

Is Business Continuity Management a Misnomer?

Business Continuity Management at the Crossroads

By Luc P. Klein MBA*

For more than ten years business continuity management (BCM) has been on the priority list of senior managers because of events such as Y2K, the implementation of the Euro, terrorist attacks, natural disasters like hurricanes, earthquakes, floods and tsunamis, and pandemic outbreaks such as SARS, H1N1 and Mexican Flu. Additionally, in some sensitive industries such as the financial sector, regulators increasingly require banks to have effective BCM measures in place.

This paper discusses why business continuity management, as a discipline and as perceived by many today, is at the crossroads of direction and focus. In fact, BCM does not currently fully cover the actual meaning of the term *business continuity*, to the extent that one could ask: Is business continuity management a misnomer?

Background

Business continuity management has evolved significantly over the recent decades. Twenty to thirty years ago, business continuity management was predominantly focused on IT, including communication and data centres. It was known as IT disaster recovery planning, IT fall back planning, resilience planning and so on. Parts of it were and still are backup and restore procedures.

Today, business continuity is concerned with “the capability of an organisation to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable pre-defined level.”¹ An incident is defined as a “situation that might be, or could lead to, a business disruption, loss, emergency or crisis.”² This, indeed, is a very broad and almost all encompassing definition.

Business continuity management, according to the British Standard 25999³, is a “holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.”⁴

However all encompassing these definitions of business continuity and incident are, BCM is too often – if not always – focused on operations, typically embodied by the following four types of plan documents:

- Crisis management plan (CMP) – often a high level organisational plan that includes when the CMP will be invoked and by whom, names and contact details of the crisis team members, their roles and responsibilities, contact details of relevant third parties, including the authorities, and the relationship with the underlying business continuity plan or plans (BCP or BCPs) and a disaster recovery plan or plans (DRP or DRPs). Part of a CMP is a crisis communications plan outlining who will or should be the spokesperson(s) on behalf of the organisation and how and what will be

communicated to its employees and their families, the authorities, clients and business partners, shareholders and financial analysts community, the media, and the general public at large, all depending of course on the nature and extent of the crisis.

- Emergency response plan (ERP) – detailed plan concerning the immediate response to a disaster and subsequent evacuation of people from a building, plant or site.
- Business continuity plan (BCP) – detailed plan concerning the relevant and necessary steps to be taken by the business to continue its operations, often at a different, alternative location.
- Disaster recovery plan (DRP) – detailed plan concerning the recovery, restoration and resumption of ICT functions, often at a secondary site.

BCM plans will be activated when a defined interruption occurs, such as a large explosion in a plant. This means that senior and executive management will be involved in managing and resolving the incident. One could compare this situation with a situation where a government calls out an emergency, for example after a massive flood, after which special funds and aid will be made available, where these resources otherwise would not have been available to the flooded region.

In short, the emphasis thus lies on the continuation of operations in case of a (major) incident or disruption.

Why is BCM difficult to understand?

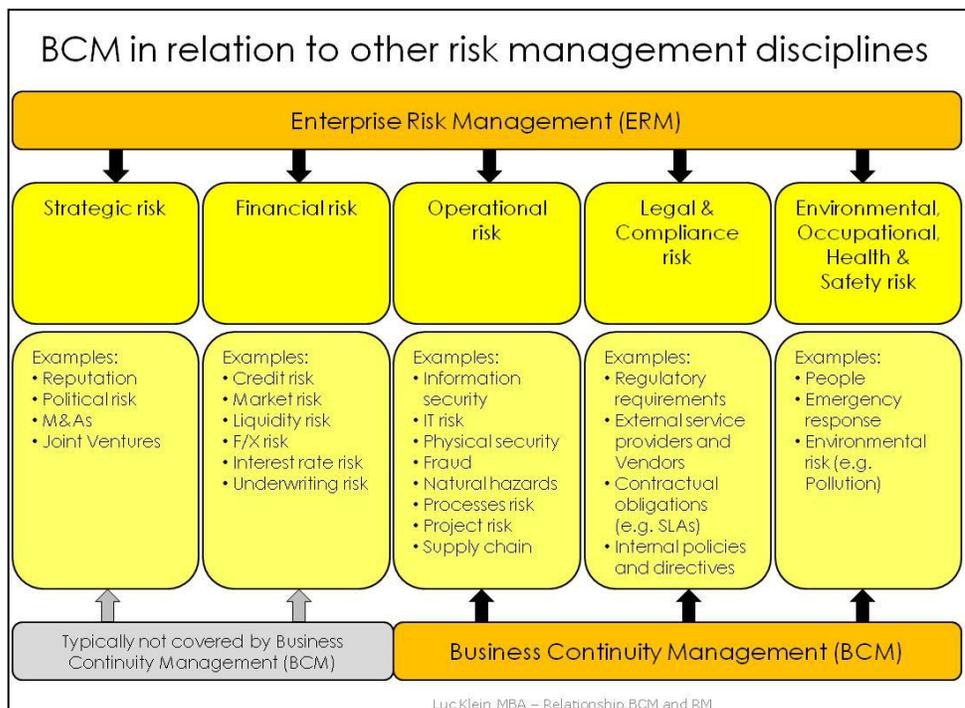
People who are not familiar with BCM and what it means often find it difficult to understand the concept of BCM for various reasons.

