Paragraph Performance Measures in Business Continuity

Ernest Jordan
Macquarie Graduate School of Management
Macquarie University, Sydney
e-mail: Ernest.Jordan@bigpond.com

Abstract
This paper is concerned with business and IT continuity, areas of increasing concern to many organisations and their regulators. It describes a research framework for conducting research in business continuity and shows how this can be populated with important issues from professional practice. The results of a survey of business continuity preparedness in Australia are then described briefly and the model is then tested for its adequacy. Improvements to research instruments are suggested.

Keywords
Business continuity, IT continuity, disaster recovery, contingency planning, business recovery

BUSINESS CONTINUITY CONTEXT
Business continuity is a term that has become standardised over the last few years. Until recently it had been common practice to refer to ‘disaster recovery’, ‘contingency planning’ or ‘business recovery’ in an ad hoc manner. While each of these terms can continue to be used for specific purposes, there is now an established consensus. ‘Business continuity’ refers to ensuring that businesses maintain their operational functioning, or, when disruption occurs, that the normal operation be resumed in a planned and predictable manner. Business managers will face the situation of having ‘the business handed back to them’ after the emergency services have left the building, or the utilities or access have been restored. It is their job to get the business running again, using the original or alternate facilities, with some degree of predictability.

Business continuity is not concerned with the crisis management issues of presenting the organisation’s situation to the media, or physical hazard reduction, or other emergency issues. Business continuity is, above all, concerned with the business services that the organisation delivers to its customers and meeting the needs of other involved stakeholders. It is about ‘getting back to normal’.

Information technology is, for many organisations, the principle focus of their business continuity planning. In a situation where the systems may all be working but the customers cannot access them, business continuity is also concerned but the solutions are generally clearer. For some organisations, the idea of a break in service is unacceptable – systems may be regarded as ‘mission critical’ or ‘fault tolerant’. For these organisations, duplicate facilities are the norm and a seamless switchover is an expectation. For other organisations buildings, machines or warehouses may be the vulnerable ‘single points of failure’ that are the focus of their planning.

This research is concerned with assisting business managers, including IT managers, make appropriate decisions about prioritising, planning and testing business continuity issues. Increasingly business continuity is being seen as a normal part of business, not the preserve of the IT specialist.

IT as a source of risk
Information technology (IT) is used here to refer to hardware, software, computers, telecommunications, applications and infrastructure in a composite manner, mirroring its use by the general business world. IT represents a wide range of risks to an organisation – where we will define the word ‘risk’ to be ‘a probability of an adverse outcome, or a factor that raises this probability’ (WHR, 2002). In the IT literature, the most frequently mentioned risks are associated with project failure and IT project risks are so commonplace that there are many books on that topic alone. But IT creates risks in many other ways for organisations, such as:

- Choosing an ERP system that does not meet long term needs
- Choosing a hardware vendor whose equipment has proprietary features that are not apparent at the time of purchase
- Having poorly designed security systems that enables malicious access
- Capacity, scalability, total cost of ownership limitations
• Building systems that cannot be enhanced or supported
• Failing to develop staff skill sets to meet ongoing needs
• Failing to set priorities between competing applications
• Failing to set sufficient priority to IT in general

The list can be extended very easily. IT is a risky area. The risk that this paper focuses on concerns the risk that the IT systems, having become important or even critical to the organisation, stop, slow down or become degraded to such an extent that the business functioning is impeded.

Business continuity and IT continuity

Business continuity and IT continuity are not synonymous. While many organisations have ‘mission-critical’ systems, they are not the only factor that can bring the organisation to a crisis. IT can be working satisfactorily, but

• Customers may not be able to access your stores, (the Newcastle, NSW, CBD was totally closed by emergency workers after the earthquake), or
• Your manufacturing process has quality control problems and there is a major recall and existing production must be terminated, (Pan Pharmaceuticals), or
• Your suppliers cannot supply key components or raw materials (very many examples, including GM Holden’s recent lack of exhaust pipes), or
• There is a fire, flood or other emergency that destroys a critical building (Bankstown City Council is the best known Sydney example).

