INSTITUTE OF BUSINESS
CONTINUITY MANAGEMENT
Leading the Business Continuity Profession

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 accredited BCM training at UK Universities and organisations within the UK and South Africa.

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 Elements of BCM (see Figure 3) which was formerly referenced as the BCM life cycle and are aligned to ISO22301:2012 - BCMS Requirements and ISO22313:2012 - BCMS Guidance and BSI associated standards[1]. In particular the paper addresses the following issues within the context of business continuity:

- Business Continuity (BC) and Business Continuity Management (BCM);
- Corporate Governance and other key drivers;
- BCM standards;
- A BCM System (BCMS);
- Building and embedding/integrating BCM within the organisation;
- Avoiding the planning bureaucracy
- Using accepted standards;
- The BCMS framework and BCM workflow:
- Incident and Corporate Crisis Management;
- A three tier response 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 and capability is essential. As part of the overall enterprise risk management (ERM) of an organisation[2] and in the face of the challenges and

[1] See suggested further reading and references
[2] ISO 31000:2009 and Global Institute for Risk Management Standards.

© Licensed Institute of Business Continuity Management NPC 2012 . All Rights Reserved

Reg. No. 2012/004736/08

threats that inevitably arise in today's national and global business and public sector service environment complacency is wholly unacceptable.

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).[3] 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'.[4]

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'.[5]

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; its associated guidelines and ISO 22313[6]. However, in recognising the differences in the raison d'être 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'.[7] Within ISO 22313 '..the word business is used as an all embracing term for the operations and services performed by an organisation in pursuit of its objectives, goals and mission. As such it is equally applicable to large medium and small organisations operating in industrial, commercial, public and not-for-profit sectors'[8]

Business Continuity (BC) and Business Continuity Management (BCM)

Business Continuity (BC) is defined by ISO 22301 and ISO 22313 as 'the **capability of the organisation** to continue delivery of products or services at acceptable predefined levels following a disruptive incident'

Business Continuity Management (BCM) is defined in ISO 22301 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 (business continuity)*[9] response** that safeguards the interests of its key stakeholders, reputation, brand and value creating activities'.[10] Whilst the term stakeholder is used within the

[3] AIRMIC (2011) 'Roads to Ruin - A Study of Major Risk Events; their origins, impacts and implications'

[4] AIRMIC (2011) 'Roads to Ruin' and 'Blac k Swan' incidents.

[5] Mark Taylorson, 2011.

[6] ISO 22313: Clause - Business Continuity, p.vii

[7] ISO 22301: Clause 5.2 - Note 1 and ISO 22313: Clause - Introduction, p.vii

[8] ISO 22313: Clause - Business Continuity, p.vii

[9] *my insertion within brackets

[10] ISO 22301: Clause - Definitions 3.4

definition the phrase 'interested parties'[11] is used throughout the ISO standards and BCMS albeit it means the same thing. The relevance of the needs and requirements of interested parties is emphasised within both ISO standards as being a part of the key building blocks of BCM and BCMS[12] (see Figure 4).

A BCM programme is defined in ISO 22301 as 'an ongoing management and governance process supported by top management and appropriately resourced to implement and maintain business continuity management'.

BCM strategy is defined 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'.

Prioritised Activities are defined to which priority must be given following an incident in order to mititage impacts... terms in common use to describe4 activities within this group include; critical, essential, vital, urgent and key'.[13]

Process is defines as a 'set of interrelated or interactive activities which transforms inputs into outputs'.

Risk Appetite is defined as the 'amount and type of risk that an organisation is willing to pursue or retain'.

Top Management is defined as 'person or group of people who directs and controls an organisation at the highest level'.

In contrast to the statement within ISO 22313 that all definitions to be applied within ISO 22313 are to be found within ISO 22301 the following definition of **BCM** is described within ISO 22313 is '**Business Continuity Management (BCM)** is **the process of achieving business continuity** and is about preparing an organisation to deal with disruptive incidents that might otherwise prevent it from achieving its objectives... **placing BCM within the framework and disciplines of a management system creates a Business Continuity Management System (BCMS)** that enables BCM to be controlled, evaluated and continually improved'[14].

THIS IS A CRITICAL STATEMENT THAT BEGINS TO CLARIFY THE DIFFERING ROLES AND FUNTIONS OF BUSINESS CONTINUITY (BC), BUSINESS CONTINUITY MANAGEMENT (BCM) AND BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS). Whilst it does not include a reference to a BCM programme it is assumed that a BCM programme is contained within a BCMS?

Consequently, a clear understanding of the terms; BC, BCM, BCMS, and BCM programme and other key definitions is not only essential to understanding but critical to providing resilience within an organisation subject to its risk appetite.

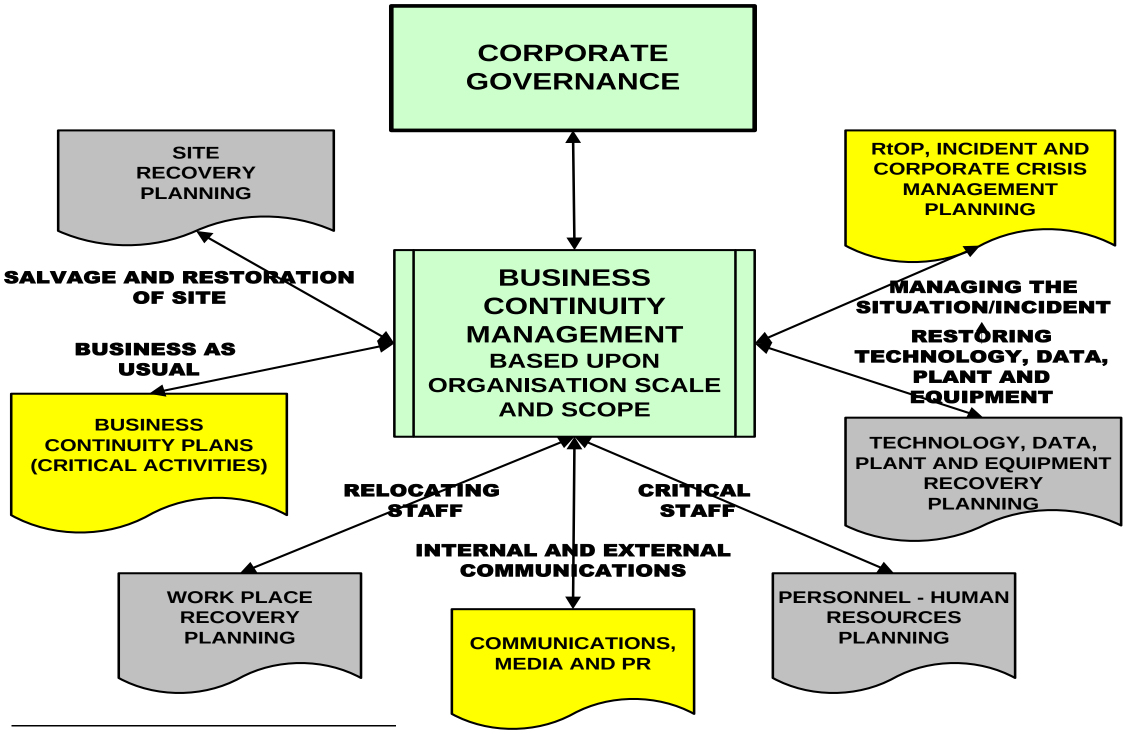
The term 'Business Continuity Management' is used rather than 'business continuity planning'. This approach is deliberate because 'planning' implies there is a start and end to the process and can lead to unwanted planning bureaucracy. However, business continuity planning is still a critical and key component of the BCM process. 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 aligned with or complete against a standard, appropriate (fit for purpose), practical, realistic, up-to-date, effective and a plausible (proven) capability.

[11] ISO 22301: Clause - Definitions 3.21
[12] ISO 22301: Clause - Scope and ISO 22313: Clause - Scope
[13] ISO 22301: Clause 3.42 - Source ISO 22300)
[14] ISO 22313: Clause - Business Continuity, p.vii

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.[15] 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[16]. Within this context there is the ever growing differentiator within the procurement process where organisations are asked to provide demonstrable 'verifiable' proof of their BCM capability and resilience. The failure to respond or be able to demonstrate/verify what is required will provide an 'exit' within the process creating a **'lost opportunity'** rather than providing a strong evidential based **'competitive advantage'**[17].