Historically, the business has placed the responsibility for developing and maintaining any business continuity management plan with the IT department. Despite increasing awareness that the business should be in the driver's seat and take control, many still perceive BCM as being an ICT responsibility. "This should not be the case as disaster recovery concerns a bigger part of the company than just IT", according to Michael Rasmussen, an internationally renowned Governance Risk & Compliance (GRC) research expert.⁵ This would certainly seem to be robust thinking, when taking into account that any business amounts to considerably more than just IT. The decision about which products or services, supporting processes, tools, assets, people, value chain partners, and dependencies are business critical in case of a disaster, therefore, should not rest with the IT division but with the business.

Secondly, BCM managers and practitioners sometimes find it difficult to make a business case that outlines the level of investment and the financial rewards/benefits to the organisation. Without a clear quantifiable return on investment (ROI), senior management will find it hard to justify the allocation of funds and resources to such initiatives, or any initiative for that matter. Benefits, however, are not always clear and transparent. In this case it would not be dissimilar to, for example, paying taxes or insurance premiums: as long as you do not need it, it is easy to only see the costs involved rather than the benefits as well. In certain sensitive industries, like the financial sector, regulators such as APRA (Australia), FSA (UK), DNB (the Netherlands) and ECB (European Union) do comprehend the importance of having in place effective BCM measures by systemic important financial sector participants, which

definitely underscores the importance of BCM to safeguarding organisations' value in crisis situations (and in this instance, the wider community at large).

Thirdly, the recent financial and economic crisis worldwide has given a different meaning altogether to the meaning of *business continuity* as perceived by many in the BCM industry, with the collapse or near collapse of many financial institutions, having spilled over to the *real* economy. In this context, it is important to understand the relationship of BCM and other risk management disciplines. These other risk management disciplines combined form enterprise risk management and consist of strategic, financial, operational, legal & compliance, and environmental, occupational health & safety risk management (see diagram below). One could argue that in the diagram below operational, legal & compliance, and environmental, occupational health & safety are all part of operational risk. The breakdown depicted, however, is not dissimilar to what large organisations do. For example, the world's second largest human resources services company, Randstad Holding NV, identifies and classifies types of risk both at Group and Operating Company level as either strategic, financial, operational or compliance risks.⁶ Not surprisingly, business continuity management – as a discipline – often if not always concerns a risk event that has occurred, which has interrupted business operations and which risk event typically falls under operational, legal & compliance, or environmental, occupational health & safety risks.



As depicted in the diagram, risk events that occur from a strategic or financial risk exposure are typically not covered by BCM, with the exception of reputation risk and perhaps political risk. For example, the risk of business discontinuity due to strategic decisions by executive management in regard to mergers and acquisitions and joint ventures would normally not fall within the scope of BCM. Other examples include the level of risk appetite, the level of gearing, or what to think about a company's culture? The point here is that contrary to the all encompassing definitions of business continuity, business continuity

management and incident, the reality is that the “daily” practice of BCM has a limited scope of risk events by not including strategic and financial risk events. To people not familiar to the BCM discipline (and they may indeed include senior and executive managers!) this may sound strange as hedging foreign exchange exposure, by way of example, may certainly constitute a business continuity risk exposure. This and other examples will be explored further in this paper.