All of these are examples of business continuity issues, not IT continuity directly. In some cases there are simultaneous IT continuity issues, as in the Bankstown City Council fire that also destroyed IT systems.

Some industries are referred to as information intensive (Porter and Millar, 1985) and their dependence on IT is such that high levels of protection are necessary. Developments such as duplicate data centres, duplicate telecommunications providers and power supplies, synchronous replication of data and processes, automatic fail-over systems and frequent testing are part of their stock-in-trade. This is demanded in some industries by the regulators. In order to maintain a banking licence, banks must provide their customers with a very high level of access to their funds. Computerised exchanges, such as those now operating in deregulated electricity markets, must operate at all times, so that power purchases can be made. Airlines and online retailers don’t have ‘business hours’ as their customers are located around the world – so their business must be ‘always on’. In addition we have the telecommunications companies, electricity suppliers and other utilities, whose customer base includes these businesses as well as critical community infrastructure such as hospitals and police services. For these organisations, business continuity intimately includes IT continuity.

It also happens that, in many organisations, the expertise, skills, knowledge and interest of continuity matters are with the IT staff. The early mainframe technologies were so vulnerable and far behind today’s reliability standards, that the processes of backing up, logging transactions, and carrying out restore operations were routine even in the 1960s. Today’s systems are vastly more complex and have greater networks of dependencies, but the skill set of IT staff has grown to accommodate them. This increase in complexity may be mirrored in some aspects of the supply chain, but most parts of the organisation have not changed in a parallel manner. Thus many organisations look to the IT function for expertise in the area of business continuity, often without recognising it explicitly.

Aims for the research program

Serendipity often has a significant role for university researchers – and this is an example. The author was approached six years ago by a small data storage company looking for a survey to help them establish the size of the market for their services, so that they could estimate their share of market and the potential market growth. A simple survey was conducted to try to establish the levels of adoption of various business continuity and IT continuity practices. This revealed (Jordan and Musson, 1997) such serious deficiencies in the preparedness of Australian organisations that a research program was born. This has resulted in a variety of surveys, case studies and presentations to concerned organisations and conferences in the region.

The overall aim of the research program is to conduct research that will enable organisations to manage their business continuity initiatives more effectively. In particular, organisations are concerned about the overall spending on business continuity, its location in the organisation – with IT, business managers or senior management, and in determining the involvement of other stakeholders. There is a strong indication that many
organisations do not take business continuity seriously, it is under-resourced and that priorities are not decided on a consistent basis. As a researcher, it is the author’s aim to provide the knowledge that will change the situation.

This paper represents an attempt to put business continuity into a research model that will facilitate the development of a cumulative tradition. The analysis presented here uses data published in the second survey (Musson and Jordan, 2000) – that are now analysed from a new perspective.

RESEARCH MODEL

Much of the activity in the domain of business continuity is based on professional practice and little research has been published. As a starting point, this paper uses a generic management research model, that features in research methods texts. The model is one of implied rational decision-making, based on assessment of the situation. Consequences of those decisions are then apparent at a later time. This model is illustrated in Figure 1.

In the generic management research model, the context of the management decisions and actions are first established. The (rational) manager then chooses actions and makes decisions based on the established context. Results of the actions are observable, typically at a later date and are described as outcomes.

This model ignores the interaction and feedback that takes place in a real environment or more realistic situations where actions are negotiated in a setting that may change the context, and then choose appropriate actions. It is a simple model, even simplistic, but the need is for a model that can be enhanced as research accumulates.

For our research, ‘context’ becomes the risk environment for the organisation, ‘actions’ refers to management actions in business continuity, and the ‘outcomes’ will be business continuity performance indicators, while are described in the subsequent sections. Thus the business continuity research model is shown in Figure 2.

