Organisational Resilience and BCM

In recognising there is a link between organisational resilience and being competitive - How do you measure up?

This paper is by Dr David J. Smith MBA LL.B(Hons) FIBCM BCCE who is a practicing business continuity professional and the current chairman of the Institute of Business Continuity Management (IBCM). He is a Director of several companies that provide business continuity consultancy and training. This is the second paper in a series authored by Dr. Smith and published by Continuity Central. It is strongly recommended that it should be read in conjunction with the first paper ‘Organisational Resilience: Business Continuity, Incident and Corporate Crisis Management.’ This can be obtained here: http://www.continuitycentral.com/feature1100.html

The purpose of this paper is to further consider organisational resilience and the issue of management review of a Business Continuity Management System (BCMS) in particular. To enable continuity and context it incorporates key and relevant parts of the first paper.

A key consideration within both papers is the importance for organisations to recognise and ‘make the link between resilience and organisational competitiveness and invest in resilience. However, for organisation's to invest in their resilience they must be able to demonstrate the need and business case’1.

This paper also provides access to a high level organisational BCMS management self-assessment review that can be obtained from the IBCM website. The IBCM self assessment review aims to help an organisation understand its current status in respect of its business continuity capability within the context of the Elements of BCM (see Figure 2) and a BCMS. It is anticipated that the information obtained from carrying out the management review will provide a high level executive overview in the absence of a full BCM(S) audit or maturity/organisational resilience assessment.

The intention of this paper is to concentrate on the management review aspect of performance management and evaluation of a BCMS rather than on how to provide or demonstrate the need and business case for a implementing a BCMS. Whilst some of the business case drivers are identified and discussed within this paper they are not covered in great detail. The issue of BCMS and organisation/board ‘buy-in’ in general is covered in considerable depth in numerous other publications and articles. In particular this paper addresses the following issues within the context of business continuity and organisational resilience:

- Corporate Governance;
- BCM standards;
- A Business Continuity Management System (BCMS);
- Management Review of BCMS;
- Self Assessment;
- Competent and Independent Reviews;
- Performance Measurement, Evaluation and Improvement;
- Quantitative and Qualitative Evidence and Verification;
- Key Purposes and Check Points;
- IBCM BCMS Self Assessment Review; and
- Suggested Further Reading

Introduction

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

---

1 Lee, Vargo and Seville (2013) p.29.
appropriate level of organisation resilience and proven BCM preparedness is an essential part of the overall enterprise risk management (ERM) of an organisation. As a result complacency is unacceptable in the face of the challenges and threats that inevitably arise in today’s national and global business and public sector service environment. This warning is reinforced by historical independent 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).2

Whilst many commentators within the public sector describe the differences between the public and private sector as reasons why business continuity does not apply to the public sector I firmly believe the management discipline of BCM, incident and corporate crisis management is common to both. This view is reinforced by King III; its associated guidelines and ISO 22301 and ISO 22313. 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/interested parties. 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’. 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’.

At a time when ‘Just In Time’ (JIT) delivery, procurement and supply chain issues in general have a high profile there is a need to consider the big picture and both the fragility and resilience of an organisation’s capability to deliver its own products and services. In particular the organisation’s supply chain and their dependency upon it.

In addition there are regulatory, legal, insurance, licence and contractual requirements to consider whereby contract management takes on a different role to that traditionally recognised. Within this context there is the ever growing differentiator within the procurement process where organisations are asked to provide demonstrable ‘verifiable’ proof of their BCM capability and resilience. This can be achieved by verifiable evidence/information from a management self review or to conduct a review as part of the due diligence process of current or prospective suppliers within the procurement process or contract management. Such requirements are now frequently built into the specific terms and conditions of procurement bids and/or contracts.

