.[4]

Business Continuity Management (BCM)

Business Continuity Management (BCM) is defined by the British Standards Institute (BSI) as 'an 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'.[5]

The term 'Business Continuity Management' is used rather than 'business continuity planning'. This approach is deliberate because 'planning' implies there is a start and end to the process and can lead to unwanted planning bureaucracy. Within this context business continuity planning is still a critical and key component of a BCM programme. In contrast to the earlier narrow and reactive approaches to BCM it is now recognised as a dynamic, proactive, and ongoing business as usual management process. To be effective it must be complete against a standard, appropriate (fit for purpose), practical, realistic, up-to-date, effective and a plausible (proven) capability.

At a time when 'Just In Time' (JIT) delivery, procurement and supply chain issues in general have a high profile there is a need to consider the big picture and both the fragility and resilience of an organisation's capability to deliver its own products and services. In particular the organisation's supply chain and their dependency upon it. In addition there are regulatory, legal, insurance, licence and contractual requirements to consider whereby contract management takes on a different role to that traditionally recognised. Within this context there is the

[1] AIRMIC (2011) 'Roads to Ruin - A Study of Major Risk Events; their origins, impacts and implications'
[2] AIRMIC (2011) 'Roads to Ruin'
[3] Mark Taylorson, 2011.
[4] ISO 22301: Section 5.2 -Note 1
[5] BS 25999 (parts 1 and 2) and ISO 22301

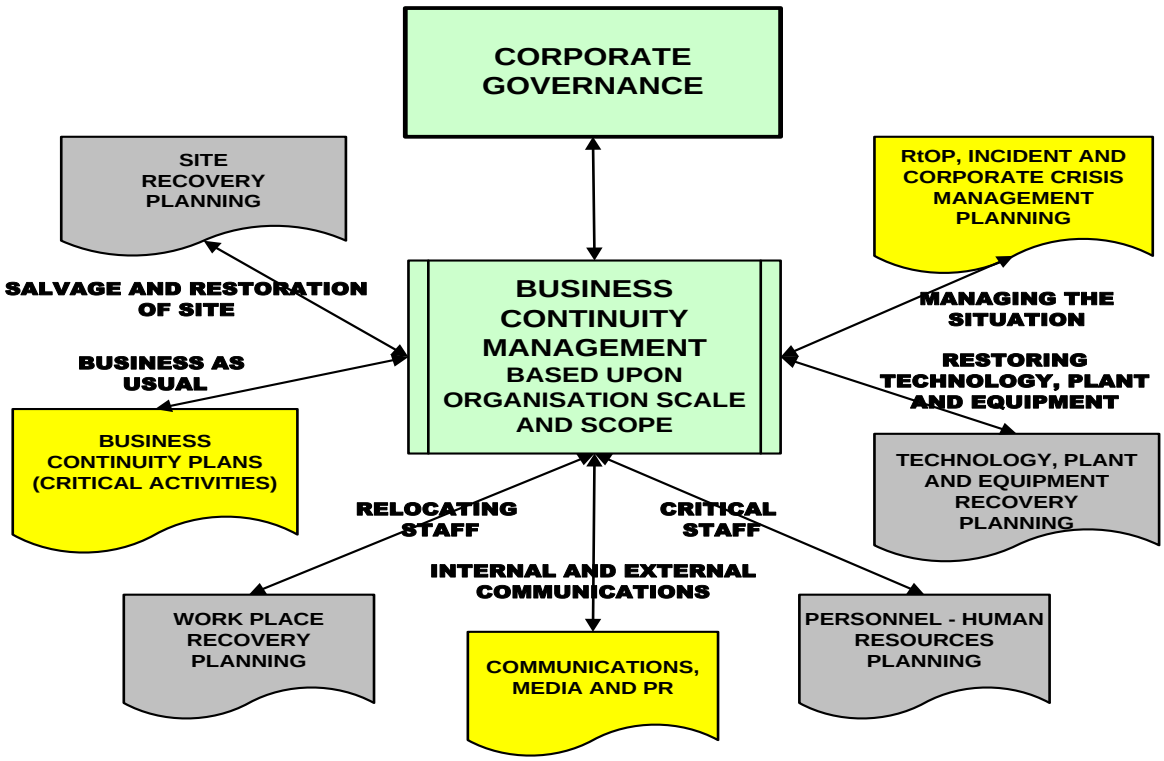
Reg. No. 2012/004736/08

ever growing differentiator within the procurement process where organisations are asked to provide demonstrable proof of their BCM capability. The failure to respond or be able to demonstrate what is required will provide an 'exit' within the process creating a **'lost opportunity'** rather than having a strong evidential based **'competitive advantage'**.

Whilst there are now accepted standards, regulations, good practice guidelines and other criteria against which an organisation can implement and measure BCM and its key components it should always be remembered that as a risk management discipline not all organisations will want to have their BCM programme certificated against a whole standard. In contrast they will properly use the standard to enable them to achieve sufficient organisation resilience, business continuity, incident and corporate crisis management capability to meet their needs based on their scale, scope and risk appetite. This approach is frequently described as good practice and is favoured by many organisations based on good risk management and cost benefit alone.

Within this context both BS 25999-2 and ISO 22301 standards 'provide a specification/requirements for use by internal and external parties, including certification bodies, to assess an organisation's ability to meet regulatory, customer and the organisation's own requirements... **it contains only those requirements that can be objectively audited...** are generic and intended to be applicable to all organisations regardless of type, size and nature of business. The extent of the application of these requirements depends on the organisation's operating environment and complexity'[6].

Figure 1: Governance and BCM Seven Key Constructs[7]



[6] BS 25999-2: Forward and Scope and ISO 22301 - Scope
[7] Dr David J Smith (2002)

Reg. No. 2012/004736/08

In essence BCM is an organisation owned and driven process that establishes a fit-for-purpose strategic and operational framework that:

1. Proactively improves an organisation's resilience against the disruption of its ability to achieve its key objectives;
2. Provide a rehearsed method of restoring an organisation's ability to supply its key products and services to an agreed level (performance and functionality) within an agreed time after a disruption/incident; and
3. Deliver a proven capability to manage a disruption/incident and protect the organisation's reputation and brand'[8]

In achieving these objectives BCM unifies a broad spectrum of management, operational and technical disciplines. It is not just about IT disaster recovery (ITDR). There are seven key constructs to Business Continuity Management (see Figure 1). Historical and current research findings indicate that too many organisations, traditionally and understandably, tend to focus all their efforts on IT because of its critical business nature. Regretfully, this approach leaves them exposed on many other fronts and to many other risks.

As a result of its all-embracing nature, the way BCM is carried out will inevitably be dependent upon, and must reflect, the nature, scale and complexity of an organisation's risk profile, risk appetite and the environment in which it operates. The importance of an integrated and whole of business/organisation approach across these areas has been reinforced in both national and international legislation, regulations, standards, codes of practice, guidelines and principles.[9] This is especially true of organisations that have operations in more than one country; not only does their BCM apply to their home country but another countries BCM criteria may apply to their BCM capability within their own country e.g. SEC - NY stock exchange listing rules.

In recognising that an organisation can never be fully in control of its operating environment, it is safe to assume that all organisations will face a business continuity incident and/or corporate crisis at some point. In addition to climatic disasters and rogue traders this simple reality has been etched in high-profile names across numerous industries and countries/continents such as Swine flu, Buncefield, Hurricane Katrina (New Orleans), 7/7 London Transport Bombings, Bhopal, Bird Flu, Piper-Alpha, Challenger, Enron, Mastercard and Visa Hackers (40 million credit cards vulnerable), Exxon-Valdez, SARS, Marsh McLellan, Slapper Worm, Sumitomo Bank (£220 million - Hackers Key logging), Hurricane Sandy and the two attacks on the World Trade Centre[10]. Experience also teaches that it is the less dramatic but more frequent business continuity incidents that can be even more problematic to deal with. The individual and corporate memory of many business continuity incidents and/or corporate crises fades over time. That is until the next time! Regrettably, it seems to be a fact of life that lessons learnt and there often drawn-out ongoing implementation from previous or other organisations incidents/crises rush to the fore and the time honoured 'blame culture scapegoating' process begins. Unfortunately, it seems that many public and private organisations still think, 'it will not happen to us' or if it does we will survive and it will not be as bad as we think.[11]

Corporate Governance and other key drivers

BCM has always been a key element of an enterprise risk management programme and consequently corporate governance. This is now fully recognised and amply demonstrated by the inclusion of Business Continuity Management within the King III Code of Practice for Corporate Governance that applies to all entities regardless of the manner of their incorporation or establishment. Within this context King III adopts the UN governance principle of 'apply or explain' to the implementation of its Code of Governance.

[8] BS 25999-1: Section 3.1
[9] See suggested further reading
[10] See also IRM (UK) (2011) 'Roads to Ruin'
[11] Smith (2011) 'A recipe for chaos'

Reg. No. 2012/004736/08

The definition of BCM within King III closely reflects the same definition within BS25999 (1 and 2) and ISO22301.[12]

The following are extracts from King III that relate to business continuity and organisational resilience/sustainability. Whilst some directly refer to BCM others are clearly linked by more than implication.

- **'Establishing a Business Continuity Programme addressing the company's information and recovery requirements, and ensuring the programme is still aligned with the successful execution of the business activities'**[13]

- **'Treating, reducing or mitigating the risk through improvements to the control environment such as development of contingencies and business continuity plans'**[14]

- 'The internal audit plan should take the form of an assessment of the company's strategic, financial, IT, human resources, environmental and other matters which could endanger the operation of the company'[15]

- 'IT Risk is an important aspect of the Audit Committee's responsibilities. This should include... **business continuity** and data recovery relating to IT'.[16]

- 'The Board should ensure that IT is aligned with business objectives and sustainability.'[17] Within this context the Code indicates that IT governance should concentrate on four key areas that includes 'addressing the safeguarding of IT assets, to ensure disaster recovery and continuity of operations'.

