A roadmap to measure and achieve enterprise operational resiliency

Karen Dye and Margaret Langsett

Received: 9th October, 2008

Global Crisis Management, Sun Microsystems, 1790 East River Road, Suite 213, Mailstop UTUS01, Tucson, AZ 85718, USA
Tel: +1 877 830 0888; E-mail: karen.dye@sun.com

Karen Dye *is Director of the Crisis Management, Emergency Response and Business Continuity Programmes for the Sun Microsystems Risk Management division. Ms Dye is a Certified Business Continuity Planner, Business Continuity Institute Member, and a Certified Business Continuity Maturity Model® Assessor. She earned her undergraduate degree from the University of San Francisco and her MBA from Pepperdine University. She is a current member of the Business Recovery Manager's Association and served on their Board of Directors from 1998 to 2003. She is also a member of the Phoenix Chapter of the Association of Contingency Planners, International Association of Emergency Managers and the Risk and Insurance Management Society.*

Margaret Langsett *is Executive Vice President for Virtual Corporation, which she co-founded in 1994. Ms Langsett has over 25 years of experience in business continuity, methodology training and support, and programme content development. She is a Certified Business Continuity Maturity Model® Assessor and Licensed BCMM® Trainer. She is frequent speaker on business continuity, crisis management, security management and technology recovery topics. In addition to her corporate responsibilities and extensive marketing background, she was Project Manager for the creation of the Business Continuity Maturity Model® and is responsible for its global distribution.*

Journal of Business Continuity & Emergency Planning
Vol. 3 No. 1, pp. 38–46

ABSTRACT

This paper presents a case study of how a multinational company researched and implemented a model for business continuity maturity measurement. While most best practices, standards and guidelines discuss what needs to be done, this tool takes it to the next step, measuring how well the project application is progressing. The techniques described can be applied to almost any benchmarking tool that is currently available. The case study describes customisation opportunities for usage elsewhere within the organisation and the process of developing a roadmap to enable a focused crisis management and business continuity improvement programme. A gap analysis is key to the development of the roadmap to ensure focus on the right activities.

Keywords: benchmarking, operational resiliency, business continuity, BCP programme measurement

INTRODUCTION

In 2005, there was an internal audit of Sun's business continuity programme management office (PMO). The audit recommended obtaining senior management approval for achieving and maintaining enterprise-level operational resiliency. The challenge was first to define operational resiliency, and then to determine how to measure it. The PMO

viewed this as an opportunity as internal audit findings are reported to the board of directors' audit committee. Business continuity status had historically been reported annually to the audit committee, but previous reports focused on what had been accomplished, as opposed to what needed to be done.

The company operates in over 100 countries and has 34,900 employees worldwide. For the financial year ending in 2008 (FY08), revenue was $13.8bn. The company is in the high-tech industry, providing network computing infrastructure solutions, with a diversity of software, systems, storage, services and microelectronics that power everything from consumer electronics to development tools and large, powerful data centres. It has traditionally been a product-focused organisation, moving towards a more service orientation. Product revenue for FY08 was 62 per cent of sales, which has gradually decreased over the past several years. Service revenue for FY08 was 38 per cent of sales, gradually increasing over the past several years. Research and development was 13 per cent of sales in FY08, gradually decreasing over the past several years.

The company has a highly developed and mature (>10 years) flexible work strategy. Worldwide, only 25 per cent of employees have assigned offices, 60 per cent are flexible, and only come into the office 2–3 days per week (aka 'hotelling'), while the other 15 per cent work entirely from home. The flexible work strategy is embedded within the corporate culture, allowing for ease of conference calls and remote activities. This has proven to be extremely valuable from a business continuity and recovery strategy perspective.

Policy is developed at the corporate level and defined at a fairly high level, with decision making being extremely decentralised. Outside the USA, each country manager functions as the CEO within each country. One of the challenges for the PMO has been that the business groups are extremely vertical, while crisis management and business continuity is horizontal.