Verification means ‘confirmation, through the provision of evidence, that specified requirements have been fulfilled’.9

As the result of the failure of an organisation to be able to respond and provide and/or demonstrate verifiably supportive evidence and/or information as to its organisational resilience and BCM capability is wholly unacceptable. In addition to any other penalty such a failure will no doubt provide an ‘exit’ within the business procurement process or termination of a contract thereby creating a ‘lost opportunity’ rather than having a strong evidential based competitive advantage.10

Within this context and in contrast to the earlier narrow and reactive approaches to BCM it is now acknowledged to be a dynamic, proactive, and ongoing business as usual management process. To be effective it must be aligned to a standard, appropriate (fit for purpose), practical, realistic, up-to-date and a plausible (proven) capability. It is therefore important to understand and distinguish some of the key definitions used within the different BCM standards to enable further discussions within this paper. The key definitions are set out in ISO 22301 that specifies the requirements for setting up and managing an effective Business Continuity Management System (BCMS).11
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.’ 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 as 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.\(^{12}\)

THIS IS A CRITICAL STATEMENT THAT BEGINS TO CLARIFY THE DIFFERING ROLES AND FUNCTIONS OF BUSINESS CONTINUITY (BC), BUSINESS CONTINUITY MANAGEMENT (BCM) AND A 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.\(^ {13}\)

In relation to any self assessment management review, audit or maturity assessment of an organisation’s BCMS or any of its components the rigorous use of verification is key and should avoid the simplistic checklist ‘tick box’ only approach of evaluation.

However, in acknowledging the flaws within a checklist ‘tick-box’ process methodology there is a need to recognise that all reviews/audits have a schedule of primary questions relating to requirements that need to be addressed and areas of activity that need to be examined. It is therefore the context and application in which such a methodology and process is used that is important and relevant i.e. the application of not only quantitative (objective) but perhaps more importantly qualitative (subjective) assessment; both via verification.

Corporate Governance

BCM has always been a key element of an enterprise risk management (ERM) programme and consequently corporate governance\(^ {14}\). This is now fully recognised and amply demonstrated by the inclusion of Business Continuity Management, IT Governance and Information Technology Disaster Recovery (ITDR) in particular 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 code of ‘apply or explain’ principle to the Code of Governance.

The definition of BCM within King III closely reflects the same definition within ISO 22301.\(^ {15}\)

The following are five, amongst many, examples from King III that relate to business continuity and organisational resilience/sustainability. Whilst some directly refer to BCM others are clearly and expressly linked.

1. **‘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’\(^ {16}\)**

2. **‘Treating, reducing or mitigating the risk through improvements to the control environment such as development of contingencies and business continuity plans’\(^ {17}\)**

\(^{12}\) ISO 22313: Clause - Business Continuity, p.vii  
\(^{13}\) ISO 22301: Clause 4 and ISO 22313: Section 4.3.2  
\(^{14}\) ISO 31000:2009  
\(^{15}\) King III 2009 - Glossary of Terms and ISO 22301: Definitions  
\(^{16}\) King III 2009 - Principle 5.6 (37.7)  
\(^{17}\) King III 2009 - Principle 4.7 (42.2)
‘IT Risk is an important aspect of the Audit Committee’s responsibilities. This should include... business continuity and data recovery relating to IT’.18

‘Management should regularly demonstrate to the board that the company has adequate business resilience arrangements in place for disaster recovery’.19

‘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’20

All of these matters are key issues and have a direct impact on an organisation, its stakeholders, interested parties, employees, managers and directors in relation to risk management, insurance, corporate and personal liabilities in respect of the organisation’s resilience and sustainability in the event of an incident or corporate crisis.

Ignoring BCM can happen for a number of reasons, ranging from corporate or personal denial through disavowal to rationalisation or too high a ‘risk appetite’21 or it will never happen to us. 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 disaster. Some become complacent, overconfident in their ability and ignore warning signals22. These are often referred to as ‘Inherent Cultural Blockers’23 and are a key and critical issue within any business continuity, BCM(S) and/or management review/audit.