- **'Management should regularly demonstrate to the board that the company has adequate business resilience arrangements in place for disaster recovery'.**[18]

- 'Information security is the protection of information from a wide range of threats in order to ensure **business continuity,** minimise business risk, and maximise return on investments and business opportunities'[19]

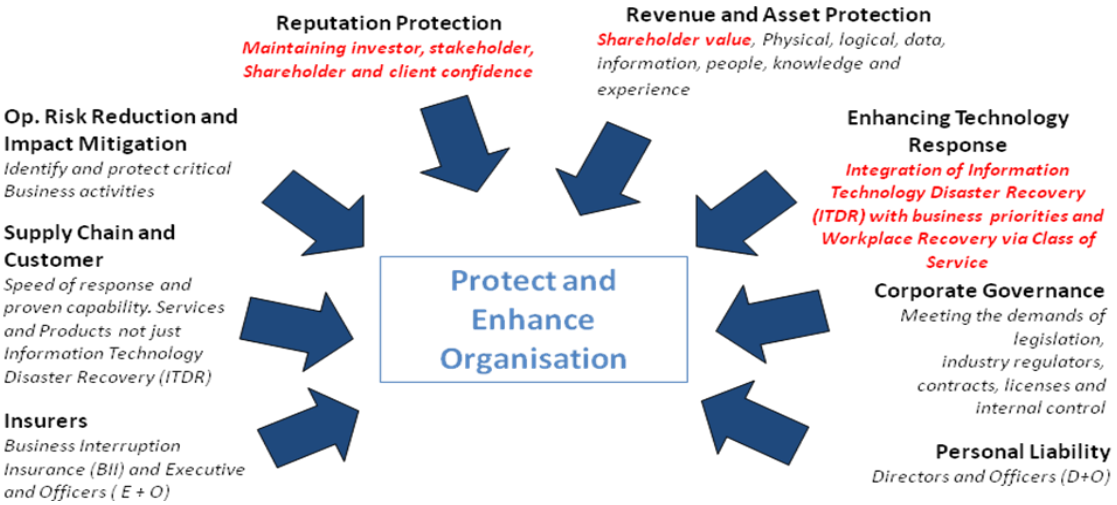
It should also be remembered that in addition to corporate governance there are also a number of other key drivers in respect of BCM (See Figure No.2).

These matters also impact on personal liabilities if the degree of corporate governance and its due diligence are not prudently exercised.[20] In this context, it is worth remembering (and reminding all senior executives) that 'managerial ignorance' is no longer an acceptable legal or moral defence if a business continuity incident or corporate crisis is handled badly or is unable to be handled due to an inadequate or non-existent BCM, incident or corporate crisis leadership and management capability.

[12] King III (2009) - Glossary of Terms
[13] King III (2009) - Principle 5.6 (37.7)
[14] King III (2009) - Principle 4.7 (42.2)
[15] King III (2009) - Principle 5.4
[16] King III (2009) - Principle 3.8
[17] King III (2009) - Principle 4.16
[18] King III (2009) - Principle 5.5 (31)
[19] King III (2009) - Glossary of Terms
[20] King III (2009)

Reg. No. 2012/004736/08

Figure 2: Corporate Governance and key drivers[21]



All managers should consider the following key questions that are likely to be asked in any subsequent inquiry:

- When did you know there was a problem?
- What did you do about it?
- If you didn't do anything, why not?
- If you didn't know there was a problem, why not?
- What would you have done if you had known such a problem could exist?

BCM Standards

In 2002 I edited and published the Business Continuity Management Good Practice Guidelines (BCM GPG). Within nine years of publishing the BCM GPG the whole issue of BCM has developed from guidelines into a recently published ISO22301:2012 BCM Requirements via BS PAS56, BS25999-1, BS25999-2:2007 BCM Specification and other national standards. Whilst BS25999-1:2006 BCM Code of Practice remains ISO22301 has updated BS25999-2 but is not that different from BS25999-2. The main changes provide greater emphasis on understanding requirements, setting objectives and measuring performance.

The key elements of BS25999-2 Specification are set out within the BCM life cycle (see Figure 3). ISO22301 does not use the BCM lifecycle but does apply the component parts. In contrast to the BCM life cycle the components of ISO22301 are best illustrated and described through the Plan-Do-Check-Act cycle model (see Figure 4). However, in time, it is expected that ISO22301 may eventually become the leading BCM framework globally. Whilst both BS 25999-2 and ISO22301 provide the specification/requirements for setting up and managing an effective BCM System (BCMS) they also both apply the Plan-Do-Check-Act implementation procedure and process[22] (see Figure 4).

[21] Dr David J Smith (2002)
[22] BS25999-2: Introduction and ISO 22301: Sections 0.2 and 0.3

Reg. No. 2012/004736/08

It is however important to distinguish some of the key definitions used within the different standards to enable further discussions within this paper. In particular the British Standard and ISO specify requirements for setting up and managing an effective **Business Continuity Management System (BCMS)**.[23]

Business continuity is defined as the 'Strategic and tactical capability of the organisation to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable pre-defined level'. It is of interest to note that neither BS25999 (parts 1 and 2) or ISO22301 make reference to operational capability within their definitions.

Figure 3: The BCM Lifecycle[24]

BCM programme is defined as 'an ongoing management and governance process supported by top management and appropriately resourced to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure continuity of products and services through training, exercising, maintenance and review'. It is of interest to note that within this definition there is no specific mention of planning as a key element of the programme. However, the mention of strategies and plans indicate key elements of the planning process and an assumption of planning.

BCM life cycle is 'a series of business continuity activities which collectively cover all aspects and phases of the BCM programme'.

BCM strategy is defines as an 'approach by an organisation that will ensure its recovery and continuity in the face of a disaster or other major incident or business disruption'.

[23] BS 25999-2: Introduction and General
[24] BS 2599-1: BCM Code of Practice

Reg. No. 2012/004736/08

A Business Continuity Management System (BCMS)

A Business Continuity Management System (BCMS) is defined as 'part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity'[25] **It is important to note that within this context an organisation's BCM programme is defined in a Business Continuity Management System (BCMS)[26]** Therefore the top management of an organisation shall develop, implement, maintain and continually improve a documented BCMS. Within this context the 'top management shall review the organisation's BCMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness... all such reviews should be documented'.[27] Within this context it is critical that there is a **BCMS Management Information System (MIS)** to not only conduct and inform the BCMS but also provide assurance and inform management reviews, performance evaluations and audits with 'verifiable' data.

The benefits of an effective BCMS (BCM Programme) are highlighted within the BS and ISO standards[28]

A BCMS is like any other management system and has the following key components[29]:

1. An organisation BCM policy;
2. Organisation roles with defined and documented BCM responsibilities;
3. A BCM management process relating to:
    a. Policy,
    b. Planning,
    c. Implementation and operation,
    d. Performance assessment,
    e. Management review, and
    f. Improvement;
4. Documentation providing auditable evidence; and
5. Any BCM processes relevant to the organisation.

The outcomes of an effective BCMS (BCM Programme) include[30]:

1. Critical activities, products and services are identified and protected via business continuity strategy, plans and arrangements ensuring their continuity and/or recovery to an acceptable level of performance and functionality;
2. An incident management and corporate crisis management structure and capability;
3. Liaison and arrangements with other organisations, supply chain, relevant regulators or government departments, civil authorities, disaster and the emergency services:
4. Relevant teams, managers and employees are trained to respond effectively to a business continuity disruption, incident or corporate crisis through appropriate exercising, restoration testing and rehearsal of BCM strategies, plans and arrangements;
5. Stakeholders, managers, employees and media receive adequate support and communications in the event of a disruption, incident or corporate crisis;
6. The organisation's supply chain is secured;
7. The organisation's reputation and brand image is protected;
8. The organisation's assets are protected;
9. The business continuity strategy, plans and arrangements are reviewed and exercised to ensure their relevance, appropriateness and plausibility;

[25] ISO22301: Section 3.5
[26] BS25999-2: Section 4
[27] ISO22301: Section 9.3 and BS 25999-2:2007- Section 6.2.1.1
[28] BS25999-1: Section 3.5
[29] ISO22301: Section 1 - General and BS25999-2: Section 4
[30] BS25999-1: Section 3.6

Reg. No. 2012/004736/08

10. The organisation remains compliant with its legal, insurance, regulatory, licence and contractual obligations

In implementing a BCMS it must be recognised that 'a number of key risks and purposes have been established in BS25999-2:2007.... each risk and purpose could form the scope for a standalone review... they act as checkpoints to ensure that an organisation's BCM System is fit for purpose and has met the needs of the BS25999-2 specification'.[31] These key risks and purposes are also reflected in ISO22301 and the BCM lifecycle (see Figure 3) as set out in BS25999-1:2006 and BS 25999-2:2007. The checkpoints are scalable and can be applied to both the public and private sectors. Critically they form the basis and represent the absolute minimum for any audit or review or maturity assessment of a BCMS and are therefore key in its implementation.

The key risks and checkpoints set out in BS 25999-2 are as follows:

1. Establishing and managing the Business Continuity Management System (BCMS) - clause 3.2;
2. Embedding BCM in the organisation's culture - clause 3.3;
3. BCMS documentation and records - clause 3.4;
4. Understanding the organisation - clause 4.1;
5. Determining BCM strategy - clause 4.2;
6. Developing and implementing a BCM response - clause 4.3;
7. Exercising, maintaining and reviewing BCM arrangements - clause 4.4;
8. Monitoring and reviewing the BCMS - clause 5;
9. Maintaining and improving the BCMS - clause 6.

Building and embedding BCM within the organisation

Ignoring BCM issues can happen for a number of reasons, ranging from corporate or personal denial through disavowal to rationalisation or too high a 'risk appetite' or it will never happen to us approach. A process of 'group think' can develop whereby an organisation genuinely starts to believe that their size, or some other feature, makes them immune from disruption, incident, crises or disaster. Some become complacent, overconfident in their ability and/or ignore warning signals[32]. These are often referred to as **'Inherent Cultural Blockers' and are a key issue within any BCMS and in particular any self review, audit or maturity assessment**.

Additionally, executives may firmly believe that insurance will cover them, without realising that insurance alone cannot indemnify against lost market share, loss of reputation or tarnished brands or supply chain failure (JIT management). Indeed Business Interruption Insurance (BII) and other types of insurance can be negated in given circumstances, especially where the insured has not taken reasonable precautions to eliminate or mitigate risk or accurately and fully provide 'material information' to the insurer. Within this context a self assessment review or internal audit or maturity assessment should be part of 'material information' disclosure and may have several consequences:

- Enable the reduction of premium and/or excess; or in contrast
- Increase of premium and/or excess

[31] John Silltow (2008) - 'Auditing Business Continuity Management Plans', pp.207 - 209.
[32] Smith (2012) 'A recipe for chaos'

Reg. No. 2012/004736/08

The latter outcome may make an organisation uninsurable because insurance becomes too expensive or not worthwhile based on the level of excess. It also raises the issue of mandatory legal requirements in respect of insurance and is a key issue covered within King III.

Research shows that crisis-prone organisations and individuals tend to exhibit **'Inherent Cultural Blockers'** tendencies seven times more often than crisis-prepared organisations. Whilst all individuals may make use of such defence mechanisms from time-to-time, the key difference is the degree, extent, and frequency with which they are used.[33] Changing such mindsets is not easy, as all organisations are different and techniques that work in one organisation will not necessarily work in another. Most executives tasked with addressing and/or implementing BCM are keen to achieve quick wins, they frequently and regrettably adopt the checklist 'tick box' audit approach which they incorrectly often refer to as best or good practice. This approach tries to copy successful BCM programmes / strategies used elsewhere but is often adopted and implemented without consideration as to suitability. A limited, costly, time consuming and disappointing level of success is usually the outcome.

