A business continuity management maturity model for the UAE banking sector

Kasim Randeree
Saïd Business School and Kellogg College, University of Oxford, Oxford, UK
Ashish Mahal
RAK Bank, Dubai, United Arab Emirates, and
Anjli Narwani
University of Sharjah, Sharjah, United Arab Emirates

Abstract

Purpose – Organisations utilise Business Continuity Management (BCM) to support sustained performance of electronic systems on which their core activities are based. These organisations require a tool that can be used to assess the maturity of their existing BCM processes. Through the examination of the banking sector of the United Arab Emirates, the purpose of this paper is to address the need for a BCM maturity model.

Design/methodology/approach – A tailored BCM maturity model was developed using a two-stage approach; the first stage was developing a model based on the analysis of five existing models; and the second stage was validation of the developed model against the formulated objectives through the use of focus groups with ten UAE banks, comprising of three BCM experts for each bank.

Findings – The research found that the provision of a standard maturity model for BCM as a situational analysis tool for the banking sector is functional and can be the basis of a tool to address the gap in organisations in general to assess the maturity level of their BCM processes.

Research limitations/implications – The developed model is limited to validation within a specific sector and geographically, with generic model validation being outside the scope of this research.

Practical implications – The framework provides different areas to which maturity can be assigned, various levels across quality and scope and how an overall BCM maturity of an organisation can be determined.

Originality/value – The development of a maturity model which could be used as a BCM self analysis tool is a significant addition to the BCM knowledge base.

Keywords United Arab Emirates, Banking, Business continuity, Business continuity management, Maturity model, Banking sector

Paper type Research paper

1. Introduction

Forces in the global context and pressures of competition are constantly pressing demands on organisations to take measures to assure the continuity of their business. Business continuity has thus become a topic of high interest to organisations striving to overcome negative forces (KPMG, 2006). To achieve operational and business

Business Process Management Journal
Vol. 18 No. 3, 2012
pp. 472-492

1463-7154
DOI 10.1108/14637151211232650

The authors would like to thank: the BT Centre for Major Programme Management and The Oxford Centre for Corporate Reputation, Saïd Business School, University of Oxford; Santander Universities; and The British University in Dubai for their support for this work.

continuity, there is a management process that addresses the processes and people that are critical for the survival of the organisation. This approach of ensuring continuity of critical processes is called business continuity management (BCM).

Dayan and Evans (2006) explain that a process is a set of practices to achieve a given purpose. It may include tools, methods, material and/or people. A process is therefore a leverage point for an organisation's sustained improvement. According to Lockamy and McCormack (2004), the concept of process maturity proposes that a process has a lifecycle that is assessed by the extent to which the process is explicitly defined, managed, measured and controlled. The process maturity concept is analogous to that of a lifecycle, which occurs in developmental stages. This concept also implies growth in the areas of process capability, richness and consistency across the entire organisation (Dorfman and Thayer, 1997). This process maturity can be determined using maturity models, which assumes that progress towards goal achievement comes in stages.

As Smit (2005) states:

> The scope of a maturity model can vary from a constituent process or a process within a certain function (e.g. software development Capability Maturity Model (Paulk, 1995)), to an integrated whole of the main processes that form the business (Instituut Nederlandse Kwaliteit-model).

BCM itself, has its roots in disaster recovery, which emerged in the 1950s and 1960s as companies began to store backup copies of their critical data, paper or electronic, at alternate sites. The functions of security and disaster recovery systems rely on the continuity of information technology (IT) systems. National and international disasters together reinforced the need for organisations to rethink their processes and systems along the lines of BCM principles. Although organisations recognise the need for BCM, they often do not know how to implement BCM processes properly and integrate them through their entire organisation (end-to-end).

The Business Continuity Institute (BCI, 2007) defines BCM as:

> A holistic management process that identifies potential impacts that threaten an organisation and provides a framework for building resilience with the capability for an effective response that safeguards the interests of key stakeholders, reputation, brand and value creating activities.

Nowhere is this truer than in the banking sector. The need for agility of banks to address the diverse needs of a varied customer base and evolution in its essence has driven banking institutions towards computerisation and IT enabled systems across all operations (Mohan and Rai, 2006; IBM Global Services, 2000; BSI, 1999). Realising that these electronic systems have been the major factor that differentiates between competitors in today's demanding banking business environment, banks are moving to protect themselves from system failures. However, protecting against such system failures is not enough. Banks need to be more concerned about the risks that threaten the operational continuity of their businesses as well. After all what good is a computer system, when there are no business processes to use them? Information possessed by banks is no longer only used by employees, but by customers and partners as well on a real time basis (usually through intranet systems). These users expect continuous availability of and instantaneous access to organisational information. Protecting their information is essential to ensure that the business has a competitive edge and maintains cash flow and a good commercial image (BSI, 1999). In order to ensure that

a bank maintains its competitive edge, the information must be kept confidential, accurate and continuously available.

Though banks utilise BCM to support sustained performance of their electronic systems, effectiveness of their systems lack maturity. Thus, by examination of the banking sector of the United Arab Emirates (UAE), this paper addresses the need for a BCM maturity model.

2. Business continuity management

Noakes-Fry and Diamond (2001) articulated that there is continuously increasing pressure that forces banks to take steps to address the continuity of their business. This includes the demanding customers who enforce requirements (of uninterrupted and continuous service) and by supervising bodies (regulatory institutions, compliances, etc.). Further, ensuring business continuity has become more difficult because of increasing threats, supply chain integration and dependency on complex information systems. BCM addresses operational continuity by concentrating on mission critical business processes. Although the awareness that something should be done to assure business continuity is present in many organisations, especially in the banking sector, they often do not know how to implement BCM processes in the appropriate manner and integrate them across their entire organisation. According to a BCM survey conducted by KPMG (2006), this is also true within organisations in the UAE, where only 20 per cent of organisations have an integrated organisation-wide BCM system. The other 80 per cent of organisations in the UAE have BCM processes in place in one form or another, but are not clear as to how to take these processes forward. Usually, organisations consider BCM as a new and complex process and thus seek specialised external advisors and consultants to develop a BCM program.