Figure 1: Governance and BCM Key Constructs24

18 King III 2009 - Principle 3.8
19 King III 2009 - Principle 5.5 (31)
20 King III 2009 - Glossary of Terms
21 ISO 22301: Clause 4 and ISO 22313: Clause 4.3.2
24 Dr David J Smith (2002)
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.25 Changing such mindsets is not easy, as all organisations are different, techniques that work in one organisation will not necessarily work in another. Most executives tasked with addressing business continuity issues are keen to achieve quick wins, and regrettably adopt the checklist ‘tick box’ audit approach which they incorrectly often refer to as best or good practice. The former is a management phrase that is frequently overused and for many organisations is not good practice. This approach tries to copy BCM approaches/arrangements used elsewhere but they are often adopted and implemented without consideration as to suitability. A limited, costly, time consuming and disappointing level of success is usually the outcome. The time honoured phrase ‘trying to put a square peg in a round hole’ comes to mind.

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 organisation resilience (BCM) ‘material information’ to the insurer. Within this context a management self assessment review or internal audit or maturity assessment should be considered as a part of an organisation’s ‘material information’ disclosure to its insurer. Indeed, insurers may begin to make such disclosure a mandatory requirement.

These matters also impact on personal liabilities if the degree of corporate governance and its due diligence are not prudently exercised.26 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 disruption or incident or corporate crisis is handled badly or is unable to be handled due to an inadequate or non-existent organisation and/or personal BCM competence and/or capability. All executives and managers within an organisation should consider the following key questions that are likely to be asked in any subsequent inquiry or part perhaps of an insurance claim:

- 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?

To overcome these problematic approaches the management self assessment review aims to provide a reference point for an organisation to assess their progress, to date, in relation to their business continuity and BCM(S) capability, in essence a ‘gap analysis’, and provide them with information to plan a way forward. However, within this context it is recognised that each organisation will adopt as much of the relevant guidance and requirements standard(s) as it needs based on the key constructs of BCM (see Figure 1) to meet its own and interested parties/stakeholder requirements, obligations and its own ‘risk appetite’.

**BCM Standards**


26 King III 2009
those from the USA, Japan, Singapore, Canada, Australia, New Zealand and UK. The international commitment and interest for ISO 22301 and ISO 22313 standards is reflected in the 50 participating countries that have supported their publication.

Whilst there are now accepted standards and practice against which an organisation can implement and measure a BCMS and its key components it should always be remembered, as indicated earlier, that as a risk management discipline not all organisations will want to have their BCMS certificated against a whole standard but will use the standard to enable them to align and achieve sufficient organisation resilience and business continuity capability to meet their and interested parties needs based on their scale, scope and risk appetite (see Figure 1). This approach is frequently described as good practice and is favoured by many organisations based on good risk management and cost benefit alone.

As a consequence of the caveats listed within them the ISO standards and regulatory guidelines are not designed to be restrictive, exhaustive, or provide a definitive procedure/process to cover every eventuality within BCM. They predominantly set out to establish the generic procedure, process, principles, and terminology and in some cases a bullet-point checklist of process activities. One provides what is described as observed practice but it should be recognised that the standards/guidelines et al rarely provide outcomes in contrast to outputs or evaluation techniques.

Figure 2: The Elements of BCM

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’. 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. Within this context ISO 22301 ‘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... are generic and intended to be applicable to all organisations regardless of type, size and nature of business. The extent of

28 ISO 22313: Clause - Introduction
30 ISO 22313: Clause 8.1.1
the application of these requirements depends on the organisation's operating environment and complexity\(^{32}\) including its risk appetite.

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\(^{33}\). However, the intention of ISO 22313 is NOT to provide general guidance on all aspects of BCM\(^{34}\).

Whilst ISO 22313 indicates it 'DOES NOT REPEAT the requirements for BCMS and its related terms and definitions\(^{35}\) as specified within ISO 22301 it DOES repeat a considerable amount of the requirements albeit some may use the exact wording or rephrase the requirement(s). This is exemplified 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 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'\(^{36}\).

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\(^{37}\). ISO 22301 defines performance as measurable results with a note 'Performance can relate either to quantitative or qualitative findings'. 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.