Whilst there are now accepted management standards, regulations, good practice guidelines and other criteria against which an organisation can implement and measure BCM/BCMS and its key components it should always be remembered that as a risk management discipline[18] not all organisations will want to have their BCMS certificated against a whole standard but rather 'align' to a standard[19]. They will properly use the standard to enable them to achieve sufficient organisation resilience via BCM, incident and corporate crisis management capability to meet their needs and the requirements of their interested parties/stakeholders. 'These needs are shaped by legal, regulatory, organisational and industry requirements, the products and services, the processes employed, the environment in which it operates, the size and structure of the organisation'[20] but its risk appetite in particular.. This approach is frequently described as good practice and is favoured by many organisations based on good risk management and cost benefit alone.

Figure 1: Governance and BCM Key Constructs[21]


CORPORATE GOVERNANCE
SITE RECOVERY PLANNING
RtOP, INCIDENT AND CORPORATE CRISIS MANAGEMENT PLANNING
SALVAGE AND RESTORATION OF SITE
BUSINESS CONTINUITY MANAGEMENT BASED UPON ORGANISATION SCALE AND SCOPE
MANAGING THE SITUATION/INCIDENT
BUSINESS AS USUAL
RESTORING TECHNOLOGY, DATA, PLANT AND EQUIPMENT
BUSINESS CONTINUITY PLANS (CRITICAL ACTIVITIES)
TECHNOLOGY, DATA, PLANT AND EQUIPMENT RECOVERY PLANNING
RELOCATING STAFF
CRITICAL STAFF
INTERNAL AND EXTERNAL COMMUNICATIONS
WORK PLACE RECOVERY PLANNING
COMMUNICATIONS, MEDIA AND PR
PERSONNEL - HUMAN RESOURCES PLANNING

[15] ISO 22301: Clause - 4.3.2 Scope of BCMS - and ISO 22313: Clause - 4.3.2 Scope of BCMS
[16] ISO 22301: Clause - Scope and ISO 22313: Clause - Scope and 4.2.2
[17] ISO 22313: Clause - Business Continuity, p.viii
[18] ISO 31000:2009
[19] BSI: City Security Magazine, July 2012, Issue 44.
[20] ISO 22313: Clause - Scope
[21] Dr David J Smith (2002)

© Licensed Institute of Business Continuity Management NPC 2012 . All Rights Reserved

Within this context ISO 22313 provides generic BCM guidance based on good international practice. However, the intention of ISO 22313 is **NOT** to provide general guidance on all aspects of business continuity[22]. Additionally, it indicates it 'cannot be used to assess an organisation's ability to meet its own business continuity, nor any customer, legal or regulatory need'[23]. In contrast the ability for an organisation to assess itself can be achieved by applying the ISO 22301 standard as it 'provides 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'[24].

In achieving its objectives a BCMS 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[25]. 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.[26] 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 disruptive 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 upon the World Trade Centre[27].

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 their 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.[28]

[22] ISO 22313: Clause - Introduction
[23] ISO 22313: Clause - Scope
[24] ISO 22301: Clause - Scope and ISO 22313: Clause - Scope
[25] ISO 31000:2009
[26] See suggested further reading
[27] See also IRM (UK) (2011) 'Roads to Ruin'
[28] Smith (2011) 'A recipe for chaos'

ISO 22313 indicates the **outcomes** indicative of an effective BCM may include the following although ISO 22301 does not indicate any outcomes throughout:[29]

1. An incident management capability is enabled and provides and effective response;
2. The organisation's understanding of itself and its relationships with other organisations, relevant regulators or government departments, local authorities and the emergency services is properly developed, documented and understood;
3. Regular exercising ensures that staff are trained to respond effectively to an incident or disruption;
4. Requirements of interested parties are understood and able to be delivered;
5. Staff receive adequate support and communications in the event of disruption;
6. The organisation's reputation is protected;
7. The organisation remains compliant with its legal and regulatory obligations; and
8. Financial controls are maintained throughout an incident.

Corporate Governance and other key drivers

BCM has always been a key element of an enterprise risk management (ERM) programme and consequently corporate governance[30]. 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.

The definition of BCM within King III closely reflects the same definition within ISO 22301 and ISO 22313.[31]

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.

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).

- **'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'**[32]

- **'Treating, reducing or mitigating the risk through improvements to the control environment such as development of contingencies and business continuity plans'**[33]

- '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'[34]

- 'IT Risk is an important aspect of the Audit Committee's responsibilities. This should include... **business continuity** and data recovery relating to IT'.[35]

[29] ISO 22313: Clause 8.1.5 - Outcomes
[30] ISO 31000:2009
[31] King III (2009) - Glossary of Terms
[32] King III (2009) - Principle 5.6 (37.7)
[33] King III (2009) - Principle 4.7 (42.2)
[34] King III (2009) - Principle 5.4
[35] King III (2009) - Principle 3.8

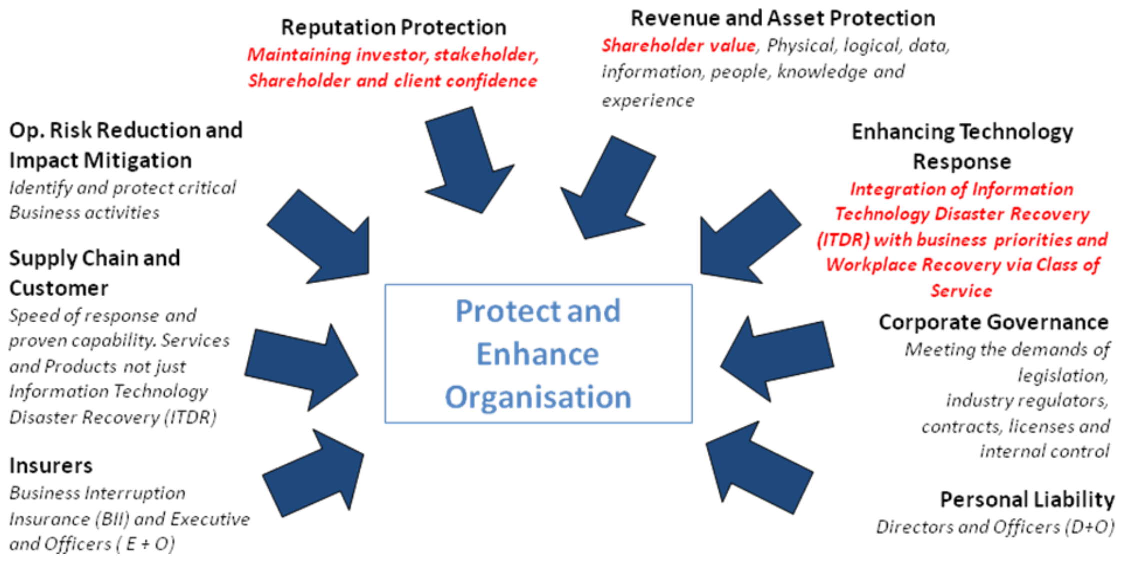
© Licensed Institute of Business Continuity Management NPC 2012 . All Rights Reserved

- 'The Board should ensure that IT is aligned with business objectives and sustainability.'[36] 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'.**[37]

- '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'[38]

Figure 2: Corporate Governance and other key drivers[39]


Reputation Protection
Maintaining investor, stakeholder, Shareholder and client confidence
Revenue and Asset Protection
Shareholder value, Physical, logical, data, information, people, knowledge and experience
Op. Risk Reduction and Impact Mitigation
Identify and protect critical Business activities
Enhancing Technology Response
Integration of Information Technology Disaster Recovery (ITDR) with business priorities and Workplace Recovery via Class of Service
Supply Chain and Customer
Speed of response and proven capability. Services and Products not just Information Technology Disaster Recovery (ITDR)
Protect and Enhance Organisation
Corporate Governance
Meeting the demands of legislation, industry regulators, contracts, licenses and internal control
Insurers
Business Interruption Insurance (BII) and Executive and Officers (E + O)
Personal Liability
Directors and Officers (D+O)

These matters also impact on personal liabilities if the degree of corporate governance and its due diligence are not prudently exercised.[40] 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.

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?

