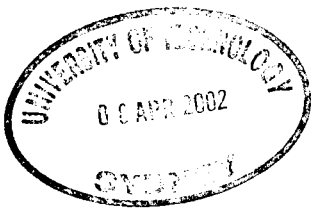
Contingency Planning Models for Government Agencies

Author

Raji Swaminathan



M. Sc. (Computer Science)
University of Technology

April 1996

Abstract

This report describes a research study into the current situation within Federal, State Government and selected private sector agencies, assessing contingency plans for Information Systems and suggests models for state-wide planning against Information Systems disasters. Following a brief look at various phases of contingency plan development, the study looks into the factors that prompt organisations to prepare contingency plans. The project involved a survey of current Information Systems contingency plans in the government agencies in the states of Victoria, Western Australia, South Australia, New South Wales and in the Australian Capital Territory. It also included two major banks, an insurance company and two computer services bureaux in the private sector within New South Wales.

The survey determined that particular factors play important roles in the decision by organisations to commence contingency planning. These include actual disaster experience, senior management support, auditor's comments, legal requirements, risk analysis and business impact study, economic considerations, insurance requirements, contract commitment, new staff and introduction of new hardware and software. The critical success factors in contingency planning include regular maintenance and testing of the plan. The project also discusses the current contingency planning environment within New South Wales Government agencies and suggests cost-effective models for state-wide adoption.

Acknowledgment

The author would like to acknowledge the help and assistance given by the following persons:

Mr. Nigel Ampherlaw, Partner, Coopers & Lybrand - Mr. Ampherlaw provided extensive guidance on the subject of contingency planning for Information Systems. As the Partner responsible for the firm's Computer Assurances Group, he was able to provide accurate information on the critical success factors of contingency planning.

Mr Gary Blair, Senior Manager, Business Continuity, Westpac Banking Corporation - Mr Blair provided extensive guidance in gathering information from selected organisations. Mr Blair's experience in contingency planning in Australia and New Zealand enabled him to make a very valuable contribution to the research project.

Senior Public Service Officers of the Commonwealth and State Government departments and senior managers within the private sector agencies for their efforts and assistance with the research project. It was only through their support that the completion of this project was possible.

Finally, the author would like to thank her supervisor, **Mr. David Wilson**, for his tireless efforts and assistance during this research project.

Declaration

I hereby declare that this report is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree or diploma of the university or any other institute of higher learning, except where acknowledgment is made in the text.

Raji Swaminathan.
April 1996.

Table of Contents

1. Introduction

1. Introduction

The expressions "***contingency planning***" and "***disaster recovery planning***" concern the preparation of plans which could be actioned when unexpected adverse events occur that would have dramatic effects on an organisation's computer facilities, and thus, on the organisation's ability to do business. The report assumes that both ***Contingency Plan*** and ***Disaster Recovery Plan*** have the same meaning and refer to a formal written plan to cater for any contingencies within an Information Systems environment. Senior management, data processing staff and users of Information Systems at various levels will be involved in the development of the plan and its ongoing maintenance. The direct beneficiaries of a contingency plan exercise are the owners and users of computer systems; while indirectly the Information Systems providers benefit from providing continuity of service to users as part of formal or informal service agreement.

The project involved detailed research on the current policies, regulatory frameworks and facilities for contingency planning for Information Systems in the public sector such as the Federal, Victorian, Western Australian, South Australian and New South Wales Government Agencies as well as in large private sector organisations such as banks, an insurance company and two computer services bureaux. A comprehensive review of the current contingency planning strategies that are in place both in the public and private sectors was carried out with a view to establishing their effectiveness.

1. Introduction

Special emphasis was given to the New South Wales Government sector. Recommendations are made and hypothetical models proposed for the provision of cost effective contingency planning services which could be used by all New South Wales Government Departments. The proposed models will cater both for the short term in proprietary platform scenario and in the long term when hardware implementation follows the Government Open Systems Standard for Interconnection Protocols (Gossip) standards and hybrid platforms.

The report includes descriptions of various stages involved in the preparation, testing and maintenance of the contingency planning process. Identification of factors that are critical to the success of contingency planning implementation in an organisation is also covered. These are included in detail in **Section 3** under the heading **"Contingency Planning Steps".**

Research also included collection of information on what factors prompted organisations to develop contingency plans. The decision of an organisation to go ahead with contingency planning, or to leave it aside is not as clear a decision as the literature on this subject presents. Understanding the factors behind this decision is an aim of this project. Each of these factors are covered in detail in **Section 4** headed **"The Need for Contingency Planning".**

2. Definitions

2. Definitions

This section will define the meanings of the terms that will be used throughout this report. The most significant term is ***contingency planning.*** The use of this phrase in the context of Information Systems is different to its use in other contexts. Here, contingency is limited to computer-related contingencies, rather than organisation-wide events.

Contingency - is an unscheduled interruption of computing services which requires measures outside the day-to-day routine operating procedures. Any unexpected disruption that causes losses in terms of a company's competitive advantage in the market and deviation from standard operating procedures.(Lane & Step, 1985; Hiatt & Motz, 1990).

Contingency Planning - is the availability of procedures which allow for continuity of business when an unscheduled disruption to computing services occurs. A contingency plan is a procedure to be followed when the contingency occurs.

2. Definitions

Information Systems department - is a functional unit within an organisation responsible for providing computer data processing and software development or maintenance services to that organisation.

Cold Site - is an area or floor space reserved for the installation of computer equipment in another building away from the primary site. The site has power, air conditioning, raised floor, and possibly communications equipment but no processors, tapes or disk storage. If a disaster occurred that caused the primary computer centre to be inoperable, the Cold Site could be equipped with hardware and software and be operational within a few days time.

Warm Site - is a computer room with only the processor hardware and other facilities such as communications equipment, power, tapes and disk storage; but without the software. When a disaster happens at the primary site, the operating system software and other application software and data stored in backup locations will be used to configure the hardware in the warm site before processing can begin within a few days time.

2. Definitions

Hot Site - is a fully functional site whereby a complete computer installation is ready for use in an emergency. If a disaster occurred that caused the primary computer centre to be inoperable the Hot Site could be operational within a few hours.

Outsourcing - is the contracting of Information Technology functions on a service agreement basis to external commercial service providers.

3. Contingency Plan

3. Contingency Plan

This section covers the aims, objectives and success factors of contingency plans. It also provides in detail the different steps involved in the process of implementing contingency plans. A contingency plan consists of the information and procedures required to enable rapid recovery from a disaster. Once the threats to availability of Information Systems and their impact on the delivery of core functions are identified and assessed, management will be in a position to implement practical disaster recovery strategies as per the contingency plan.

3.1. Aims

The main aims of a contingency plan are:

- to keep the organisation in business
- to provide an organisation with its core services
- to help an organisation to fulfil its mission with minimum disruption.

3. Contingency Plan

3.2. Objectives

The objectives of preparing a contingency plan are to:

- identify and assess the threats to the availability of Information Systems
- analyse the impact of Information Systems unavailability
- develop recovery strategies for an organisation's critical Information Systems and
- document a contingency plan for identified Information Systems.

3.3. Success Factors

Successful recovery and continuity of business depends on the availability of the following:

- A plan of action (contingency plan) which is regularly tested
- A trigger mechanism to initiate execution of the plan when a disaster occurs
- Assigned and trained personnel (Contingency Planning Team)
- Resources with which to manage the recovery (a back-up site, copies of critical data and programs).

3. Contingency Plan

3.4. Contingency Planning Steps

The following steps are identified in the preparation of a contingency plan for Information Systems.

3.4.1. Business Impact Analysis

The aim of the business impact analysis is to understand the nature of an organisation's business processes in detail, thereby to determine the way the organisation uses its resources, which resources are critical for the organisation to meet its stated goals, the risk associated with the use of those resources, and the impact of the unavailability of those resources. The business impact analysis includes the study of various critical functions and the applications necessary to support those functions together with an assessment of required time for recovery. This phase of contingency planning process involves determining which computerised applications are mission critical to an organisation's continued operation, by analysing the impact of those applications unavailability. Critical applications which are required for continued performance of core business activities are identified in this phase.

3. Contingency Plan

3.4.2. Recovery Strategies

In this phase the requirements for recovery are agreed upon with the users of the application systems. This phase identifies the functions that would normally be provided by the application system, describes the alternate system which will replace the computer system when the contingency plan is activated and establishes procedures to return to normal operations when the disaster is over. With the help of users the contingency planner documents in detail, the processes to be followed to perform these critical functions while the systems are unavailable. Depending on the circumstances these processes may be manual systems or micro computer-based systems. The procedures should allow for orderly return to normal processing after the computer systems have been restored.

When the detailed recovery procedures are in draft form, they will require approval of both management and users. The procedures also should be reviewed in detail by the personnel responsible for carrying out the plans.

3.4.3. Contingency Plan Development

The contingency plan will include the decisions and assumptions that were made, the scope of the disaster catered for by the plan, the selection of preferred

3. Contingency Plan

strategies and the recovery strategies. The contingency plan provides in detail specific routines for action, personnel team formation and definitions of their roles and backup arrangements which are in place to ensure timely and effective response to a disaster. The plan also identifies all applications designated as critical over the expected period of outage and provides for the resumption of processing of those applications within a specified timespan after they become critical. The recovery procedures which must have been developed for each critical application will be included along with the plan for action when required. When a disaster strikes, the plan will direct the disaster team to follow the recovery procedures within their sections, confident that they are working as per plan. The majority of the recovery activities will take place in parallel. This is because the contingency team will have to work to a short time frame. Each member of the team will be performing different functions while working towards the same objective. The contingency plan will provide a checklist of actions to be taken by the individual contingency planning team members.

3.4.4. Team Personnel Training

Training of relevant personnel is necessary to ensure that all staff appreciate the need for contingency planning and are familiar with the plan and the recovery strategies proposed. In particular the team members must be trained in their roles

3. Contingency Plan

and responsibilities during the recovery process. Training of staff in the recovery procedures should begin as soon as the draft procedures have been approved and should include an awareness of security issues of the primary processing site as well as the alternate processing site. It is imperative that staff receive periodic refresher training as well as when the plan or the recovery procedures undergo massive changes.