This is reinforced within ISO 22313 which indicates 'a set of performance indicators should (recommendation\(^{38}\)) 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'.\(^{39}\)

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?

This interpretation, if correct, provides a significant and substantial statement in respect of both ISO standards.

**Business Continuity Management System (BCMS)**

A Business Continuity Management System (BCMS) is defined as 'part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity. The management system includes organisational structures, policies, planning activities, responsibilities, procedures, processes and resources'.\(^{40}\) It is important to note that within this context an organisation's BC, BCM and BCM programme is defined in terms of a Business Continuity Management System (BCMS)\(^{41}\)

\(^{32}\) ISO 22301: Clause - Scope
\(^{34}\) ISO 22313: Clause - Introduction
\(^{36}\) ISO 22301: Clause 0.1 General and ISO 22313: Clause - General
\(^{37}\) ISO 22301: Clause 9.1.1(d) - Performance Evaluation
\(^{38}\) * My insert
\(^{39}\) ISO 22313: Clause 9.1.1 Performance Evaluation
\(^{40}\) ISO 22301: Clause 3.5
\(^{41}\) ISO 22301: Clause 4 and ISO 22313: Clause - Business Continuity p.vii
A BCMS is like any other management system and has the following key components:

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

The BCMS emphasises the importance of:

1. Understanding the organisation’s needs and the necessity for establishing business continuity policy and objectives;
2. Implementing and operating controls and 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.

Within this context both ISO standards apply the Plan-Do-Check-Act (PDCA) cycle model to planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving the effectiveness of an organisation’s BCMS (see Figure 3).

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’ whilst the Act (Maintain and Improve - Clause 10) element ‘covers the corrective action needed to address nonconformity identified through performance evaluation’.

---

42 ISO 22301: Clause 0.1 General and ISO 22313: Clause - General
43 ISO 22301: Clause 0.1 General and ISO 22313: Clause - General
44 ISO 22301: Clause - 0.3 p.v and ISO 22313: Clause - Plan-Do-Check-Act cycle p.v
45 ISO 22301: Clause - 0.3 p.vii and ISO 22313: Clause - Components of PDCA p.vi
46 ISO 22313: Table 2
Management Review of BCMS

Both ISO standards indicate the top management of an organisation shall develop, implement, maintain and continually improve a documented BCMS. Within this context the purpose and objectives of a management review are described as the ‘top management shall review the organisation’s BCMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness... including the effective operation of its continuity procedures and capabilities’.47 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 both quantitative (objective) and qualitative (subjective) ‘verifiable’ data.48

“The role of audit/review is to assess and evaluate the activities and function of an organisation against standards, guidelines, good practice, legislation, contractual and regulatory issues to form a view on whether that activity or function is performing effectively... this provides the reviewer with unique insight into how organisations operate and how things may be improved or simplified”49

48 ISO 22301: Definitions 3.54
In respect of performance evaluation ‘the organisation shall determine (a) what needs to be monitored and measured..(b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results’. and ‘the procedures for monitoring performance shall provide for... the setting of performance metrics appropriate to the needs of the organisation... performance of the processes, procedures and functions that protect its prioritised activities’

This latter statement is taken to mean business continuity procedures, procedures and functions (Clause 8 of both standards) that deals with the operational (DO) aspect of BCM. Within this context ISO 22313 indicates ‘the procedures for the performance and the effectiveness of the BCMS should include setting of performance metrics including qualitative and quantitative measurements that are appropriate to the needs of the organisation’.

This latter comment concerning qualitative measurements within performance metrics is also supported by ISO 22301.

In particular ‘the organisation shall conduct evaluations of its business continuity procedures and capability in order to ensure their suitability, adequacy and effectiveness... these evaluations shall be undertaken through periodic reviews.. and performance evaluations’

As indicated earlier the performance measurement of business continuity procedures relates to the Do (Implement and Operate) phase of the PDCA cycle of BCMS and Clause 8 of both standards. This clause begins to address the key question of ‘does it work’.