Difference between (enterprise) risk management and business continuity management

Enterprise risk management (ERM) is considered *top-down*, as it looks at preventive measures to mitigate risks that would otherwise have an adverse impact on the organisation. ERM is concerned with both cause and consequence of any type of risk, where BCM is not about the cause of the disaster (a worst case scenario) but rather the response to and the impact of the disaster no matter the cause. BCM is concerned with what happens if the (ERM) controls fail. In other words, if something, a disaster, happens: What do you do? Who does what? The BCM bottom-up approach complements the top-down approach inherent in the over-arching risk management process.⁷

What is missing?

The problem lies in that there are many other events to consider that may jeopardise the continuity of an organisation, while at the same time no BCM plans are being activated.

As stated earlier, the recent financial and economic crisis worldwide has given a different meaning to the term *business continuity*, with the collapse or near collapse of many financial institutions, spilling over to the *real* economy. In many cases the value of assets in whatever form or shape, combined with diminished and shortage of liquidity, were often the cause of putting organisations into default and ultimately into receivership.

Other examples of events not usually considered by BCM include:

- **Fraud** – Fraud activities typically do not trigger the invocation of a business continuity or (IT) disaster recovery plan (BCP/DRP), while at the same time it can constitute a serious threat to the continuity of organisations. The epitome of fraud that ultimately has led to the demise of organisations are the cases of Barings Bank and Enron, and certainly did cost Société Générale dearly.
- **Reputation**
 - In 2002, Arthur Andersen voluntarily surrendered its licenses to practice as Certified Public Accountants in the United States after being found guilty of criminal charges relating to the firm's handling of the auditing of Enron, the energy corporation, resulting in the loss of 85,000 jobs worldwide. However, the verdict was subsequently overturned by the Supreme Court of the United States. Whilst still technically a business, having not filed for bankruptcy or dissolved, Arthur Andersen is no longer viable, as the brand name was too damaged in its reputation to continue as a firm.⁸

- After the terrorist bomb on a PanAm airplane above the Scottish town of Lockerbie, travellers avoided flying with PanAm, which ultimately resulted in the demise of the company.⁹
 - After almost 170 years, the UK newspaper News Of The World printed its last edition on 10 July 2011 in response to various phone hacking scandals. The allegations led to a public backlash and the loss of advertising revenue, as a number of companies advertising with the paper pulled out pending an investigation. Amid these allegations, the endeavours of its (ultimate) parent company News Corp, to take full control over BSkyB received strong political opposition and public outcry, which has forced News Corp to back down, at least for the time being. Following these developments, the share price of News Corp fell dramatically wiping off more than US\$7 billion of its value in a few days in July 2011.¹⁰
- **Joint Ventures / Mergers & Acquisitions**
 - The decision of Fortis to take over (parts of) ABNAMRO proved too burdensome, ultimately resulting in the sale of large parts of the Fortis business to various parties. This meant the end of the Fortis brand, at least in the Netherlands.¹¹
 - When Royal Philips Electronics sold eighty percent of its semi-conductors division to a panel of private investors including Kohlberg Kravis Roberts & Co. (KKR), the buy-out was financed by means of bonds sold by NXP, the new name of the former Philips division. Due to the economic and financial slowdown resulting in decreased turnover and profits turned into losses, NXP found itself in a position that paying interest became a burden. In fact, it had slid out of the top ten position (even top twenty, according to DataWeek in 2009¹²) of global semiconductors. As a consequence NXP sold some of its operations.¹³
 - **Hedging** – The world’s largest lead and zinc company at the time, Pasminco Ltd, was put into voluntary administration after it had wrongly hedged its foreign exchange risk and the losses, combined with record low zinc prices and high gearing (high levels of debt), became too large to bear.¹⁴
 - **Pricing and services** – HIH Insurance, at the time the second largest general insurance company in Australia, went into receivership after a period of poorly conceived and even more poorly executed management decisions. These included the failure to provide adequately for future claims, called *under reserving or under provisioning*, and re-entering the Workers Compensation insurance domain in California, USA¹⁵, at a time when other insurance companies shied away from it due to increased long-tail risks and premiums capped by the Californian government.
 - **Major trend breaks** – Misjudgements or misreading market or technology developments by organisations may also lead to the discontinuation of a product, service or indeed an entire company. For example, when the old Polaroid Corporation filed for bankruptcy in 2001, it was widely believed to be the result of the failure of its senior management to anticipate the effect of digital cameras and one-hour photo shops on its film business.^{16 17}

It is safe to say that in all of these instances none of the previously mentioned BCM plan documents were activated, let alone that secondary sites have come into active operations.