Multiple BCM best practices and methodologies exist (Kenny, 2006; Koch, 2001) but their contents do not vary much. These best practice models and methodologies provide information as to how to implement BCM process but do not provide any mechanism to prescribe the extent to which an organisation should implement the BCM process. The methodologies do not offer a way to assess where an organisation currently stands in terms of BCM maturity, how far they have to go and what they need to do to get there. The BCI released a BCM standard called BS25999 in 2007, which too does not provide any kind of framework against which organisations can benchmark their current status. Software-based maturity models, such as the capability maturity model (CMM), rely on the fact that a target maturity level can be achieved only after going through several phased steps. The need for organisations to create formal BCM systems has been discussed by researchers (e.g. Mohan and Rai, 2006). They point out that there has been a significant increase in perceived importance by management for implementing business continuity planning (BCP). For example, Digital Research, Inc. (2002)) reported that three in four companies with plans in place to deal with such disruptions have reviewed the adequacy of their plans in light of the events of 11 September 2001. Initially, the focus of BCP had been on IT (Savage, 2002). However, writers are recognising that one of the most critical activities inherent in managing risk is ensuring the flow of inbound products and services as inputs to production (Burt *et al.*, 2003; Gilbert and Gips, 2000). According to Zsidisin *et al.* (2005), supply chains are increasingly susceptible to unplanned disruptions. With the implementation of total quality management (TQM), time-based competition and other supply chain improvement initiatives, managers now

realise that their supply chains are fragile, particularly to environmental disruptions outside their control (Randeree, 2010). The BCM: *Best Practices Guidelines* document (2002) as adapted in *Publicly Available Specification (PAS 56) Guide* to BCM (BCI, 2006) portrays BCM as an activity:

> [. . .] that unifies a broad spectrum of business and management disciplines in both the private and public sectors, including crisis management, risk management and technology recovery, and should not be limited to IT disaster recovery.

BCM is not only a professional specialist discipline but also a business owned and driven issue that unifies a broad spectrum of business and management processes. These include risk, facilities, supply chain and quality management; disaster recovery; security; crisis communication and PR; and health and safety (Burtles, 2005). In particular, BCM provides the strategic and operational framework to both review, and where appropriate, redesign the way an organisation provides its product and services whilst increasing its resistance to disruption, interruption or loss. BCM is about managing risk and ensuring an organisation can continue operating. Zsidisin *et al.* (2005) state that business continuity is a system that has been developed by practitioners to minimise the effects of unanticipated events on the firm's ability to meet customer requirements. Elliott *et al.* (1999) view BCP from a finance market perspective, as:

> [. . .] planning which identifies the organisation's exposure to internal and external threats and synthesises hard and soft assets to provide effective prevention and recovery for the organisation, whilst maintaining competitive advantage and value system integrity.

Shaw and Harrald (2004) recognise that BCP is an essential facet of BCM, which consists of business practices that provide focus and guidance for the decisions and actions required for a firm to prevent, mitigate, prepare for, respond to, resume, recover, restore and transition from a crisis event. BCP involves developing a collection of procedures for the various business units that will ensure the continuance of critical business processes while the data centre is recovering from the disaster. BCP can also be defined as a complete process of developing measures and procedures to ensure an organisation's disaster preparedness. This includes ensuring that the organisation would be able to respond effectively and efficiently to a disaster and that their critical business processes can continue as usual.

From the existing definitions of BCM some important features identified include:

- The objective of BCM is to ensure the continuity of the organisation's mission critical processes, which are core to the business at at-least the minimum acceptable level.
- BCM activities should be prioritised with major attention towards mission critical business processes.
- BCM covers both the prevention of disasters/disruptions and reducing the impact to business in case of a disaster/disruption. Hence, it has preventive, repressive and corrective actions.
- BCM is an iterative management process – not a one-off project. BCM becomes obsolete if not maintained or tested.

Processes that are not critical also need to be recovered in the end, but not necessarily within a given (often short) timeframe. Of course their protection and recovery

is also important, but it does not belong within the scope of BCM. Thus, a successful BCM process requires an organisation to identify its critical processes and to determine all resources these processes depend on. However, the focus is not primarily on these resources, but on the critical business processes. All BCM demands should therefore be derived from requirements regarding the critical business processes.

3. The importance of BCM

The focus of BCM is on essential processes as opposed to business functions. Organisations have thus undergone a paradigm shift in their thinking, with a realisation that process-based approaches, like business process reengineering/redesign (BPR), business process improvement (BPI) and TQM create value for organisations in a way that business functions alone do not (Smit, 2005). Further, BCM aids in overcoming issues such as disruption to the supply chain, risk and meeting the growing demands of regulation.

3.1 Supply chain disruptions

Supply chains are increasingly susceptible to unplanned disruptions. With the implementation of practices such as TQM, time-based competition and other supply chain improvement initiatives, managers now realise that their supply chains are fragile, particularly to environmental disruptions outside their control. Therefore, it is becoming increasingly important to address the continuity of supply chains.

In order to address supply risk, many managers are now adopting an approach for dealing with these specific types of disruptions-disruptions that are difficult to predict, have a small probability of occurring but that, when they occur, have an immediate and significant impact on the ability of the supply chain to meet customer demands. This approach is BCP or BCM (Zsidisin *et al.*, 2005).

3.2 Customer demands amidst rising competition

Smit (2005) argues that customers now demand round the clock e-commerce services and this can only occur if they can ensure the continuity of their IT systems supporting these services. Disruption would likely incur financial loss and contribute to diminishing brand value and reputational damage. In an aggressive and competitive environment, this could result in customer attrition to opponent organisations and, as a result, customers are in the driving seat, demanding guaranteed service continuity from supplying companies. Rising demand also leads to a need for cost efficiency (Randeree, 2010) and means organisations outsource more of their secondary activities allowing a more dedicated approach to primary activities.

3.3 Regulation and risk

Increasing regulation warrants greater need for BCM as companies are impacted through regulation to ensure continuity of business processes. The requirements of "De Nederlandsche Bank" (DNB) regarding Dutch financial institutions, BASLE II, the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act (SOXA) and the regulations for municipalities regarding the municipal base administration (GBA) are examples ever increasing regulation. Furthermore, external dangers such as terrorism, natural disaster, industrial espionage and fraudulent behaviour at all organisational levels have increased in recent years, putting business

continuity at ever increasing risk. The perception of risk is further heightened through the media spotlight, which often over emphasises or exaggerates risk (Randeree and El Faramawy, 2011; Randeree, 2008). A further risk factor is the dependency of corporations on their IT systems and the robustness of all related infrastructure (Randeree and Gaad, 2008), which increases their susceptibility to interruption or crisis (Randeree and Ninan, 2011; Smit, 2005).