[36] King III (2009) - Principle 4.16
[37] King III (2009) - Principle 5.5 (31)
[38] King III (2009) - Glossary of Terms
[39] Dr David J Smith (2002)
[40] King III (2009)

BCM Standards

In 2002 I edited and published the Business Continuity Management Good Practice Guidelines (BCM GPG). Within ten years of publishing the BCM GPG the whole issue of BCM has developed from guidelines into a recently published ISO 22301:2012 - Requirements and ISO 22313: BCMS Guidance via BS PAS56, BS 25999-1:2006 BCM Code of Practice, BS 25999-2:2007 BCM Specification and other national standards. The international commitment and interest for ISO 22301 and ISO 22313 standards is reflected in the 50 participating countries that have supported their publication.

As a consequence of the caveats listed within them the ISO standards and regulatory guidelines are not designed to be a restrictive, exhaustive, or provide a definitive procedure/process to cover every eventuality within BCM.[41] They predominantly set out to establish the generic procedure, process, principles, and terminology and in some cases a bullet point checklist of process activities.

Both ISO 22301:2012 and ISO 20313:2012 incorporate and 'blend the requirements from several national standards including those from the USA, Japan, Singapore, Canada, Australia, New Zealand and UK[42].

In essence the ISO 22301 standard contains little difference from BS 25999-2:2007 BCM Specification; 'the BCM requirements in BS 25999-2 are mirrored in ISO 22301'[43]. The main changes provide greater emphasis on understanding requirements, setting objectives and measuring performance. However, as with all requirement standards ISO 22301 is concise and contains many 'shall' statements although the meaning of 'shall' is not defined. Given its literal meaning it probably has the same meaning as 'must' and therefore considered a mandatory requirement.

Whilst ISO 22313 provides more information than that in BS 25999-1, it does not add any additional concepts (or requirements) that are not already in ISO 22301[44]. However, the intention of ISO 22313 is **NOT** to provide general guidance on all aspects of BCM[45]. In particular, ISO 22313 'includes the same headings as ISO 22301 but **DOES NOT REPEAT** the requirements for business continuity management systems and its related terms and definitions'.[46]

Whilst ISO 22313 indicates it 'DOES NOT REPEAT the requirements for BCMS and its related terms and definitions'[47] as specified within ISO 22301 it <u>DOES</u> repeat a considerable amount of the requirements albeit some may use the exact wording or rephrase the requirement(s). This is exampled in the section BCMS Scope and Section 9 Performance Evaluation and management review within each ISO standard. A further issue is the differing definition of BCM within ISO 22313 in contrast to ISO 22301 albeit the definition in ISO 22313 provides more clarity of the functions of BC, BCM and BCMS.

A further key issue is that ISO 22313 provides guidance, where appropriate, on the requirements specified in ISO 22301 but it also provides recommendations of 'should' and permissions of 'may' in relation to them that also clarifies the intent of the 'shall'.[48]

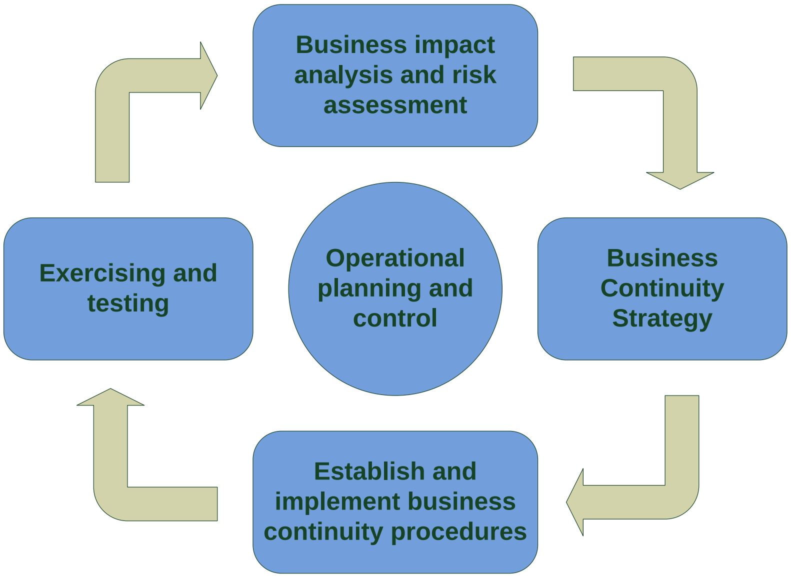
[41] ISO 22313: Clause - Introduction
[42] BSI: City Security Magazine, July 2012, Issue 44.
[43] BSI: City Security Magazine, July 2012, Issue 44.
[44] BSI: City Security Magazine, July 2012, Issue 44.
[45] ISO 22313: Clause - Introduction
[46] ISO 22313: Clause - General and BSI: City Security Magazine, July 2012, Issue 44.
[47] ISO 22313: Clause - General and BSI: City Security Magazine, July 2012, Issue 44.
[48] ISO 22313: Clause - General and BSI: City Security Magazine, July 2012, Issue 44.

This comment within ISO 22313 and the BSI does not help as the intent (meaning) of a word should be clearly set out in the 'normative reference' clause or terms and definitions within a standard as it is critical to the application of the standard and certification criteria. As indicated earlier this is not done within ISO 22301 in contrast to ISO 22313 where the standard 'provides guidance, where appropriate, on the requirements specified within ISO 22301 and provides recommendations ('should') and permissions ('may') in relation to them'.[49]

THIS POTENTIALLY CREATES CONFUSION AS THE 'SHALL' REQUIREMENT OF ISO 22301 REQUIREMENTS ARE NOW SHOWN AS BEING EITHER A 'SHOULD' RECOMMENDATION OR 'MAY' PERMISSION WITHIN ISO 22313. This is exampled within sections 4.2.2 (scope of BCMS) and 5.2 (Management Commitment) amongst many others.

In contrast to the BCM life cycle, ISO 22313 applies the component parts/elements of the BCM life cycle within a new model.. The new model is best illustrated and described through the 'Elements of BCM'[50] (see Figure 3) and Plan-Do-Check-Act cycle model (see Figure 4).[51]

Figure 3: The Elements of BCM[52]


Business impact analysis and risk assessment
Business Continuity Strategy
Establish and implement business continuity procedures
Exercising and testing
Operational planning and control

A Business Continuity Management System (BCMS)

As indicated earlier it is important to fully understand the key definitions and descriptions used within the ISO standards to enable further discussions within this paper. In particular the ISO requirements for setting up and managing an effective **Business Continuity Management System (BCMS) (see Figure 4).**[53]

[49] ISO 22313: Clause - General
[50] ISO 22313: Clause - 8.1.1 and Figure 5
[51] ISO 22301: Clause 0.2 and 0.3
[52] ISO 22313: Clause 8.1.1 - Elements of BCM
[53] ISO 22301: Clauses 0.2 and 0.3 and ISO 22313: Clause - Introduction/General

© Licensed Institute of Business Continuity Management NPC 2012 . All Rights Reserved

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'[54] **It is important to note that within this context an organisation's BCM is defined in a Business Continuity Management System (BCMS)[55]** 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'.[56] 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.

A BCMS is like any other management system and has the following key components[57]:

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 business continuity management (BCM) processes relevant to the organisation.**

The BCMS emphasises the importance of[58]:

1. Understanding the organisation's needs and the necessity for establishing business continuity policy and objectives;
2. Implementing and operating controls ad measures for managing an organisation's overall capability to manage disruptive incidents;
3. Monitoring and reviewing the performance and effectiveness of BCMS; and
4. Continual improvement based on objective measurement.

THERE IS A NEED HERE TO AGAIN HIGHLIGHT THAT THE BCMS IS A MANAGEMENT PROCESS AND A MEANS TO AN END AND NOT AN END IN ITSELF.

Whilst neither ISO indicates the **outcomes** indicative of an effective BCMS; BS 25999-1 indicates they include[59]:

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;

[54] ISO 22301: Clause 3.5 and ISO 22313: Clause - Scope

[55] BS 25999-2: Section 4

[56] ISO 22301: Clause 9.3 and ISO 22313: Clause - General

[57] ISO 22301: Clause 1 - General and ISO 22313: Clause - Introduction/General

[58] ISO 22301: Clause 0.1 General and ISO 22313: Clause - General

[59] BS 25999-1: Clause 3.6

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

Building and embedding/integrating 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[60]. 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 insurance consequences that may (a) enable the reduction of premium and/or excess; or in contrast (b) Increase of premium and/or excess.