The crisis management and business continuity PMO sets policy, defines the methodology, designs templates and provides training. All plans are owned by the business groups and supporting functions. The PMO has two executive champions: the chief financial officer is the executive champion for business continuity, while the chief human resources officer is the champion for crisis management and emergency response. Each business group has an executive sponsor who reports directly to an executive vice president. The executive sponsor ensures the appropriate level of resources within the business group and approves criticality tiers. There is also a business continuity coordinator who is more tactical and coordinates the plan development within each business group.

The crisis management structure includes a corporate team with representation from security, HR, IT, finance and other key functions. These same functions are represented locally at each of the 27 regional crisis management teams. The incident command system is used at the local level for emergency response.

BACKGROUND

It is important to measure the maturity of a business continuity programme (BCP) because it directly reflects how business continuity has matured as a discipline.

During the 1960s and 1970s, companies realised they needed to backup their electronic data and have contingency plans for alternate data centres — usually provided by a third party. Most of

the vulnerabilities were power outages, with the occasional hardware or software outage on the mainframe. Technology was expensive and personnel were usually focused on the more clerical and task-oriented activities. Data processing was primarily batch processing.

In the 1980s and 1990s, the focus was still only on IT-based recovery solutions, with some increase in real-time computing. Large financial institutions began to see the need for more emphasis on business recovery. Regulations became a concern and there was an increased awareness of the impact of natural disasters to businesses.

From the 1990s, continuing into 2000, there was a reduction in the cost of technology and the role of the knowledge worker increased, along with an increase in salaries for those knowledge workers. This resulted in more online capability with increased end-user susceptibility. Recovery of networks now was also an issue. Terrorism (for example, the 1993 World Trade Center bombing and the Oklahoma City bombing) was seen as a new threat. Business continuity as a discipline started to emerge with new emphasis.

The September 11 attacks provided a wake-up call for those organisations that had previously paid little attention to business continuity. While the data recovery plans worked for some companies, they quickly realised that their business continuity plans were outdated (if they existed at all) and that the loss of key employees had not been considered. It was apparent that business continuity plans had to be broader. Pandemic planning, which started in late 2005, also emphasised the vulnerability of dependencies on the supply chain.

Companies have moved from data recovery, to business recovery, to continuity of operations, to operational resiliency. There are increasing standards and regulations. There is a recognised need to integrate and collaborate with other corporate functions involved in risk-related functions, such as IT security, physical security, privacy, enterprise risk management, contract compliance, supplier management, ethics and corporate governance.

Metrics and the measurement of BCPs have not, however, matured at the same rate as the industry. IT departments have been able to measure technical performance, but this has little applicability to business recovery. Various companies and Certified Public Accountant (CPA) firms provide business continuity benchmarking data. But these surveys tend to be subjective, calling for conclusions by participants rather than providing specific metrics by which to measure. Questions that ask for status provide choices such as 'no plans in place', 'currently developing', 'local plans in place', or 'organisation-wide plans in place'. Questions may also ask participants what they consider as sources of risk/vulnerability and when plans were last tested. The resulting data provide some basis for comparison for the company commissioning the survery, with respect to their own BCP programme, but little insight as to how to improve one's own programme.

COMPANY CASE STUDY

Prior to 2003, Sun had a BCP in place. However, it was very much bottom-up endeavour with no executive support and managed by a non-business continuity professional. A BCP professional was hired to reignite the programme. A gap analysis was conducted to identify what was in place, what needed to be changed, and what needed to be added. A roadmap was developed that focused on how to improve the methodology, how