What is of note is that the performance measures can be either objective (quantitative) or subjective (qualitative).

This is relevant when endeavouring to evaluate the review criteria of suitability, adequacy and effectiveness of business continuity procedures, processes and functions.

An audit or ‘management review shall/should cover the scope of the BCMS, although it is not necessary to review all elements at once and the review process may take place over a period of time’. Within this context the organisation can carry out thematic reviews whereby ‘audits/reviews may be divided into smaller parts, so long as the audit/review programme ensures that all organisational units, functions, activities and system elements and the full scope of the BCMS are audited/reviewed in the audit/review programme within the period designated by the organisation’

In implementing a BCMS it must be recognised that ‘a number of key risks and purposes have been established.... each risk and purpose could form the scope for a standalone review... they act as checkpoints to ensure that an organisation’s BCMs is fit for purpose and has met the needs of the specification’. The checkpoints are scalable and can be applied to both the public and private sectors. Critically they form the basis and represent the absolute minimum for any audit or review or maturity assessment of a BCMS and are therefore key in its implementation.

The key risks and checkpoints are as follows:

1. Establishing and managing the Business Continuity Management System (BCMS);
2. Embedding/integrating BCM in the organisation’s culture;
3. BCMS documentation and records;
4. Understanding the organisation;
5. Determining Business Continuity strategy(ies);
6. Developing and implementing a (competent and capable) BCM, incident and corporate crisis management response;
7. Exercising, maintaining and reviewing (evaluating) BCM arrangements;
8. Monitoring and reviewing (evaluating) the BCMS;
9. Maintaining and improving the BCMS.

ISO 22301: Clause 9.1.1 and ISO 22313: Clause 9.1.1
ISO 22313: Clause 9.1.1
ISO 22301: Clause 3.35 (Note)
‘Capability’ not included in ISO 22313 guidance
ISO 22301: Clause 9.1.2 and ISO 22313: Clause 9.1.2
ISO 22313: Clause 9.3
ISO 22313: Clause 9.2 and 9.3
Within the review process the primary role of the reviewer is to provide independent assurance and advice to top and operations management about the organisation's BCMS (business continuity capability) and by extension its organisational resilience. A key consideration and issue concerns the competence and capability of reviewers in terms of skills, knowledge and experience of the type of organisation and BCM in relation to them conducting a credible BCM review. ‘Independent reviews/audits should be conducted by competent persons, whether internal or external’ 58 This latter issue is of particular importance and is in addition to ISO 22301 and ISO 22313 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’. 59

In addition this 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 and BCMS to allow them to conduct a credible review and make credible judgements and recommendations. 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 shall/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’. 60 However, ISO 22313 indicates that ‘persons who are involved in implementing the BCMS and allocating its resources should be involved in the management review’ 61 but the standard does not indicate in what capacity.

As a result of its all-embracing nature, the way BCM is carried out will inevitably be dependent upon, and must reflect, the nature, scale and complexity of an organisation’s risk profile, risk appetite and the environment in which it operates. The importance of a 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. 62 This is especially true of organisations that have operations in other countries; 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. USA Security Exchange Commission (SEC) Rules - NY stock exchange listing rules. This is a key consideration within any audit or management review.

Within the context of either audit or management review ISO 22301 indicates its specification and requirements only addresses the issue of quantitative (objective) verification and says 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...’. 63

However, whilst objectivity is one facet measurement the other key element is subjective (qualitative) process 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 (quantitative) benchmarking and Process (qualitative) 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

---

58 ISO 22301: Clause 9.2 and ISO 22313: Clause 9.2
59 Principle 5.7 King III 2009
60 ISO 22301: Clause 9.2 ad ISO 22313: Clause 9.1.2
61 ISO 22313: Clause 9.3
62 See suggested further reading
63 ISO 22301: Clause - Scope
However... one is rarely of any value without the other.