Underlying the checklist 'tick box' approach is the persuasive belief that a structure and plan are all that is required. Whilst these are critical enablers, relying on a structure and plan alone tends to overlook the key issue; it is people that deal with business continuity, incidents and corporate crises.

To overcome this problematic approach a self review aims to provide a reference point for an organisation to review and assess their progress, to date, on their BCM capability. This should provide them with information to plan a way forward to ensure full compliance with the Risk Management and Internal Controls of the King III Code and guidelines on corporate governance. However, within this context it is recognised that each organisation will adopt as much as it needs based on the seven (7) key constructs of BCM (see Figure 1) to meet its own requirements and 'risk appetite'.

As indicated earlier, in contrast to BS25999 (parts 1 and 2); ISO22301 does not use the principle of embedding BCM in the organisation's culture (see BCM life cycle - Figure 3). It adopts a more managerial and pragmatic approach by advocating that 'top management shall ensure 'the integration of the business continuity management system (BCMS) requirements into the organisation's business processes'[34] Again this approach is reinforced by King III.

Avoiding the planning bureaucracy

Unfortunately, reputations and trust that have been built up over decades can be destroyed within minutes unless vigorously defended at a time when the speed and scale of events can overwhelm the normal operational and management systems. There is no doubt that a business continuity and incident/corporate crisis management capability expressed as policy, strategy, structure, teams, arrangements and plan(s) within the context of a BCMS is essential. The strategy, arrangements and plan(s) becomes a source of reference and/or enablers at the time of a business continuity disruption, incident or corporate crisis and the blueprint upon which the strategy and tactics of managing it are designed. In particular it can provide essential guidance on damage limitation in those short windows of opportunity which often occurs at the beginning of a disruption, incident or a corporate crisis.

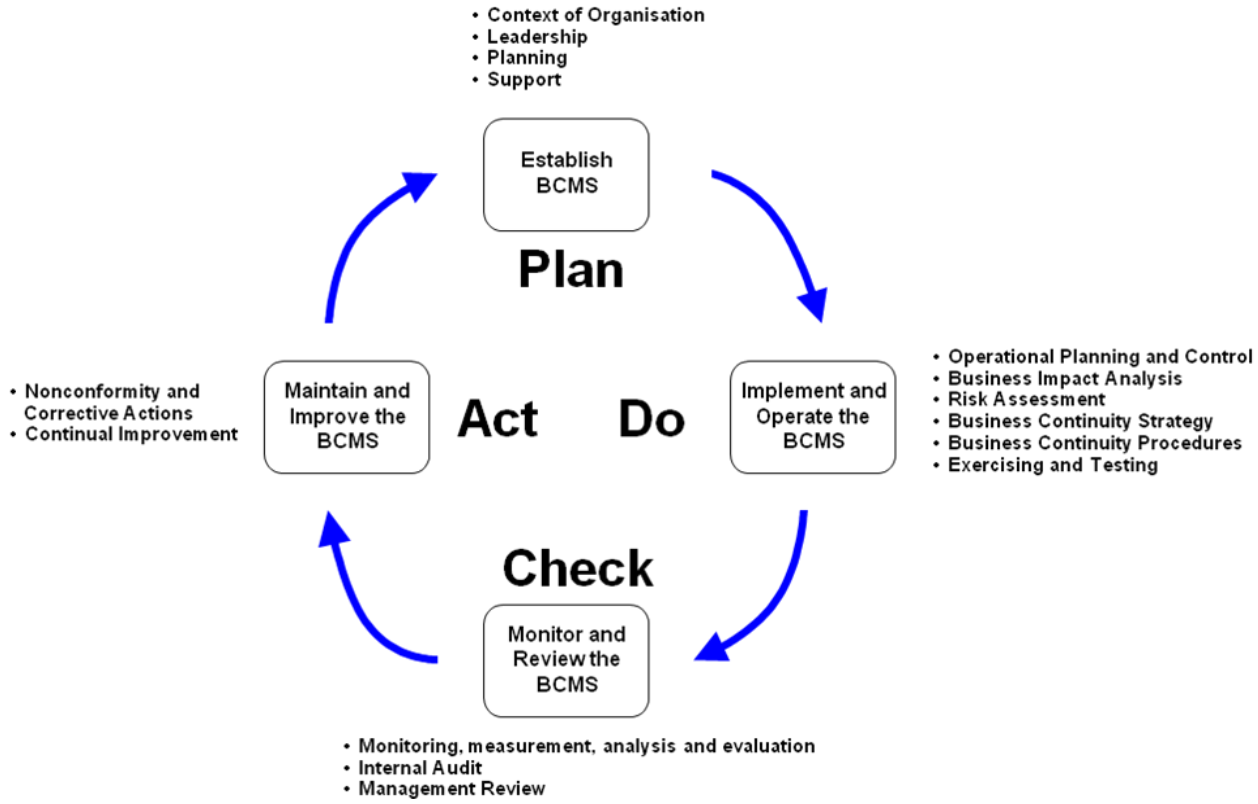
A further and critical reason for having a planning process within the BCMS is so that the individuals and teams that are required to implement the strategy, plan and arrangements can exercise, rehearse and test what they might do in different situations i.e. scenario planning[35]. The **maxim 'It's not in the plan but in the planning'** should be the clarion cry that brings knowledge and understanding to provide the business continuity capability. Scenario planning exercises are a very helpful technique for destruct-testing different

[33] Pauchant and Mitroff (1992) 'Crisis Prone Organisations'
[34] ISO22301: Section 5.2
[35] See Smith (2011) 'A recipe for chaos'.

Reg. No. 2012/004736/08

strategies and plans. Having said this, it is simply not possible to plan for every eventuality, and if an organisation tries, there is a great danger of creating plans that are simply too heavy to lift. A trade-off needs to be achieved between creating an effective, appropriate and proven capability and the alternative of relying on untrained and untried individuals and hoping they will cope.

Figure 4: PDCA cycle applied to the BCMS process[36]



The spanning of the gap between the planning and developing the competence and capability of those that carry it out can be achieved by both formal training and exercises as part of the BCM programme. The well-known maxim that '**a team is only as strong as its weakest link'** is worth remembering here. The exercising of plans, rehearsing of team members and restoration testing of arrangements, systems and facilities are the elements that provide and prove an effective and fit-for-purpose BCM capability. This approach is mindful of the Gary Player comment; **'the more I practice the luckier I get'**.

However, simulations are not always easy to devise, and because of this, many organisations do not venture beyond the development of a plan. This failure provides a fatal flaw in the BCMS (BCM programme and planning process). In particular a robust planning process and exercises are also a positive way to avoid the flawed planning bureaucracy and enable engagement in the BCMS process using the Plan, Do, Correct, Act cycle (see Figure 4) whilst applying the BCM life cycle (see Figure 3) if appropriate to an organisation. In using this proven iterative methodology to implement a BCMS (BCM Programme) it ensures that business continuity is established and continuously managed to meet the organisation's requirements.

[36] BS25999-2: Plan-Do-Check-Act (PDCA) cycle model and ISO22301: BCM - Requirements

Reg. No. 2012/004736/08

Using accepted standards

As a consequence of the caveats listed within them the BCM standards and regulatory guidelines are not designed to be a restrictive, exhaustive, or provide a definitive procedure/process to cover every eventuality within BCM. They predominantly set out to establish the generic procedure, process, principles, terminology and in some cases a checklist of activities. One provides what is described as observed practice[37] but it should be recognised that the standards/guidelines et al rarely provide outcomes in contrast to outputs or evaluation techniques[38]. Within this context it should always be remembered that the standards ...'**contains only those requirements that can be objectively audited... are generic and intended to be applicable to all organisations regardless of type, size and nature of business'.**[39]

The BS 25999-1:2006 BCM Code of Practice, BS 2599-2:2007 BCM Specification, ISO 22301:2012 and other national standards draw together the collective experience, knowledge and expertise of many leading business continuity practitioners and other authoritative professional disciplines and their organisations. Within this context the structure and format of a BCM programme should, in addition to the BCMS specification/requirements within the standards, consider the most frequently asked questions in relation to implementing a BCMS within the establishment part of the process (see Table 1) in relation to their organisation in particular.

Table 1: Most Frequent BCM Questions[40]

BCM QUESTIONS	
GUIDELINE COMPONENT	**MOST FREQUENTLY ASKED QUESTIONS**
PURPOSE	Why do we need to do it?
OUTCOMES	What will it achieve?
COMPONENTS	What does it consist of? Any pre-requisites?
METHODOLOGIES AND TECHNIQUES	What are the tools we need to do it?
PROCESS	How do we do it?
FREQUENCY AND TRIGGERS	When should it be done?
PARTICIPANTS (RACI)	Who does it? Who should be involved?
DELIVERABLES	What is the output(s)?
REVIEW AND EVALUATION CRITERIA	How do we know if we have got it right?

The BCMS Framework and Workflow

The BCM lifecycle (see Figure 3) together with the most frequently asked questions (see Table 1) have been drawn together to create a BCMS framework and workflow (see Figure 5) to guide the implementation of an effective BCM programme (BCMS) process. This process to implement the organisation's BCMS should employ the Plan-Do-Check-Act cycle (see Figure 4) as an iterative process to achieve its required outputs and outcomes throughout all stages of the BCMS (BCM programme).