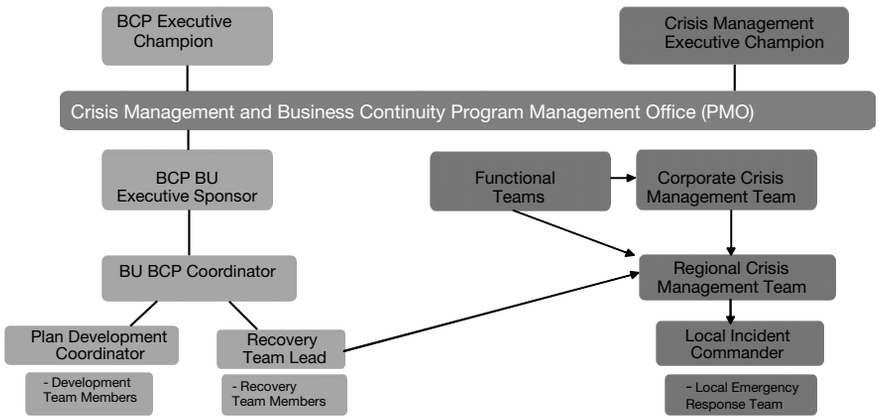

Figure 1 Enterprise organisation

to get the business units more engaged, and how to obtain more senior management support. This resulted in the organisational structure in Figure 1.

Following the internal audit in 2005, there began an investigation of tools to measure resiliency.

In his book 'The Resilient Enterprise', Yossi Sheffi discusses the need for companies to reduce their vulnerability to disruption, regardless of the cause.[1] He further indicates that companies must reduce the likelihood of a disruption, but also need to build in capabilities for bouncing back quickly. Thus, the challenge was to find a tool that measured those capabilities. It was necessary to have a measurement that could be repeated on a regular basis and that would provide an audit trail. The goal was to find something that was action and results-oriented. In 2005, there were few choices. Although Disaster Recovery Institute International (DRII) and Business Continuity Institute (BCI) had the best practices and some workbooks for gap analysis, these focused more on the methodology and how one developed a programme and plans. There was little available that measured the actual results.

In 2003, Contingency Planning & Management published an article comparing three models — the Business Continuity Maturity Model® (BCMM), The Core Value Chain, and The BCI Audit Workbook.[2]

After some research and evaluation, the BCMM® from Virtual Corporate was selected. It is open source and has the option to use proprietary scoring, a specific number that can be measured over time. Using the athlete analogy, it provides a growth progression starting at the crawling stage, advancing to walking, running, then a fit runner, a competitive runner and finally an Olympic runner. In an article describing the BCMM(r), Larry Kalmis highlights the advantages of using this tool to establish a baseline and then raise the level of business continuity preparedness.3 Figure 2 illustrates the BCMM®.

BUSINESS CONTINUITY MATURITY MODEL®

The BCMM® was developed as a result of a working team of business continuity professionals from various companies. They began their activity with a review of the DRII/BCI Professional Practices (for more information, see www.drii.org and

Increasing Business Continuity Competency Maturity

Maturity Model Levels	Level 1 Self-Governed	Level 2 Supported Self-Governed	Level 3 Centrally Governed	Level 4 Enterprise Awakening	Level 5 Planned Growth	Level 6 Synergistic
Athlete Analogy	Able to Crawl	Able to Walk	Able to Run	"Fit" Runner"	Competitive Runner	Olympic Runner
Comparative Model	Organization "At Risk"		"Competent" Performer		"Best of Breed"	
Corporate Competencies	**General Attributes of an Organization at Each Maturity Level**					
Leadership	VL	L	M	H	H	H
BC Awareness	VL	L	L	M	H	H
BC Program Structure	VL	L	L	M	H	H
Program Pervasiveness	VL	L	L	L	M	H
Metrics	VL	L	M	M	H	H
Resource Commitment	VL	L	M	H	H	H
External Coordination	VL	L	L	M	H	H
BC Program Content	VL	L	M	H	H	H

(VL=Very Low; L=Low; M=Medium; H=High)

Figure 2 The Business Continuity Maturity Model®

www.thebci.org). It was hoped that the team could map the individual requirements from these established practices into a useful organisation framework. After struggling for several months, they decided a new reference frame was required. The notion of 'corporate competencies' was considered. Attributes had been assembled during the previous months' work and these were organised into logical groupings. Each corporate competency categorised a critical attribute of an organisation's ability to create a sustainable business continuity programme. In this manner, the working team created an organisational counterpoint to the DRII/BCI Professional Practices.