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 (corporate governance).

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.[61] 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 by other organisation but is often adopted and implemented

[60] Smith (2012) 'A recipe for chaos'

[61] Pauchant and Mitroff (1992) 'Crisis Prone Organisations'

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 management review aims to provide a reference point for an organisation to review and assess their progress, to date, on their BCMS 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 key constructs of BCM (see Figure 1) to meet its own requirements, those of its interested and parties and its 'risk appetite'.

Whilst ISO 22301 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'; ISO 22313 still addresses the issue of embedding BCM within the organisational culture.[62] Again this approach is reinforced by King III.

Avoiding the planning bureaucracy

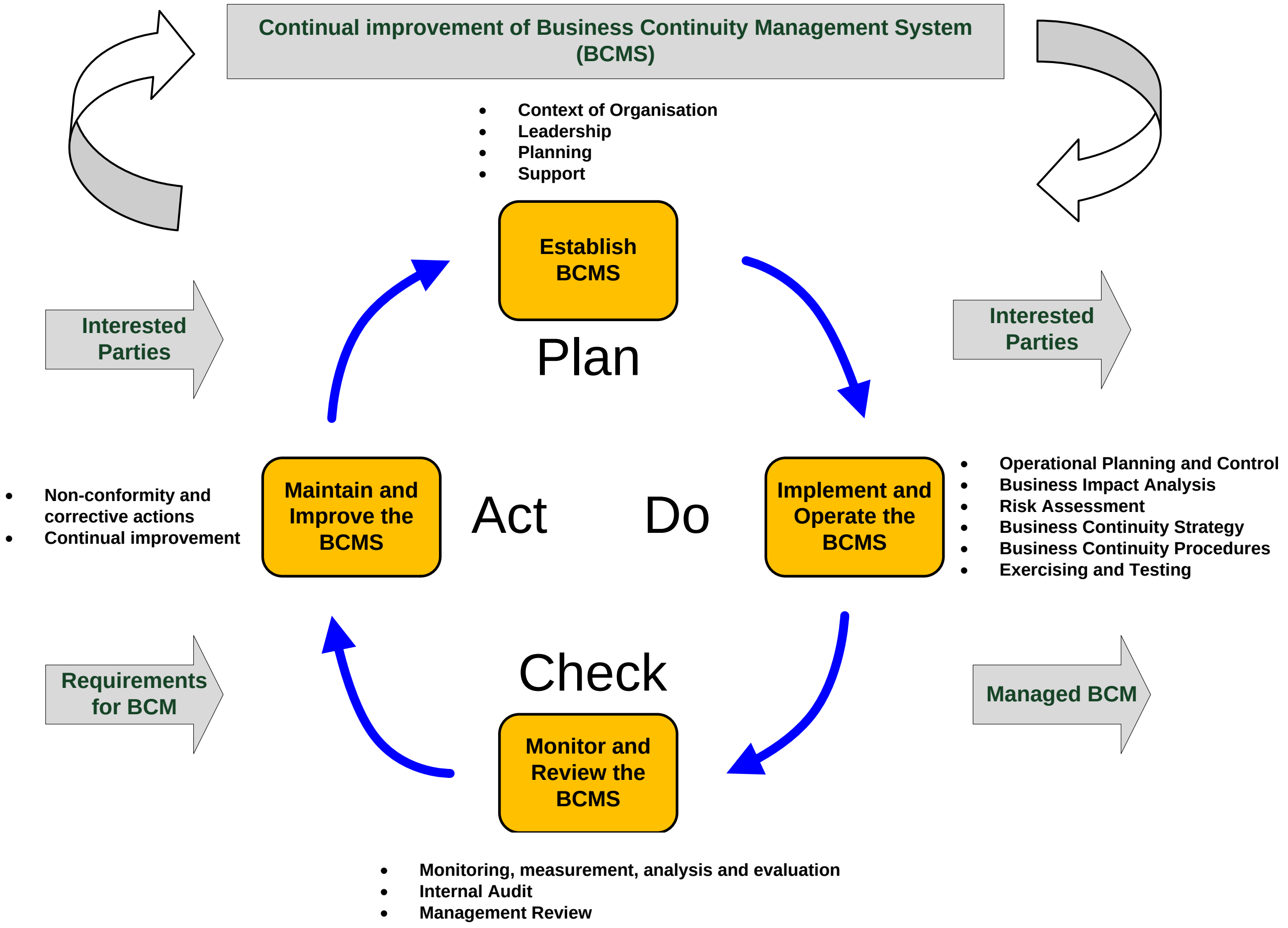
Unfortunately, reputations and trust that have been built up over decades can be destroyed within minutes unless vigorously defended at a time when the speed and scale of events can overwhelm an organisation's normal operational and management systems. There is no doubt that a proven business continuity 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 interested parties, 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[63]. The **maxim 'It's not in the plan but in the planning'** should be the clarion cry that brings knowledge and understanding and thereby competence to enable and provide the business continuity capability. Scenario planning exercises are a very helpful technique for destruct-testing different 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. Both ISO standards 'apply the 'Plan-Do-Check-Act' (PDCA) cycle to planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving the effectiveness of an organisation's BCMS'.[64]

Figure 4 illustrates how the BCMS takes interested parties' requirements as inputs for business continuity management (BCM) and, through the required BCM processes, produces business continuity outcomes (i.e. managed business continuity) that meet those requirements[65].

[62] ISO 22301: Section 5.2 and ISO 22313: Section 7.3 Awareness and 8.1.2 Managing the BCM environment
[63] See Smith (2011) 'A recipe for chaos'.
[64] ISO 22301: Clause - Introduction p.vi and ISO 22313: Clause - Introduction, p.v
[65] ISO 22313: Clause - Plan-Do-Check-Act cycle, p.vi

Figure 4: PDCA cycle applied to the BCMS/BCMS process[66]


Continual improvement of Business Continuity Management System (BCMS)
Context of Organisation
Leadership
Planning
Support
Establish BCMS
Plan
Interested Parties
Interested Parties
Non-conformity and corrective actions
Continual improvement
Maintain and Improve the BCMS
Act
Do
Implement and Operate the BCMS
Operational Planning and Control
Business Impact Analysis
Risk Assessment
Business Continuity Strategy
Business Continuity Procedures
Exercising and Testing
Requirements for BCM
Check
Managed BCM
Monitor and Review the BCMS
Monitoring, measurement, analysis and evaluation
Internal Audit
Management Review

The **Plan (Establish - Clauses 4/5/6/7)** part of the PDCA cycle 'sets out what the organisation has to do in order to make sure that the BCMS meets its requirement; sets out the role of management; describes the actions (planning) required to establish strategic objectives and guiding principles for the BCMS as a whole and identifies the key elements that need to be in place to support the BCMS' whilst the **Do (Implement and Operate - Clause 8)** identifies and sets-out the requirements of BCM that are needed to achieve business continuity and determines how to address them and develops the procedures to manage a disruptive incident'. The **Check (Monitor and Review - Clause 9)** deals with the performance review and 'it summarises requirements necessary to measure business continuity performance and BCMS compliance with ISO 22301[67]' whilst the **Act (Maintain and Improve - Clause 10)** element 'covers the corrective action needed to address nonconformity identified through performance evaluation'.[68]

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

[66] ISO 22301: Clause 0.2 and ISO 22313: Clause - Introduction/The Plan-Do-Check-Act Model
[67] ISO 22301: Clause - 0.3 p.vii and ISO 22313: Clause - Components of PDCA p.vi
[68] ISO 22313: Table 2

the comment of Gary Player the international golf player who when asked for the reasons for his success said **'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 development 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 Elements of BCM (see Figure 3) (former BCM life cycle). In using this proven iterative methodology to implement BCM via a BCMS ensures that business continuity is established and continuously managed to meet the organisation's requirements.

Using accepted standards

As a consequence of the caveats listed within them the ISO standards and regulatory guidelines are not designed to be a restrictive, exhaustive, or provide a definitive procedure/process to cover every eventuality within BCM. As indicated earlier the intention of ISO 22313 is **NOT** to provide general guidance on all aspects of BCM[69].