![Figure 1 Generic management research model](image1.png)

![Figure 2 The business continuity research model](image2.png)

The risk environment for the organisation

Organisations that are in riskier environments, whether from internal or external sources, would be expected to take greater preparation to counter those untoward events. There are many approaches used by risk managers and business continuity professionals. One approach requires the organisation to identify its assets and examine the vulnerability of each of these. The vulnerability of assets is summarised in a matrix of the likelihood of the loss of the asset together with the consequence of that loss, demonstrated in Figure 3.

This approach may also be known as a ‘business impact analysis’, where the impact to the business of a range of foreseeable events is assessed. IFAC (1999) uses a ‘risk map’ to represent this assessment.

Factors that add to the risk environment are:

- Pressure from regulators
- Vulnerability caused by ‘single points of failure’ – key resources that are not duplicated
- Complexity of the organisational environment
- Lack of internal controls, security and senior management oversight
- External hostile parties – hackers, fraudsters, thieves, vandals
• Systems and components with low reliability performance

In this paper we report on a study where only simple assessments were made of the organisation’s risk environment. Managers were asked to rate how critical their systems were, and also asked what would be the longest acceptable outage for a key business system or facility – often referred to as a ‘maximum acceptable outage’ or MAO. In future studies, more attention will be given to developing additional measurements in this area.

**Business continuity actions**

The range of actions available to managers fall into few categories: mitigate, insure, ignore, plan and test. Dealing with the simplest first – for vulnerabilities that appear in the lower left hand corner of the asset vulnerability matrix (Figure 3), where both the likelihood and consequence are low, it may well be satisfactory to ignore the issue and accept the risk. The failure of a monitor on a user’s system may be just such a risk. Other systems may be able to be out of action for a week without disrupting the business. Parts of the organisation’s facilities could similarly be out of action without jeopardising continuous operations.

A common response to risks is to mitigate them, either reduce the likelihood or reduce the consequence (or both). We mitigate the risk of a hard disk crash by carrying out a backup or by purchasing more robust hardware, certified to a high standard. The choice to mitigate will be based upon the likelihood and consequence, when held up against the cost of mitigation. Another method of mitigation is to transfer the risk to another party. Outsourcing a data centre transfers the downtime risk to the vendor, leaving the organisation with the business impacts only, not the hardware costs.

Insurance is the most direct form of risk transfer. In this case the insurance company will provide a benefit that compensates for the negative consequences. Clearly the insurance company intends to make a profit, so the expected payout would normally be less than the premium. The issue for the organisation is that it is the absolute loss that needs to be mitigated, even though the expected loss is actually increased. This issue is faced by homeowners who insure their property against fire loss, with probability \( p \), for \( $100,000 \), say, for a premium that represents more than the expected loss \( ($100,000 \times p) \). Insurance costs, however, are real costs, while the misadventure has only a probability of occurrence and the loss may never occur.

The final business continuity actions, planning and testing, are normally considered together. Business continuity plans should deal with all the continuity risks that are significant and outline what actions are supposed to take place in that eventuality. Tests are undertaken to verify that the planned action is achievable and enables the organisation to resume business. Tests also perform the important function of keeping business continuity in the consciousness of the people liable to be affected. Plans are widely derided – gathering dust on a shelf, never examined after being written, costly and impractical, but represent the only assurance to senior management that the organisation has any level of preparedness. Without testing, plans are in danger of meeting the statements of their detractors. Testing reveals weaknesses in plans and allows their revision.

In this study many questions concerned the business continuity actions but the focus was on the plans. How complete they were, how recently modified or adopted, whether tested or not, whether approved by senior management. Associated questions concerned the budget for business continuity and the sitting of the responsibility. Together these questions should give a comprehensive assessment of the management preparedness and competence in business continuity. Peter Power (2002) suggests that the plan represents a ‘statement of management capability’ – and should include only affirmations of what management are actually able to do in the circumstances, not their hopes or wishes. Testing distinguishes between capability and hope.