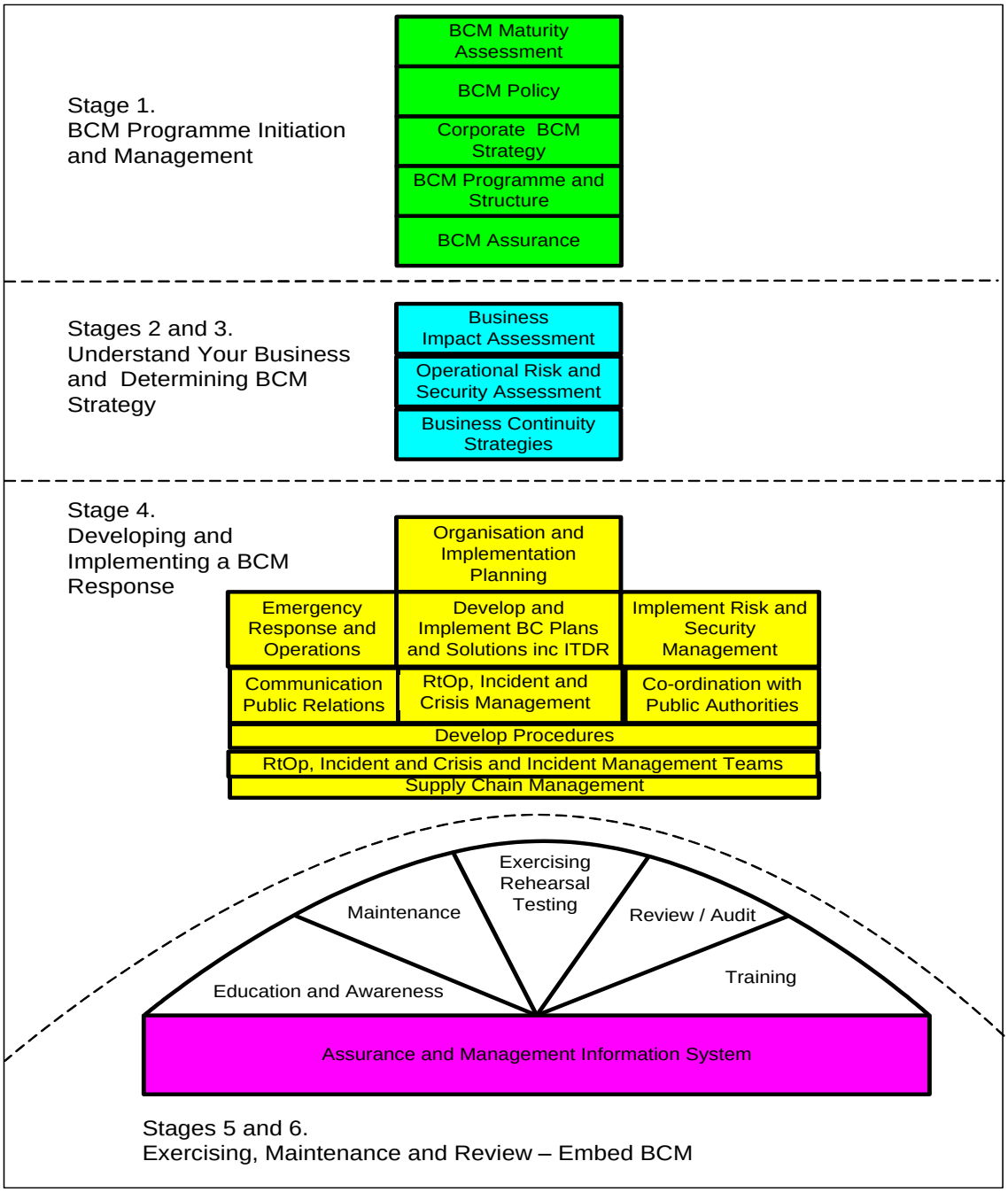
---

[37] FSA (2006) 'Business Continuity Management Practice Guide'
[38] Smith (2011) 'BCM Benchmarking, legislation, regulation, standards' and Smith (2012) 'BCM - How do you measure up'?
[39] BS 25999-2: Forward and Scope and ISO22301 - Scope
[40] Smith (2002) 'BCM - Good Practice Guidelines'

Reg. No. 2012/004736/08

It is recognised that the current standards do not imply uniformity in the structure of a BCMS but an organisation should design its own BCMS to be appropriate to its needs and that it meets its stakeholder's requirements... additionally, these need to be shaped by legal, regulatory, organisational and industry requirements, the products and services, the process employed, the size and structure of the organisation'[41]

Figure 5: BCMS Framework and workflow[42] - The Six Stages of the BCM Lifecycle



[41] BS25999-2: Scope and ISO 22301: Scope and Section 4 - Context of Organisation
[42] Dr David J Smith (2002) adapted from CCTA 1998 p.14

Reg. No. 2012/004736/08

Consequently, each organisation needs to assess how to apply the BCMS framework and workflow across its enterprise. It must ensure that its BCM competence and capability maturity meets the nature, scale, and complexity of their business, and reflects their individual culture and operating environment. Utilising the framework and workflow will develop an organisation's BCM capabilities within a structured implementation process. It can also be used within the review process to test technical, logistical, administrative and procedural BCM plans and arrangements to highlight parts of the BCM programme that are incomplete or need changing.

Incident and Corporate Crisis Management

Both BS25999 (parts 1 and 2) and ISO22301 indicated that an organisation shall establish, document, implement and develop an incident response structure which is also a key element of the BCM lifecycle.[43]

It is well recognised by professional business continuity practitioners that the ability to quickly respond and be seen to manage an incident or corporate crisis can drastically alter its outcome. The initial impact curve of an incident or corporate crisis is far steeper and immediate than that of a business continuity event and if not managed well will cause irreparable damage to an organisation albeit its business continuity recovery may be good. In particular, effective communication before; during and after an incident /corporate crisis can also drastically alter its outcome[44].

Table 2: Key elements of an Incident Response Process[45]

INCIDENT / CORPORATE CRISIS MANAGEMENT RESPONSE PROCESS
BUSINESS RISK CONTROL • Monitoring • Prevention • Planning and preparation • Crisis identification **IDENTIFICATION AND ASSESSMENT** • Crisis evaluation - Know the problem and where it exits • Threat assessment - Understand the seriousness and impact upon the organisation **INVOCATION AND ESCALATION** • Set up a team and structure to manage the incident/crisis **COMMUNICATION AND THE MEDIA** **MANAGEMENT AND RECOVERY** • Address the immediate actions • Remedial actions and recovery **STAKEHOLDER MANAGEMENT** **CLOSURE AND REVIEW** • Formal closure • Understand the problems and lessons learned • Ongoing issues, e.g. investigation and litigation • Post crisis review and report **IMPROVEMENT** • Post incident/crisis review report • Implementation of agreed review report recommendations

[43] BS25999-1: Section 8 and ISO22301: Section 8
[44] Knight and Pretty (2001)
[45] Dr David J Smith (2002)

Reg. No. 2012/004736/08

As with business continuity the key elements of a corporate crisis management process are similar to incident management and include those set out below (see Table 2). However, the list should not be seen as restrictive or exhaustive. There are many advantages to adopting a modular approach to an incident or corporate crisis management process, not least that it can be easily and quickly modified to suit local, national as well as global requirements. In many ways the format and structure of incident and corporate crisis management can trace its origins in disaster management.

In support of this view research clearly indicates there are three key factors used by stakeholders to evaluate and judge a successful outcome of an incident or corporate crisis. These three evaluation criteria can also be said of civil protection and Disaster Management.

The three critical criteria are:

1. **The organisation's recovery response; and**
2. **Communications with all stakeholder audiences: and**
3. **The perceived competence and capability of the management in dealing with the incident and/or corporate crisis[46].**

The stakeholder perceptions and communication should be seen as the critical success factors with an equal, if not more urgent priority over the organisation's recovery. Consequently, the ultimate test is to convincingly demonstrate an effective business continuity, incident and/or corporate crisis management capability to enable business as usual whilst keeping all stakeholders informed.

In his experience Bland[47] considers that 'Most companies have no crisis management plans and hope that disaster will never strike'.[48] He further argues that consumerism, legislation, environmentalism, pressure groups, and investigative media all necessitate the development of an incident/corporate crisis management plan of which a communications plan is a critical element.

Klann considers that 'there are many books written about crisis management, but few focus on crisis leadership. Managing a crisis and providing leadership in a crisis is not the same thing. Each addresses different aspects of a difficult situation. He differentiates the two by saying that crisis management relates mainly to operational issues, whilst crisis leadership principally deals with how leaders handle the human responses to a crisis including their own'[49].

A three tier response structure

'In any incident situation there should be a simple and quickly-formed structure that will enable the organisation to:

- Confirm the nature and extent of the incident;
- Take control of the situation;
- Contain the incident, and
- Communicate with stakeholders.

The same structure should trigger an appropriate business continuity response'[50]

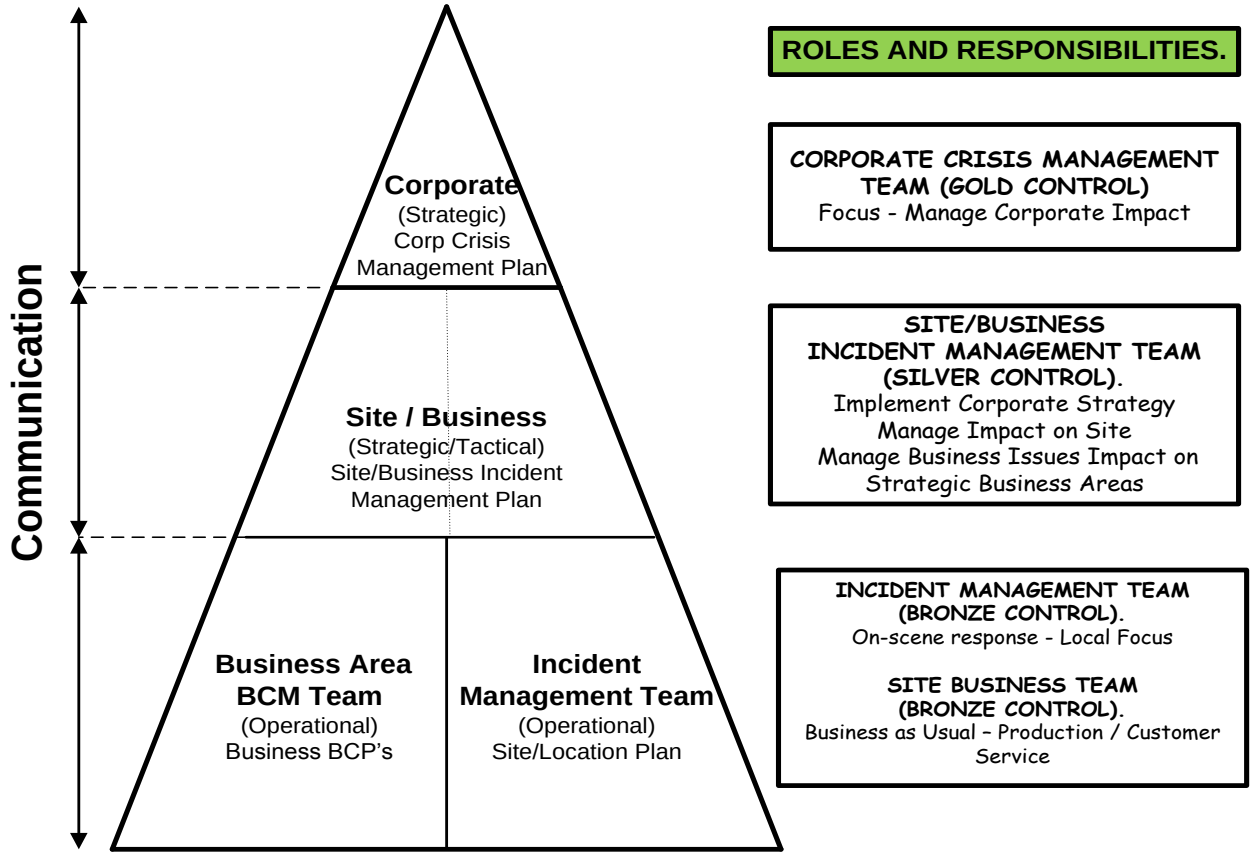
---

[46] Knight and Pretty (2001)
[47] Bland (2010) 'When it hits the fan', Centre Publishing, UK.
[48] Smith (2012) 'A recipe for chaos'
[49] Klann, (2003) 'Crisis Leadership'
[50] BS25999-1: Section 8.2

Reg. No. 2012/004736/08

This paper utilises a three tier response structure (see Figures 6 and 7) that will also be recognised by many civil disaster management, emergency services and military organisations. The key issue is that a three tier structure provides an integrated benchmarked capability. It is based on a simple concept; that if an individual can simultaneously manage all functional areas then no further organisation is required. If one or more of the areas require independent management a person is appointed to be responsible for that function. However the model can be utilised as a two tier structure whereby the corporate (strategic) level and site/business (tactical) level are combined. It is recognised there is some overlap between the various teams within the model. This is inevitable and essential to ensure that all aspects of the incident/corporate crisis are being addressed and that there is effective communication between each team and relevant stakeholders.