4. Maturity models

Based on the description of the Gartner Maturity Model (Mingay, 2002) a maturity model can be defined as a staged structure of maturity levels, which defines the extent to which a specific process is defined, managed, measured, controlled and/or effective, assuming the organisation develops and adopts new processes and practices, from which it learns, optimises and moves on to the next level, until the desired level is reached. Thus, are enlisted the following objectives of the maturity models:

(1) to measure the maturity of the process under consideration, i.e. assign a level to the existing process;

(2) to compare the maturity of an organisation to other organisations and with best practices; and

(3) to provide a mechanism of learning to improve the maturity level.

Smit (2005) identified two BCM maturity models that demonstrate the required merits, namely the Complete Public Domain Business Continuity Maturity Model (BCMM) and the Gartner BCP Maturity Model (Mingay, 2002). The former measures the extent to which an organisation is prepared for a serious negative eventuality, such as a disaster. It classifies according to six maturity levels, where levels one to three represent organisations that are immature, to the extent that preliminary phases have yet to be completed in order to instigate an enterprise-wide business continuity system, whereas levels 4-6 represent organisations in the process of achieving maturity towards this goal.

Smit (2005) cites Mingay (2002) who purports that the Gartner BCP Maturity Model is designed and functions to allow corporations to realise four objectives, namely, the evaluation of BCP processes; allow high-ranking personnel to understand the requirements needed to achieve enterprise-wide BCP application; "complete a gap analysis so realistic targets can be set; and provide a basis for peer-group comparison and establishment of industry standards." The distinctive levels of maturity the model classifies are based on the COBIT maturity model, which are partially based on the CMM maturity levels. Gartner identifies 19 performance measures required for of an organisation's BCP maturity. However, the criticism levelled against BCMM also applies to the Gartner BCP Maturity Model.

Overall, the findings of this review demonstrated that the two maturity models presented for BCM are inadequate in their entirety to satisfy all the needs of the required maturity model and cannot be consolidated. The resolution was therefore to create a tailored BCM maturity model, which concurs with the conclusions of Smit (2005).

5. Developing a BCM maturity model

The final BCM maturity model developed is shown in Figure 1. Arriving at this model was based on several stages. First, a consolidation exercise of inputs from five existing

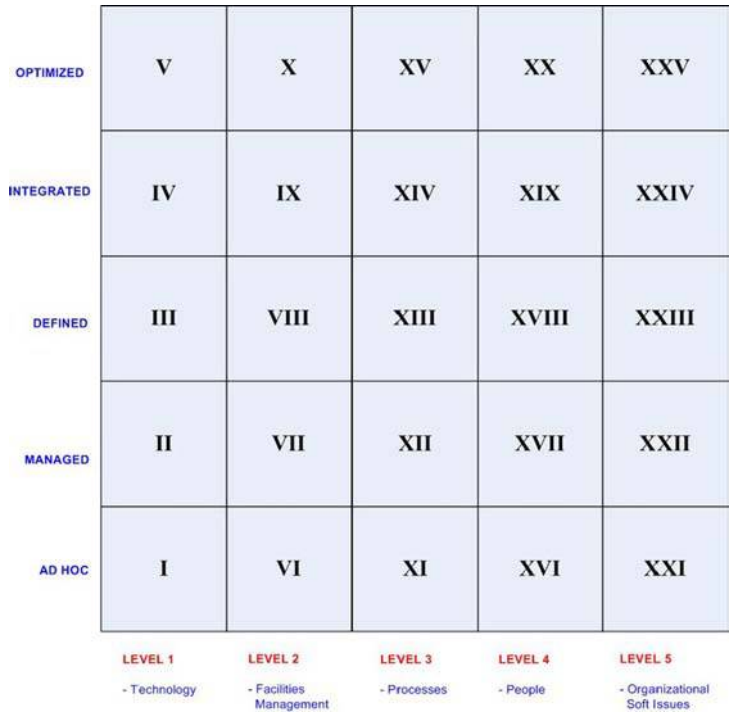

Figure 1.
Developed BCM maturity model

BCM/maturity models (five models); second, an iterative process, which comprised of seven steps applied across (third) maturity levels within five areas. Finally, the focus group validation process was undertaken to test the validity of the developed model within the context of banks in the UAE.

Five models

(1) CMM and CMMI models for software process improvement.

(2) Business process orientation (BPO) maturity model (SEI, 2002).

(3) Business continuity model for banks in India (Mohan and Rai, 2006).

(4) Maturity model for the implementation of software process improvement (Niazi *et al.*, 2005).

(5) GPIS model (Saleh and Alshawi, 2005).

CMM assigns a maturity level to the whole software development process based on the process areas covered. The process is for instance either repeatable or managed based on the number of process areas covered by the organisation. Therefore, each maturity level will cover a different number of process areas. The same concept holds good for the BPO maturity model. The business continuity model developed by Mohan and Rai (2006) identifies five components namely organisational soft issues, processes, people, technology and facilities management and defines a variety of metrics at four levels (corporate/policy level, tactical/organisational level, tools/methods, up gradation/

review/testing mechanism level) to measure the "resilience" and "vulnerability" of a bank in the event of business disruption.

Seven steps

(1) Initiate BCM program, develop a BCM charter (containing strategy/policy) and assign responsibility/accountability.
(2) Perform a business impact analysis (BIA).
(3) Perform a risk analysis.
(4) Select the business recovery strategies.
(5) Develop the complete BCP along with preventive, corrective and repressive measures (incident response crisis management, PR and media).
(6) Implement BCP by embedding in organisation culture through training and awareness.
(7) Test, audit and maintain the BCP (Smit, 2005).

Five areas

Within the framework, five areas are identified to which one of five maturity levels is assigned (Figure 2). The detailed description of each of the five areas is given in Appendix 1. The seven step iterative process is thus executed as follows:

(1) AREA 1: BCM program management (step 1).
(2) AREA 2: planning and analysis (steps 2-4).
(3) AREA 3: development of the BCP (step 5).
(4) AREA 4: implementation (step 6).
(5) AREA 5: maintenance (step 7).