**Business continuity outcomes**

Professional practice concentrates on two key performance areas:

- resilience – the ability to withstand unwelcome events, and building such capacity, and
- recovery – the ability to come back after a forced outage.

Resilience can be likened to our personal health issues of ‘having our shots’, ‘getting health checks’, ‘keeping fit’ and ‘keeping our resistance up’. For a business organisation intent on building business continuity resilience, it must work to identify single points of failure and remove them; it must monitor the reliability of components and replace the inadequate, and so on. With a high level of resilience, more disruptions and failures can be tolerated without degradation in business services. Resilience in terms of hardware, telecommunications connections, power supplies and other physical assets can be assessed in a straightforward manner, however the issue to the organisation’s customer is one of service delivery, and other factors are important. Thus assessing resilience in terms of the delivery of services can be much more difficult than for infrastructural components.
Recovery is concerned with bringing back the organisation to an acceptable performance level, in particular the costs and time involved, although for many organisations, simply being able to recover – at all – is in itself the necessary achievement. It could be argued that recovery can only be measured when there is some significant event. However, the realistic situation is that outages of a minor nature are frequently occurring. Power outages are very common, as are telecommunications breaks. Increasingly today, we find that network outages due to viruses, worms and the like, are also routine. While simple breaks are routine, there are usually distinguishing features of each event, and the duration is seldom known at the outset. Thus those concerned must bring into action their procedures for dealing with extended breaks. Most large IT installations routinely log all such service breaks and record their durations. It is uncommon that business performance, e.g. customer service levels, is also recorded during these episodes. This study asked organisations about their experience of outages and their recovery performance.

A third component of business continuity outcomes is not part of the standard professional practice. This concerns the business benefits obtained by the very process of carrying out business continuity assessment exercises. The close examination of the importance and vulnerability of business systems and processes may bring about a better understanding – revealing the potential for improvement, rationalisation or redesign. These outcomes from business continuity planning are the current benefits. These have been investigated independently by case studies but are difficult to approach in a survey methodology, due to their distinct individual nature. This study made no attempt to assess these current outcomes.

HYPOTHESES

Effect of risk on planning

It is to be anticipated that organisations that are in a riskier environment, from whatever causes, will be more likely to be carrying out business continuity planning. In this study the only measures of environmental risk are

- the maximum acceptable outage (MAO) and
- degree of criticality of systems (CRIT).

There were many measures of management business continuity actions:

- extent of plans (EXP),
- age of plans (AGEP),
- test currency of plans (TEST),
- budget for business continuity (BUDG), and
- management responsibility level for business continuity (LEVL).

Thus we expect higher levels of risk to lead to higher levels of management action, in particular:

- Higher MAO or CRIT leads to greater EXP – higher risk settings are associated with greater extent of plans, i.e. more and better plans;
- Higher MAO or CRIT leads to greater AGEP – higher risk settings are associated with greater age of plans; planning started longer ago;
- Higher MAO or CRIT leads to greater TEST – higher risk settings are associated with greater testing of plans; the need to test is increased;
- Higher MAO or CRIT leads to greater BUDG – higher risk settings are associated with greater budget for plans;
- Higher MAO or CRIT leads to higher LEVL – higher risk settings are associated with higher level of responsibility for business continuity.