The following corporate competencies were defined:

- *Leadership:* The commitment and understanding demonstrated by executive management with regard to the implementation of an appropriately scaled, enterprise-wide BCP. In addition, the degree to which the 'business case' for implementing sustainable business continuity has been articulated to and understood by executive management.
- *Employee awareness:* The breadth and depth of business continuity conceptual awareness throughout all staff levels of the organisation, including consideration for the quality and sustainability of the business continuity training and awareness programme.
- *Business continuity programme structure:* The scale and appropriateness of the business continuity programme implemented across the enterprise. The degree to which the BCP matches the articulated 'business case'.
- *Programme pervasiveness:* The level of business continuity coordination between departments, functions and business units across the enterprise. The degree to which business continuity considerations have been incorporated in other appropriate business initiatives, programmes and processes.

- *Metrics:* The development and monitoring of appropriate measures of BCP performance. The establishment and tracking of a business continuity competency baseline.
- *Resource commitment:* The application of sufficient, properly trained and supported personnel, financial and other resources to ensure the sustainability of the BCP.
- *External coordination:* Coordination of business continuity issues and requirements with external community including customers, vendors, government, unions, banks, creditors, insurance carriers, etc. Ensuring that critical supply chain partners have adequate BCPs of their own in place.
- *BCP content:* The previous seven corporate competencies address the key behaviours of the BCP. This eighth corporate competency addresses how the organisation implements the four central disciplines of business continuity (the following definitions are not definitive, but rather descriptive of the range of concepts, tasks, roles and responsibilities included within each discipline):
  - — *incident management* — ensuring that all aspects of emergency response, crisis management, and any other activities involved in command, control and communications during an organisational crisis and/or disastrous event are appropriately addressed;
  - — *security management* — ensuring that physical security, information security and any other activities associated with protecting the integrity of targeted information and resources are appropriately addressed;
  - — *technology recovery* — ensuring that critical information systems hardware, software, networks and applications are adequately recoverable within defined recovery time objectives;
  - — *business recovery* — ensuring that critical business functions and resources are adequately recoverable within defined recovery time objectives.

The working team members then defined specific organisational attributes within each competency at each level. The resulting matrices contain over 270 criteria to help the company conduct self-assessment to determine the 'score' for each competency. The self-assessment methodology included in the open access BCMM® describes how to conduct and score the assessment. If a more rigorous assessment is desired, business continuity professionals have the option of attending a two-day class to become licensed. Once the class is successfully completed, the assessor gains access to a proprietary web-based survey that produces a scorecard and aggregates data for reporting purposes.

CUSTOMISATION PROCESS

The recommendation was made to the BCP executive champion, the CFO, to target a maturity level of 4. Although neither a telecommunications company nor a financial services company, the company does support those industries. This level was also approved by internal audit. It should be noted that when this level 4 was recommended, the current score was not known. Within different environments, different cultures, and the demands of different industries, a company may choose a different goal. Each company needs to evaluate its own requirements to determine what score is best for them.

Within the proprietary model there are

Table 1: Baseline score, 2006

Corporate competencies	*BCMM® Score*
Leadership	3.1
Employee Awareness	1
Business Continuity Program Structure	3.1
Program Pervasiveness	3.5
Metrics	2.6
Resource Commitment	4
External Coordination	2.6
Combined score for competencies	2.8
Business continuity program content	
Incident Management/Crisis Management	1.4
Information Technology	2.4
Security Management (physical and IT)	4
Business Recovery	2
Combined score for content	2.4
Total score	2.8

over 250 questions, so it was necessary to look at the questions and ask how they applied in the present case. Again, returning to the requirements of being auditable and repeatable, consistency was necessary for year-on-year measurement. To provide a comprehensive response to the questions, each one required evaluation and provision of appropriate evidence. Thus, if the question asked whether a business recovery support function and staff existed, a documented plan was the evidence required. The wording of the question was not changed, although terms were redefined based on the company's culture and practice, for example, 'incident management' was defined as 'crisis management'. A spreadsheet was developed. In addition to the evidence required, a subject matter expert was identified as the best person to know the response to each question. The subject matter experts were then interviewed to obtain the answers to those particular questions. The responses were entered and the score was calculated (Table 1).