Validation process

The final model is validated by applying it to organisations and through focus group sessions to determine whether all its objectives are met or not. Through the use of the focus groups, the maturity level within each area (Figure 3) could now be established for any UAE bank. During these sessions, the attendees gave feedback on the practicality of the model based on their industry experience, taking the requirements of the model into account. To illustrate the process, focus group responses to structured questions addressing those aspects were divided into several standard answer categories. For example: the answers to the level of BCM policy of an organisation was divided into: "No BCM Policy", "Part of IT security", "'Basic BCM policy', organisation wide BCM policy" and "Strategy driven BCM policy." For each area, a similar categorisation of standard answers is followed to derive five different maturity levels (which are independent of each other) among organisations in UAE.

Figure 2 thus shows maturity of each area separately.

Developed model

The developed model (Figure 1) is further enhanced by an organisation's maturity across two dimensions – BCM process quality (y-axis) and the BCM process scope (x-axis) as shown in Figure 3. By defining maturity on both axes, the maturity level

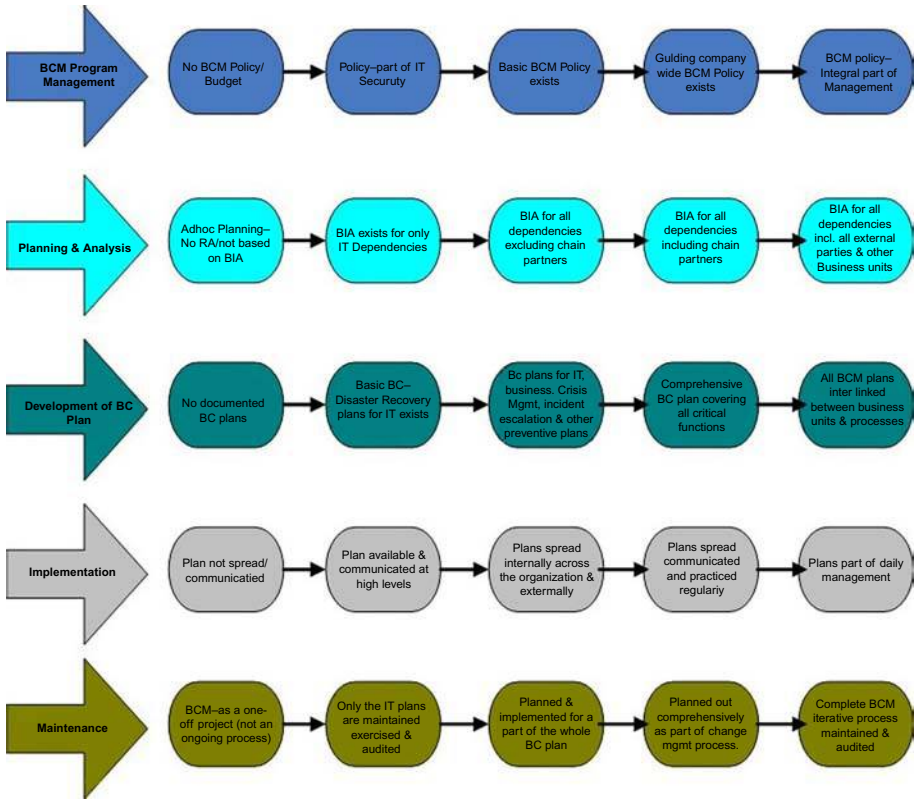

Figure 2.
Maturity levels from the data collections exercise

based on the occupied grid space (known as a scope quality box (SQB)) for which an organisation meets its goals can be derived. Each SQB is described by specific process areas (Appendix 2) and each area is specified by a specific goal. Each goal has certain generic practices associated with it, which provides a roadmap on how to improve organisational maturity level.

6. Results and analysis

The focus group session performed a check on whether the model satisfies the requirements.

1. Substantiated judgement of BCM process maturity within an organisation

It was agreed that the model met this requirement. None of the attendees criticised the model with respect to this requirement. However, certain questions were raised on the completeness of the requirements of each aspect/goal and it was agreed that it would require further research to achieve completeness.

There was also a remark for the addition of a level 0 for process quality indicating an organisation that does not have practice of BCM. This was then challenged as to which scope level 0 would be applicable. The overall assessment was that it is complete and gives a fair judgment of the current situation of BCM in an organisation.

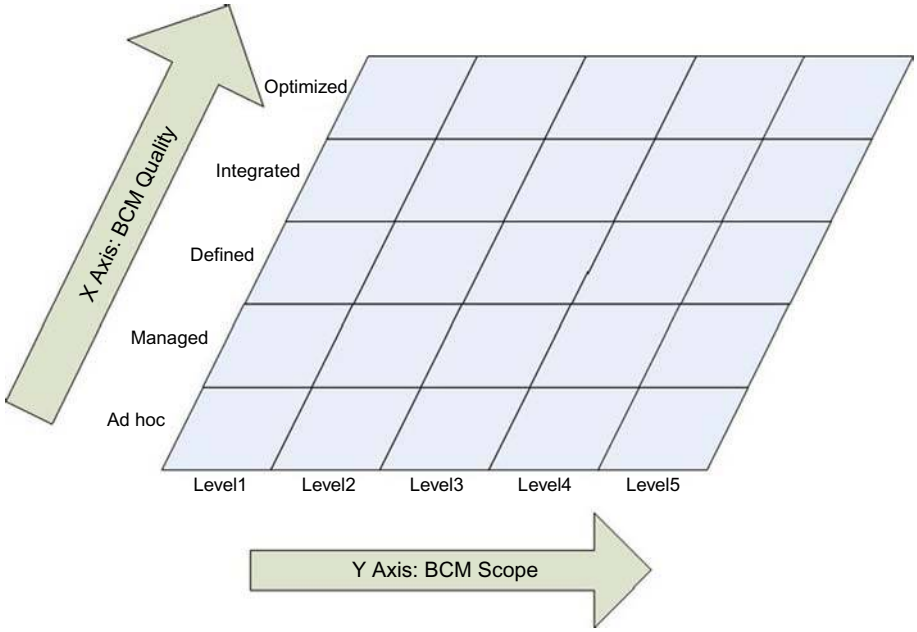

Figure 3.
BCM maturity model based on the five models described

2. Easily communicable model

During the focus group sessions, this particular requirement was not challenged at all. The SQB with certain process areas and goals were easily understood by all. The diagrammatic representation was remarked as user friendly (Figure 3).