Effect of planning on outcomes

It is to be hoped or expected that those organisations with better planning and preparedness will fare better during a disturbance – assuming that they have the same risk level. We have considered the measurements of management action above, which leaves only the outcomes to be assessed. In this study the outcomes were:

- The manager’s confidence that the organisation would survive an outage (SURV) as a simple measure of resilience
- The quantity and duration of outages actually experienced (OUTG), which could be a measure of the lack of resilience (although the consequences of these outages need not necessarily be business interruption), it is also a measure of the recovery capacity.
The hypotheses are therefore, for a given level of risk (MAO or CRIT),

- Greater EXP leads to greater SURV and fewer OUTG – greater extent of plans are associated with higher confidence of survival and lower levels of outages
- Greater AGEP leads to greater SURV and fewer OUTG – greater age of plans are associated with higher confidence of survival and lower levels of outages
- Greater TEST leads to greater SURV and fewer OUTG – greater testing of plans are associated with higher confidence of survival and lower levels of outages
- Greater BUDG leads to greater SURV and fewer OUTG – greater budgets for planning are associated with higher confidence of survival and lower levels of outages
- Greater LEVL leads to greater SURV and fewer OUTG – greater level of authority for business continuity is associated with higher confidence of survival and lower levels of outages

In terms of the graphical model in Figure 2, this can now be annotated with the variables that are obtained in the investigation. This is shown in Figure 4.

---

**METHODOLOGY**

The survey data analysed here has been previously reported (Musson and Jordan, 2000). The survey instrument was revised from an earlier version (Musson and Jordan, 1997) that had, itself, been developed by considering a range of documents; sources included Australian Standard AS4444 (Standards Australia, 1999), Coopers & Lybrand (1992), Ernst & Young (1996), FEMA (1996), Hardy (1992), Higgins and Tilley (1998), Hiles and Barnes (1999), Internal Auditor (1997), Kearvell-White (1996), Maslen (1996), NCC (1994, 1996), Survive (1996) and Tilley (1998). It addressed four key areas:

- The nature of emergencies experienced by respondents
- The extent of planning to combat such emergencies
- The degree to which the plans are operational
- The backup and data storage practices of respondents.

The purpose of the survey, at the time it was implemented, was simply to ‘paint the landscape’. At that stage there was no intention to develop or test theory. This paper is thus only able to make selective reference from the survey instrument, as the intention here is to build a firmer theoretical basis for further research. The selections are based on those items that constitute close matches between theoretical and practical aspects. Many of the original survey questions are at too detailed a level to be considered part of the model at this stage.

**Instrument design**

As suggested above, guidelines such as Australian Standard AS4444 on Information Security Management (which was itself developed from British Standard BS7799 – which served as the model for the new international standard, ISO17799) and a range of Business Continuity Institute publications were influential in
developing the questionnaires. While the questionnaire in full has over 30 questions, this paper is concerned with relatively few of them. Earlier publications have included the full questionnaire Musson and Jordan, 1997, 2000).

Survey distribution

This survey includes local government, but not State or Federal organisations. The survey sample was taken from a database of Australian organisations with significant computer configurations, thus excluding smaller organisations.

It was decided to target the CEO of the organisations to be polled. This reflects the view that business continuity planning (and thus the survival of the organisation) is a matter of corporate governance. A letter was produced, which was designed to obtain the commitment of the addressee; it was sent to the CEO (or equivalent) and was individually signed. It asked the recipient to pass on the enclosed questionnaire to the manager concerned, and also asked that the recipient completed a notification form, giving the name of the person to whom the questionnaire had been passed. The notification form also asked the CEOs whether they would like a copy of the survey report.

The questionnaire is available on the author’s website\(^1\). It is a five-page document with a total of 37 questions. The mailing list was based on the MIS 5000 database of Australian computer users, ranked by the number of computer screens in the organisation (Strategic Publishing 1998). To prepare the mailing list, multiple references to the same organisation were removed from the list. Federal and State Government users were removed from the list and, because of our interest in local government users, the resulting list was augmented by those Australian local authorities not already listed. This gave a population of 3576 organisations.

From the augmented list, a stratified random sample of organisations was selected, representing some 16% of each industry group except for local government. In the case of local government, all Greater Sydney councils were included (due to the manageable number), and a sample of some 15% of the remaining councils was selected.