3.4.5. Contingency Plan Testing

In order to ensure the adequacy of the plan and proficiency of the plan by contingency team personnel, regular training and testing is essential. It is important to budget and schedule for periodic testing of the plan. The testing can be done for individual phases of the plan followed by testing of the whole plan. Testing the contingency plan is considered by most authors to be the only way of judging the success of contingency planning in an organisation. This is because testing ensures that the contingency plan is current and working if ever an organisation is faced with the situation of putting the plan in action. Datapro (1991) writes that ***"a plan isn't a plan until it has been tested"*** (p108). Datapro (1991) sees testing the plan as a critical activity for staff contingency plan training, and plan maintenance. Information Systems managers must ensure the test is meaningfully conducted, and that all problems are duly noted.

3. Contingency Plan

Lane and Step (1985) suggest that it is not unusual for companies to invest significant resources in the development of a contingency plan, but to fail to provide the necessary resources for testing the plan. Articles published on the subject urging organisations to test their contingency plans imply that contingency plan testing is infrequently carried out in organisations.

Some specialists in this area recommend surprise contingency plan tests as well an regular ***announced*** tests. Overall, authors in this field overwhelmingly agree that frequently testing the plan is critical to the success of contingency planning.

3.4.6. Contingency Plan Maintenance

Contingency plan maintenance consists primarily of keeping information current as to personnel, supplies, facilities and recovery procedures. It is necessary to ensure that the plan reflects the up to date environment. The plan maintenance schedule must coincide directly with problem and change control activities. Update of the contingency plan should be considered a normal part of daily business activities. An outdated plan can lead to creation of a new plan from scratch.

It is vital that all systems development methodologies include contingency planning stage within the methodology. This will ensure that development of any

3. Contingency Plan

new system or modifications to existing systems are catered for in the contingency plan. Computer systems' development or external acquisition must not be signed off unless the development or the purchase incorporates alternate procedures for those applications as part of an organisation's contingency plan.

> "Even after the plan has been distributed and tested, it is not done. In fact, it is never really done. The plan must be continually updated and tested to be of any true value. It is a living document with constantly changing variables" (p18) Lane and Step (1985).

Monitoring and maintenance activities of the contingency plan are emphasised by some authors.Buckland(1991).

4. Contingency Planning - Literature Overview

4. Contingency Planning - Literature Overview

This section describes the views of various authors on the ***need*** for contingency planning and the ***factors which motivate*** organisations to implement such plans. Some well publicised cases of disasters both within Australia and overseas, as reported in the media are also included.

4.1 The Need

The need for contingency planning is made abundantly clear in much of the published literature reviewed. Datapro 1991; Haight & Byers, 1991; John William Toigo, 1989; Robert Brigden Jones, 1992, all stress that contingency planning is an essential activity in a modern organisation. These authors very clearly view the contingency plan as being necessary in the modern organisation which is driven by computer-based systems.

- Robert Brigden Jones(1992), states that it is only in recent years that Australian organisations have earnestly commenced contingency planning. Compared to countries like North America, Australia in general has still a long way to go before the concept is fully accepted. This is because, in North America, the contingency planning concept has grown very rapidly and has been accepted mainly because of the following factors:

4. Contingency Planning - Literature Overview

- existence of well documented cases of corporate disaster
- government regulations which demands compliance and standards to be met
- natural disasters are more frequent and of greater magnitude than in Australia
- director liabilities clearly spell out the need for DRP (Disaster Recovery Planning).

- Datapro (1991) promotes the importance of contingency planning very strongly as follows:

"No longer are computers merely a useful utility. Business has become utterly dependent upon the availability of high-speed information processing, storage, and retrieval. DP [Data Processing] departments tend to serve every area of the organisation, creating a nerve centre that is probably the most critical dependency within the business. The necessity for a DP contingency plan is clear." (p113).

4. Contingency Planning - Literature Overview

- John William Toigo (1989) stresses the responsibility of data processing managers to ensure a contingency plan is in place for the Information Systems they manage. "Service level agreements between the data processing or MIS department and company user departments are a manifestation of this commitment to quality and excellence in information processing. Contingency plans must exist if service level agreements are to be made in good faith." (p7).

- Haight & Byers (1991) make a similar comment on the necessity of contingency planning:

  "Most organisations are so dependent on computer processing that they cannot live without it. The loss of critical computing services - even for a short time - can seriously affect a company's ability to compete. Yet, many organisations do not have an adequate disaster recovery plan (**DRP**) or, if they do, it is nothing more than a collection of manuals, guides and plans that have never been tested." (p13).

4. Contingency Planning - Literature Overview

- An Australasian study, by Moss (1992), found that only 50% of organisations had documented contingency plans. Information System managers find it difficult to convince senior managers to spend on contingency plans since the latter, in general, still believe contingency plans to be a discretionary expense and the risk of losing processing capabilities if it happens is worth taking.

4.2 Motivation Factors

The main factors which prompted organisations to implement contingency plans, as stated in the literature, are:

- actual disaster experience and disaster knowledge
- legal requirements
- auditors' role
- insurance requirements
- economic considerations
- risk and business impact analysis
- management support.

4. Contingency Planning - Literature Overview

4.2.1. Disaster Experience and Disaster Knowledge

McNurlin (1988) points out the possibility of a link between knowledge of published disasters and contingency planning efforts by organisations. Firms which experienced disasters have expanded their contingency planning efforts.

These disasters have focussed management attention on the vulnerability of their own Information Technology environment and the risk of not having contingency plans in place.

The following examples of disasters, both within Australia and overseas, will help clarify the concept. Some well-publicised cases, as reported in computer magazines and news media are described in the following paragraphs.

The 1994 power failure in Western Australia, crippled large sections of the State for lengthy periods. While vital services such as hospitals suffered without the ability to obtain computerised patient information and other medical data, the supermarkets could not get the computers to read barcodes of products and were forced to close. Most areas of business discovered lack of manual procedures for business continuity when their critical computer systems were unavailable.

4. Contingency Planning - Literature Overview

The cutting of Telstra's communication lines within the Sydney Central Business District disconnected access to several computers disrupting the services to users. The earthquake which brought about heavy losses in Newcastle affected several organisations' information processing capacity.

Terrorist bombing in central London caused several computer installations to be destroyed (Fleming,1995). Publications on contingency planning have reported on this disaster as to how prepared some of the affected organisations were when disaster struck. Computer processing in Commercial Union's British operations resumed within a few days due to contingency plans in place for alternative processing (Reed, 1992). An underground flooding paralysed the Chicago central business district in mid-April 1992 (Winkler, 1992) and destroyed a number of offices with data processing facilities. While many organisations were unprepared for such a disaster, those with tested contingency plans and trained recovery teams managed to recover from the industry's ***"biggest crisis to date".*** These organisations were able to achieve business continuity due to alternate processing facilities arranged as a result of contingency planning. The terrorist bombing of the World Trade Centre in the United States of America (IBM, 1994) affected 900 companies and the centre was closed for seven weeks. Those offices which had contingency plans and stored data from their Local Area Networks offsite were able to restore their operations quickly.

4. Contingency Planning - Literature Overview

4.2.2. Legal Requirements

Compliance with legal requirements was another factor behind the effort that organisations in general spent on contingency planning. In the U.S.A. the requirement for contingency planning was introduced whereby all financial institutions chartered by the US government have a demonstrable contingency and business recovery plan (Brigden-Jones, 1992). The UK has the Data Protection Act (1984), which states in part, "appropriate security measures shall be taken against ... accidental loss or destruction of personal data". This Act stipulates that there must be procedures in place (contingency plans) to protect against loss of data. On 26 November 1992, the OECD, including Australia, adopted guidelines for security of Information Systems. These guidelines were prepared by a group of experts headed by Mr. Justice Michael Kirby. Proposals are also being considered with the Standards Association of Australia on the possibility of developing a national standard for the security of Information Systems based on the OECD guidelines. (Commonwealth Government, 1994).

Within the private sector the legal requirements can be divided into two main groups. The first group of requirements relates to the ***customer.*** Wexler (1990) describes the legal impact that an information systems outage might have where an organisation has a twenty-four hour service contract with the customer. If the outage prevented the organisation from satisfying the requirements of the contract,

4. Contingency Planning - Literature Overview

then the customer could seek legal redress for the breach of service level agreements in the civil courts. Those organisations especially those providing computer processing bureau services to government agencies will be unable to provide contracted services if a disaster renders their information processing environment unavailable.

The second group of legal requirements relates to ***confidential information*** held by the organisation. Where an organisation has accepted confidential information, it has a responsibility to protect that information. Wexler suggests that "you should arrange for some reasonable level of protective programs to be maintained on an interim basis" (Wexler, 1990, p41). The data needs to be adequately backed up and safely stored off-site.

Commercial organisations such as banks and insurance companies who are charged with the duty of safeguarding investors' and shareholders' interests may be subject to legal action if it is found that sufficient asset protection arrangements were not in place. An organisation's directors and officers may be subject to personal civil action or even to criminal action if it can be demonstrated that they were, among other things, "negligent by not providing security and continuity of the company though good contingency planning" (Andrews, 1990).

4. Contingency Planning - Literature Overview

4.2.3. Auditors' Role

Haight and Byers (1991) report that internal auditors have taken on the responsibility of appraising the organisation's contingency plans, and presenting the evaluation to information systems managers "as a matter of law" (p13). Major contingency planning projects were undertaken as a result of the evaluations made by auditors.

The auditors can be a powerful force in convincing senior executives to commence contingency planning where the Information Systems manager may be unable to do so. This is because comments from an auditor (internal or other external consultant) telling senior management that a commitment to contingency planning is required carries a lot more weight than the Information Systems manager giving senior management the same message.