Figure 6: A three tier response and governance structure[51]



The proposed structure is designed to be flexible, to meet the differing needs of each incident/crisis, whilst still providing clear reporting channels, governance and accountability. At the core of the structure is the Accountable Executive, who is responsible for incident/corporate crisis management, day to day tactical decisions and reporting to the corporate crisis management team as appropriate. The Accountable Executive and incident/corporate crisis management team should have clear authority to **command and co-ordinate (control)** the incident/crisis at either a strategic and/or tactical and/or operational level.

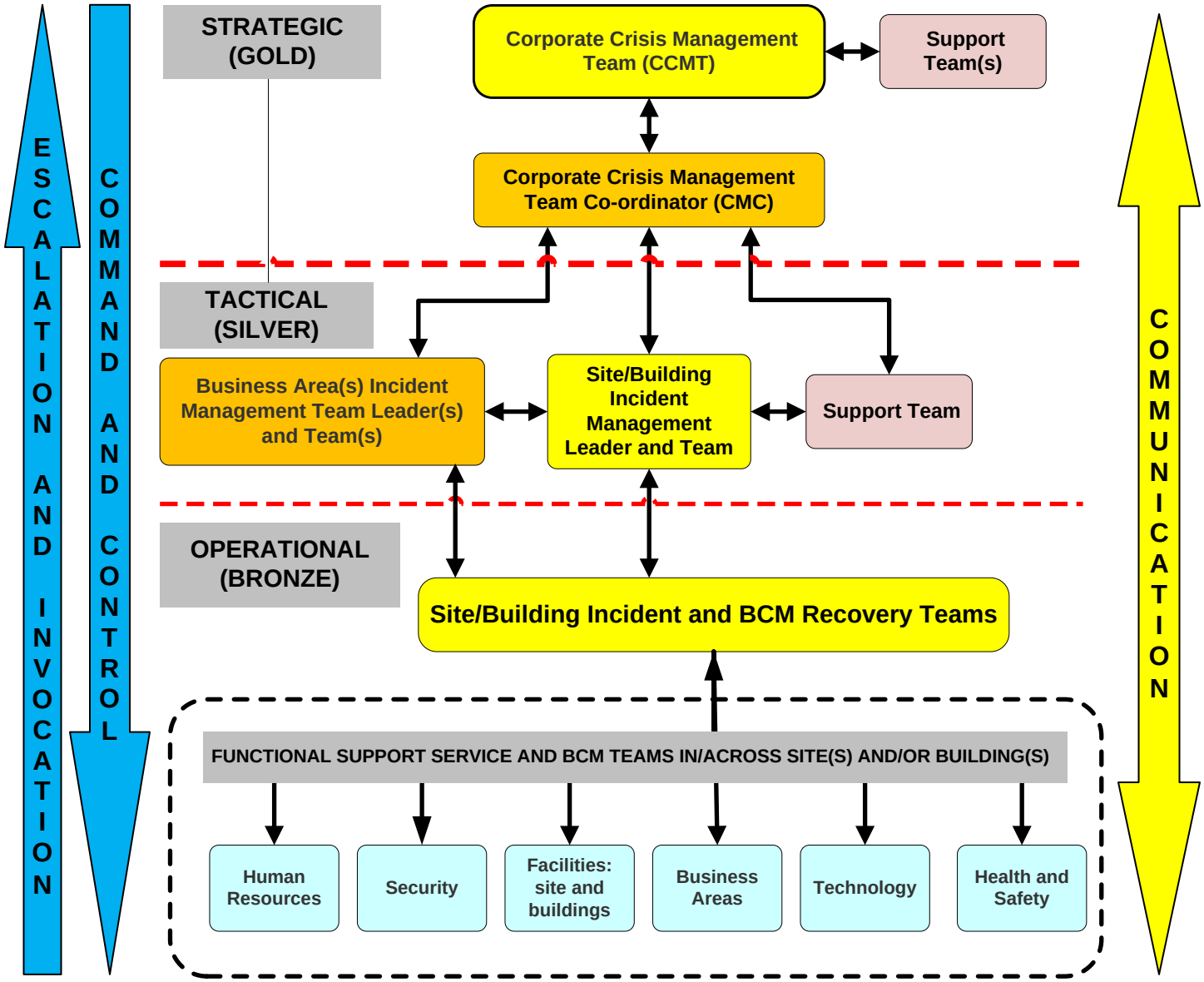
[51] Dr D.J. Smith (2002)

Reg. No. 2012/004736/08

The command and co-ordination (control) aspect of the structure is a key issue not always fully understood within the context of business-as-usual organisation management. It is in total contrast to the business-as-usual model as it is leadership based and is predominantly subjective and directive rather than objective and consultative. A key and important conclusion is that the application of conventional management techniques can ironically be quite dangerous in a crisis.

A further consideration is that despite their business management skills and experiences not all executives or managers should automatically be considered good incident and/or corporate crisis managers.[52] It should be remembered that 'there is no training in the hot seat'[53]

Figure 7: A three tier response and governance structure[54]



[52] Smith (2011) 'A recipe for chaos'
[53] Flin (1996) 'Sitting in the hot seat'
[54] Dr D.J. Smith (2002)

Reg. No. 2012/004736/08

In addition, skilled resources should be added to the core membership of each team as dictated by the nature of the disruption, incident or crisis, with representation, where appropriate, on the corporate crisis management team. In essence an organisation 'shall identify incident response personnel, who shall have the necessary seniority, authority and competence to take control of the situation and communicate with stakeholders'.[55]

- **Corporate Crisis Management Team:** provides a strategic capability and is responsible for the organisation wide strategic issues management. Its role is to minimise and manage the impact across the organisation of a corporate crisis occurring anywhere in the world. In particular this includes, image,

  reputation, long term operability, legislative and regulatory issues, communications and the media, stakeholder management and finance. This strategic level of command may be referred to as 'Gold Control' by Disaster Management professionals including emergency services e.g. police, ambulance and fire service.

- **Site and/or Business Support Services and/or Business Area Incident Management Team(s):** provides a tactical capability to implement the corporate crisis management team strategy or deal with an incident at a site and/or business area level without its escalation to the corporate crisis management team. This tactical level of command may be referred to as 'Silver Control' by Disaster Management professionals including emergency services. The primary role of this team is to minimise and manage the impact of an incident on the site or business area. In particular this includes:

  - Provide overall guidance for the response;
  - Provide all necessary resources (including expertise, equipment and finance) from within the organisation or external specialists;
  - Ensure that well rehearsed Incident and Business Continuity Plans are in place;
  - Ensure that timely and accurate information is passed to corporate crisis management team about the incident and actions that are being taken; and
  - Manage the ongoing business to ensure that the financial well-being of the organisation, its supply chain and stakeholders.

- **Site Incident Management Team** provides an 'on-site' operational response and capability to implement the site incident management teams tactical plan to minimise and manage the impact of the incident at a site level. This level of response may be referred to as 'Bronze Control'.

- **Business Area BCM Team** provides an operational response and capability to implement the business areas business continuity plan. This level of response may also be referred to as 'Bronze Control.

Categories of incident and corporate crisis

In considering business continuity, incidents and corporate crises it is important to note that they come as various types that primarily include:

- Natural disasters;
- Manmade disasters;
- Terrorism;
- IT/IS;
- Supply chain;
- Internal support services;
- Incident driven (site/location); and
- Issues (business).

Disruptions, incidents and corporate crises have historically centred upon physical threats to sites, people and processes. However, as trading, service provision, supply chain, IT/IS and communication dynamics change, so does the types of threats facing an organisation. Whilst still exposed to physical threats an organisation is ever more exposed to reputational threats and attacks on its brand and image.

[55] BS25999-2: Section 5.4.1.1

Reg. No. 2012/004736/08

An organisation (and its brand) is judged, by the media, markets, stakeholders and regulators, upon its ability to effectively manage an incident or crisis and continue to provide 'business as usual' production and/or services. The inability to fulfil these objectives, or a badly positioned or wrongly perceived media response, can result in a negative stakeholder outrage factor and a negative media profile. These in turn may lead to regulatory pressures through concerns over the effectiveness of management processes.

Corporate Crisis: May or may not be confined /specific to the organisation. It could be industry sector wide and usually has strong media and stakeholder involvement and requires corporate level management and co-ordination.

Business Area Incident: May or may not be organisation specific and may impact upon one or more business areas. It requires business area level management and co-ordination.

Site / Support Services Incident: may impact on one or a number sites and/or business areas and requires both business area business continuity and site incident management and co-ordination

Incident and corporate crisis management implementation programme

Having illustrated a generic implementation framework and process for a BCMS (see Figure 5) a further implementation framework and programme for Stage 4 of the BCMS programme is set out at Figure 8. This sub-programme incorporates many of the components within stage 4 of the programme. It provides a generic framework and management process that aims to guide an organisation through the implementation programme. This sub-programme to implement stage 4 of the organisation's BCMS should employ the Plan-Do-Check-Act cycle (see Figure 4) as an iterative process to achieve its required outputs and outcomes.

Review and Evaluating Performance

BS 25999-1:2006 indicates 'a BCM self-assessment and performance evaluation process plays a role in ensuring that an organisation has a robust, effective and fit-for-purpose BCM competence and capability ... it provides the **qualitative verification** of an organisation's ability to recover from an incident...self-assessment is regarded as good practice.. and conducted against the organisation's objectives and also take into account relevant industry standards and good practice'.[56] Whilst the issue of **qualitative (subjective) verification** is raised within BS 25999-1 it is not mentioned in either BS 25999-2:2007 or ISO 22301:2012. The latter specification and requirements address only the issue of **quantitive (objective) verification** and say that they 'provide a specification for use by internal and external parties, including certification bodies, to assess an organisation's ability to meet regulatory, customer and the organisation's own requirements... **it contains only those requirements that can be objectively audited**...'.[57]

This is a critical statement and issue that should not be under-estimated and fully illustrates that **a BCMS is a means to an end and not an end in itself.** Whilst the standards provide a procedure and process they do not, and clearly indicate they cannot provide the subjective requirement of a review/audit based on the caveat criteria of an organisation's own requirements and its risk appetite. In this case 'one size does not fit all'.