They predominantly set out to establish the generic procedure, process, principles, terminology and in some cases a checklist of process activities. One provides what is described as observed practice[70] but it should be recognised that the standards/guidelines et al rarely provide outcomes in contrast to outputs or evaluation techniques[71]. Within this context it should always be remembered that ISO 22301 ...'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'.[72]

A further consideration is that both ISO standards indicate that BCMS emphasises the importance of 'continued improvement based on objective measurement ... via monitoring and reviewing the performance and effectiveness of the BCMS'.[73] However ISO 22301 does indicate that performance of the BCMS should be subject to performance metrics and within this context the organisation **shall** determine the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results'[74] **ISO 22301 defines performance as measureable results with a note 'Performance can relate either to quantitative or qualitative findings'.[75]** This appears to be at odds with the issue of objective (only) measurement described as being important within BCMS. In accepting review findings of a qualitative nature it recognises and opens the door to subjective measurement/findings in respect of a BCMS as a whole. As indicated, this is a matter for the organisation itself.

This is reinforced within ISO 22313 which indicates 'a set of performance indicators should (recommendation*)[76] be developed to measure both the management system and its outcomes. Measurements may be either quantitative or qualitative... performance indicators may be management, operational or economic indicators'.[77]

It is assumed that the 'management system' means the BCMS itself. Should this be interpreted as ISO 22301 setting out a given series of 'shall' objective criteria in respect of the BCMS whereas the

[69] ISO 22313: Clause - Introduction

[70] FSA (2006) 'Business Continuity Management Practice Guide'

[71] Smith (2011) 'BCM Benchmarking, legislation, regulation, standards' and Smith (2012) 'BCM - How do you measure up'?

[72] ISO 22301: Clause - Scope

[73] ISO 22301: Clause 0.1 General and ISO 22313: Clause - General

[74] ISO 22301: Clause 9.1.1(d) - Performance Evaluation

[75] ISO 22301: Clause 3.35 (Note)

[76] * My insert

[77] ISO 22313: Clause 9.1.1 Performance Evaluation

organisation should set the objective performance indicators in respect of the BCMS? This interpretation, if correct, provides a significant and substantial statement in respect of both ISO standards.

Table 1: Most Frequent BCM Questions[78]

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?

Both ISO and other national standards/regulations 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 BCM implementation programme should, in addition to the BCMS specification/requirements/process within the standards, consider the most frequently asked questions in relation to implementing BCM within the establishment part of the process (see Table 1) in relation to their organisation in particular.

The BCMS Framework and BCM Workflow

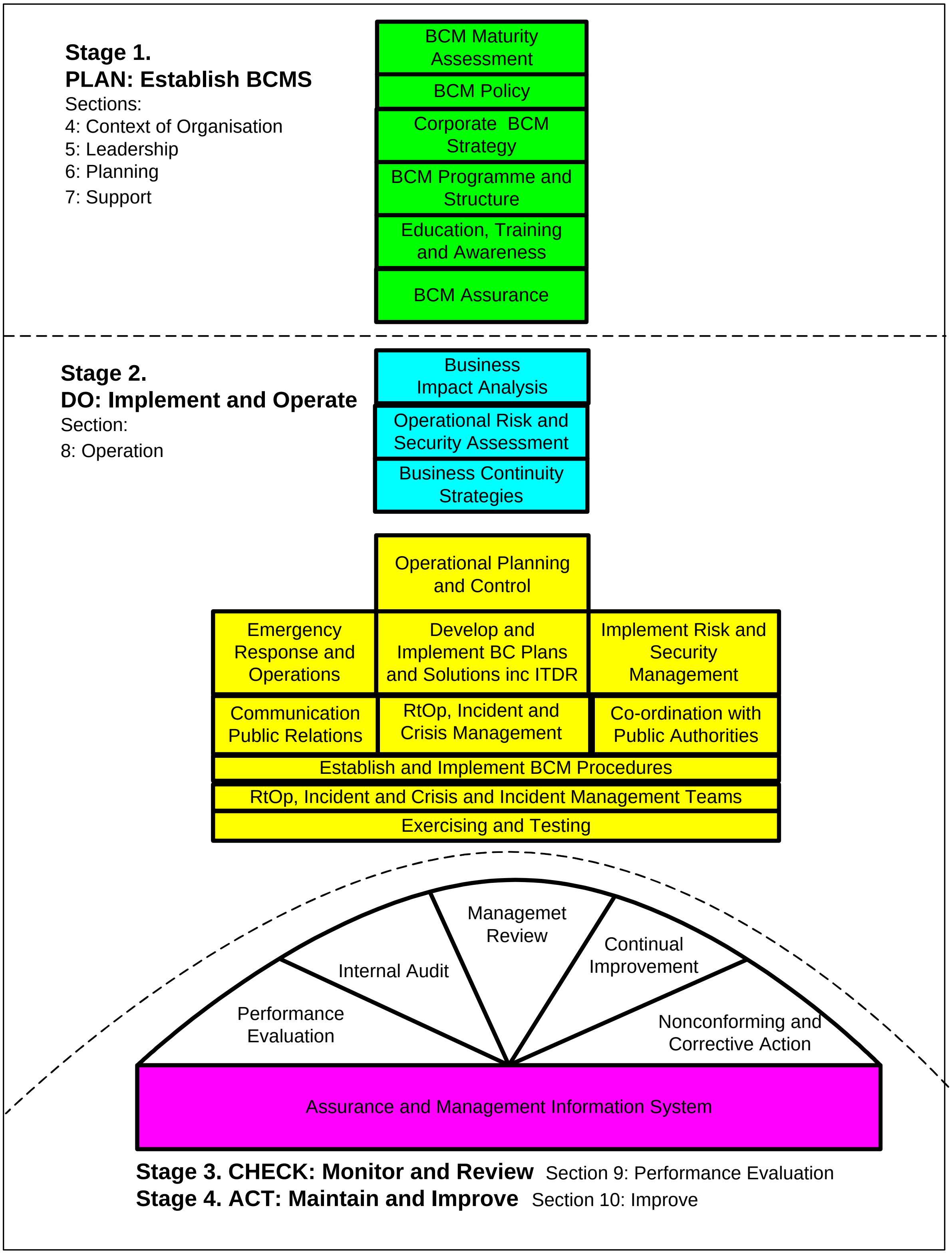
The Elements of BCM (see Figure 3) together with the most frequently asked questions (see Table 1) and BCMS criteria have been drawn together to create a BCMS framework and BCM workflow (see Figure 5) to guide the implementation of an effective BCM process and capability. This framework and workflow to implement the organisation's BCMS employs 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.

In developing the framework and workflow 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'[79] 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 BCMS that are incomplete or need changing or improved.

[78] Smith (2002) 'BCM - Good Practice Guidelines'
[79] ISO 22301: Clause - Scope and Clause 4 - Context of Organisation

© Licensed Institute of Business Continuity Management NPC 2012 . All Rights Reserved

Figure 5: PDCA/BCMS Framework and workflow[80]


Stage 1.
PLAN: Establish BCMS
Sections:
4: Context of Organisation
5: Leadership
6: Planning
7: Support
BCM Maturity Assessment
BCM Policy
Corporate BCM Strategy
BCM Programme and Structure
Education, Training and Awareness
BCM Assurance
Stage 2.
DO: Implement and Operate
Section:
8: Operation
Business Impact Analysis
Operational Risk and Security Assessment
Business Continuity Strategies
Operational Planning and Control
Emergency Response and Operations
Develop and Implement BC Plans and Solutions inc ITDR
Implement Risk and Security Management
Communication Public Relations
RtOp, Incident and Crisis Management
Co-ordination with Public Authorities
Establish and Implement BCM Procedures
RtOp, Incident and Crisis and Incident Management Teams
Exercising and Testing
Performance Evaluation
Internal Audit
Managemet Review
Continual Improvement
Nonconforming and Corrective Action
Assurance and Management Information System
Stage 3. CHECK: Monitor and Review Section 9: Performance Evaluation
Stage 4. ACT: Maintain and Improve Section 10: Improve

[80] Dr David J Smith (2002) adapted from CCTA 1998 p.14

© Licensed Institute of Business Continuity Management NPC 2012 . All Rights Reserved

Incident[81] and Corporate Crisis Management

Both ISO standards indicated that an organisation shall establish, document, implement and develop an incident response structure[82] 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[83].