The management 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. As indicated earlier the role of setting both qualitative and quantitative (process) assessment criteria within performance objectives/measurement/metrics is recognised within both ISO 22301 and ISO 22313.

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’.

Within any review there is, as indicated earlier, limited value in a checklist ‘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 or not it works (proven). It is at this stage it should be remembered that the review needs to verify the BCM competence and capability of the organisation whereby ‘verification’ is defined within ISO as confirmation, through the provision of supporting evidence, that specified requirements have been fulfilled. The level of supporting evidence should not only be objectively reviewed but also be subjected to critical qualitative evaluation which falls within the remit of the independent professional BCM practitioner reviewer and subject to the organisation's 'risk appetite'. 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.

Further, underlying the checklist ‘tick box’ approach is the persuasive belief that a structure, policy, framework and plan are all that is required. Whilst these are critical enablers, relying on them alone tends to overlook the key issue - it is people that deal with business continuity, incidents and corporate crises. Therefore the people issues such as training and awareness including exercising, to develop competence and capability, should be a key consideration and highlighted in any review/audit.

In conducting a review of an organisation’s BCMS and capability it must be remembered that BCM is a complex issue and covers a whole enterprise. As a consequence the scope of any review should be specific. In particular a review should consider the overall risk and BCM approach of the organisation; does it wholly rely on preventative measures or is less risk averse and to the exclusion of preventative measures implements a robust BCM capability that includes incident and corporate crisis management or adopts a mixture of both? Is there consistency of approach and application rather than it being piecemeal and haphazard?

In conducting a review of an organisation’s BCMS and capability it must be remembered that BCM is a complex issue and covers a whole enterprise. As a consequence the scope of any review should be specific. In particular a review should consider the overall risk and BCM approach of the organisation; does it wholly rely on preventative measures or is less risk averse and to the exclusion of preventative measures implements a robust BCM capability that includes incident and corporate crisis management or adopts a mixture of both? Is there consistency of approach and application rather than it being piecemeal and haphazard?

Within this context there are a number of key questions and steps to be taken in developing and planning a management review/audit including its scope and framework:

**Step 1:** Determine the BCM maturity of the organisation under review- whilst most organisations will have some limited BCM capability it may be informal and sporadic across the organisation. In such circumstances there is little point in conducting a review when the answers are already known. In contrast where an organisation has a high level of BCM capability the scope of the review will be focused as to where it can be of best value;

**Step 2:** What is the review trying to achieve? What question(s) need to be answered? It is important to address the key areas rather than a wider review that is spread too thin and over reaches thereby providing little or limited value.

**Step 3:** Does the lead reviewer and the review team have the necessary knowledge, skills and experience to credibly conduct the review/audit? Within this context there is a need to establish the areas of review that require the assistance of experts or 3rd party assistance;

---

64 ISO 22301: - Clause 9 - Performance Evaluation and 22313: Clause 9 - Performance Evaluation

Step 4: Establish the review resources, timescale and budget - Is the proposed scope realistic and a review feasible within the constraints of the resources, timescale and budget?

Step 5: Consider the scope within or as an integral part of a review framework and work plan. What does it require to be done e.g. is it thematic? This should also eliminate scope creep.

The outputs of a management review shall include decisions related to continual improvement opportunities and the possible need for changes to the BCMS, and include the following:

a) variations to the scope of the BCMS;
b) improvement of the effectiveness of the BCMS;
c) update of the risk assessment, business impact analysis, business continuity plans and related procedures;
d) modification of procedures and controls to respond to internal or external events that may impact on the BCMS, including changes to
   1) business and operational requirements;
   2) risk reduction and security requirements;
   3) operational conditions and processes;
   4) legal and regulatory requirements;
   5) contractual obligations;
   6) levels of risk and/or criteria for accepting risks;
   7) resource needs;
   8) funding and budget requirements;
   9) Competence and capability of individuals;
   10) Embedding/integration of business continuity within the organisation;
   11) Training and awareness; and
e) how the effectiveness of controls are measured.