In addition it also raises the issue of the reviewer's knowledge of the organisation and industry sector in particular beside their own professional skills, experience, knowledge and skills concerning BCM to allow them to conduct a credible review and make credible judgements and recommendations.

[56] BS25999-1: Section 9.5.6
[57] BS25999-2: Forward and Scope and ISO 22301: Scope

Reg. No. 2012/004736/08

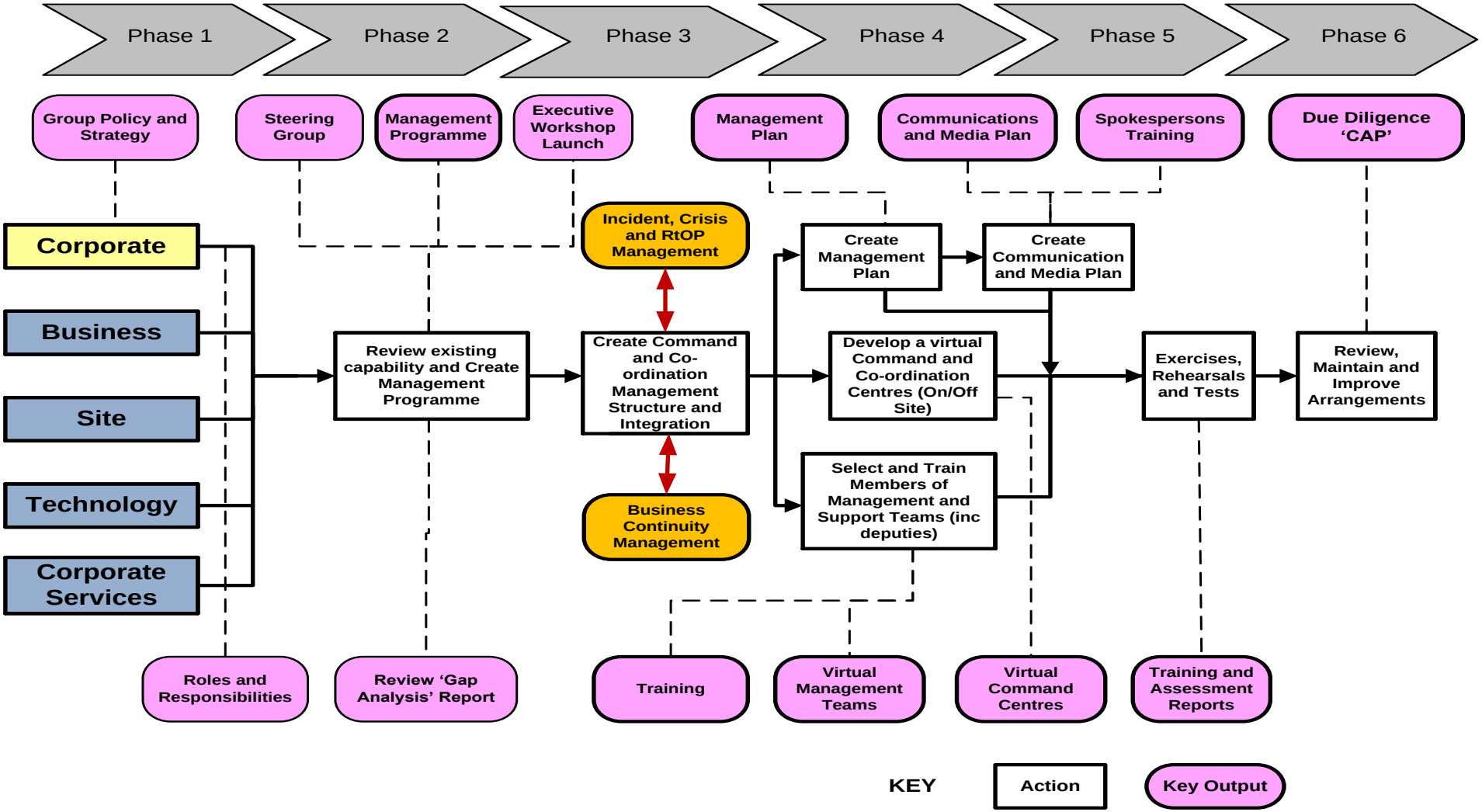
This latter issue is of particular importance and is referenced in King III in relation to the internal audit function of an organisation and risk management; '**the internal audit function should be staffed with a competent, independent team. Internal auditors should have appropriate technical and business skills'**.[58] The issue of competence and capability should apply equally to professional BCM practitioners engaged in the delivery of BCM services and internal personnel engaged in the delivery of BCM within the organisation.

Within any review there is, as indicated earlier, limited value in a 'tick box' approach which within its own methodology creates a substantial risk to the organisation i.e. tick all the right boxes and pass regardless of whether it works. It is at this stage it should be remembered that the review needs to verify the BCM competence and capability of the organisation whereby **'verification' is defined within ISO as confirmation, through the provision of evidence, that specified requirements have been fulfilled.** The level of evidence and its subjective evaluation is probably within the remit of the independent professional BCM practitioner reviewer/auditor or maturity assessor. Within this context 'verification' is a key and of paramount importance to any review, audit or maturity assessment findings and recommendations.

[58] King III (2009) Principle 5.7

Reg. No. 2012/004736/08

Figure 8: Incident and corporate crisis management implementation programme[59]



[59] Dr DJ Smith (2004)

Reg. No. 2012/004736/08

Summary

At the beginning of this paper I raised a question 'so what is the difference between what is already in place and why is it so important'? I trust that the contents of this paper and summary provide a level of information to begin to answer the question. It can only provide an overview and the reader's attention is drawn to the suggested further reading at the end of the paper.

This paper is the first in a series that feed into each other; the second is 'BCM - how do you measure up'? and discusses the issue of BCM self assessment review and will provide access to an executive/manger review questionnaire based on BS25999 (parts 1 and 2) and ISO22301. The third paper is 'BCM - a recipe for chaos' and discusses the issue of the characteristics and personalities of individuals tasked with BCM or membership of a BCM, incident or corporate crisis management team within an organisation. Subsequent papers will deal with key issues concerning BCM and it is hoped that students from the Hatfield Tuition College BCM diploma course as well as members of the IBCM will contribute freely in the form of additional papers, discussion comment and feedback for the benefit of all engaged in BCM.

The most current and historical research findings[60] clearly identify that not just regulators but customers (existing and potential), stakeholders, shareholders, auditors, financial markets and insurers require an organisation to have a demonstrable, robust, workable, effective and fit-for-purpose BCM and incident/corporate crisis management competence and capability. This is driven by the need for all organisations to clearly demonstrate the discharge of their corporate governance accountabilities and responsibilities at an executive, managerial, personnel and organisational level[61].

This provides a key, welcome, and for some challenging shift from the flawed one-size-fits-all BCM approach that considers a BCM plan and the standard tick box methodology for its completion, provides an effective BCM capability. It also highlights the fallacy of the current Planning Bureaucracy approach that believes you can plan for every eventuality. Both provide a mechanistic approach and cognitive rigidity that can be summed up by the analogy of baking a cake. The methodology is based on the belief that a recipe (plan) is a cake. The objective of baking a cake is lost in the attempt to produce a perfect recipe. Consequently a standard BCM programme and plan template approach designed to facilitate a BCMS by 'filling-in-boxes' should be wholly rejected because of the varying and individual nature of each organisation/business[62].

'Simply identifying attributes of success is like identifying attributes of people in excellent health during the age of the bubonic plague. The path of insight, of course, requires the study of both the sick and the healthy. Consequently, the study and lessons of failure are equally if not more important than identifying the best of breed or practice. The former provides valuable learning, the latter is doubtful in its validity and not may not provide the type of learning that is appropriate or required'.[63]

The steps outlined in this paper are not intended to provide an exhaustive list or to cover every eventuality, as by their nature all business continuity incidents and corporate crises are different. An organisation consists of people and top management that provide a lead. As a consequence, BCM, incident and corporate crisis management are not solely a set of tools, techniques and mechanisms to be implemented in an organisation. They should reflect a more general mood, attitude and type of action taken by executives, managers and personnel. **Individual personalities play a crucial and critical role. It is the human factor that is frequently underestimated in BCM, incident and corporate crisis management[64].** This is of particular importance because the examination of the cause of business continuity incidents and/or site incident and/or

[60] AIRMIC (2011) 'Roads to Ruin'
[61] King III (2009)
[62] BS25999 (Parts 1 and 2) and ISO22301
[63] Pascale (1990)
[64] Smith (2011) ' Recipe for chaos'

Reg. No. 2012/004736/08

corporate crises usually identifies several early or perhaps long term warning signals that were ignored or not recognised. The key to a successful business continuity incident and corporate crisis management capability is to adopt an integrated whole-of-business/organisation approach to validate each of the key building blocks of the BCM life cycle and relevant implementation and maintenance processes.

The first task is always to identify the right people. It is on this criterion that the success or failure of creating an effective and appropriate BCM capability will be determined and sustained. Having identified the right people, an organisation should engage in the BCMS (BCM programme) process, using the appropriate standards, regulations, legislation, good practice and training via the exercising of plans, rehearsal of people/teams and restoration testing of systems, processes, technology, structures and communications.

Within this context there is a need to engage in scenario planning and provide investment to deal with the three differing types of impact that affect an organisation i.e. site incident, corporate crisis and business continuity. In particular, a key element of any organisation's BCM programme is to liaise and actively work with external agencies and organisations tasked with civil protection and disaster management to enable a working relationship and understanding of others needs to enable them to carry out their tasks and the organisation to successfully achieve its BCM objectives. This element should encompass the organisation's supply chain, communications and media and a stakeholder management process.

Disaster Management practitioners look at whole communities, inclusive of commerce and industry, in terms of hazards, vulnerability and capacity. They depend on these communities to address their own vulnerabilities and capacity as far as possible, and to be effective first responders to hazard impacts within the community. A business with an effective business continuity system and crisis response team will be less vulnerable, more resilient and better able to bounce back from adversity. Disaster Management practitioners will therefore be highly supportive of any effort by their corporate citizens to become resilient organizations. **The Disaster Management Institute of Southern Africa (DMISA)** recognizes the critical importance and value of resilient organizations that can continue business, manage incidents and contain crises. DMISA therefore supports the efforts of the Institute of Business Continuity Management and its members.

It should also be remembered that in relation to civil protection and disaster management the situation may arise where an incident affects the civil authority's ability to deal with the incident in that it impacts on the civil authority's ability to provide disaster or emergency services to deal and/or manage of the incident which is their critical activity. In such cases the civil authority will need to recovery its disaster management capability (business continuity) via its own BCM arrangements; once this has been achieved to then deal with the impact of the incident in respect of civil protection.