Business Continuity versus Operations Continuity?

The current definition of business continuity, incident and business continuity management as defined in the BS25999 suggests the inclusion of all kind of threats to the continuity of a business. This, however, is not normally the case, as we have seen.

Most if not all BCM managers and BCM practitioners only look at operational issues in regard to BCM, as is depicted above. To others, however, business continuity risks may extend to include strategic and financial risks, whose impacts are typically not currently covered by BCM plans.

There are two ways to overcome the current mismatch between the term *business continuity* as used mostly by BCM practitioners on one hand and perceived by other people, mostly outside the BCM community on the other hand.

1. Either the term *business continuity* as used by (mostly) the BCM practitioners and BCM community at large should be broadened to include the impact of strategic and financial risks. The question then remains what the relationship will be between, for example, the situation where diminished liquidity jeopardises the continuity of the business and the invocation of a BCM plan (and which BCM plan?). This obviously is still a green field which will need to be further explored. For example, this may require a new way of thinking, including the development of new types of BCM plan document(s) to address the impacts of strategic and financial risks. One could argue that – to a certain degree – banks already provide a form of business continuity test with regard to certain forms of financial risks by conducting stress tests for these exposures. The latest stress test of July 2011, however, attracted much criticism in that sovereignty risk was not part of the stress test.

In his article “Six Ways Companies Mismatch Risk” (HBR, March 2009, pages 86-94), Rene M. Stulz strongly promotes that (financial) risk managers should augment the (risk management) models with scenario analysis. Instead of focusing on the fact that the probabilities of catastrophic risks are extremely small, risk managers should build scenarios for such risks to understand the various ways a crisis might unfold and the organisation should design strategies for surviving them. In other words take a leaf from the disaster management handbook. Stulz calls this “sustainable risk management.”¹⁸

2. Or is the term *business continuity* indeed a misnomer? Should it be altered to *operations continuity* instead, and subsequently BCM changes to OCM or Operations Continuity Management, to better reflect what is actually meant? And does the current all encompassing definition of, for example incident, need to be narrowed down to align with the “daily” practice of BCM being actually OCM? An alternative term could be Operational Resilience Management, however, its abbreviation ORM would be confused with ORM as in Operational Risk Management.

In the latter case (change to OCM), no other changes are required to the current situation. However, in case of the former, the BCM discipline including the work of BCM managers and BCM practitioners, will (have to) become much more comprehensive....and, to some, more interesting!

Maintaining the status quo and leaving the current term as it is, will mean that the current mismatch and confusion – especially outside the BCM community – will remain.

Conclusion

Business continuity management has evolved significantly in the past decade. It is simply inconceivable to run an organisation today without having proper business continuity management measures in place to preserve the organisation's reputation and shareholder value, as well as its sustainability in crisis situations. However, business continuity management is now at the crossroads. One direction is for BCM to "own up" to being exclusively focused on operations continuity, in which case it needs a name change to better reflect its intent and scope. A change in definitions will also be required to align with what is actually already "daily" practice.

In the other direction, business continuity management must become broader by extending its current operations focus to include the impacts of strategic and financial risks. By including both strategic and financial risk, business continuity management would be truly about managing the continuity of the business, rather than solely its operations. Indeed, BCM would be well-positioned to enable senior and executive management to be better prepared to manage future crisis situations, regardless the type of threat....and against any kind of worst case scenario.....