The organization shall retain documented information as evidence of the results of management reviews.

The organization shall
- communicate the results of management review to relevant interested parties, and
- take appropriate action relating to those results.

**IBCM BCMS Self Assessment Review**

The IBCM self assessment review has been produced and licensed to the Institute of Business Continuity Management; it encompasses the key elements of both ISO standards. The structure of the review requires critical verification of answers to questions. The provision of verification evidence/information should be of either or both a quantitative (objective) and qualitative (subjective) nature. It is recognised that a qualitative verification assessment will require the assistance of a professional certificated risk and/or business continuity practitioner e.g. MIBCM, to carry out a ‘due diligence’ verification and validation of any supporting evidence provided e.g. an organisation may have completed a BIA but it may not reflect good practice and thereby be wholly unfit for purpose?

The self assessment review is designed around pragmatic implementation and ongoing workflow that incorporates the Elements of BCMS (see Figure 2) and its various stages and is aligned to the key BCMS requirements set out within both ISO standards (see Figure 3).

---

66 ISO 22301: Clause 9.3 - Management Review
67 ISO 22301 and ISO 22313: Clause 8 and Do part of PDCA cycle.
The review is intended to encompass the different elements of an organisation’s BCMS in the context of its resilience and sustainability. The primary questions and ‘verification’ supporting evidence criteria within the self-assessment review are not intended to be comprehensive/exhaustive in terms of addressing all issues associated with organisational resilience, but they do begin to address the key issues that are relevant to a BCMS; its implementation, operation, management and maintenance. Although it contains the key elements of ISO 22313 and ISO 22301 it is not a ‘tick-box’ checklist for the ISO standards and critically requires both quantitative (objective) and qualitative (subjective) review ‘verification’ support evidence to enable the answering of primary questions as a key element in its application. Therein is the critical difference.

It must be stressed that just using the management self assessment review as a checklist 'tick-box’ set of questions without rigorous quantitative and qualitative ‘verification’ via supporting evidence/information is of extremely limited use, value or benefit.

The review is designed to provide a broad pragmatic approach against which an organisation can assess and review its current BCMS and organisational resilience. It should also be used to provide information to initiate discussion of how to minimise and mitigate risk and maximise the resilience/sustainability of an organisation’s prioritised activities (products and services). In particular it provides a high level overview to provide information that can indicate the need for a more in-depth or detailed review, or audit, or maturity assessment to establish a more detailed ‘gap analysis’ and ongoing work programme including clear recommendations for improvement.

Whereas the management self assessment review begins to enable an organisation to assess and demonstrate its implementation of BCMS against the ISO standards its finding may, subject to rigorous ‘verification’, be applicable for use by an organisation to assure interested parties that an appropriate BCMS and effective business continuity capability is in place.


**USAGE NOTE:**

The management self assessment review or any part thereof is not to be used for commercial purposes e.g. consultancy or certification of a BCMS unless expressly authorised and licensed for such by the copyright holder. It is intended for use by organisations as part of an internal management BCMS self assessment review or their supply chain or within their procurement process or contract management where applicable and appropriate. In using the review an organisation or individual should make themselves fully aware of the disclaimer associated with advice and use of the review together with the usage note within this paper and the assessment review spreadsheet.
Summary

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

The most current and historical research findings clearly identify that not just regulators but 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 via a BCMS. In addition to good business and risk management practice this is driven by the need for all organisations to clearly demonstrate the discharge of their legal, contractual, corporate governance and other accountabilities and responsibilities at both a managerial (personal) and organisational level. 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 checklist 'tick box' methodology for its completion, operation and maintenance provides effective organisation resilience. 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 generic plan template approach designed to facilitate a BCMS by ‘filling-in-boxes’ should be wholly rejected.