4.2.4. Insurance Requirements

The private sector, especially banks need to have contingency plans in place as part of insurance policies available for the protection of company directors and officers from personal liability . Apart from personal liability insurance, there are three other types of insurance that might bear influence on contingency planning

4. Contingency Planning - Literature Overview

decisions: ***property, data and personnel, and business continuation insurance.*** Insurance for the first two types are commonplace and readily available. Business continuity insurance covers the profits that an organisation would have made during the time of a disaster which has caused loss of business due to prolonged Information Systems outage. Most organisations are eligible for the first two types of insurance, but business continuation insurance can be more difficult to obtain. This is because insurance companies will expect the insured to make a commitment to contingency planning before they are willing to provide business continuation insurance (Cheeseman, 1990). Without contingency plans, an organisation is likely only to be offered basic building, staff and equipment insurance coverage.

4.2.5. Economic Considerations

During recession periods and budget cuts within organisations other priorities such as keeping the organisations' core business operations functional takes priority over contingency planning. These organisations prefer to continue using Information Systems even for their critical operations without any plans for contingencies and are prepared to take risks. The financial cost/benefit analysis of having a plan in place before a disaster strikes and the loss to an organisation in not having alternative procedures in place as soon as a disaster occurs were

4. Contingency Planning - Literature Overview

motivating factors which prompted management in those organisations to commence the plan. This is because a disaster within the Information Systems environment deprives the organisations from using its critical systems. The lost value of business due to lack of core business information helped management to decide on a contingency plan implementation. Executive management, however, needs to justify the contingency planning project like any other project before approving the preparation of such plans (Hiatt and Motz, 1990).

4.2.6. Risk And Business Impact Analysis

The conducting of risk analysis involves a review of the existing computer environment and the impact on the organisation's ability to conduct its core functions if such facilities are made unavailable due to a disaster situation. Following the risk analysis, the business impact analysis report is prepared which highlights the extent to which the organisation relies on its Information Systems. This report can be a powerful force in the decision to commence contingency planning efforts. This is because a computer contingency deprives an organisation from using its Information Systems to fulfil its core commitments (Hiatt and Motz, 1990).

4. Contingency Planning - Literature Overview

4.2.7. Management Support

Most authors on this subject stress the importance of gaining the approval and support of top management in any organisation before commencing contingency planning in earnest.

According to Hiatt and Motz (1990), an organisation's senior management must be convinced of the need to protect the information resources before obtaining their support for the development of contingency plans. One suggested method for such convincing would be to prepare Risk Analysis and Business Impact Analysis reports as detailed in **Section 3.4.1**. These reports will help quantify the impact of a disaster and help management to take appropriate decisions to safeguard the investment in information resources.

It is the role of Information Systems management and staff to inform executive management of the need for contingency planning. Moss (1992) found that public sector organisations showed greater management support for security considerations, higher willingness to educate staff on security matters, and were more likely to perform cost/benefit and risk analyses than their private sector counterparts. The Moss study also found a relationship between organisation size and performance in computer security and contingency planning practices. Large

4. Contingency Planning - Literature Overview

organisations were more likely to have formal policies on security and contingency planning, to have developed contingency plans, and tend to test and update their contingency plans more frequently.

5. The Survey

5.1. Research Methods

Research involved the study of selected organisations both in the public and private sectors. A total of 14 organisations were approached. Of the 14 organisations, 9 were from the public sector and the remaining 5 were from the private sector. The public sector organisations included agencies from both the Commonwealth and State Governments. Within the private sector, two major banks , a major insurance company and two computer services bureaux were selected. Information gathered included existing policies and guidelines on contingency planning, factors which prompted the organisations to commence plans and the level of contingency planning practices in those organisations.

The organisations which were included in the study have been classified under public sector and private sector as follows:

- ***Public Sector Organisations***

  Commonwealth Government -

  - The Commonwealth Department of Finance
  - University of Western Sydney

5. The Survey

State of Victoria -

- Department of Finance, Victoria

State of New South Wales -

- NSW Department of Health
- Maritime Services Board of NSW
- NSW Department of Community Services
- NSW Lotteries

State of Western Australia

- Department of State Services, Western Australia

South Australia

- Department of Transport

- ***Private Sector Organisations***
  - Private Banks
  - Private Insurance Company
  - First State Computing Pty. Ltd.
  - Ferntree.

Telephone conversations and a questionnaire (**Appendix A**) were used to gather information. All fourteen organisations responded to the questionnaire. The study focused on finding out what was currently available by way of policies, regulatory framework and facilities for Information Systems contingency

5. The Survey

planning, the existence of a plan, motivating factors that led those organisations to implement such plans and summaries of individual plans. With the intention of minimising the time spent by the organisations in providing the information for this project, interviews and telephone enquires which were made to the personnel responsible for contingency planning were kept as brief as possible. For these reasons, apart from being requested to complete the questionnaire, the staff only answered questions about existing policies and procedures and their involvement in the contingency planning process in their organisations, the extent of their reliance on their Information Systems and about their perceptions of critical success factors for their organisations' continuity of business.

The questionnaire asked the respondents about the existence or otherwise of a fully documented contingency plan for their organisations, the management, testing frequency, performance of risk assessment and any loss suffered by the organisation as a result of disaster. Respondents were also asked to estimate the maximum tolerable period of unavailability of Information Systems which provided core functionalities for their organisation. The tolerable period would provide a measure of the organisation's reliance on their Information Systems.

5. The Survey

5.2. General Data Analysis

It was evident from the information gathered, that in Australia, there is no specific Government legislation regarding contingency planning for Information Systems to protect shareholders, directors, staff and other stakeholders of companies in the private sector. There are indirect rulings built into business law which make directors and other finance professionals including auditors, liable for any loss of business resulting from loss of computer processing facilities for extended periods of time. All the private sector agencies had comprehensive contingency plans with focus on business continuity. The two computer processing bureaux provided alternate processing facilities for organisations both in the private and public sectors as well as catering for their individual contingencies.

One of the two Commonwealth Government respondents stated that approximately 80% of the Commonwealth Government agencies have comprehensive contingency plans. This is because the Commonwealth Government has a centralised policy making body which establishes policies and guidelines on behalf of all agencies within the Federal Government. Only two out of four State Government respondents had contingency policies and guidelines prepared by central bodies on behalf of the other agencies within their states. Those respondents stated that approximately 75% of agencies under their State

5. The Survey

Governments have comprehensive contingency plans and use the standards established by the central bodies.

The other two State Government respondents do not have centralised policies or standards. The agencies within this group depend on internal or external auditors to highlight the risk involved before formulating a plan. In **Section 3.4** the various steps involved in the preparation of an effective contingency plan were covered. Due to lack of standards and sample plans, the agencies within the latter group of State Governments employed consultants to determine the various facets of their plans. **Section 6** provides detailed analysis of each government's position on the adoption or otherwise of the concept. The adherence by these organisations, to the various steps covered in **Section 3.4** will also be analysed in that section.

All the respondents within the private sector and one State Government agency stated that these organisations could tolerate only an hour of unavailability of Information Systems, proving high reliance on these systems to conduct their core business. The tolerance period within the public sector varied between 24 hours to 72 hours.

Despite the fact that there is a lack of standards and guidelines for agencies within the New South Wales State Government, 75% of the respondents in New South Wales Government had developed detailed contingency plans. These agencies had

5. The Survey

completed Business Impact Analysis and Risk Analysis before formulating plans. The remaining 25% were considering the development of a plan. In **Section 3.4.5.** the importance of testing the contingency plans at regular intervals was stressed. The survey revealed that 75% of the agencies which had plans did not test them even annually. Maintenance of the plans also suffered the same fate. The consequence of this was, as highlighted in **Section 3.4.6.,** the plans were outdated and did not reflect the true picture.

5.3. Analysis of Motivation Factors

One of the aims of this project was to determine what factors prompted the individual organisations studied to commence contingency planning work and the importance given by them to this project. In **Section 4.2** , the seven main factors which prompted organisations to commence contingency planning, as stated in the literature, were discussed. The respondents who had contingency plans in place, were each asked to consider which of the seven factors motivated them to prepare such plans. The study showed that not one factor but a mixture of several factors prompted the individual agencies to prepare contingency plans; while the individual agencies within the public sector, gave low priorities to the plans' testing or maintenance. Respondents also provided three additional factors not mentioned in literature which led them to plan preparation. These are ***"contract***

5. The Survey

commitment", "introduction of new hardware and software" and ***"entry of new staff to the organisation".***

The seven factors described in **Section 4.2**, three additional factors provided by the respondents and the number of respondents who were motivated by the individual factors are summarised in **Table-1**. The factors themselves have been prioritised in descending order of importance as seen by the respondents. Details of information collected from the respondents are also analysed against individual factor headings.

Table 1: Contingency Planning Decision Factors

Contingency Planning Decision Factor	Description	Number Motivated
Actual disaster experience/ Disaster knowledge	The decision to commence contingency planning was made as a response to experiencing a near disaster.	12
Senior Management Support	The organisation's senior management supported the acceptance of a contingency planning project.	12
Auditor's role	Contingency planning began after the auditors (internal or external) made comments on the organisation's contingency planning or the lack of it.	11
Legal requirements	Indirect legal requirements and government regulations demanded contingency plans to protect shareholders and customers.	9
Risk analysis or Business Impact Study	Acceptance of a contingency planning project was based on the result of a business impact analysis or risk analysis.	9
Economic considerations	Organisations performed cost/benefit analysis before the project was economically justified	8
Insurance requirements	The organisation's insurer demanded that contingency planning be performed before insurance is offered, as is often the case with business continuity insurance.	5
Contract Commitment	The contingency planning project was initiated due to contract commitment as a service provider	3
New staff	The entry of new staff to the organisation with knowledge of contingency planning prompted the organisation to develop contingency plan when it was not considered earlier.	1
New Hardware & Software	New hardware and software have been introduced which prompted the organisation to consider commencing contingency planning where previously it did not have.	1

5. The Survey

- ***Knowledge of actual disasters*** from well-publicised cases have made all organisations studied realise how vulnerable they are to similar experiences and how vital it is to have in place comprehensive contingency plans. Most cases of disaster or near disaster situations are generally not reported for fear of adverse publicity. All the Information Systems managers interviewed were aware of the recent disasters experienced within Australia **(Section 4.2.1.).** Although all organisations were aware of the risks involved, two respondents did not pursue the idea of developing contingency plans. These agencies gave low priorities to safeguarding investments in Information Technology even though they were aware of the possibility of their core services to the public being unavailable for long periods of time. This could be due to the political instability the government agencies undergo with each change of government. About 50% of the respondents experienced near disasters and commenced contingency plans as a result of it.