The next step was to take each competency and determine what was needed to raise the score. A gap analysis was developed for the low-scoring competencies, which included the measurement, the current state, the desired state, priority and effort (Table 2). A rolling roadmap was created from the gap analysis and was input to annual goals. This provided focus by year for specific activities to improve the score.

Twelve months after the baseline was taken, the survey was taken again in 2007. 2008 results were recently computed. In Table 3, one can see from the results of the two-year effort, which clearly demonstrates that what gets measured does get attention. Each year the PMO meets for four days to develop the next year's goals. The BCMM® results are used as input to that goal development.

These scores are from a corporate, enterprise perspective. The survey questions have been analysed and a subset is now being used for individual business unit measurement. Again, the documen-

Table 2: Gap analysis example

Competency	*Measurement*	*Current state*	*Gaps and/or desired state*	*Dependencies & implementation needs*	*Priority*	*Effort*
Employee awareness	Training module for all employees	None	On line training module	Budget for training development	2	H
Program structure	Standards and policies in place	Policies in place, some standards	Expand standards	PMO resources	3	H
Metrics	Method of measuring level of preparedness	Red, green, yellow for BU plan completion	Enterprise measurement Implement	BCMM®	2	M
Incident Management/ Crisis Management	Local BU plans integrated with corporate crisis management plan	No corporate crisis management plan	Corporate crisis management team	Implement cross functional team	1	H

Table 3: Results

	Sept. 2006	*July 2007*	*% Increase 07 over 06*	*Sept. 2008*	*% Increase 08 over 07*
Leadership	3.1	4.3	27.9%	4.9	12.2%
Employee Awareness	1.0	3.5	71.4%	4.0	12.5%
BC Program Structure	3.1	3.5	11.4%	4.4	20.5%
Program Pervasiveness	3.5	3.7	5.4%	4.1	9.8%
Metrics	2.6	3.2	18.8%	5.2	38.5%
Resource Commitment	4.0	5.0	20.0%	5.5	9.1%
External Coordination	2.6	3.8	31.6%	4.2	9.5%
Incident Management	1.4	2.5	44.0%	3.6	30.6%
Technical Recovery	2.4	2.8	14.3%	2.9	3.4%
Security Management	4.0	4.1	2.4%	4.8	14.6%
Business Recovery	2.0	2.8	28.6%	4.0	30.0%
Total Score	2.8	3.7	24.3%	4.5	17.8%

tation requirements are defined. If the documentation is not current, the business unit only gets a 50 per cent credit instead of 100 per cent. This is an incentive to ensure plans are current and complete. Using the gap analysis at the business unit level provides the opportunity to show the individual departments what they need to do to improve their score.

This same process can be used to evaluate the quality of supplier business continuity plans and to map to various country standards. It can also be used as an audit checklist to evaluate departmental plans.

This customisation can be done with virtually any benchmarking tool. The key is the gap analysis and developing a road-map to achieve one's goals. It is important to look at the tools being used from a broader perspective and explore possibilities to expand the use of those tools.

It is important to have a consistent and auditable measurement, to ensure one maintains focus on the right activities.

References

(1) Sheffi, Y. (2007) 'The Resilient Enterprise', MIT Press, Cambridge, MA.
(2) Contingency Planning (2004) 'Measuring your program: 3 methods for evaluating business continuity', available at: www.contingencyplanning.com.
(3) Kalmis, L. (2004) 'Business Continuity Maturity Model', available at: www.virtual-corp.net/html/show_news2.cfm?id=8.