Table 2: Key elements of an Incident Response Process[84]

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

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.

[81] ISO 22301: Clause 3.19 (Source ISO 22300)

[82] ISO 22301: Clause 8 - Incident Response and ISO 22313: Clauses 8.1.5 Outcomes; 8.4.2 Structure and 8.4.3.2 Communications

[83] Knight and Pretty (2001)

[84] Dr David J Smith (2002)

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: [85]

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

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/interested parties informed.

In his experience Bland considers that 'Most companies have no crisis management plans and hope that disaster will never strike'. He further argues that consumerism, legislation, environmentalism, pressure groups, and investigative media all necessitate the development of an incident/corporate crisis management response of which a communications plan is a critical element. [86]

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'[87].

A three tier response structure

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

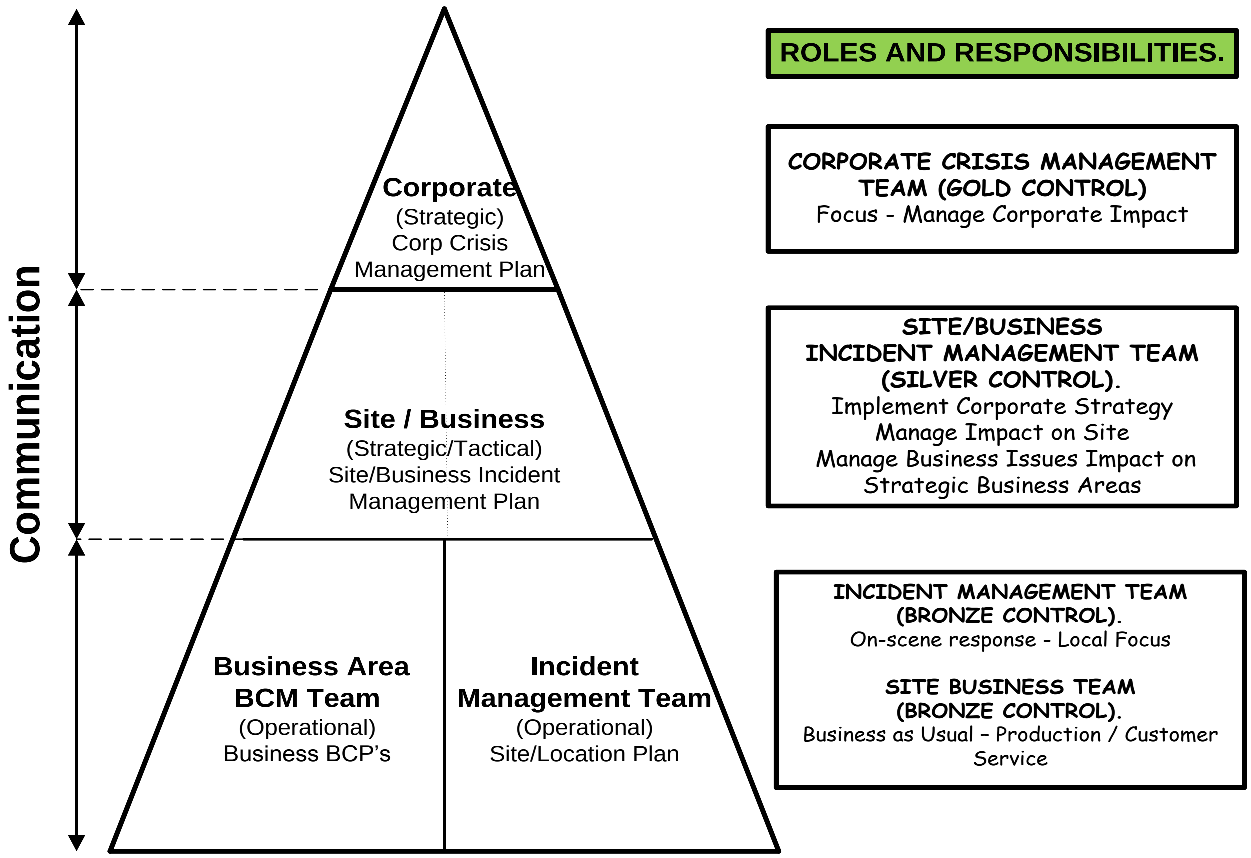
- Confirm the nature and extent of the incident;
- Take control of the situation;
- Contain and manage the incident, and
- Communicate with stakeholders/interested parties.

The same structure should trigger an appropriate business continuity response where required'[88]

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.

[85] Knight and Pretty (2001)
[86] Bland (2010) 'When it hits the fan', Centre Publishing, UK.
[87] Klann, (2003) 'Crisis Leadership'
[88] ISO 22313: Clause 8.4.2 and ISO22301: Clause 8

Figure 6: A three tier response and governance structure[89]



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.

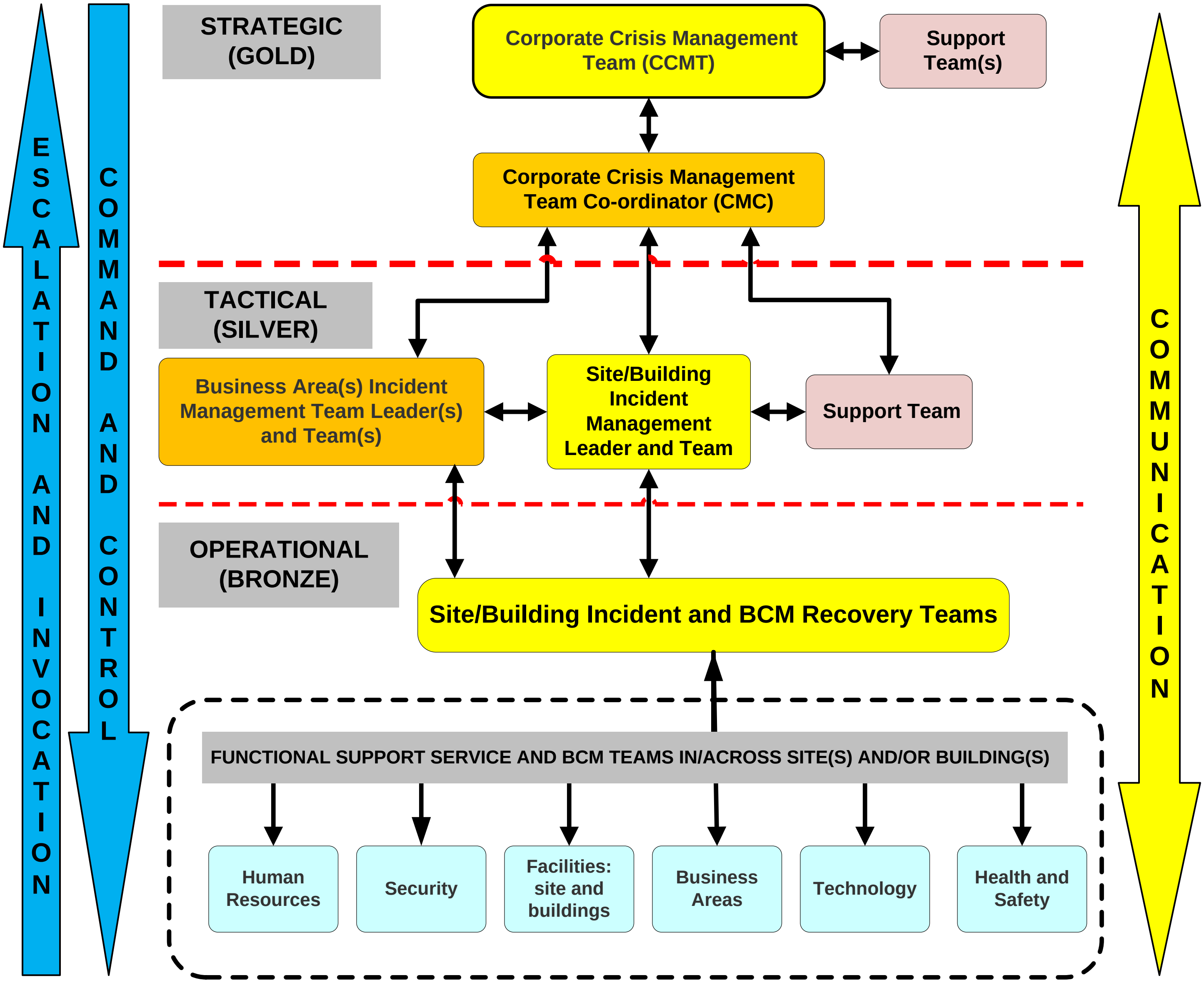
The command and co-ordination (control) aspect of the structure is a key issue not always fully understood within the context of business-as-usual organisation management. It is in total contrast to the business-as-usual model as it is leadership based and is predominantly subjective and directive rather 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. Consequently, 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.[90] It should be remembered that 'there is no training in the hot seat'[91]