3. Model must give recommendation to improve maturity in terms of action oriented goals

The determination of recommendation is done in two steps. First, the current status of the organisation is determined. Second, the target level is to be determined. Ideally, in order to reach a target level, organisations must work towards attaining all level on the way. For instance, if an organisation is in managed level covering all scope levels and if it wants to achieve integrated level across all scope levels, it must first achieve all defined levels across all scope levels. It was agreed that not all organisations follow this growth strategy and the model must provide recommendations to directly jump to a level without having to go through levels on the way. Also the current model is limited to defining the goals under each process area but the detail requirement of achieving this goal requires further research.

4. The model must be suitable for benchmarking with other organisations and industry best practices

It was agreed that for a model to be used in comparisons, it should have distinguishing capabilities to position organisations with different BCM maturity within the model.

5. The model must be based on a generally accepted best practices methodology
Since the development of this model is a bespoke version of existing best practice, this requirement has been met. The focus group also validated this by trying to map process areas with best practice existing in the field of BCM.

7. Conclusions

Given increasing regulation and rising competition in the UAE coupled with a demand for continuous and uninterrupted service, organisations in the UAE are beginning to pay attention to BCM. The extent to which they need to incorporate BCM in their organisations (IT-based, critical site-based, organisation wide or integrated) depends on the complexity and criticality of their businesses. Moreover, compliance to industry standards and regulators also drives decisions on the scope of BCM that an organisation intends to implement. Based on these observations, the maturity model developed serves as an analysis tool to aid organisations on how to achieve their target maturity. Thus, through the examination of the banking sector of the UAE, this paper addresses the need for a BCM maturity model. The research has yielded a highly successful BCM maturity model, which was validated through focus groups with BCM experts across ten banks in the UAE. The scope for broadening the model across organisational sectors is proven. It can further be stated that volatile sectors, such as the UAE construction sector, need great attention in this regard (Randeree and Chaudhry, 2012; Randeree and Chaudhry, 2007).

The reason for development of a BCM maturity model is based on the underlying assumption that a more mature BCM process will result in better business continuity capability/results. If an organisation has better control over BCM processes, it is also more likely to have a higher maturity level when tested.

References

BCI (2006), *BCI PAS 56 Audit Workbook*, available at: www.thebci.org (accessed 15 December 2008).

BCI (2007), *Business Guide to Continuity Management*, available at: www.thebci.org (accessed 15 March 2009).

BSI (1999), *Information Security Management: Part 1: Code of Practice for Information Security Management*, British Standards Institution, London.

Burt, D.N., Dobler, D.W. and Starling, S.L. (2003), *World Class Supply Management: The Key to Supply Chain Management*, 7th ed., McGraw-Hill, New York, NY.

Burtles, J. (2005), *PAS 56: 2003 an Overview from Automata*, p. 3, available at: www.automataservices.com (accessed 22 February 2012).

Dayan, R. and Evans, S. (2006), "KM your way to CMMI", *Journal of Knowledge Management*, Vol. 10 No. 1, pp. 69-80.

Digital Research, Inc (2002), *Business Continuity and Disaster Recovery Planning*, AT&T, Kennebunk, ME.

Dorfman, M. and Thayer, R.H. (1997), "Capability maturity model for software", in Dorfman, M. and Thayer, R.H. (Eds), *Software Engineering*, IEEE Computer Society Press, Los Alamitos, CA.

Elliott, D., Swartz, E. and Herbane, B. (1999), "Just waiting for the next big bang: business continuity planning in the UK finance sector", *Journal of Applied Management Studies*, Vol. 8 No. 1, p. 43.

Gilbert, G.A. and Gips, M.A. (2000), "Supply side contingency planning", *Security Management*, Vol. 44 No. 3, pp. 70-3.

IBM Global Services (2000), "Managing information technology in a new age", available at: www.ibm.com/services/whitepapers/gsw1178f.html (accessed 15 February 2009).

Kenny, J. (2006), "Strategy and the learning organization: a maturity model for the formation of strategy", *The Learning Organization*, Vol. 13 No. 4, pp. 353-68.

Koch, R. (2001), "Business continuity best practices", *Disaster Recovery Journal*, Vol. 14 No. 1, pp. 58-61.

KPMG (2006), *Information Security and Business Continuity: When Business is Not as Usual!*, KPMG, Sharjah.

Lockamy, A. III and McCormack, K. (2004), "The development of a supply chain management process maturity model using the concepts of business process orientation", *Supply Chain Management: An International Journal*, Vol. 9 No. 4, pp. 272-8.

Mingay, S. (2002), *Outlining the Gartner BCP Maturity Model*, Gartner Research Group, Stamford, CT.

Mohan, L. and Rai, S. (2006), "Business continuity model: a reality check for banks in India", *Journal of Internet Banking and Commerce*, Vol. 11 No. 2.

Niazi, M., Wilson, D. and Zowghi, D. (2005), "A maturity model for the implementation of software process improvement: an empirical study", *The Journal of Systems and Software*, Vol. 74, pp. 155-72.

Noakes-Fry, N. and Diamond, T. (2001), *Business Continuity Planning and Management: Perspective*, Gartner Research Group, Stamford, CT.

Paulk, M.C. (1995), *The Capability Maturity Model for Software*, Software Engineering Institute, Pittsburgh, PA.

Randeree, K. (2008), "Ethical leadership: a study of integrity in organizations in the Middle East", *Journal of Business Systems, Governance and Ethics* (*JBSGE*), Vol. 3 No. 4, pp. 57-67.

Randeree, K. (2010), "Leading change in organizations: a focus on quality management", in Westover, J.H. (Ed.), *Globalization, Labor and the Transformation of Work: Readings for Seeking a Competitive Advantage in an Increasingly Global Economy*, The University Press, Cambridge, MA, pp. 363-76.

Randeree, K. and Chaudhry, A.G. (2007), "Leadership in project managed environments: employee perceptions of leadership styles within infrastructure development in Dubai", *International Review of Business Research Papers*, Vol. 3 No. 4, pp. 220-32.

Randeree, K. and Chaudhry, A. (2012), "Leadership-style, satisfaction and commitment: an exploration in the United Arab Emirates' construction sector", *Engineering, Construction and Architectural Management*, Vol. 19 No. 1, pp. 61-85.

Randeree, K. and El Faramawy, A. (2011), "Islamic perspectives on conflict management within project managed environments", *International Journal of Project Management*, Vol. 29 No. 1, pp. 26-32.