An organisation can assist this process by appointing a BCM 'champion' at executive level whose role is to draw together, under a matrix team approach, representatives from the various organisation support functions e.g. human resources, together with key line of business heads to ensure a co-ordinated approach. This BCM Forum rather than a committee that historically seem to do little should be linked to the organisation's enterprise risk management programme and report to the organisations risk committee. The key advantage of this approach is that it builds on what already exists thereby enabling and providing a cost efficient 'virtual capability'. A further benefit is that it ensures 'buy-in' throughout the organisation. **It is a key point to note that individuals support what they have helped to create.**

In adopting this methodology and regularly exercising, rehearsing, restoration testing and reviewing the organisation maintains an appropriate, effective, up-to-date and plausible business continuity, incident and crisis management capability. So, when an business continuity incident or corporate crisis hits an organisation everyone knows what to do and a smooth invocation of the business continuity, incident and corporate crisis strategy(ies), plan(s) and arrangements takes place ensuring that the impact(s) on the organisation is minimised and its reputation and brand image are not tarnished but enhanced.

Reg. No. 2012/004736/08

However, to speak of an organisation as an entity in itself, is a powerful mechanism for forgetting, hiding or fudging the responsibilities and accountabilities of the 'individuals' managing or working within it. The term 'Top Management' when used as a practical figure of speech has a similar effect. In such circumstances the generalisations are frequently used by individuals seeking to avoid their responsibility and accountability. They hide behind the group or Board consensus which they are reluctant to shape and/or concentrate on registering objections that will provide an alibi after the event.[65] Within this process they will employ **'Inherent Cultural Blockers'** to achieve their personal or corporate agenda objectives.

The necessity of a sound and effective BCMS as specified within BS25999 (parts 1 and 2) and ISO22301 is considered by many to be paramount because the creation of an enabling infrastructure, arrangements and plans is central to any business continuity management effort. They are seen as the core drivers in the development of a reactive business continuity management capability. However, the critical capability of an organisation to successfully deal with a business continuity management incident/corporate crisis is not solely dependent upon the supporting organisational infrastructure, arrangements and/or plan. **Whilst recognising their importance the cornerstone to the success of the contrasting whole proactive BCM process is the BCM/incident/corporate crisis management team and supporting individuals at both a planning, implementation, maintenance and operational level. In particular the role of the professionally accredited business continuity practitioner.**

In considering the vexed question of 'forming an efficient and effective business continuity team' I am always brought to earth by the following quote attributed to the former world heavyweight boxer Mike Tyson; **'everyone has a plan until they're hit'**. The strength of the comment lies in the recognition that the objective of many organisations is to provide the façade of an unproven business continuity plan and infrastructure to achieve a tick-in-the-box for an audit. This attitude strongly highlights the critical difference between a business continuity plan, arrangements and infrastructure and the individuals that provide a proactive BCM competence and capability and make it work. The two latter and critical issues need to be recognised and acknowledged if successful progress is to be made in the creation, development and sustaining of an effective BCMS. **In essence it is people that deal with business continuity management incidents/crises; not plans, arrangements or an infrastructure which together with the other key constructs are the enablers of the process (see Figure 1).** A business continuity management plan, arrangements and infrastructure without an effective Business Continuity Management Team can be likened to a Michelin restaurant and menu without the chef; it is a recipe for chaos[66].

Consequently, it is recognised that the effectiveness of a BCM, incident or corporate crisis management capability is founded upon the maxim that a team is only as strong as its weakest link. Proven experience and ability are generally obtained through either dealing with actual crises and/or business continuity incidents, training and/or simulations. In essence the exercising of plans, rehearsing of team members and testing of solutions, systems, arrangements and facilities are the elements that provide competence and prove an effective capability. It is realistic scenario planning and simulations that creates added value. This again raises the quote of Gary Player; **'The more I practice the luckier I get'**. A BCM infrastructure, arrangements and plan(s), no matter how thoroughly prepared, are only as effective as an organisations ability to turn them into successful action by a team of competent and capable people. However, there is a strong body of evidence that indicates it is not possible to train anybody and guarantee their response at a time of a crisis or business continuity incident.

The management fallacy is that 'the conventional selection and training of executives/managers in no guarantee of ability to cope, if the man himself is not able in the end to take critical decisions and lead those under his command in a time of extreme stress'.[67]

[65] Henry Kissinger (1979) Vol.1, p.598
[66] Smith (2011) 'A recipe for chaos'
[67] Lord Cullen (1988) 'Piper Alpha Inquiry Report'

Reg. No. 2012/004736/08

A this point it is worth reflecting an earlier explanation and recognising that despite their business management skills and experience not all top managers, executives or managers in general should automatically be considered good BCM, incident and/or corporate crisis managers or team players.

As a result the first task is always to identify the right people.[68] This creates the question of who does it and who should be involved? (see Table 1). The acronym of RACI is often used within this process. It means individuals that are Responsible, Accountable or should be consulted or informed. This is in addition to those that will carry out the work and the BCM Team(s). A further consideration within this specific issue is the 'churn' and replacement of trained and experienced BCM leaders, deputies, team members and personnel as they are promoted, retire or move to another organisation.

The issue of professional accredited BCM practitioners and/or trained and experienced BCM practitioners is an area much neglected by organisations attempting to implement a BCMS (BCM programme). In essence would you allow an untrained or unaccredited or unqualified and/or inexperienced surgeon to operate on you or any member of your family? Why then do so many individuals and organisations use such an approach in relation to the key issue of BCM and incident/corporate crisis management that affects their organisation and personal liabilities?

Within this approach many organisations still believe BCM is just an IT issue or use the 'tick box' methodology whilst others attempt to find a convenient home based on their perceived area of organisation managerial responsibility in which it belongs i.e. a box. Whilst the former begins to address a part of the BCMS it falls far short of a genuine capability. Needless to say, the latter is a convenient dumping ground for what is perceived to be an unwanted problem or 'too difficult box'.

This is not helped by current standards that do not fully address this issue in any depth in contrast to the mechanics, procedure, process and checklists of a BCMS as a whole. In addressing Leadership, ISO 22301 does not really address competence and capability of individuals but concentrates on tasks and activities to be completed by 'top management' to implement and maintain a BSMS.[69]

Whilst some organisations provide BCM, incident and/or corporate crisis management training/education, its structure, quality, content and relevance can frequently be questioned and found wanting. The difference between training and education should be seen as two clearly distinct activities with differing outcomes. All too frequently the training or education is not accredited. As a consequence it is difficult to assess the competence and capability of individuals that style themselves as professional business continuity practitioners. To address this and other issues the **Institute of Business Continuity Management** has been created within South Africa. It applies a rigorous application membership process based on a skills and experience profile (portfolio) that includes accredited and non-accredited training/education. Within this context the **Hatfield Tuition College of the HTC group of higher education colleges** is the only training/education institution within South Africa to provide an accredited BCM training programme that leads via examination to a 'diploma' certification.

The fatal price of failure

'The explosion on Piper Alpha that led to the disaster was not devastating. We shall never know, but it probably killed only a small number of men. As the resulting fire spread, most of the Piper Alpha workforce made their way to the accommodation where they expected someone would be in charge and would lead them to safety. Apparently they were disappointed. It seems the whole system of command had broken down'.[70]

[68] Smith (2011) 'A recipe for chaos'
[69] ISO 22301: Leadership - Section 5
[70] Lord Cullen (1988) 'Piper Alpha Inquiry Report'.

Reg. No. 2012/004736/08

About the author:

Dr. David J. Smith, MBA, LL.B(Hons), FIBCM BCCE is a practicing certificated business continuity professional and currently the Chairman of the Institute of Business Continuity Management which is the professional business continuity practitioner institute of South Africa. He is an accredited Fellow of the Institute of Business Continuity Management (IBCM SA), a Business Continuity Expert of the Business Continuity Management Institute (BCMI) and former Fellow of the Business Continuity Institute (BCI).

He has a doctorate in Business Continuity Management (BCM) and Crisis Management from Liverpool University (UK) in addition to his Masters Degree in Business Administration and an Honours Bachelor of Laws degree.

David is a former executive member of the Business Continuity Institute Board of Directors and Chairman of its Education Committee. He is a globally recognised expert concerning Business Continuity, Incident and Corporate Crisis Management. He has extensive global experience within the Emergency Services, Public Sector, Financial, Insurance, Oil and Telecommunications sectors and has held UK government security clearance.

He has been involved in defining and advising on BCM, Incident and Corporate Crisis Management good practice and benchmarking initiatives within Governments, industry groups, including the UK Financial Services Authority, Asia Productivity Organisation (17 countries including Japan) and British Standards Institute. He is the Editor of the Business Continuity Management (BCM) Good Practice Guidelines 2002**;** a key contributor to the British Standards Institute (BSI) BCM Good Practice Publicly Available Specification (PAS56) 2003, BSI 25999-1 Code of Practice for BCM 2006 and accredited academic syllabus for the first Business Continuity Management Certificate/Diploma/MSc course within the UK at Coventry University.

David is also the Business Continuity lead, author and principle trainer of the accredited BCM Diploma at the Hatfield Tuition College of HTC Further Education Training Colleges in Pretoria, Johannesburg and Cape Town. Further, he is also the Business Continuity lead, author and trainer of the accredited Post Graduate Certificate / Post Graduate Diploma / MSC syllabus at the Resilience Centre, Department of Applied Science, Security and Resilience of Cranfield University (UK) at the Joint Services UK Defence Academy, Shrivenham.

He is a retired senior police officer with over 30 years experience in both the detective and uniform branches of the UK Police Service and has considerable experience in emergency and disaster management. Within this context he attended the Civil Aviation Authority Fire Service Academy, Home Office Crime Prevention College, Police Staff College and Emergency Planning College.

Amongst his various policing roles he was responsible for particular areas of specialism that included project management, crisis and business continuity management, physical security, risk management, forensic investigation, integrated management of disaster and civil emergency, audit, assurance, planning, training, exercising of plans, rehearsing of staff and restoration testing of equipment and facilities. In particular his role concerned the planning and directing of counter-terrorism and major incident exercises for multi-agency and emergency services, also the planning and implementation of live counter terrorism operations. He was also a visiting lecturer at the Police Staff College, Bramshill.

Since retiring from the Police Service he has successfully built a career as a Director of several consulting companies and an internationally recognised subject matter expert (SME) and practicing consultant, trainer and lecturer in Incident/Crisis Management, Security, Operational Risk and Business Continuity Management of which he and his companies enjoy preferred supplier status. He has managed some of the largest and most complex business continuity consulting engagements for blue chip companies throughout the world and several UK Government departments.

David is an accomplished and successful author, chairman and key-note speaker at national and international conferences and special interest groups and has received several prestigious industry achievement awards.