[89] Dr D.J. Smith (2002)
[90] Smith (2011) 'A recipe for chaos'
[91] Flin (1996) 'Sitting in the hot seat'

© Licensed Institute of Business Continuity Management NPC 2012 . All Rights Reserved

Figure 7: A three tier response and governance structure[92]


ESCALATION AND INVOCATION
COMMAND AND CONTROL
STRATEGIC (GOLD)
Corporate Crisis Management Team (CCMT)
Support Team(s)
Corporate Crisis Management Team Co-ordinator (CMC)
TACTICAL (SILVER)
Business Area(s) Incident Management Team Leader(s) and Team(s)
Site/Building Incident Management Leader and Team
Support Team
OPERATIONAL (BRONZE)
Site/Building Incident and BCM Recovery Teams
FUNCTIONAL SUPPORT SERVICE AND BCM TEAMS IN/ACROSS SITE(S) AND/OR BUILDING(S)
Human Resources
Security
Facilities: site and buildings
Business Areas
Technology
Health and Safety
COMMUNICATION

In addition, skilled resources e.g. technology (ICT) and facilities management, 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 incident/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'.[93]

- **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

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

[93] ISO 22301: Clause 8.4.2 and ISO 22313: Clause 8

© Licensed Institute of Business Continuity Management NPC 2012 . All Rights Reserved

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 specific threats and disruptive incidents:

- 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, technology, data 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.

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 the incident/corporate crisis element of Stage 2 of the BCMS programme is set out at Figure 8. It provides a generic framework and management process that aims to guide an organisation through the implementation process. This sub-programme 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

In addition to internal audits 'top management shall review the organization's BCMS, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness that is appropriate to the level of risk (risk appetite) faced by the organization.[94]

The self-assessment and performance evaluation process plays a key role in ensuring that an organisation has a robust, effective and fit-for-purpose BCMS competence and capability. Performance 'evaluations may take the form of internal or external audits, or self-assessments... **a set of performance indicators should be developed to measure both the management system and its outcomes .... in addition they can provide the qualitative (subjective) verification of an organisation's ability by 'setting performance metrics including qualitative and quantitative measurements that are appropriate to the needs of the organisation... performance indicators may be management, operational or economic indicators'**[95]

As indicated earlier it is assumed that the 'management system' means the BCMS itself. Should this be interpreted as ISO 22301 setting out a given series of 'shall' objective criteria in respect of the BCMS whereas the organisation should set the objective performance indicators in respect of the BCMS?[96]

In contrast the ISO 22301 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**...'.[97]

However, whilst objectivity is one facet measurement the other key element is subjective assessment and interpretation which provides context to objectivity e.g. a plan and its contents may be objectively audited but are they proven as fit-for-purpose? The former almost suggests a 'tick box' methodology.

Within this context Performance benchmarking and Process benchmarking are distinct types of benchmarking activity that are often confused:

- **Performance benchmarking focuses on quantitative data by obtaining the numbers, the performance measures, indicators or metrics; by contrast**

- **Process benchmarking focuses on qualitative and process data by obtaining the 'how', 'what', 'where', 'when' and 'why' which explain the performance gap which has been identified**

However… one is rarely of any value without the other

[94] ISO 22301 and ISO 22313: Clauses 9.1.2, 9.2 and 9.3

[95] ISO 22313: Clause 9.1.1 Performance evaluation, audit and management review

[96] Also see section on Review and Evaluating Performance within this paper

[97] ISO 22301: Clause - Scope

These are critical statements and issues 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 or performance 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 they 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.

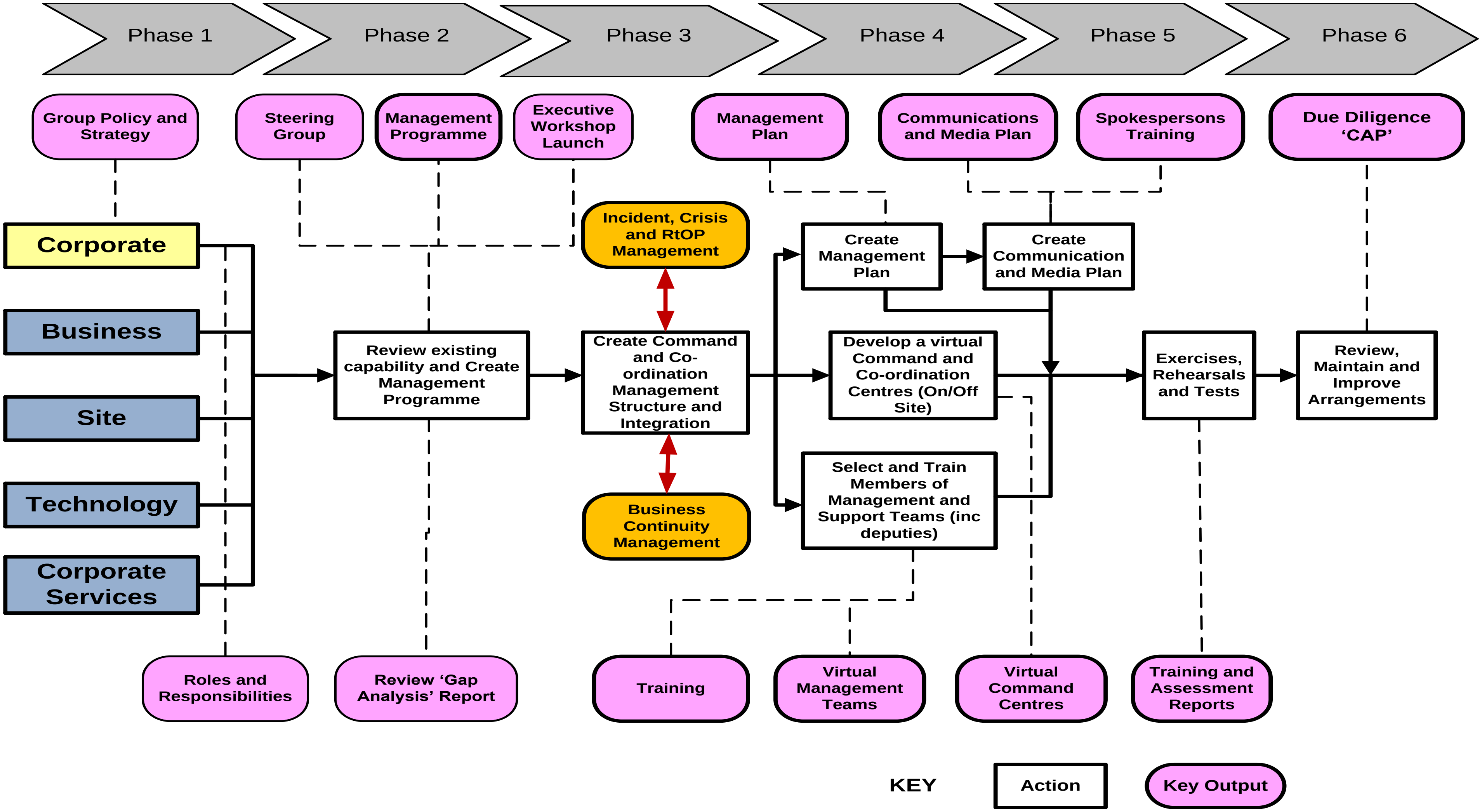
This latter issue is of particular importance and is referenced in King III in relation to the internal audit function of an organisation and risk management; '**the internal audit function should be staffed with a competent, independent team. Internal auditors should have appropriate technical and business skills'**.[98] 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 BCMS within the organisation. Internal 'audits of the BCMS may be performed by personnel from within the organization or by external persons selected by the organization, working on its behalf. In either case, the persons conducting the audit should be competent and in a position to do so impartially and objectively. In smaller organizations, auditor independence may be demonstrated by an auditor being free from responsibility for the activity being audited'**.**[99] This statement from ISO does not address the key issue of objective performance assessment or capability audits/management reviews which usually addresses the question 'Does it work'?