Response and validity

The survey response was 16%. Factors contributing towards the low rate include the size of the questionnaire and the then-current Y2K overload – the number of questionnaires being requested of senior managers for Y2K purposes. Analysis of non-response showed that they did not exhibit systematic patterns. The overall results were also very similar to the earlier study (which had a higher response rate), increasing the author’s confidence that the results were reliable.

RESULTS

In this section we look at the results under each of the three major categories: risk environment, business continuity actions and business continuity outcomes.

Risk environment

The degree of criticality is reported on a scale of 0 to 4. It is derived from questions that ask the importance of a range of applications. The mean value of all the reported levels of importance is taken as the score. The MAO figure is a scale variable, using standard levels of out-of service times. Figures 5 and 6 reveal a wide range of scores.

\(^1\) http://www.gsm.mq.edu.au/facultyhome/ernest.jordan/

Jordan (Paper #233)
Further analysis revealed that CRIT and MAO were statistically independent. Thus the respondents’ perceptions of the extent of criticality and the longest tolerable outages had no relationship. These two dimensions are therefore maintained for further analysis.

**Business continuity actions**

**IT budget**

In the subsequent analysis, the percentage of IT budget spent on continuity is used only as a scale variable, with values from 0 (no expenditure), 1 (less than 1%) to 4 (more than 5%). It only represents part of the total business continuity expenditure, but for many organisations it is easier to record and report.

<table>
<thead>
<tr>
<th>Percentage of IT budget spent on IT business continuity</th>
<th>Business</th>
<th>%</th>
<th>Count</th>
<th>%</th>
<th>Count</th>
<th>%</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>less than 1%</td>
<td>23</td>
<td>35%</td>
<td>12</td>
<td>43%</td>
<td>35</td>
<td>100%</td>
<td>66</td>
</tr>
<tr>
<td>1% to 2%</td>
<td>13</td>
<td>20%</td>
<td>6</td>
<td>21.5%</td>
<td>19</td>
<td>100%</td>
<td>38</td>
</tr>
<tr>
<td>2% to 3%</td>
<td>12</td>
<td>18%</td>
<td>1</td>
<td>3.5%</td>
<td>13</td>
<td>100%</td>
<td>26</td>
</tr>
<tr>
<td>3% to 5%</td>
<td>3</td>
<td>4.5%</td>
<td>1</td>
<td>3.5%</td>
<td>4</td>
<td>100%</td>
<td>8</td>
</tr>
<tr>
<td>More than 5%</td>
<td>7</td>
<td>10.5%</td>
<td>2</td>
<td>7%</td>
<td>9</td>
<td>100%</td>
<td>18</td>
</tr>
<tr>
<td>no expenditure</td>
<td>8</td>
<td>12%</td>
<td>5</td>
<td>18%</td>
<td>4</td>
<td>3.5%</td>
<td>13</td>
</tr>
<tr>
<td>no response</td>
<td>0</td>
<td>-</td>
<td>1</td>
<td>3.5%</td>
<td>1</td>
<td>100%</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td>66</td>
<td>100%</td>
<td>28</td>
<td>100%</td>
<td>94</td>
<td>100%</td>
<td>94</td>
</tr>
</tbody>
</table>

*Figure 7: IT budget allocation for business continuity*

**Extent of plans**

Two questions asked about the business continuity plans and the IT continuity plans. Fully documented and approved plans scored the maximum 4 in each category. Lack of plans scored zero and other values were in between; the score EXP was derived by adding the scores on the two plans. Thus the maximum value is 8. The distribution is shown in Figure 8.

**Age of plans**

Two questions asked about the duration since the business continuity plans and IT continuity plans were written. No plans scored 0, recent plans scored 1 and plans more than 5 years old scored 4. The total score was taken as the value for AGEP. The distribution is shown in figure 9.
Management level of continuity planning (LEVL)

High level of responsibility (CEO or board level) scored the maximum 5 points (for each of the business continuity and IT continuity plans). Thus the maximum score is 10 and the minimum is zero. The distribution is shown in figure 10.