Reg. No. 2012/004736/08

Disclaimer:

The information contained within this paper is based on sources that are believed to be reliable but are not a guarantee of its accuracy and it should be understood to be general information only. The author or licensees make no representations or warranties, expressed or implied, concerning the information. The information is not intended to be taken as advice with respect to any individual(s), organisation(s) or collection of situation(s) and cannot be relied upon as such. All such matters should be reviewed with the readers own qualified advisors.

Copyright Notice:

Institute of Business Continuity Management NPC:

The Institute of Business Continuity Management (IBCM) is a not for profit company registered in the Republic of South Africa No. 2012/004736/08.

Its mission is to promote the art, science and good practice of Business Continuity Management within Southern Africa for the benefit of its members, their organisations and stakeholders.

Its role is to be the independent and recognised Institute for the professional development of all practitioners and associated disciplines engaged in business continuity and its management within Southern Africa by the promotion of the highest standards of professional competence, capability and commercial ethics in the provision and maintenance of BCM and BCM services.

It provides a recognised practitioner certification scheme for BCM managers, practitioners and individuals in associated risk disciplines.

The institute's professional recognition programme creates a benchmark for the assessment of the good practice. Members of the institute are drawn from all sectors of industry and commerce including finance, insurance, government, health, transport, retail and manufacturing.

Contact details:

E-mail: info.ibcm.org@gmail.com

Fax: +27 (0)86 653 2912

PO Box 31854, Kyalami, 1684, South Africa

www.ibcm-sa.org

Linkedin:
http://www.linkedin.com/groups?home=&gid=4699159&trk=anet_ug_hm

Hatfield Tuition College - HTC Group of FET Colleges:

As a leading provider of Education and Training in mainly the Further Education and Training (FET) field, Hatfield Tuition & Skills Development Centre has much to offer and their courses lead to recognised, accredited qualifications that are in high demand by commerce and industry.

In line with their vision to be the leading education and job creating institution in Africa the Hatfield T raining Group of FET colleges (HTC) has developed a pace setting educational and training model.

HTC has formed partnership with government and corporates and has integrated the SETA (Sector Education Training Authority) leadership programmes into its model to intensify the drive for practical training and workplace experience.

The HTC Group Mentors Forum under the chairmanship of Dr Kelvin Kemm, Nuclear Physicist and business strategist, is placing increased emphasis on accelerating the empowerment initiates on skill transfer, SMME development and co-operative education.

Armed with its education model, innovative ICT based series of teach and learning resources, teacher development course from the University of North West, highly qualified retired professionals as mentors, lecturers and facilitators, HTC will be a leading player in the national development plan of 2030 conference on education in 2013.

HTC will offer a Cambridge international school facility in January, 2013 and is pursuing the establishment of a business school to accommodate the increased demand for BCM and other corporate training.

Accreditations:

Department of Education: (2009/FE07/113)

****UMALUSI (FET00554 PA)***

****MICT SETA (LPA/2009/05/1526)***

**** FASSET SETA (585/01040/09)***

Contact details:

E-mail: info@htccollege.co.za

Fax: +27 (0)86537 0452

www.htccollege.co.za

IBCM Partner:

Disaster Management Institute of Southern Africa

The Disaster Management Institute of Southern Africa (DMISA) is the internationally recognised professional body for Disaster Management in Southern Africa. One of its key aims is to advance the discipline and create learning and networking opportunities in respect of Disaster Management and Disaster Risk Reduction.

DMISA is a well established organisation with a long successful history and is regularly engaged with the South African National Disaster Management Centre (NDMC). This ensures a constant flow of information from functionaries in all spheres of government, directly to the NDMC – cutting red tape and improving cooperation and understanding.

In partnership with the NDMC, DMISA plays an important role in furthering the interests of Disaster Management practitioners in South Africa and in the Southern Africa region as a whole. Originally founded in April 1985 as the Civil Defence Association of South Africa, it has contributed significantly to South Africa's legislative reform in Disaster Management.

It is a self-governing body committed to standardisation, and hosts the biggest annual Disaster Risk Reduction conference in Africa - routinely attracting more than 350 delegates.

The objectives of the Institute include recognition as the established professional body that will:

- serve as the officially recognised spokesperson of the organised disaster management and associated professions in Southern Africa;
- actively promote the need for and concept of disaster management;
- actively participate in the formulation of disaster management legislation and policy;
- establish and maintain the disaster management profession as a profession in its own right;
- provide training and continuous development for professional disaster management practitioners and managers ;
- attain closer co-operation with national and international organisations and institutions involved in, and who have similar objectives to, or could positively contribute to the field of disaster management.

Disaster Management practitioners look at whole communities, inclusive of commerce and industry, in terms of hazards, vulnerability and capacity. They depend on these communities to address their own vulnerabilities and capacity as far as possible, and to be effective first responders to hazard impacts within the community. The Disaster Management Institute of Southern Africa recognizes the critical importance and value of resilient organizations that can continue business, manage incidents and contain crises. DMISA therefore supports the efforts of the Institute of Business Continuity Management and its members.

Contact details:

E-mail: disaster@disaster.co.za

Fax: +27 (0)11 822 3563

www.disaster.co.za

Reg. No. 2012/004736/08

IBCM Sponsors:

The IBCM would like to thank the following sponsors for their support in relation to the publication of this paper:

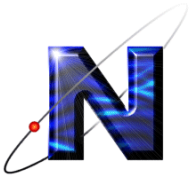
Puisano BCM Consulting

Contact details:

E-mail: puisano.bcm@gmail.com

Fax: +27 (0)86650 9319

www.puisano-bcm.co.za



Newlog - Systems Management and Engineering

Contact details:

E-mail: info@newlog.co.za **or** newlogcc@worldonline.co.za

Fax: +27 (0)118832610

www.newlog.co.za

Reg. No. 2012/004736/08

Suggested Further Reading and References

- AIRMIC (2002) 'A Risk Management Standard', AIRMIC, ALARM and IRM, London.
- AIRMIC (2011) 'A Roads to Ruin', AIRMIC, London
- Schmidt, D. (Ed) (2010) 'NFPA 1600 Standard for Disaster Emergency Management and Business Continuity Programmes' National Fire Protection Agency, USA (ISBN 978-0-87765956-3)
- Australia National Audit Office (2009) 'Business Continuity Management - Building resilience in public sector entities', ANAO, Canberra (ISBN 0-644-390182-2)
- Basel Committee on Banking Supervision (2006) 'High level principles for business continuity', Bank of International Settlements (ISBN 92-9131`-859-0)
- Bland, M. (1998) 'Communicating out of a crisis', Macmillan Press Ltd, London (ISBN 0-333-72097-0)
- British Standards Institute (2006) 'BS 25999-1 Code of practice for business continuity management', British Standards Institute, London (ISBN 978-0-580-59426
- British Standards Institute (2007) 'BS 25999-2 BCM Specification', British Standards Institute, London. (ISBN 978-0-580-59913)
- British Standards Institute (2008) 'Exercising for Excellence: Delivering a successful BCM exercise', British Standards Institute, London. (ISBN 978-0-580-509537)
- British Standards Institute (2011) ' ISO/IEC 27031 Information and communications technology (ICT) Continuity Management Code of Practice, British Standards Institute, London (ISBN 978-0-58059426-7)
- Cabinet Office Civil Contingencies Secretariat, (2005) ' Civil Contingencies Act 2004 : A short guide', HMSO, London
- Cabinet Office (2012) 'Business Continuity for Dummies', John Wiley and Sons Ltd, UK (ISBN 978-1-118-32683-1)
- Central Computer and Telecommunications Agency (1998) 'A guide to Business Continuity Management' HMSO, London (ISBN 0-11-330675X)
- Centre for the Protection of National Infrastructure (2006) 'Telecommunications Resilience - Good Practice Guide (version 3)' CPNI, London
- Estall, H. (2012) 'Business Continuity Management Systems Implementation and Certification to ISO 22301', British Informats Society Ltd, UK (ISBN 10:1780171463)
- Fawcett, H. (2010) 'Communicating in a Crisis: What really works', Siemens, UK
- Financial Services Authority (2006)'A Business Continuity Management Practice Guide' FSA, London
- Flin, R. (1996) 'Sitting in the Hot Seat', Wiley and Sons, Chichester (ISBN 978-04719579666)
- Harvard Business Essentials (2004) 'Crisis Management: Master the skills to prevent disasters', Harvard Business School Publishing Corp, USA (ISBN 1-59139-437-6)
- Institute of Risk Management South Africa '2011' Code of Practice for Enterprise Risk Management' IRMSA, Johannesburg
- International Organisation for Standardisation (2007) ISO/PAS 22399 'Guideline for incident preparedness and operational continuity management' IOS, Geneva
- International Organisation for Standardisation (2012) 'ISO 22301 Societal Security BCM Systems - Requirements' International Organisation for Standardisation, Geneva (ISBN 978-0-580-68680-1)
- IoDSA (2009) King III Report and Code of Corporate Governance' King Committee, Republic of South Africa
- Kaye, D. (2008) 'Managing Risk and Resilience in the Supply Chain', British Standards Institute, UK. (BIP 2149:2008) (ISBN 978-0-580-607264)
- Klann, G. (2003) 'Crisis Leadership', CCL Press Publication, USA (ISBN 1-932973-70-2)
- Knight, R. and Pretty, D. (2001) 'The impact of catastrophes on shareholder value', Oxford Executive Research Briefings, Templeton College, Oxford
- London Emergency Services Liaison Panel (2012) 'Major Incident Procedure Manual 8th Ed', Metropolitan Police. London
- Mitroff, I., Pearson, M., Harrington, K. (1996) 'The essential guide to managing corporate crises', Oxford University Press, UK (ISBN 0-19-509744-0)
- Myers, K. (2006) Business Continuity Strategies: Protecting against unplanned disasters', John Wiley and Sons Ltd, UK (ISBN 10:0470040386)
- Preen, J. (2012) 'Business Continuity Communications: Successful incident communications planning with ISO 22301', British Standards Institute, London (ISBN 10: 0580766152)
- Preen, J. (2012) 'Business Continuity Exercises and Tests: Delivering successful exercise programmes with ISO 22301', British Standards Institute, London (ISBN 10: 0580766144)
- Securities and Exchange Commission (2004) ' Business Continuity Plans Rule 3510 and Rule 3520', Securities and Exchange Commission, USA
- Sharp, J. (2012) 'The route map to BCM: Meeting the requirements of ISO 22301', British Standards Institute, London (ISBN 978-0-580-74341-2);
- Silltow, J. (2008) 'Auditing Business Continuity Plans', British Standards Institute, London (BIP 2151:2008) (ISBN 978-0580-626401)
- Smith D.J. (2011) 'BCM - A recipe for chaos', Institute of Business Continuity Management, RSA
- Smith D.J. (2012) 'How resilient or vulnerable is the availability of government and public sector services', Institute of Business Continuity Management, RSA
- Smith D.J. (2012) 'BCM: How do you measure up?', Institute of Business Continuity Management, RSA