- ***Senior Management Support*** was an essential factor critical to the success of contingency planning projects for 90% of the respondents. Management support was considered critical for all computer systems development projects and the respondents stated that contingency planning projects were expected to be no different in this regard. It was evident that this factor contributed to the

5. The Survey

lack of plans within 25% of New South Wales Government agencies. Lack of management support was a real problem in those organisations.

- ***Auditor's Comments*** played important part in 100% of the private sector and 85% of the public sector agencies. Information systems auditors have played major roles in bringing to the notice of Information System managers the need for maintaining contingency plans in those organisations. One agency within the New South Wales Government was considering planning for contingencies following an internal auditor's report. 79% of the respondents agreed this factor to be an important motivating force.

- ***Legal Requirements factor*** including government regulations was instrumental in persuading 9 respondents to commence contingency plans. The Federal Government respondents stated that the Federal Attorney-General's Department has taken the responsibility for coordinating the implementation of OECD guidelines for security of Information Systems within Australia. It has been agreed by the Commonwealth that the guidelines should constitute the minimum standards for safeguarding investments in Information Technology within the Federal Government agencies. Fifty percent of State Government respondents are setting tight contingency planning guidelines and policies for agencies under their control. In particular the Victorian and Western Australian

5. The Survey

government agencies have realised the benefits of contingency planning and have established policies on this subject. These policies ensure that all new computer systems purchased have contingency planning as an integral part of the total solution. The financial institutions, both the banks and an insurance company for this project stated that although there are no direct laws enforcing such organisations to have contingency planning for Information Systems, legal requirements pertaining to finance management insisted that such a plan was in place to safeguard stakeholders interests.

- ***Risk Analysis/Business Impact Analysis*** studies are seen as important by the Information Systems management in 50% of the public sector organisations to gain corporate support for contingency planning and to obtain the necessary funding. A strong business case which focused on mission-critical business functions that depend on computer systems needed to be prepared. As these organisations become more dependent on Information Systems to achieve their business objectives and maintain good public image, the pressure is on Information Systems management to implement contingency plans. An important issue facing Information Systems management of organisations was that, until a Business Impact Analysis study is completed and the business case for a contingency plan preparation is developed, it was impossible to prove to senior management the impact of disaster on the business. Managers interviewed also

5. The Survey

stated that this report helped them to cost-justify the development of a contingency plan and associated recovery strategies. All the private sector organisation studied used this factor initially to justify expenditure on Information Systems contingency planning efforts and later to provide guidance for the development of the contingency plan.

- ***Economic Motivations*** drove one public service respondent and all the private sector respondents to commence contingency planning activities. These organisations functioned as commercial service providers and any loss of processing will result in loss of income and loss of customers. Information gathered from three State Government agencies showed that these organisations treated the plan preparation as any other Information Technology project and performed cost/benefit analysis before accepting a project for contingency planning. Budget cut-backs especially at a time of recession and largescale redundancies within the public sector may have been contributing factor to those agencies which chose to ignore the concept of contingency planning.

- ***Insurance Requirements*** factor was given similar importance as the Auditor's Comments factor in prompting 100% of the private sector respondents to commence contingency plans. Due to privacy reasons the banks could not give details of types of insurance policies which demanded such plans. However one

5. The Survey

can deduce that business continuation insurance and personal liability insurance may have provided motivation for commencing the construction of contingency plans by these institutions. This is because in the case of financial institutions such as banks and insurance companies the need to get computer operations back within a short period to perform core business makes contingency planning part of core activities. None of the public sector respondents were motivated by this factor.

- ***Contract Commitment*** with organisations which were using their services was one of the factors which led two service bureaux in the private sector (18% of respondents) to implement comprehensive contingency plans and alternative processing facilities for their customers. These organisations have signed service-level agreements with their customers and were contractually committed to provide acceptable services. These organisations may be liable for penalty payments to their customers if they fail to provide the agreed level of services.

- ***New Computer Hardware/Software*** introduction was one of the factors which led one State Government agency to commence contingency planning. The organisation introduced Local Area Network technology in all its offices around the state and having invested substantial amount of funds was determined to protect the investment.

5. The Survey

- *New Staff* joining the organisation prompted one State Government agency to develop a plan. The newly appointed officer who had past experience in developing contingency plans prepared risk analysis and business impact analysis reports and convinced management to invest in contingency planning for all their core computer applications.

6. Review of Current Models

6. Review of Current Models

This section provides details of contingency planning efforts in the individual organisations included in the survey and analyses the strategies adopted by those organisations. The whole contingency planning environment in each organisation is treated as a unique model.

6.1. The Commonwealth Government

The background to the establishment of this model is discussed first. The Commonwealth Government's Information Exchange Steering Committee (IESC) is an advisory body, responsible for providing guidance on policies and strategic directions regarding Information Technology (IT) and related issues, including contingency planning for Information Systems and telecommunications for all agencies within the Federal Government. The Committee comprises senior officers from six Commonwealth Departments and Agencies and its main objective is to provide a central body for the coordination of policies and strategies and to promote exchange of information between government agencies. The Committee is chaired by the Deputy Secretary of the Federal Department of Finance. Apart from this Committee, the Federal Government has also established an Information Technology Review Group and on its recommendations is in the process of setting up an Office of Government Information Technology (OGIT) to

6. Review of Current Models

develop a whole-of-government approach to Information Technology use and planning. (Computerworld April 21, 1995).

In late 1990 a working group of the Information Exchange Steering Committee looked at options for encouraging Commonwealth agencies to have in place some kind of contingency plan, with suitable backup arrangements. The contingency planning model set up by this body included guidelines and policy directives to all Federal Government agencies. The first step was a recommendation for amendment of Finance Direction 34 (24) which was promulgated by the issue of Finance Circular 1990/2. From a policy viewpoint, this circular was a mandatory requirement which the agencies had to follow. The main thrust of this policy was the safeguarding of computer records and installations. The circular informed departments and agencies of a variation to Finance Direction 34 (24), relating to the protection of computer records and installations. New procedures were set up which aimed at reducing the risk of major interruptions to essential operations due to disaster within the agencies' Information Systems environment. They also apply to software records, data and documentation related to computer systems which, if lost or corrupted would have a significant impact on the provision of critical services for which a department is responsible.(Circular No. 1990/2).

The Commonwealth Government's centralised model included the distribution of a directive to all agencies to establish strategies which minimise the impact of

6. Review of Current Models

disaster including contingency procedures for the continued provision of critical services until normal services are restored and a contingency plan to determine a course of action when a disaster occurs. "It is the responsibility of senior management to ensure that appropriate contingency planning procedures are in place, are effective and fit the organisation's particular ADP configuration" - (Security in the ADP Environment, Personnel Management Manual).

The standards and guidelines for the plan preparation followed the stages included in **Section 3.4**. These standards provided templates which the agencies could follow in their plans preparation. Apart from issuing directives and guidelines, the model included the setting up of an appropriate computer site to be nominated as a ***"cold site"*** for use in emergencies where an agency loses computer processing capability for an unacceptable length of time. Following negotiations, an agreement was drawn up between the Health Insurance Commission and the Department of Administrative Services to use approximately 500 square metres of floor space and processing facilities belonging to the Health Insurance Commission. About nine agencies joined the agreement to use the ***"cold site"*** by subscribing on a monthly basis. The member agencies were given the option to use the processing facilities provided by this site whenever an emergency occurred in their home sites which resulted in loss of computer processing capability for an unacceptable length of time. The agreement was renegotiated in late 1993. However only three agencies are using this facility presently while the other six

6. Review of Current Models

have decided to make their own arrangements for contingency planning. It is likely that this arrangement may cease for lack of support from the individual agencies.

The paradigm described above provides for centralised regulation and guidance with facilities which can be shared by all government agencies and provides for cost effective insurance in the event of disruption to information services of any agency. In **Sections 3.1. and 3.2.** the aims and objectives of contingency planning were stated. This model included those aims and objectives in the guidelines. However, one can assume that while the guidelines and policies have been successful in imparting a sense of responsibility of securing Information Technology infrastructure on the agencies, the common ***"cold site"*** facility has been a failure. Within the Commonwealth Government agencies, some agencies have developed comprehensive contingency plans which are tested on a regular basis. Others are in the process of developing or redeveloping Information Systems contingency plans to suit their critical business continuity. Almost all agencies have made their own arrangements for ***"hot site"*** or ***"cold site"*** with some having even dual information processing sites. With the proposed formation of the Office of Government Information Technology as the centralised body to co-ordinate the ***"whole-of-government"*** information resources, a return to a well-defined centralised model for contingency planning which can be used by all Federal Government agencies appears to be possible.

6. Review of Current Models

A senior public servant from a Federal Government agency stated that one of the key factors of contingency planning for that agency was to ensure the revenue collections are processed and banked on time to help the government's cash-flow situation. The hardware platform changed with introduction of Local Area Networks in all Branch offices. The agency recognised the need for a workable contingency plan which helped business resumption and not just computer recovery. This case demonstrates the role of economic factors in the decision for contingency planning. The agency initially developed a plan for their mainframe systems in 1988 and have subsequently updated and tested the plan for their varying hardware platforms and decided to introduce packaged software to manage their contingency plan in 1992. The software was tailored to their requirements with the support of the individual branches. The Department is committed to contingency planning and even made use of **"actual experience"** of a flood and a fire in one of their branch offices to improve on their original plan. This agency was committed to maintaining the plan for reasons included in **Section 3.4.6.**

The motivating factors for contingency planning in the above model were a combination of several factors, which in descending order of importance, include actual disaster experience, legal requirements such as government regulations, risk analysis and economic considerations.