Randeree, K. and Gaad, E. (2008), "Views on the 'knowledge economy project' of the Arabian Gulf: a gender perspective from the UAE in education and management", *The International Journal of Diversity in Organisations, Communities and Nations*, Vol. 8 No. 2, pp. 69-77.

Randeree, K. and Ninan, M. (2011), "Leadership and teams in business: a study of IT projects in the United Arab Emirates", *International Journal of Managing Projects in Business*, Vol. 4 No. 1, pp. 28-48.

Saleh, Y. and Alshawi, M. (2005), "An alternative model for measuring the success of IS projects: the GPIS model", *Journal of Enterprise Information Management*, Vol. 18 No. 1, pp. 47-63.

Savage, M. (2002), "Business continuity planning", *Work Study*, Vol. 51 No. 5, pp. 254-61.

SEI (2002), *The Rational Unified Process and the Capability Maturity Model'*, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA.

Shaw, G.L. and Harrald, J.R. (2004), "Identification of the core competencies required of executive level business crisis and continuity managers", *Journal of Homeland Security and Emergency Management*, Vol. 1, pp. 1-14.

Smit, N. (2005), "Business continuity management – a maturity model", Masters thesis, Erasmus University Rotterdam, from Erasmus University Thesis database (accessed 25 December 2006).

Zsidisin, G.A., Melnyk, S.A. and Ragatz, G.L. (2005), "An institutional theory perspective of business continuity planning for purchasing supply chain management", *International Journal of Production Research*, Vol. 43 No. 16, pp. 3401-20.

Further reading

Barnes, D. (2002), "The manufacturing strategy formation process in small and medium-sized enterprises", *Journal of Small Business and Enterprise Development*, Vol. 9 No. 2, pp. 130-49.

Randeree, K. (2009), "Strategy, policy and practice in the nationalisation of human capital: 'project emiratisation'", *Research and Practice in Human Resource Management*, Vol. 17 No. 1, pp. 71-91.

Appendix 1

AREA 1: BCM program management

Responsibility	A person placed high in the organisation hierarchy must be responsible for BCM. The person should have enough authority to over right functional reporting line for any person in case of a crisis
Budgeting	Importance of BCM in an organisation is determined based on whether it has a separate BCM budget and also how large is this budget?
Top management commitment	Successful BCM require resources and cooperation from various departments, which consider BCM as an added burden. So, commitment from the top management is necessary to drive BCM initiative
BCM charter/policy	A clear, transparent and communicated BCM policy/charter give the BCM program the right direction. It defines the scope and quality of the BCM process
Integration of BCM in other processes	Integration of BCM into other management processes and projects ensures pro active incorporation of continuity rather than considering continuity aspects at a later stage of projects or processes
BCM awareness	Without staff awareness, BCM can never be implemented as per their intention (scope and quality)

Table AI.

AREA 2: planning and analysis

Process analysis and selection of BCM methodology	Using a standard (industry specific) BCM methodology can clearly indicate the quality of the BCM process in an organisation
Quality of BIA	Whether or not an organisation has classified its business areas/system/processes based on their criticality, will indicate the scope of BIA and its associated quality
Quality of risk analysis	Same as "Quality of BIA". Whether or not an organisation identifies its critical processes and how it analysis the risks determines the quality of BCM process
Quality of selecting business recovery strategies	The way an organisation selects its business recovery strategies highlight the quality of BCM process. Whether this selection is based on result of BIA and RA?
Level of analysis	The extent of analysis – what minute details and dependencies are considered in BIA/RA will influence the quality of BCM in an organisation
Tuning with external stakeholders	The extent to which external stakeholders (vendors, suppliers, etc.) are involved in the BCM process also determines the quality of the BCM process

Table AII.

AREA 3: development of the BC plan

The number of available plans indicates the quality of the BCM process in an organisation	
Test plan	Describes the test (schedules based on the criticality of areas) for the BCM plans
Maintenance plan	Gives the procedure of how to maintain BCM plans. How can stakeholders communicate the changes?
Crisis communication plan	Highlights how communication should occur in case of a crisis? Responding to Media, etc.
Incident response plan	This gives the reactive measures to be undertaken in case of a crisis/disruption, parties involved, etc.
Security plan	Gives the preventive continuity measures
Escalation plan	Describes the procedures to be followed to be followed by staff in case of a disruption. Who to escalate and when? This forms a basis whether contingency plan must be activated or not?
Disaster recovery plan	Gives the recovery procedures of IT (corrective and repressive actions)
Process salvage and recovery plan	Describes, how critical processes can be resumed from an other site in case of a disaster and how to return back to "Business as usual"
Training plan	Describes the training (schedules) for the BC plans, which help in embedding BCM in the organisation's culture
Form of the plan	Not just having a plan is sufficient! What's important is whether it is written in a usable format?

Table AIII.

AREA 4: implementation

Execution of the plan	Whether an organisation considers BCM is an ongoing exercise, or a *ad hoc* project which has just started or already finished, will indicate the quality of the BCM process. Has the plan been executed in all facilities of the organisation? Does it cover all processes? Are the employees trained? All these are indicators of BCM quality
Disaster response organisation	Is there an execution of a virtual body, in case of a disaster, which will coordinate all activities (corrective and repressive measure)? Are the succession plans for key staff executed (preventive measure)? These also indicate the BCM process quality

Table AIV.

AREA 5: maintenance

Tests and exercises	Regular testing and exercising of plans under simulated or live situations, help in gaining confidence and prepare to face disasters. Whether the gaps arising out of tests are addressed or not, is also an indicator of the BCM process quality? Which facilities are tested? – is an indicator of BCM scope
Maintenance of all plans	An organisation must treat BCM as an iterative process. It should not remain as a project which is over some day. It should be treated as a cyclic process, keeping it up to date
BCM audit	An independent check on the BCM process can provide a useful insight and recommendations to improve

Table AV.