Within this context a BCMS management self assessment review should be a part of every organisations enterprise risk management (ERM) programme. It is hoped that the IBCM self assessment review will be beneficial and aid that process that links to corporate governance via an organisations risk committee. However, in conducting any review/audit there are several key issues that it should be considered mandatory and omitted at an organisation’s peril:

1. Ensure top management review the organisation’s BCMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness and that all such reviews are be documented;
2. In addition to the current BCM standards specification/requirements ensure the review considers legislative, regulatory, contractual and licence issues that recognise and include relevant impact issues from other countries sector requirements e.g. SEC and Basel III.
3. Clearly define the scope and purpose of the review/audit - What is it trying to answer/establish/achieve?
4. Ensure the scope of any review/audit includes the key risks and requirements set out in both ISO 22313 and ISO 22301 so they form the basis and represent the absolute minimum for any audit or review or maturity/organisational resilience assessment of a BCMS;
5. Use only professional qualified and accredited BCM practitioners who know the organisation’s business to carry out a review/audit;
6. Ensure both objective (quantifiable) and subjective (qualitative) ‘verification’ is a key criteria of the review evaluation procedure and process of performance indicators and metrics;
7. Ensure a report is produced after each review that not only provides information as the organisation’s current BCM status but includes issues concerning non-conformities and recommendations of corrective action including improvements together with implementation timescales;
8. Recognition and awareness of the danger of Inherent Cultural Blockers and their bias influence in audit and management self assessment review;
9. Provide 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.
10. Remember the importance of audit/management self assessment review in respect of insurance ‘material information’ disclosure, supply chain management, procurement, contract management and assurance of interested parties that an appropriate BCMS is in place.

[69] King III (2009)
About the author:

Dr. David J. Smith, MBA, LLB(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.

He is a former executive member of the Business Continuity Institute Board of Directors and Chairman of its Education Committee. He is a retired senior police officer and globally recognised expert concerning Business Continuity 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 best practice and benchmarking initiatives within Governments, industry groups, including the UK Financial Services Authority, Asia Productivity Organisation and British Standards Institute. He is a key contributor and 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 and BSI 25999-1 Code of Practice for BCM 2006 and author of the accredited academic syllabus for the first Business Continuity Management Certificate/Diploma/MSc course within the UK at Coventry University.

He is also the Business Continuity lead, author and trainer of the accredited Post Graduate Certificate / Post Graduate Diploma / MSc syllabus at the Resilience Centre, Department of Applied Science, Security and Resilience of Cranfield University (UK) at the Joint Services UK Defence Academy, Shrivenham.

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

Amongst his various policing roles he was responsible for particular areas of specialism that included project management, crisis and business continuity management, physical security, risk management, forensic investigation, integrated management of disaster and civil emergency, audit, assurance, planning, training, exercising of plans, rehearsing of staff and 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 UK 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:

Within the context of this paper and providing the IBCM BCMS self assessment review the IBCM endeavours to ensure that the information contained within it is correct, and whilst every effort is made to ensure the accuracy of such information, it accepts no liability for any error or omission in the same. Consequently, the author, IBCM and licensees make no representations or warranties, expressed or implied, concerning the BCMS self assessment review and each individual or organisation should consult their advisors with respect to individual or organisation issues. The information contained herein is based on sources that are believed to reliable, but their accuracy is not guaranteed, and it should be understood to be general information only. The information is not intended to be taken as advice with respect to any individual situation and cannot be relied upon as such. All such matters should be reviewed with the readers own qualified advisors.

All trademarks and product names used within this document are here by acknowledged.

Copyright Notice:

© The copyright to this document and self assessment review with all rights reserved is owned by Dr. David J. Smith and Stamford Consulting Limited and is licensed to the Institute of Business Continuity Management 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, maintenance and services for BCM.

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 for 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
Website: www.ibcm-sa.org
Linkedin: http://www.linkedin.com/groups?home=&gid=4699159&trk=anet_ug_hm
IBC M Partners:

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.

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

- Institute of Risk Management South Africa (2011) ‘Code of Practice for Enterprise Risk Management’ IRMSA,
- IoDSA (2009) King III Report and Code of Corporate Governance’ King Committee, Republic of South Africa