6. Review of Current Models

6.2. Victorian State Government

In Victoria, the Information Technology Policy Division of the Department of Finance is the policy-making authority for all public sector organisations within the state. The individual agencies manage their own Information Technology. The Victorian Government is currently in the process of handing over the Information Technology service provision in the public sector to private agencies. Those agencies which require security and confidentiality of data or systems which cannot be adequately provided by an external organisation, have their own information processing infrastructure. As far as contingency planning is concerned, this body is a regulatory authority which provides guidelines and policies to all government agencies. The guidelines produced by this office on **"outsourcing"** of Information Technology functions to commercial service providers, includes in its list of Information Technology services and functions, mandatory contingency planning requirements which must be provided by the outside provider. Typical contingency plan functions will include archival services for backup data, business continuity processing requirements and contingency plan. The document "Information Technology Outsourcing Best Practice Methodology", dated April 1993 produced by this office contains a separate section on security and privacy protection. It includes a section entitled "Proposed Disaster Recovery Plans and insurance coverage should be detailed by the outsourcing vendor".

6. Review of Current Models

Following the Ash Wednesday fires in 1983, a review was taken on the existing contingency plans by the Commissioner of Victorian Police who was made responsible by the Government of the day to prepare a state-wide disaster plan to counter the effect of emergencies within the state. This plan established a vast committee structure to include municipal, regional and State levels. It is the responsibility of individual organisations within that committee to cater for their own contingency plans. (Roberts, 1992)

In the above model, the decision factor Legal Requirements such as government regulations plays a leading role in establishing the need for contingency planning. From the above facts it is obvious that in Victoria there are no centrally prepared standards similar to the Federal Government model for contingency planning which can be shared by all government agencies in the event of an emergency. Each public sector agency has made its own contingency plans and ***"hot site"*** or ***"cold site"*** arrangements. Where an agency has contracted its information processing functions to an external service provider, it is the responsibility of the service provider to provide contingency plan and procedures as part of the negotiated contract.

Since most agencies in the state are considering ***"outsourcing"*** of information services, the providers of such services are motivated by **Contract Commitment** factor in the provision of contingency plans. Those agencies which have

6. Review of Current Models

completed contingency plans have followed all the steps detailed in **Section 3.4.** These organisations have prepared risk analysis and business impact analysis for core applications and ensure regular testing and maintenance of the plans. This model provides for regulatory measures only, without a centralised infrastructure for common alternate processing facilities.

6.3. South Australian Government

Information obtained from a South Australian government agency showed that there were no central regulations or standards relating to contingency planning for Information Systems. In general most agencies did not have any contingency plans in place making their Information Technology environment vulnerable for loss. This was despite the fact that these agencies were highly dependent on information processing to carry out their core business. Knowledge of disasters in other organisations was not a factor which encouraged these agencies to start a plan.

More recently the State Government has awarded the contract for the provision of computer processing services for all State Government agencies to an external organisation. All the individual agencies have been asked to standardise to common hardware and software platforms which will be managed centrally. The contract includes comprehensive contingency planning provisions which have to

6. Review of Current Models

be provided by the contractor. Since all processing on behalf of all agencies is done centrally by the contractor, ***"hot site"*** provisions for continuity of processing services will be compulsory and the contractor is obliged to provide such services. This will enable this state to establish a centralised model for contingency planning similar to the Federal Government. This may become cost-effective and efficient centralised facilities for contingency planning for all South Australian Government agencies without the need for the individual agencies to make their own arrangements.

6.4. Government of Western Australia

The study found that the Western Australian Government model for contingency planning included comprehensive guidelines and standards for the plan preparation for the various departments. The Western Australian Department of Computing and Information Technology produced a "Disaster Recovery and Contingency Planning Manual" which provides advice and templates to the other public sector agencies within the State in developing their individual contingency plans. The manual was prepared in partnership with a number of public sector agencies. This document was intended both as a reference document and a discussion paper which addresses the policy issues that are relevant to the preparation of such plans. The guidelines also entrusted the responsibility for Information Technology contingency planning with the Chief

6. Review of Current Models

Executive Officer of each agency and stressed that the plan should be an integral part of an agency's overall business strategy.

The central authority provided useful guidelines to alert the various public sector agencies on the importance of having a contingency plan in place and provided detailed plans on policy, environment and the performance criteria around which a contingency plan can be developed. It was a blueprint on what to expect from such a plan and provided a checklist of tasks which need to be completed at various phase of the plan. The details included in the checklist are similar to those in **Section 3.4**.

The main objectives of a contingency plan as stated in the manual includes continuity of core business services with minimum disruption. So as to achieve these objectives the manual recommends the various facets of contingency plan as included in **Section 3.4.**

In 1989, the Department of Computing and Information Technology prepared plans for establishing a central Data Centre which could provide Facilities Management for all agencies within the State. The contingency planning model included a ***"warm site"*** centre which would provide back-up processing facilities for IBM -compatible hardware environment for those agencies which had IBM mainframes. The hardware in the ***"warm site"*** would be used mainly as a backup

6. Review of Current Models

site in the event of a disaster in an agency's home site. The hardware was to be used for development purposes but will provide disaster recovery backup for any agency which requires it. This model acknowledges the fact that any disruption in information processing can cause serious disruption to the provision of core services and as such the prevention of a disaster should be a key part of the strategy to provide core business services.

The Western Australian model is ideal in the sense that not only did it provide detailed guidelines with reasons for establishing a well-documented contingency plan for Information Systems processing, it also included a proposal for a centralised infrastructure which can be shared by all agencies when a disaster occurs in any one agency. The motivating factors were, legal requirements (government regulations), auditor's role and new staff who joined the organisation.

The proposal, however did not materialise. While the model was accepted by the Department of Premier and Cabinet, the proposal was not adopted for various reasons. The model, however was based on a very good concept and would have provided all agencies with cost-effective contingency plans. If it was successfully implemented the model would have provided an effective blueprint for government agencies. The concept of central processing facilities to be shared by a number of agencies , although expensive initially, would have been economic in

6. Review of Current Models

the long run. It would have saved the cost of setting up individual alternate processing capabilities.

The main reasons behind the failure of the proposal, as stated by the respondent, and ***which need to be taken into account for successful implementation of models recommended in this report*** are as follows:

- change of policy directions within the Government
- perceived high cost of establishing the infrastructure
- perceived reduction in mainframe processing
- failure of Western Australia Inc.
- political differences of opinions
- non-standard configuration of agencies hardware/software
- low priority given to contingency planning
- poor marketing of the proposal to the agencies
- lack of commitment and distrust on the part of the agencies.

More recently the Department of Premier and Cabinet has established a Strategic Management and Information Technology Unit to oversee Information Technology delivery within the Western Australia State. This Unit is in the process of updating the contingency planning document of 1989 with new suite of policies and guidelines on risk management and business continuity to cater for

6. Review of Current Models

1990's information processing which has seen decrease in mainframe processing and an increase in midrange and Local Area Network-based systems.

The Department is currently conducting a rationalisation programme of mainframe processing whereby all agencies which still continue mainframe processing (both old systems and current business systems) would be grouped together into one site so as to save on spare capacity on individual machines . Contingency planning for this site would be the responsibility of an external provider or any office which would be managing the facility. Until this model is established, it is the responsibility of individual agencies to arrange contingency planning for their Information Technology infrastructure.

Enquiries on the current status at some of the agencies revealed the following:

- some have made ***"cold site"*** arrangements with another organisation
- some depend on backup storage of data only
- some use the spare capacity in another agency for back-up purposes
- some use ***"hot site"*** facilities offered by the hardware vendors.

6.5. New South Wales State Government

In New South Wales, there is no central agency nominated to manage the contingency planning functions on behalf of the other agencies similar to the

6. Review of Current Models

Western Australian model. There are no specific guidelines or policies from a central authority. The Office of Public Management which is currently merged with the Department of Public Works and Services issued a series of documents under the title "Management of Information Technology - Statement of Best Practices" for use by the agencies. This document, however does not include policies or standards on contingency planning. There are sections on security and safeguard of data held in computers. Each agency is responsible to take whatever measures are appropriate to safeguard their investment in Information Technology. The trend towards Personal Computers, Local Area Networks and end-user computing increases the risk within the Information Systems environment. Yet 25% of the respondents who are aware of their vulnerability to electronic intrusion and failure have chosen not to plan for recovery from such risks. Seventy five percent, however have implemented contingency plans and have made individual arrangements for alternate processing facilities. Each agency's arrangement is described in the following paragraphs. For confidentiality reasons, the actual names of these agencies have been suppressed.

Case Study Agency A has formulated a detailed contingency plan for its core computer systems residing on the mainframe. Alternative procedures have been defined for each application with the help of users. The plan is updated regularly and staff are trained in alternate procedures. The team responsible for contingency planning receive good support from senior management. ***"Hot site"*** arrangements

6. Review of Current Models

have been made by the contract company which provides bureau processing services. The plan is tested regularly. With the expansion of LANs within the agency, the Department is looking into updating the plan to cater for communication-related emergencies.

Case Study Agency B also has a comprehensive contingency plan and on the advice of consultants, has made ***"warm site"*** arrangements with a private bank located in another suburb to the agency. Back-up tapes are stored at the alternate site and will be used in the event of a disaster at the home site. The agency would be able to resume processing almost immediately if a disaster renders the prime site unoperational.

Case Study Agency C has a contingency plan with back-up processing facilities with a hardware vendor. Spare processing capacities within the agency's branches are also used to provide for contingency processing capabilities. Maintenance and testing of the plan did not occur on a regular basis.

Case Study Agency D does not have any contingency plan or alternate processing facilities. Main reasons for not having a plan in place include lack of management support and economic factors at a time when the agency is going through a major reorganisation and cost cutting process. A project for contingency planning has been initiated as a result of internal auditor's report over the lack of such a plan.