About the author:



**Luc P. Klein MBA is a Senior Business Consultant, within the Governance, Risk & Compliance (GRC) practice of Logica Business Consulting. Logica is a business and technology service company, employing 41,000 people. It provides business consulting, systems integration and outsourcing to clients around the world, including many of Europe's largest businesses. Luc Klein's area of GRC expertise includes business continuity management. He has consulted to a large variety of organisations, ranging from global organisations to medium size enterprises, in many industry sectors including financial services, oil/energy and the public sector, and in various countries including Australia, the UK, Germany and the Netherlands. He has been a guest speaker at conferences in the UK, the Netherlands and France; and was a guest lecturer at universities in Hong Kong and the Netherlands. He has published and co-authored various articles on GRC related topics. Luc can be contacted at: luc.klein@logica.com*

End Notes:

¹ British Standard 25999-1:2006 Business Continuity Management – Part 1: Code of practice, section 2.2 Business Continuity

² Id, section 2.18 Incident

³ It is acknowledged that the current BCM standard, BS25999, most likely will be replaced by the ISO 22301.

However, this may well be in early 2012 or even later, according to "ISO 22301 update" on [continuitycentral.com](http://www.continuitycentral.com), <http://www.continuitycentral.com/news05729.html>, accessed 22 July 2011, and respectively "ISO Update",

Chapter News, July 2011, Australasian Chapter, BSI,

http://www.thebci.org.au/images/documents/news/40_BCI%20Chapter%20Newsletter%20-%20July%202011.pdf, accessed 25 July 2011

⁴ British Standard 25999-1:2006 Business Continuity Management – Part 1: Code of practice, section 2.3 Business continuity management (BCM)

⁵ Thomas, Daniel, “Major disasters and minor downtime: are you ready?”, Computing, 9 Feb 2006, <http://www.computing.co.uk/ctg/feature/1858940/major-disasters-minor-downtime-ready>, accessed 15 July 2011

⁶ 2010 Annual Report, page 58, Randstad Holding NV, <http://www.ir.randstad.com/downloads.cfm> accessed 13 July 2011

⁷ Australian National Audit Office, “Business Continuity Management, Keeping the wheels in motion, A Guide to Effective Control”, page 8, January 2000

⁸ Wikipedia, the free encyclopedia, “Arthur Andersen”, http://en.wikipedia.org/wiki/Arthur_Andersen, accessed 13 July 2011

⁹ Reed, Dan, “Pan Am about to make its final exit”, USA Today, updated 31 Oct 2006, http://www.usatoday.com/money/biztravel/2006-10-30-pan-am-usat_x.htm accessed 21 July 2011

¹⁰ De Telegraaf, “Murdoch verliest \$7 miljard”, (English: “Murdoch loses US\$7 billion”), http://www.telegraaf.nl/incoming/10187025/_Murdoch_verliest_7_miljard_.html?p=32,1 accessed: 13 July 2011

¹¹ Smit, Jeroen, “The Perfect Prey: The Fall of ABN Amro, or, What Went Wrong in the Banking Industry?”, Quercus, 2009

¹² “Top 20 semiconductor companies shakeup”, June 2009, <http://www.dataweek.co.za/article.aspx?pklaarticleid=5687>, accessed: 21/07/2011

¹³ Crooijmans, Hans, “NXP semiconductors, Haalt NXP de kerstdagen nog wel?”, Management Team, 25 May 2009, <http://www.mt.nl/157/11262/magazine/nxp-semiconductors.html>, accessed: 21 July 2011

¹⁴ Sydney Morning Herald, “How poor choices Savaged Pasmenco”, 13 July 2002 <http://www.smh.com.au/articles/2002/07/12/1026185108351.html>, accessed: 13 July 2011

¹⁵ The HIH Royal Commission, The Hon Justice Owen, Commissioner, “The failure of HIH Insurance”, Volume I, a corporate collapse and its lessons, 4 April 2003 http://www.hihroyalcom.gov.au/finalreport/Front%20Matter,%20critical%20assessment%20and%20summary.HTM#_Toc37086537, accessed: 13 July 2011

¹⁶ Polaroid Corporation http://en.wikipedia.org/wiki/Polaroid_Corporation, accessed 18 July 2011

¹⁷ Schepp, David, “Bankruptcy looms for Polaroid”, BBC News Online, 11 October 2001, <http://news.bbc.co.uk/2/hi/business/1593976.stm>, accessed 18 July 2011

¹⁸ Stulz, Rene M., “Six Ways Companies Mismanage Risk”, Harvard Business Review, pages 86-94, March 2009.