Appendix 2

I. SQB I: *ad hoc* – level 1 (technology):

a. Process area: BCM program management:

i. Goal 1: responsibility – not defined.

ii. Goal 2: budgeting – no dedicated budget for disaster planning.

iii. Goal 3: top management commitment – no commitment.

iv. Goal 4: BCM charter and policy – no format charter.

v. Goal 5: integration of BCM in other processes – no integration taken into consideration.

vi. Goal 6: BCM awareness – no training/awareness.

b. Process area: planning and analysis:

i. Goal 1: process analysis and selection of BCM methodology – no formal methodology in place.

ii. Goal 2: quality of BIA – no prioritisation of IT services based on their impact is in place. Quality of BIA is very low.

iii. Goal 3: quality of risk analysis – low quality as no formal risk assessment is undertaken.

iv. Goal 4: quality of selecting business recovery strategies – low quality as it is not based on BIA or RA.

v. Goal 5: level of analysis – only limited to certain IT services without any process related dependencies/integration.

vi. Goal 6: tuning with external stakeholders – no external stakeholder dependencies taken into consideration.

c. Process area: development of BCM plan:

i. Goals 1: test plan – do not exist.

ii. Goal 2: maintenance plan – do not exist.

iii. Goal 3: crisis communication plan – do not exist.

iv. Goal 4: incident response plan – do not exist.

v. Goal 5: security plan – do not exist.

vi. Goal 6: escalation plan – may or may not exist as a part of BAU.

vii. Goal 7: disaster recovery plan – may exist for random systems.

viii. Goal 8: process salvage and recovery plan – do not exist.

ix. Goal 9: training plan – do not exist.

x. Goal 10: format of the plan – not very easy. Cumbersome in nature.

d. Process area: implementation:

i. Goal 1: execution of the plan – only for random systems. Does not prioritise the critical ones.

ii. Goal 2: disaster response organisation – do not exist.

e. Process area: maintenance:

i. Goal 1: tests and exercises – not tested or exercised. May happen for one odd case during implementation of the system.

ii. Goal 2: maintenance of all plans: no formal process in place.

iii. Goal 3: BCM audit – not audited.

II. SQB II: managed – level 1 (technology):

a. Process area: BCM program management:

i. Goal 1: responsibility – a middle level IT manager.

ii. Goal 2: budgeting – no dedicated budget but part of IT budget.

iii. Goal 3: top management commitment – low commitment.

iv. Goal 4: BCM charter and policy – charter is a part of IT services charter. No dedicated BCM charter.

v. Goal 5: integration of BCM in other processes – integration is limited to mission critical systems.

vi. Goal 6: BCM awareness – limited training/awareness to mission critical systems.

b. Process area: planning and analysis:

i. Goal 1: process analysis and selection of BCM methodology-methodology is a part of IT services.

ii. Goal 2: quality of BIA – basic first level BIA is conducted to identify mission critical systems. Quality is still low.

iii. Goal 3: quality of risk analysis – detailed RA is not done. Only a high level RA is carried out.

iv. Goal 4: quality of selecting business recovery strategies – quality is moderate as basic BIA and RA is conducted.

v. Goal 5: level of analysis – only limited to certain critical IT services with direct process related dependencies/integration.

vi. Goal 6: tuning with external stakeholders – no external stakeholder dependencies taken into consideration.

c. Process area: development of BCM plan:

i. Goals 1: test plan – exists.

ii. Goal 2: maintenance plan – do not exist.

iii. Goal 3: crisis communication plan – do not exist.

iv. Goal 4: incident response plan – do not exist.

v. Goal 5: security plan – exists.

vi. Goal 6: escalation plan – exists.

vii. Goal 7: disaster recovery plan – exists for mission critical systems.

viii. Goal 8: process salvage and recovery plan – exists.

ix. Goal 9: training plan – may or may not exist.

x. Goal 10: format of the plan – not very easy. Cumbersome in nature.

d. Process area: implementation:

i. Goal 1: execution of the plan – only for critical systems.

ii. Goal 2: disaster response organisation – may or may not exist. It may be defined but never practiced.

e. Process area: maintenance:

i. Goal 1: tests and exercises – only tested for mission critical systems.

ii. Goal 2: maintenance of all plans: no formal process in place.

iii. Goal 3: BCM audit – audited as a part of IT.

III. SQB III: defined – level 1 (technology):

a. Process area: BCM program management:

i. Goal 1: responsibility – a senior level IT manager.

ii. Goal 2: budgeting – dedicated budget for BCM.

iii. Goal 3: top management commitment – high commitment.

iv. Goal 4: BCM charter and policy – dedicated BCM charter.

v. Goal 5: integration of BCM in other processes – integration is limited to mission critical systems. All processes, people and facilities dependencies are taken into account.

vi. Goal 6: BCM awareness – good amount of training and awareness exists.

b. Process area: planning and analysis:

i. Goal 1: process analysis and selection of BCM methodology – best practice BCM practices are followed.

ii. Goal 2: quality of BIA – detailed BIA is conducted to prioritise business processes and underlying IT systems.

iii. Goal 3: quality of risk analysis – detailed RA is done covering all aspects of business processes.

iv. Goal 4: quality of selecting business recovery strategies – quality is good as it is based on BIA and RA.

v. Goal 5: level of analysis – covers all critical IT services with process related dependencies/integration. Less priority systems are also covered.

vi. Goal 6: tuning with external stakeholders – external stakeholder dependencies are considered for mission critical systems/processes.

c. Process area: development of BCM plan:

i. Goals 1: test plan – exists.

ii. Goal 2: maintenance plan – exists.

iii. Goal 3: crisis communication plan – exists.

iv. Goal 4: incident response plan – exists..

v. Goal 5: security plan – exists.

vi. Goal 6: escalation plan – exists.

vii. Goal 7: disaster recovery plan – exists for all systems.

viii. Goal 8: process salvage and recovery plan – exists.

ix. Goal 9: training plan – exists.

x. Goal 10: format of the plan – easy and user friendly.

d. Process area: implementation:

i. Goal 1: execution of the plan – covers all systems and underlying processes, people, infrastructure, etc..

ii. Goal 2: disaster response organisation – exists. A virtual body is identified which would be activated to handle disasters. Other supporting groups like logistics and IT support are also identified.

e. Process area: maintenance:

i. Goal 1: tests and exercises – all plans are tested. Especially mission critical ones are tested every year.

ii. Goal 2: maintenance of all plans: plans are maintained on a regular basis. This could be triggered by test results, process changes, incidents, etc.

iii. Goal 3: BCM audit – a separate audit is carried out.