6. Review of Current Models

In general each agency has its own contingency plan or is in the process of developing one due to pressure from the auditors. Those agencies which have developed contingency plans have followed some of the steps as included in **Section 3** in developing the plans. The factors which motivated these agencies to prepare the plan or to prepare a business case include knowledge of disasters especially within New South Wales, reports from internal auditors on the lack of such plans, economic considerations, Risk and Business Impact studies and support from senior management. The respondents which had contingency plans used some form of preset priorities for recovering the systems. The reasons for the prioritisation of applications were to reduce the demand for management decisions at the time of the contingency. Owners of the applications determine which applications are important for the core functions of an organisation and are identified during the Risk Analysis stage. Managers responsible for contingency planning operations can put the agreed plan into action without having to take spot decisions on setting priorities.

6.6. Private Sector

All the private sector organisations included in the study had comprehensive plans for recovering from disaster within a few hours and to continue business services. The insurance company has taken a proactive approach in putting in place security provisions for safeguarding equipment and data against intrusion. Internal ***"hot***

6. Review of Current Models

site" facility has been set up in a different geographical area from the prime computer site. "Electronic vaulting" whereby transactions are recorded at a backup site as they are entered have been arranged with the hardware vendor. This enables this organisation to recover from any disaster in their prime site within a few hours. Since transactions are stored on disc, time is saved in recovering from tape storage.

The critical factors which led a major insurance company and major banks to introduce comprehensive contingency plans for their Information Systems include legal, insurance and economic considerations as well as support from senior management. Strategic reasons also played an important role. As McNurlin et al (1988) point out "strategic use of information systems in banking and financial services is not merely valuable, it is a matter of survival." Information Systems for these organisations play a strategic role as they develop profitable products based on Information Systems. The organisations studied believe that their investment in Information Technology can influence their competitive position in the industry by providing products which cost less and use resources economically. Apart from fiscal and legal factors, the main driving force for these organisations to develop contingency plans is for business continuity. These organisations need to maintain their customer base by providing unique products and valuable information at little or no charge to their customers. These organisations believe that disruption in processing information for lengthy periods

6. Review of Current Models

of time, will lead to losing the competitive edge in the market place and their customer base.

The two bureaux service providers in the private sector were governed mainly by the contract commitment factor to establish comprehensive contingency plans including ***"hot site"*** facilities. As computer processing service providers, these organisations need to meet service level agreements with their customers. Disruption in the provision of services will lead to penalty payments to their customers.

The contingency planning environment in the private sector follows all the steps of effective contingency planning (**Section 3.4**). Business impact analysis of their various products are done every time a new product is developed. Following the analysis, recovery strategies are designed with the help of users of the specific applications. These are then incorporated into their contingency plans which are maintained on a regular basis. Training of staff is carried out on a regular basis. The recovery strategies and alternate processing facilities are tested periodically as per pre-set schedules. The private sector has full support of senior management and considers investment in contingency planning as crucial to business continuity.

7. Discussion

This section analyses the current situation within the New South Wales Government agencies and then suggests two models for the provision of cost-effective contingency planning services for those agencies.

7.1. Current Status

The discussion involves an analysis of the current situation within New South Wales Government sector and its drawbacks. As stated in Section 6.5, only 75% of the agencies surveyed had formulated some form of contingency plans. The remaining 25% did not have such plans in place. There were no central standards or guidelines which all agencies could follow in developing or maintaining the plans. As a result interested agencies engaged external consultants to prepare individual guidelines and contingency plans. Consultant fees were incurred by the agencies individually due to lack of internal expertise. Those agencies who had already developed contingency plans made their own individual alternative processing facilities as per their plans and invoked those procedures when disasters happened. The infrastructure varied between ***"hot site", "warm site"*** or ***"cold site"*** facilities which had been arranged individually by each agency and paid for from funds within the agencies' individual budgets. Some agencies had made alternative processing facilities with hardware vendors, bureau services and

7. Discussion

with other organisations in the private sector. These were individual arrangements, some of them informal, and were paid for individually by each agency. It was evident that funding played a major part in the ability of an agency to secure their individual Information Systems infrastructure. Yet there were no attempts made to sharing alternative processing capabilities among the agencies, nor building internal expertise in the area. External consultants were engaged by each agency every time the plan required updating. The contingency plans themselves were not maintained regularly nor tested periodically. Lack of internal expertise in this area of information processing rendered these agencies vulnerable to loss of information by using outdated plans. Staff turnover has increased the risk of lack of trained staff. This was because, whenever new staff joined the agencies, they were not given training in the operation of the plan.

The agencies which had no provision for contingencies within their Information Technology environment would be unable to provide processing for its users in the case of a disaster. If a disaster strikes which disrupts computer processing, the situation would be evaluated and appropriate action would be taken on a ***"best can"*** basis. These agencies would continue to remain without any formal arrangements for alternative processing arrangements as they are now.

7. Discussion

It is obvious that the cost to the State Government as a whole is enormous due to lack of shared facilities for alternative processing and lack of guidelines which can be shared by all. Analysing the costs further, it can be seen that the cost for those agencies which do not have any contingency plans in place is nil in terms of dollar value but very high in terms of intangible costs such as loss of public image and trust if a disaster occurs. Agencies wishing to put contingency plans in place are spending consulting fees individually for the preparation of Business Impact Analysis, contingency plans and recovery procedures. These fees vary from site to site. The other agencies with individual plans continue to spend separate funds to maintain the alternative processing arrangements even though some of them use identical hardware platforms. Each agency is paying for the establishment or the use of ***"hot site"***, ***"warm site"*** or ***"cold site"*** facilities individually. The total cost for the State Government as a whole would continue to increase. Agencies which have co-operative processing arrangements with other organisations in the event of a disaster may find that alternate processing facilities totally inadequate when required. This is because testing is not conducted on a regular basis.

7. Discussion

The disadvantages of continuing the current situation are summarised below:

- If a disaster occurs, the disruption to the core business of an agency without any contingency plan could be severe. The extent of the disruption to computer processing is directly related to the nature and extent of the disaster. These agencies are running the risk of suffering severe tangible and intangible losses in their service delivery.

- The backup site may not be operational when required. Depending on the alternate processing selected, each agency could be liable for individual capital investment or recurring expenses for maintaining the alternate facilities.

- Since there are no central guidelines or co-ordination, the cost to the State Government as a whole by way of consultants fees to prepare individual guidelines and plan would be enormous. There is no economy of scale gained by the government as a whole.

- Whilst most agencies use IBM-compatible hardware platforms, there is no coordination among them to develop common alternate processing facilities to save funds spent on individual arrangements.

7. Discussion

- For those agencies without any contingency arrangements, maintaining the status quo is certainly the least expensive option, provided the computing centre is disaster free. However, in the event of a disaster, the cost to the agency , both politically and monetarily would be considerable. In a disaster scenario those agencies with no plans in place would be liable for heavy losses and loss of confidence by the users and customers.

- Individual agencies, by making their own investments in contingency planning and arranging for alternative processing facilities would be duplicating the expenditure. This is despite the fact that each one of them may have similar hardware and software platforms. As a result, the State Government as a whole would be spending heavily for the alternate processing arrangements by individual agencies.

- The agencies which have cooperative arrangements with other organisations, run the risk of not being able to use those facilities when actually required.

Certainly this is not an economic or efficient means for the provision of contingency planning services for the State Government as a whole. There are no economies of scale gained by collective bargaining on a high volume basis. If this situation continues, the State Government would continue to incur wasteful

7. Discussion

expenditure in duplicate services in some of its agencies and the investments in Information Technology in the others would not be protected.

The following two models are suggested with the objective of improving the current situation and to ensure that all agencies within the State Government have comprehensive contingency plans in place. Another advantage will be to obtain effective value for each contingency planning dollar spent by the State Government. The report will discuss each model under the following headings:

- description of the model
- cost estimate of implementation
- advantages of the model
- disadvantages of the model
- overall assessment.

7.2. Model 1 - Centralised Government Owned Infrastructure

7.2.1. Description

This model is similar to the Western Australian model where the State Government nominates one agency under its control to establish a ***Contingency Planning Centre*** for Information Systems on behalf of all its agencies. All

7. Discussion

agencies within the State Government will be vetted by this agency for adequate contingency planning infrastructure. For this model to be successfully implemented, the reasons for the failure of the Western Australian model **(Section 6.4)** need to be studied carefully. The central agency will co-ordinate contingency planning activities for all New South Wales Government agencies. This is a whole-of-government approach to contingency planning. The emphasis should be to create an awareness of the concept of securing the Information Systems investments among the agencies.

The main responsibilities of the centre are to:

- take a proactive approach to contingency management in that the centre would be responsible for providing guidelines and documentation on risk management, with emphasis on how to avoid disaster situations and provide different strategies for protection of data and computer environment against damage
- be responsible for providing detailed information on contingency plan preparation for the various agencies which may not have internal contingency planning expertise
- prepare a blueprint on the steps involved in the plan preparation as detailed in **Section 3**
- have access to a range of alternate processing facilities

7. Discussion

- maintain a pool of experts in the field and provide trained staff to agencies for contingency planning projects
- provide ***"hot site", "warm site", "cold site"*** and ***"cooperative processing"*** facilities.

7.2.1.1. Alternate Processing Facilities

The co-ordinating agency would be responsible for the establishment and maintenance of alternate processing facilities such as ***"hot site", "warm site" "cold site"*** and ***"co-operative processing"*** for a range of hardware platforms. Telecommunication lines would be installed connecting the member agencies to these sites. The users of the facilities would be only the agencies within the State Government. The centre would have sufficient processing power to service ***critical applications*** of the ***largest participating member*** agency. The facilities would be used to provide data processing services on an interruptible basis when not required for contingency backup. Agencies would be able to use the facilities for systems development and testing purposes.

Those agencies which require alternate processing within a short timeframe would require ***"hot site"*** facilities which host similar hardware and software ready for use in an emergency. The site could be used to provide developmental resource

7. Discussion

for these agencies thus reducing the load on the primary site. This facility is the most expensive contingency option; but for those agencies which require rapid resumption to normal processing of highly critical applications this alternative is mandatory.

