Boathouse, Canberra

Business Continuity Management: Opening remarks at a launch of a Better Practice Guide

23 February 2000

Pat Barrett
Auditor-General for Australia

I would like to extend everyone a warm welcome to what I am confident you will find to be an informative and interesting series of presentations.

In my view, business (or function) continuity management can be considered basically in terms of risk and investment. As such, the issue is important for everyone in an organisation. It is not just a decision and concern of top management and/or a Board. The problem is, nevertheless, making sure that it is a shared concern of all stakeholders.

Business continuity is at the core of effective corporate governance. When it comes to the crunch, there is little point in us establishing a best practice governance framework, with all the associated discipline if, at the end of the day, the business becomes impaired for some foreseeable reason or, worse still, ceases to operate for any length of time.

While there is clearly a cost that needs to be taken into account as part of any risk assessment, and indeed of the application of risk management approaches and techniques, I would suggest that a more positive approach by decision-makers would regard such a cost as an investment in the future of the business.

As Auditor-General, business continuity management affects me in two ways:

·   First, as the Chief Executive Officer of the Australian National Audit Office, I am responsible for the quality and continued operation of the ANAO's business – and I must do this (as the FMA Act clearly indicates) in an efficient, effective and ethical manner ... some issues with which I will deal shortly.

·   Second, as Auditor-General, the Parliament seeks my assurance that all Commonwealth organisations are not only achieving their objectives, but that they do it in an efficient and effective manner, and can continue to do so even if they are interrupted by particular events, calamities or disasters – possibly beyond their control. With the possible exception of the Y2K preparations, the work which lead to the development of the Guide (including from observations in our annual audits of financial statements) suggested more attention needed to be placed on planning to recover from business interruptions.

Given our reliance on information technology to deliver even the most fundamental of services, it is not surprising that it was the Y2K bug that focussed our attention on the issue of business continuity. That is, Y2K risks were basically all about business continuity. Importantly, however, the consideration of business continuity also focussed many Chief Executive Officers' (CEOs) attention on other non-information technology and communications (ITC) factors that could have similar effects, such as water and fire damage.

DRAFT

Recently, there has been much said about the cost of Y2K testing and remediation: whether it was all necessary, or whether it was done well. Without a great deal of empirical evidence, I (and, may I suggest, any detractors) are not in a position to make a judgement at this time, nor perhaps at all. However, this work has left us with a valuable legacy which I would like to expand on briefly.

The first is, quite simply, raising awareness. If the onset of the Y2K problem did nothing else, it made us aware of our <u>vulnerability</u> to business interruptions as I have indicated. While its original focus was *IT-centric*, the Y2K exercise eventually and, more appropriately, extended to a consideration of <u>all</u> business systems – ITC and non-ITC – and the impact on our businesses, individually and collectively. It is no exaggeration to suggest that having to address Y2K issues raised our collective consciousness in the areas of risk management generally and business continuity management specifically.

The second legacy of the Y2K efforts is the work we did in relation to addressing the risks of system failures. Having had our attention firmly focussed on the Y2K/business continuity issue, most of us went through a rigorous process of risk management. Even in the absence of hard data, I am pleased to say that the ANAO observed throughout development of this Guide that most Y2K projects took a considered (and by that I mean a sensible and risk-managed) business approach to dealing with the continuity risks associated with Y2K issues illustrated as follows:

· identifying the particular Y2K risk event(s) [such as date dependent systems, but also non-date dependent facilities which were otherwise reliant on embedded chips in their system];

· identifying the systems and business processes which may be affected;

· ranking the systems in priority order in relation to the organisation's business imperatives;

· examining the treatment options available, that is, systems replacement, system enhancement, alternative processing options, or accepting the risk and preparing a contingency plan for dealing with the issue should it occur; and

· implementing the selected treatment(s) in accordance with a plan approved by a CEO and/or Board.

This is the approach we advocate in the Guide for business continuity which is also proposed by the risk management industry generally. The Guide therefore,

DRAFT

not surprisingly, recommends that the business continuity plan be developed in conjunction with the Risk Management Plan for the organisation. There are no short cuts in this area and no substitutes for systematic risk identification, assessment, prioritisation, treatment, monitoring and review, including systems testing. As an aside, I was very pleased to see the prominence given in the Guide to our most critical resource, our people and their interdependence with facilities, telecommunications, information systems and business processes (see pages 40 and 41).

But where does this all fit in terms of efficient, effective and ethical management of resources? In short, good process is necessary for achievement of required outputs and outcomes. I am not talking about a pre-occupation with process but its complementary relationship with results. Doing the hard yards on systematic risk management not only provides the necessary information for corporate planning, strategic decision-making and business operations, it can also create real ownership among the participants as well as a better understanding of the business. This is essential for good corporate governance and the resultant confidence of <u>all</u> stakeholders.

Given the effort and resources invested in Y2K projects, it would be remiss to let all that good work, the intelligence gathered and the knowledge accumulated (that is, investment) go to waste. These projects provide a useful basis for a consideration of a broader business continuity events, including their likelihood and impact. As a result, it will not take much more effort to extend this work to encompass a consideration of <u>all</u> business continuity risks.

The intelligence and knowledge created is still current … well, hopefully, it should be mostly up-to-date. Effective service delivery, risk management, business continuity management, and resources management – all depend on readily available up-to-date, relevant and reliable information. Consequently, if the assembled information before you is current, the plan you have derived can only be made more effective. Therefore it is sensible to take advantage of the information while it is still useful. The cost would be much less than having to repeat the exercise again later.

By way of example, while we were collecting information for the Guide, the Australian Customs Service Y2K Team pointed out their contingency plan *was not* just a Y2K contingency plan. Rather it was a contingency plan which dealt with Y2K. This is a small, but subtle and important, distinction emphasising the ease with which such a plan could be expanded to accommodate a broader consideration of business continuity events.

In closing, I commend the Business Continuity Management Guide to you either as a check on which you already have in place or as a basis for developing a suitable management approach to the issue. It offers a framework which supports a high-quality business continuity project. What it lacks is your knowledge and

DRAFT

insight of your business, your business objectives and deliverables, your business risks and exposures and, most importantly, your business's strategic direction. Put these elements together and you should have a comprehensive business continuity plan which accords with best practice in risk management.

The next speaker is Simon Moore from our Business Assurance Services Group. That Group was responsible for the development of this Better Practice Guide. Simon has seen considerable action in the ANAO both as an auditor and working in audit policy areas. He managed the early stages of our own business continuity planning project and is well placed to guide you through the background, development and approach being suggested.

Thank you for your interest in what is a timely and important presentation on an issue of fundamental importance to all of us.