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/BCMS 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 both objective and subjective 'verification' is a key and of paramount importance to any review, audit or maturity assessment findings and recommendations especially within the procurement process or ongoing contract management.

[98] King III (2009) Principle 5.7

[99] ISO 22313: Clause 9.1.2

Figure 8: Incident and corporate crisis management implementation programme[100]


Phase 1
Phase 2
Phase 3
Phase 4
Phase 5
Phase 6
Group Policy and Strategy
Steering Group
Management Programme
Executive Workshop Launch
Management Plan
Communications and Media Plan
Spokespersons Training
Due Diligence 'CAP'
Corporate
Business
Site
Technology
Corporate Services
Review existing capability and Create Management Programme
Incident, Crisis and RtOP Management
Create Command and Co-ordination Management Structure and Integration
Business Continuity Management
Create Management Plan
Create Communication and Media Plan
Develop a virtual Command and Co-ordination Centres (On/Off Site)
Select and Train Members of Management and Support Teams (inc deputies)
Exercises, Rehearsals and Tests
Review, Maintain and Improve Arrangements
Roles and Responsibilities
Review 'Gap Analysis' Report
Training
Virtual Management Teams
Virtual Command Centres
Training and Assessment Reports
KEY
Action
Key Output

[100] Dr DJ Smith (2004)

© Licensed Institute of Business Continuity Management NPC 2012 . All Rights Reserved

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 discusses the issue of a management BCM self assessment review and provides access to an executive/manger review questionnaire based upon ISO 22301 and ISO 22313. 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 other key issues concerning BCM.

The most current and historical research findings[101] clearly identify that not just regulators but other interested parties that include customers (existing and potential), stakeholders, interested parties, 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[102].

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 BCM programme and plan template approach designed to facilitate a BCMS by 'filling-in-boxes', albeit using ISO criteria, should be wholly rejected because of the varying and individual nature of each organisation/business.

'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 good practice. The former provides valuable learning; the latter is doubtful in its validity and not may not provide the type of learning or capability that is appropriate or required'.[103]

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 requirements, 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[104].** This is of particular importance because the examination of the cause of business continuity incidents and/or site incident and/or corporate crises usually identifies several early or perhaps long term warning signals that were ignored or not recognised or might is some circumstances be classified as Black Swan events. 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 BCMS and

[101] AIRMIC (2011) 'Roads to Ruin'

[102] King III (2009)

[103] Pascale (1990)

[104] Smith (2011) ' Recipe for chaos'

Elements of BCM. **However, it is timely to again remind the reader that the BCMS is a means to an end and not an end in itself.**

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/BCMS capability will be determined and sustained. Having identified the right people, an organisation should engage in the BCMS 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 to create both competence and capability in individuals, teams and functions.

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 BCMS 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, media and a stakeholder/interested parties management processes.

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 a proven and effective business continuity capability 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 organisations. **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 and other relevant stakeholders to ensure a co-ordinated approach. This BCM steering committee[105] should be linked to the organisation's enterprise risk management (ERM) programme[106] 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.

[105] ISO 22313: Clause 5.4

[106] ISO 31000:2009

© Licensed Institute of Business Continuity Management NPC 2012. All Rights Reserved

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.[107] Within this process they will employ **'Inherent Cultural Blockers'** to achieve their personal or corporate agenda objectives.

As a result the necessity of a sound and effective BCMS as specified within ISO 22301 and ISO 22313 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 business continuity, incident and corporate crisis 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 both the competence and capability of BCM/incident/corporate crisis management teams 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 a usually 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[108].

Consequently, it is recognised that the effectiveness of a BCMS, 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 an effective capability. It is realistic scenario planning and simulations that creates added value. This again raises the quote of Gary Player the successful world famous golfer who said of his success; **'The more I practice the luckier I get'**. In essence 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'.[109]

[107] Henry Kissinger (1979) Vol.1, p.598

[108] Smith (2011) 'A recipe for chaos'

[109] Lord Cullen (1988) 'Piper Alpha Inquiry Report'

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.[110] 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, in essence interested parties. 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. leave or move to another part of 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/maintain a BCMS. 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'.

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 of the quality or content necessary. 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.

Whilst the issue of objective and subjective verifiable evidence including performance (assurance) indicators in respect of BCMS and its audit or management review or maturity assessment have been highlighted within this paper they are discussed further in the paper - IBCM Organisational Resilience and BCM. In recognising there is a link between organisational resilience and being competitive - How do you measure up? **In particular it discusses the issue of a management BCM self assessment review and provides access to an executive/manger review questionnaire based upon ISO 22301 and ISO 22313.**

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'.[111]

[110] Smith (2011) 'A recipe for chaos'

[111] Lord Cullen (1988) 'Piper Alpha Inquiry Report'.

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 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.

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:

© The copyright to this document with all rights reserved is owned by Dr. David J. Smith and Stamford Consulting Limited and is licensed to the IBCM, Puisano BCM Consulting cc, Newlog - Systems Management and Engineering cc and DMISA with all rights reserved.

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@bcm-sa.org

Fax: +27 (0)86 653 2912

PO Box 786213, Sandton 2146, South Africa

ibcm INSTITUTE OF BUSINESS CONTINUITY MANAGEMENT
Leading the Business Continuity Profession

www.ibcm-sa.org

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

IBCM Partners:

DMISA **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

Global Institute for Risk Management Standards:

Launched in May 2012, G31000, the Global Institute for Risk Management Standards, is a non-for-profit international association dedicated to raising awareness about the ISO 31000 risk management standard. It supports events, training and certification of individuals through a network of contacts, worldwide.

G31000
the Global Platform for ISO 31000

Contact details:

Global Institute for Risk Management Standards
39 rue de la Sabotte, Residence 6
78160 Marly-le-Roi
Paris - France
Tel! +33 (0) 6 60 45 42 80
Fax +33 (0) 1 82 09 67 72
Email : Conference2013@G31000.org

IBCM Sponsors:

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

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

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)
- 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 978-0-580-50953-7)
- British Standards Institute (2010) 'BCM: Guidance on human aspects of business continuity'. British Standards Institute, London (PD 25111:2010) (ISBN 978-0-580-71975-2)
- British Standards Institute (2010) 'BCM Guidance on exercising and testing for continuity and contingency programmes', British Standards Institute, London. (PD 25666:2010)(ISBN 978-0-580-67840-0)
- British Standards Institute (2011) 'Crisis Management: Guidance and Good Practice', British Standards Institute, London (PAS 200:2011) (ISBN 978-0-580-76478-3)
- 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
- 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,
- International Organisation for Standardisation (2009) IS) 31000 'Risk Management: Principles and Guidelines' ISO, Geneva (ISBN 978-1-903494-24-0)
- International Organisation for Standardisation (2012) 'ISO 22301 Societal Security BCM Systems - Requirements' ISO, Geneva (ISBN 978-0-580-68680-1)
- International Organisation for Standardisation (2012) 'ISO 22301 Societal Security BCM Systems - Guidance' ISO, 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
- Lacey, D. (2011) 'BCM for small and medium sized enterprises', British Standards Institute, UK (ISBN 978-0-580-74108-1)
- 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)
- Preen, J. (2012) 'Business Continuity Communications: Successful incident communications planning with ISO 22301 (2nd Edition)', British Standards Institute, London (BIP 2185:2012) (ISBN 978-0-580-7661-2))
- Preen, J. (2012) 'Business Continuity Exercises and Tests: Delivering successful exercise programmes with ISO 22301', British Standards Institute, London (BIP 2143:2012) (ISBN 978-0-580-76614-5)
- 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. (2012) 'Auditing business continuity plans; Assess and improve your performance against ISO 22301', British Standards Institute, London (BIP 2151:2012) (ISBN 978-0-580-74342-9)
- Smith D.J. (2011) 'BCM - A recipe for chaos', Institute of Business Continuity Management, RSA
- Smith D.J. (2012) 'BCM: How do you measure up?', Institute of Business Continuity Management, RSA