IV. SQB IV: integrated – level 1 (technology):

a. Process area: BCM program management:

i. Goal 1: responsibility – a senior level IT manager.

ii. Goal 2: budgeting – dedicated budget for BCM.

iii. Goal 3: top management commitment – high commitment.

iv. Goal 4: BCM charter and policy – dedicated BCM charter, which covers external stakeholders.

v. Goal 5: integration of BCM in other processes – integration for all systems, processes, people and facilities dependencies are taken into account.

vi. Goal 6: BCM awareness – good amount of training and awareness exists including supply chain training.

b. Process area: planning and analysis:

i. Goal 1: process analysis and selection of BCM methodology – best practice BCM practices are followed and in certain cases modified according to the organisation's culture.

ii. Goal 2: quality of BIA – detailed BIA is conducted to prioritise business processes and underlying IT systems.

iii. Goal 3: quality of risk analysis – detailed RA is done covering all aspects of business processes.

iv. Goal 4: quality of selecting business recovery strategies – quality is good as it is based on BIA and RA.

v. Goal 5: level of analysis – covers all IT services with process related dependencies/integration with supply chain and cross functional processes.

vi. Goal 6: tuning with external stakeholders – external stakeholder dependencies are taken into consideration for all systems/processes.

c. Process area: development of BCM plan:

i. Goals 1: test plan – exists.

ii. Goal 2: maintenance plan – exists.

iii. Goal 3: crisis communication plan – exists.

iv. Goal 4: incident response plan – exists.

v. Goal 5: security plan – exists.

vi. Goal 6: escalation plan – exists.

vii. Goal 7: disaster recovery plan – exists for all systems.

viii. Goal 8: process salvage and recovery plan – exists.

ix. Goal 9: training plan – exists.

x. Goal 10: format of the plan – easy and user friendly.

d. Process area: implementation:

i. Goal 1: execution of the plan – covers all systems and underlying processes, people, infrastructure, etc. Also these are tested.

ii. Goal 2: disaster response organisation – exists. A virtual body is identified which would be activated to handle disasters. Other supporting groups like logistics and IT support are also identified and trained.

e. Process area: maintenance:

i. Goal 1: tests and exercises – all plans are tested. Especially mission critical ones are tested twice a year and less priority one once a year.

ii. Goal 2: maintenance of all plans: plans are maintained on a regular basis. This could be triggered by test results, process changes, incidents, etc..

iii. Goal 3: BCM audit – a separate audit is carried out. These include both external as well as internal audit.

V. SQB V: optimised – level 1 (technology):

a. Process area: BCM program management:

i. Goal 1: responsibility – a senior level IT manager or BCP manager reporting to CEO or COO.

ii. Goal 2: budgeting – dedicated budget for BCM.

iii. Goal 3: top management commitment – high commitment.

iv. Goal 4: BCM charter and policy – dedicated BCM charter, which covers external stakeholders and reviewed regularly.

v. Goal 5: integration of BCM in other processes – integration for all systems, processes, people and facilities dependencies are taken into account.

vi. Goal 6: BCM awareness – good amount of training and awareness exists including supply chain training. External training is also included.

b. Process area: planning and analysis:

i. Goal 1: process analysis and selection of BCM methodology – best practice BCM practices are followed and in certain cases modified according to the organisation's culture.

ii. Goal 2: quality of BIA – detailed BIA is conducted to prioritise business processes and underlying IT systems. BIA also covers the non availability of supply chain elements.

iii. Goal 3: quality of risk analysis – detailed RA is done covering all aspects of business processes.

iv. Goal 4: quality of selecting business recovery strategies – quality is good as it is based on BIA and RA.

v. Goal 5: level of analysis – covers all IT services with process related dependencies/integration with supply chain and cross functional processes.

vi. Goal 6: tuning with external stakeholders – external stakeholder dependencies are taken into consideration for all systems/processes.

c. Process area: development of BCM plan:

i. Goals 1: test plan – exists.

ii. Goal 2: maintenance plan – exists and updated regularly.

iii. Goal 3: crisis communication plan – exists.

iv. Goal 4: incident response plan – exists.

v. Goal 5: security plan – exists.

vi. Goal 6: escalation plan – exists.

vii. Goal 7: disaster recovery plan – exists for all systems.

viii. Goal 8: process salvage and recovery plan – exists.

ix. Goal 9: training plan – exists.

x. Goal 10: format of the plan – easy and user friendly.

d. Process area: implementation:

i. Goal 1: execution of the plan – covers all systems and underlying processes, people, infrastructure, etc. Also these are tested.

ii. Goal 2: disaster response organisation – exists. A virtual body is identified which would be activated to handle disasters. Other supporting groups like logistics and IT support are also identified and trained.

e. Process area: maintenance:

i. Goal 1: tests and exercises – all plans are tested. Especially mission critical ones are tested twice a year and less priority one once a year. Crisis management plans and

disaster recovery teams undergo regular drills and results are captured to make changes to existing plans.

ii. Goal 2: maintenance of all plans: plans are maintained on a regular basis. This could be triggered by test results, process changes, incidents, etc..

iii. Goal 3: BCM audit – a separate audit is carried out. These include both external as well as internal audit. Recommendations are incorporated in the plans.

These first five levels give the process quality for technology. Similarly these five levels will be repeated across each of the scope areas, i.e. facilities management (premises), processes, people and organisational soft issues:

VI. SQB VI: *ad hoc* – LEVEL 2 (facilities management).

VII. SQB VII: managed – level 2 (facilities management).

VIII. SQB VIII: defined – level 2 (facilities management).

IX. SQB IX: integrated – level 2 (facilities management).

X. SQB X: optimised – level 2 (facilities management).

XI. SQB XI: *ad hoc* – level 3 (processes).

XII. SQB XII: managed – level 3 (processes).

XIII. SQB XIII: define – level 3 (processes).

XIV. SQB XIV: integrated – level 3 (processes).

XV. SQB XV: optimised – level 3 (processes).

XVI. SQB XVI: *ad hoc* – level 4 (people).

XVII. SQB XVII: managed – level 4 (people).

XVIII. SQB XVIII: defined – level 4 (people).

XIX. SQB XIX: integrated – level 4 (people).

XX. SQB XX: optimised – level 4 (people).

XXI. SQB XXI: *ad hoc* – level 5 (organisational soft issues).

XXII. SQB XXII: managed – level 5 (organisational soft issues).

XXIII. SQB XXIII: defined – level 5 (organisational soft issues).

XXIV. SQB XXIV: integrated – level 5 (organisational soft issues).

XXV. SQB XXV: optimised – level 5 (organisational soft issues).

Corresponding author
Kasim Randeree can be contacted at: kasim.randeree@sbs.ox.ac.uk