Currency of testing of plans (TEST)

Recent testing scored the maximum 4 points (for each of business plans and IT plans) while lack of testing scored zero. Thus the maximum score is 8 and the minimum is zero. The scores are shown in figure 11.

Correlation analysis showed that all five of these variables were significantly related. A confirmatory factor analysis showed that a single factor was present, representing more than 50% of the variation in the data. Given that there was insufficient data for a thorough factor analysis, a composite ‘management actions’ variable (MGTACT) was constructed by adding the scores for all five variables. This new construct was used in supplementary analysis.

\[
\text{MGTACT} = \text{EXP} + \text{AGEP} + \text{BUDG} + \text{LEVL} + \text{TEST}
\]

Business continuity outcomes

There are two variables that are regarded as the outcomes of business continuity in this paper. The confidence that the organisation will survive was scored negatively, so that a score of 1 represented
complete confidence and 5 a complete lack of confidence. The raw data is shown in figure 12. The second variable was constructed as a weighted sum of the outage counts reported. About half of the respondents gave detailed counts of outages experienced, against a range of time categories. No report was scored as zero. Only one outage of a very short duration, scored one. Increasing time out led to increasing scores, as did increasing counts. The construction of this score, OUTG, can only be described as exploratory. Thus

$$\text{OUTG} = \sum_{i} f_i w_i$$

where $f_i$ is the frequency (count of interruptions of a time range) and $w_i$ is the weight for that time range (increasing with increasing times). As can be seen from Figure 13, the raw scores are far from normally distributed.

These variables were also found to be independent. Even when the zero scores from OUTG were excluded, there was still no correlation. It has to be said, frankly, that the OUTG construct was perhaps too insubstantial to be useful.
ANALYSIS AND DISCUSSION

Relationship between environment and business continuity actions

No relationship was found between the risk environment variables (MAO, CRIT) and any of the business continuity action variables. Clearly other factors are at work in leading management to engage in business continuity activities. Unfortunately in this survey, there were no variables that explained this management action. Thus if the maximum acceptable outage, and the perception of the critical status of the systems do not explain management’s business continuity action, other factors need to be investigated. The influence of regulators may be one such factor. Another could be the demand from customers or suppliers. On the other hand, it may be more to do with organisational culture or style. There is plenty of opportunity for further research.

Relationship between business continuity actions and business continuity outcomes

Here the research found a valuable result. The MGTACT scores were strongly correlated with the CONF scores. Higher levels of business continuity action led to higher levels of confidence in survival. Perhaps ‘confidence’ needs to be restated as a goal, that could be a driver of management action – an effective context variable.

As the analysis is simple and the results so far are only of limited value, further analysis trying to link the context variables to the outcomes was not undertaken.

CONCLUSION

The strong correlations between the components of the ‘management action’ construct are very encouraging. Thus there is good support for maintaining and developing this part of future studies. Similarly confidence in survival is a variable that can be supported. At this stage, the risk environment variables and the outage variables leave substantial room for improvement.

The generic management model has proven useful in establishing a foundation for cumulative development of research in the area. It is concerning that there are no effective predictors for ‘good’ management action. Further research should consider summative indicators in all three domains: context, actions and outcomes, so that new components can be added to the model and greater explanation power developed.

REFERENCES


IBM (1996) A Risk too Far, IBM, London, with Cranfield University, Cranfield, UK

Insurance council of Australia, 1996. Report to Insurers on under insurance and non-insurance.


Jordan (Paper #233)


Strategic Publishing (1998) The MIS 5000, Strategic Publishing Group, Sydney


COPYRIGHT

Ernest Jordan © 2003. The authors assign to ACIS and educational and non-profit institutions a non-exclusive licence to use this document for personal use and in courses of instruction provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive licence to ACIS to publish this document in full in the Conference Papers and Proceedings. Those documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.