Since the majority of agencies use IBM-compatible mainframe computers **a** ***"warm site"*** fully equipped with IBM-compatible hardware can be established. Backup tapes of participating agencies including data and individual operating systems would be stored in this site. In the event of a disaster, the affected agency would restore both operating system and data from these tapes on the available hardware and run critical applications on it. The site could be used for development of systems by some agencies thus reducing the processing load on the primary computer. Since the site would be used by a number of agencies, a schedule of testing plans of the site by the participating agencies would be drawn. Depending on the number of agencies using the site the computer hardware would be kept utilised for testing purposes of individual agencies contingency plans.

Apart from the centralised ***"hot site"*** and ***"warm site"*** facilities described above, the centre could arrange for ***"Co-operative processing"*** arrangements between member agencies with identical hardware and software platforms. Firm arrangements need to be made between the members for guaranteed mutual help

7. Discussion

when required. One agency would accept the work of another agency temporarily during the time the affected agency is inoperable for processing the critical applications. The mutual arrangement may also be made within an agency with multiple sites holding similar hardware and software platforms. The co-ordinating agency would be responsible for ensuring that the participating agencies have ***"letters/memorandum of understanding"*** of the scope of backup which would be provided. Formal agreements need to be signed by the various parties. Rehearsals should be conducted on a regular basis and should include full operations of critical functions as stated in the agreement.

As for ***"cold site"*** facilities, a vacant site with computer room capabilities including raised floor, power, communication and other facilities could be nominated for use by any agency within the State Government if their individual home site experiences a disaster. The site would always be in a standby ready status and would be capable of accepting any agency's hardware at the time of disaster. The site could also be used as a common backup site for storage of data disks and tapes. Any agency could take over the site during occupancy, convert it to their command centre and install its own hardware. Because of the relative low cost for maintaining the site and the ability for any agency to hire or lease computers to be installed at the site, this solution would be a cost-effective alternative for long-term contingencies. In the event of a disaster in their home

7. Discussion

sites, the agencies would be provided the use of the empty rooms to assemble backup computer systems that could be brought in by vendors by pre-existing arrangements. High speed communication lines to the various agencies would be required either to be installed permanently or leased at short notice. Being a ***multiple-agency-user-site,*** a time limit would be put on the duration of emergency usage that would be allowed. Continued use of the facility by any one agency for long periods of emergency use would render the particular hardware platform useless for other members with similar equipment.

7.2.2. Cost Estimate

There are initial capital costs of setting up the various alternative processing infrastructures. Computer hardware and software for the ***"hot site"*** facility needs to be either purchased or leased. All types of alternate processing sites would require maintenance and establishment costs. Staff costs also need to be considered. The costs could be recovered on a ***"user pays"*** basis from the member agencies thus making it more justifiable. Currently, each agency pays for individual arrangements with external organisations. These funds could be used to pay the central agency. Since the centre would be operating on a non-profit basis, the costs to the individual agencies would be less than the amount currently being paid to external companies.

7. Discussion

"Co-operative processing" option would be cost effective as an alternative processing strategy in that only the extra capacity which would normally be used for development or training would be used when a disaster strikes a member agency. The direct cost of setting up this option would be nil and the effort required to establish, test and maintain this option would be relatively small compared to the other options. There would be no outlay for building, computer equipment or facilities.

7.2.3. Advantages

The main advantages of this model are:

- the co-ordinating agency would ensure that all agencies had contingency plans in place and the State Government's investment in Information Systems was protected
- this model would provide for cost-effective contingency planning services for the State Government as a whole
- savings could be made by the State Government by eliminating duplicate services among its agencies
- obtaining management support for contingency planning projects would be easier for the member agencies

7. Discussion

- agencies would be given detailed guidelines, consultancy and documentation to develop their individual plans saving in external consultancy costs
- each agency would have autonomy and independence of processing; while having access to guaranteed alternate processing facilities
- planning for contingency would be made easy for the members with help and guidelines readily available
- expertise would be held centrally without duplication of effort in different agencies
- the hardware in the ***"hot site"*** and ***"co-operative processing site"*** would be ready to operate as soon as backup data was loaded which is frequently within four hours
- software and operational support would be readily available in the recovery sites
- each agency need not be concerned with the logistics of ensuring the availability of alternative site.

7.2.4. Disadvantages

The disadvantages of this model are:

- the model may be perceived as expensive because of capital costs to set up the different infrastructure, telecommunications and staffing for ***"hot site", "warm site"*** and ***"cold site"***

7. Discussion

- the backup site in a ***"Co-operative processing"*** arrangement may not be operational when required. Depending on alternative processing selected the use of such facilities would be limited to critical applications only for a short term
- logistical problems could be significant if the centre cannot get the co-operation of the other agencies
- member agencies may consider the centre as a political ploy to gain central control of their Information Technology activities
- each agency may not be willing to part with a portion of their budget for these services
- member agencies may be concerned about security if other organisations were sharing the same facility.

7.2.5. Overall Assessment

Provided the disadvantages of this model are overcome, this model would provide the necessary guarantee for the safeguard of the State Government's investments in Information Technology and protection against loss of processing if a disaster happens in any of its agency's Information Technology environment. Economies of scale could be gained by collective bargaining on a high volume basis. The tasks involved for the co-ordinating agency to establish efficient contingency planning for all other agencies would be made easier if the New

7. Discussion

South Wales Government passed legislation on compulsory contingency planning for Information Systems and security for data.

This model certainly would provide for contingency planning and recovery strategies for those agencies without any contingency arrangements. Information Technology managers in these agencies could overcome senior management resistance to contingency planning by the coordinating agency attending to the issue on their behalf.

By centralised planning on behalf of all agencies, the individual agencies could save on investments in contingency planning and arranging for alternate processing individually. Although the centre would be face staffing costs, this would be offset by each agency spending consultancy fees for external consultants.

The initial capital costs of setting up the various alternate processing sites could be easily offset against the costs of individual arrangements made by each agency. State Government owned premises located in remote sites which are vacant could be utilised for setting up the ***"cold site"*** facilities. Facilities are already in place for the storage of computer backup tapes which are shared by all agencies.

7. Discussion

7.3. Model 2 - Service Provider Period Contract Model

7.3.1. Description

This model is similar to **Model 1**, the difference being in the provision and facilities management of alternative processing infrastructure. The central co-ordinating agency could purchase contingency planning facilities from organisations in the private sector which specialise in such services, rather than spending capital in establishing state-government owned ***"hot site"***, ***"warm site"*** or ***"cold site"*** facilities centrally. Organisations such as First State Computing and Ferntree provide commercial ***"hot"*** , ***"warm"*** or ***"cold"*** sites. There are other consortiums of companies which are prepared to provide such services to a range of hardware and software configurations. One approach could be via commercial organisations which provide the individual services, developing alliances with each other to provide state-wide services for contingency planning and security. This would ensure there was capacity to cope, giving vendors greater credibility and help reduce the cost of the service in the event of vendors having to provide individually.

The main advantage of this model would be that, the coordinating body negotiating collective services on behalf of all agencies, rather than individual agencies negotiating and contracting the services. This would gain economies of

7. Discussion

scale for the State Government as a whole and eliminate duplication of effort within the individual agencies. By collective bargaining the State Government would see dramatic reduction in the cost of products and services.

Before arranging for period/common-use contracts with private agencies, the co-ordinating agency needs to identify the individual alternative processing requirements of all agencies. Period contracts, as the name implies are negotiated for a specific period of time, during which all agencies may purchase contingency planning and associated alternative processing services from one or more contractors nominated. All contracts negotiated should cater for proprietary platforms which exist currently but be adaptable for open hybrid platforms which allow for seamless integration of various systems. In future these hybrid hardware and software would allow for standard environment which could be shared by all agencies.

The main responsibilities of the centre are to:

- take a proactive approach to contingency management in that the centre would be responsible for providing guidelines and documentation on risk management, with emphasis on how to avoid disaster situations and provide different strategies for protection of data and computer environment against damage

7. Discussion

- be responsible for providing detailed information on contingency plan preparation for the various agencies which may not have internal contingency planning expertise
- prepare a blueprint on the need for and the steps involved in the plan preparation as included in **Section 3**
- prepare safety and security guidelines for inclusion in contracts
- maintain a pool of experts in the field and provide trained staff to agencies for contingency planning projects
- call for tenders for the state-wide provision of contingency planning services
- arrange for period contracts for the provision of ***"hot site", "warm site", "cold site"*** and ***"co-operative processing"*** facilities.

7.3.2. Cost Estimate

The State Government need not be concerned with the capital costs of setting up the ***"hot site"***, ***"warm site"*** and ***"cold site"*** infrastructure. There would be no maintenance and running costs to maintain government-owned infrastructure. Staff costs of running the centre need to be considered. However there would be ongoing costs of leasing or renting the services from the external organisations. These costs could be negotiated by the central agency; which must ensure that

7. Discussion

competitive quotes were obtained before selecting efficient and cost effective provider or providers of such services. This approach would be more economical than the individual agencies seeking their own contracts. This is due to the fact that the State Government could gain volume discounts by the centre negotiating on behalf of all agencies.

7.3.3. Advantages

The advantages of this model are:

- all government agencies could use standandard terms and conditions negotiated by the central agency thus decreasing the possibility of misunderstanding between purchasers and vendors
- competition between the vendors of services for government business would help keep the prices of these services low thereby leading to significant savings to the Government as a whole
- the co-ordinating agency would ensure that all agencies have contingency plans in place and the State Government's investment in Information Systems was protected
- agencies would be given detailed guidelines, consultancy and documentation to develop their individual plans saving in external consultancy costs

7. Discussion

- each agency would have autonomy and independence of processing; while having access to guaranteed alternate processing facilities
- planning for contingency would be made easy for the members with help and guidelines readily available
- expertise would be held centrally without duplication of effort in different agencies
- the hardware in the commercial processing site would be ready to operate as soon as backup data is loaded, which is frequently within four hours
- software and operational support would be readily available in the recovery sites
- each agency need not be concerned with the logistics of ensuring the availability of alternate site
- member agencies would not feel threatened since each agency would be autonomous in arranging for their own contingency planning according to their budget.

7.3.4. Disadvantages

The drawbacks of this model are:

- there may be additional costs to the service bureau if an agency required immediate attention and therefore came under the category of ***important***

7. Discussion

customer. If only monthly modest charges were negotiated, then obtaining priority instantly to the detriment of other high-fee paying customers may be difficult

- depending on charging mechanism chosen such facilities would be limited to critical applications only for a short term
- member agencies may be concerned about security if other organisations were sharing the same facility.

7.3.5. Overall Assessment

For the whole-of-government approach this model could be implemented within a short time frame. Apart from eliminating political problems of being forced to use the government-owned infrastructure as in **Model 1**, this model would provide help and guidance from the central body in obtaining consultancy and choice of vendors whose credentials would have already been audited. This model certainly would provide for contingency planning and recovery strategies in place of nil arrangements. Information Technology managers in these agencies could overcome senior management resistance to contingency planning by the coordinating agency attending to the issue on their behalf.

7. Discussion

By centralised planning on behalf of all agencies, the individual agencies could save on costs which would have been negotiated on a group basis. Although the centre would face staffing costs, this would be offset by each agency spending consultancy fees for external consultants. This model would provide for guaranteed safeguard of the State Government investment in Information Technology and protection against loss of processing. Economies of scale could be gained by collective bargaining on a high volume basis.

Under this model all aspects of security required by the individual agencies should be examined and documented and could be incorporated within the contracts with the service providers. This would cover both physical, application access and data security. Careful consideration must be given to the privacy of data held with an external contractor.

Problems relating to non-cooperation of participating agencies would not be significant since each agency would be independent to chose any vendor suitable to their requirements provided the vendor is in the period contract. This model would be in accordance with the current trend in Government policy to ***"outsource"*** all non-core functions performed by the agencies.

7. Discussion

7.4. Recommended Model

The models described previously have their individual advantages and disadvantages. However, in my opinion, **Model 1 - Centralised Government Owned Infrastructure**, is the better of the two models for the following reasons:

- savings could be made by the State Government by eliminating duplicate arrangements by the individual agencies with external service providers
- the capital costs of setting up the infrastructure could be recovered over a period of three to five years compared to payments made to the external service providers
- the ***"co-operative processing"*** option, if arranged efficiently, would be very economic for the State Government as a whole
- volume discounts and economies of scale could be gained by centralised bargaining for state-wide services
- the recommended model, if implemented, would ensure to remedy the current situation and safeguard the Government's investments in Information Systems and more importantly help the various agencies to deliver to the public efficient services for which they are responsible.

8. Conclusions

8. Conclusions

- Contingency planning is an important emerging area of Information Systems.
- A contingency plan is a form of insurance policy which is managed internally by an organisation or contracted out to an external service provider
- Modern organisations, including government agencies, depend on computer-based systems to deliver their core services.
- Information held in computers are vital for the provision of efficient services. As such Information Systems managers must be able to protect such information and be able to continue providing such information even after disasters render the computers inoperable.
- No organisation either in the public sector or the private sector could afford to ignore this important aspect of Information Technology.
- Organisations should take a more critical view of their Information Technology investments due to rapidly changing technology and continuing difficult economic conditions.
- Management should deliver the core functions at the right time using minimum resources.
- Consideration needs to be given by the New South Wales State Government , through legislation, for Contingency Planning and protection of data held in computers.

8. Conclusions

- There is a need for each case of disaster within the Information Technology environment to be well documented and information disseminated and advertised.
- Senior management need to be convinced that investment in contingency planning is a sensible business decision, one which cannot be ignored if the business and/or core services are to be provided without disruption.
- Seventy five percent of the agencies surveyed in New South Wales had contingency plans and were motivated by a number of factors to introduce contingency plans.
- Twenty five percent of the agencies surveyed in New South Wales chose not to have any such plans in place.
- The review of the current practices indicated that contingency planning arrangements for the State Government as a whole are inefficient and not cost-effective.
- The Government's investments in Information Technology in some of it's agencies are not protected and these agencies also run the risk of being unable to provide core functions to the public.

8. Conclusions

In the light of the above discussions and analysis, I recommend **Model 1 - Centralised Government Owned Infrastructure** for implementation of contingency planning within the New South Wales State Government. While the report describes the advantages and disadvantages of the recommended model, detailed study of the requirements of each of the agency within the State of New South Wales needs to be carried out before adopting the most suitable strategy. Cost/benefit analysis of individual requirements must also be completed before choosing a strategy.

A ***"whole-of-government"*** approach to contingency planning may conflict with individual agencies' own strategic directions. However, there is likely to be a rapid acceptance of the fact that **working with the central co-ordinating agency would develop solutions which would cost less and benefit all.**

REFERENCES

1. Alan J. Flemming, ***"Terrorism Coverage in the U.K. - An Explosive Topic",*** Disaster Recovery Journal, March 1995.

2. Alan Reed, ***"Recovery From Bombing Disaster",*** Business Recovery, International Business Recovery Newsletter, Volume 1 No. 2, September 1992.

3. Cheeseman, I. (1990): ***"Disaster Protection: Insurers will rescue only what you protect",*** Computerworld, April 23 1990, p 81-83.

4. Commonwealth Government: ***"Circular Memorandum To Departments",*** Finance Circular No. 1990/2.

5. ***"The Commonwealth Government Information Exchange Steering Committee - Roles and Responsibilities"*** , Information Paper, IESC Secretariat, April 1994.

6. Datapro (1989): ***"Selection of a Disaster Recovery Facility Vendor",*** Information Security.

7. Datapro (1990): ***"IBM Disaster Recovery Services",*** Information Security.

8. Datapro (1990): ***"An Overview of Disaster Recovery",*** Management of EDP Systems, p102-104.

9. Datapro (1991): ***"Corporate Contingency Planning: A Blueprint for Survival",*** Information Security, p101-104.

10. Department of Computing & Information Technology, Government of Western Australia, ***"Disaster Recovery And Contingency Planning - Executive Overview"***, February 1989.

11. Department of Computing & Information Technology, Government of Western Australia: ***" Disaster Recovery And Contingency Planning Manual"***, May 1989.

12. Haight, N;Byers, C.R. (1991)***:"Disaster Recovery Planning:Don't Wait Until It's Too Late"***, Journal of Systems Management, April 1991, p15-16.

13. Hiatt, C.; Motz, A. (1990): ***"Disaster Recovery Planning:What it Should Be, What it is, How to Improve it"***, EDPACS - The EDP Audit, Control, and Security Newsletter, March 1990, p1-9.

14. Hiatt,C.; Motz, A. (1990): ***"Disaster Recovery Planning"***, Information Technology Resources Utilisation and Management: Issues and Trends, p 450-471.

15. IBM's Business Recovery Services, ***"World Trade Centre Disaster"***, Information Systems Outsourcing Presentation, 1994.

16. Information Technology Policy Division, Department of Finance,Victorian Government: ***"Information Technology Outsourcing Best Practice Methodology"***, April 1993.

17. Inspector D. Roberts (1992)***: "Contingency Planning In The Victorian Community - Experiences With Displan"***, Contingency Planning 1992 Conference, April 1992.

18. ***"I.T.S. Contract News"*** (1993), Information Technology Service, Commercial Services Group, New South Wales Government.

19. Dr. John Buckland (1991): D***isaster Recovery Handbook***, Chantico Publishing Company, INC, p1-10.

20. John William Toigo (1989): ***Disaster Recovery Planning: Managing Risk & Catastrophe In Information Systems***, Prentice Hall, ISBN 0-13-214941-9, p.7.

21. Lane, V.; Step, P. (1985): ***"The Formidable - If Not Insurmountable - Organisational Problems of Disaster Recovery Planning***", Computer Security, p 361-369.

22. McNurlin, B.C. (1988): ***"Trends in Disaster Recovery",*** I/S Analyser, November 1988, p1-12.

23. Moss, I. (1992): ***"Corporate Security and Contingency Planning: Survey of Management Attitudes, Current Capabilities and Initiatives",*** Contingency Planning 1992 Conference, April 1992.

24. ***"OECD Guidelines for the Security of Information Systems",*** Information Technology News, Volume 5, Number 2, April 1994.

25. Robert Brigden-Jones (1992): ***"Trends In Contingency Planning",*** Contingency Planning 1992 Conference, April 1992.

26. Robert Winkler & Gene LaValle, ***"Crisis Management: Planning Pays Off",*** Disaster Recovery Journal, September 1992, Vol. 5.

27. Wexler, Alan (1990): ***"Data Processing Legal Obligations of Disaster Recovery"***, Technical Support, October 1990, p41.

28. Royal P. Fisher (1984): **Information Systems Security**, Prentice Hall, ISBN 0-13-464727-0, p83.

APPENDIX - 1

Questionnaire

Definitions

"Disaster" - A disaster is described as "any physical event which interferes with the continued availability of Information Systems.

"Contingency Planning" - is the availability of procedures which allow for continuity of business when an unscheduled disruption to computing services occurs. A contingency plan is a procedure to be followed when the contingency occurs.

1. Does your organisation have a comprehensive contingency plan for its computer systems that is fully documented?

Yes/No

2. If "Yes", please go to question 3. If your answer is "No", what is the major reason for your organisation not having a formal corporate computer contingency plan?

- Has not been considered
- Not considered necessary
- Considered worthwhile, but low priority

- Insufficient resources

- Not applicable

3. How is contingency planning administered in your organisation?

- Full time contingency personnel

- Part time contingency personnel

- Line management function

- No formal allocation of responsibility

4. When was your contingency plan last updated?

- During the last 12 months

- During the last 2 - 3 years

- Over 3 years ago

- Not applicable

5. When were aspects of the contingency plan last tested?

- During the last year

- During the last 2 years

- Over 2 years ago

- Not applicable

6. Has risk assessment been performed for your organisation?

- Within the last 2 Years

- Over 2 years ago

- Never

7. Has your organisation suffered from a loss of availability of services or computer system during the last three years which resulted in putting the contingency plan in action?

Yes/No

8. If "Yes", how long did that unavailability last?

<= 1 day > 1 day > 1 week

END