International
Federation of
Accountants

Small and Medium
Practices
Task Force

December 2003

Controlling Computers in Business: Computer Disaster Recovery Planning

The fifth in a series of guidance documents for SMPs and SMEs

PRICEWATERHOUSECOOPERS

IFAC

The International Federation of Accountants (IFAC) is the global organization for the accountancy profession with 159 member organizations in 118 countries representing 2.5 million accountants employed in public practice, industry and commerce, government and academe.

IFAC's mission is to serve the public interest, strengthen the worldwide accountancy profession and contribute to the development of strong international economies by establishing and promoting adherence to high-quality professional standards, furthering the international convergence of such standards, and speaking out on public interest issues where the profession's expertise is most relevant.

The IFAC Board established the Small/Medium Practices (SMP) Task Force to investigate ways in which IFAC can respond to the needs of members operating in the small and medium-sized practice whose dealings are principally with small and medium-sized enterprises (SMEs). The SMP Task Force does not issue standards or guidelines such as those set out in the IFAC Handbook. Rather, it is authorized by the IFAC Board to publish the types of documents listed below on issues and practices it considers to be of interest to small and medium-sized practices and enterprises.

1. Guidance documents for small and medium-sized practices and enterprises, which provide practical advice on relevant issues.

2. Research reports, which describe the results of in-depth studies carried out on behalf of the SMP Task Force.

In accordance with these terms of reference, the IFAC SMP Task Force convened two meetings during 2002 for IFAC Member Bodies with particular interests in the SMP/SME area. The principle aim was to ascertain what particular products or services might be of use in the global market place. One such product that met the criteria was a series of guidance documents entitled "Controlling Computers in Business" which was produced under the control of the Information Technology Committee of the Institute of Chartered Accountants of Scotland (ICAS). The majority of the research and drafting in connection with these publications was undertaken by PricewaterhouseCoopers LLP (PwC LLP).

IFAC, in agreement with both ICAS and PwC LLP, has updated the guidance documents under the IFAC banner, with the objective of exposing these documents to the wider SME/SMP market.

This publication is therefore the fifth in a series designed to provide practical advice on computing controls. The series, whilst aimed mainly at SMEs, will be of use to SMPs, both for use in their own offices and also for their clients who will mainly be SMEs. Why the Task Force considers computer controls to be of significance to SMPs and SMEs is explained in the Foreword.

The SMP Task Force welcomes any comments you may have. Comments should be sent to:

Technical Manager, SMP Task Force
International Federation of Accountants
545 Fifth Avenue, 14th Floor
New York, NY 10017 USA
Fax: +1 212-286-9344
Email: SMPpubs@ifac.org

Copies of this paper may be downloaded free of charge from the IFAC website at www.ifac.org.

This document is summary in form and is not intended to: (i) constitute professional advice or a substitute for professional advice; (ii) be a definitive statement of best practice; (iii) replace the expertise and judgment of your independent accounting, legal, information technology or other professional adviser. Consequently, this document is provided "as-is," with no guarantee of completeness or accuracy, and without warranty of any kind, express or implied, including, but not limited to, warranties of performance, merchantability and fitness for a particular purpose. In no event will PricewaterhouseCoopers, its related partnerships or corporations, or the partners, agents or employees thereof be liable to you or anyone else for any decision made or action taken in reliance on the information in this document or for any consequential, special or similar damages, even if advised of the possibility of such damages.

ISBN: 1-931949-16-6

Foreword

Computers and systems are part of our daily lives. Many of the benefits that were previously derived only from significant investment within large organizations are now available to SMPs and SMEs. Although this brings the potential for substantial business improvement, it also brings the risks associated with ensuring the proper use, management and operational control to deliver the potential returns from systems investment.

SMPs and SMEs need to devote management time to systems management and control issues. To ignore them greatly increases business risk. IFAC's SMP Task Force is aware of the pressures and constraints affecting SMPs and SMEs. The Task Force guidance notes are therefore of a thoroughly practical nature. The Task Force hopes that busy SMP and SME managers will gain considerable benefit from them. The checklists built into the guidance are designed to allow users of the notes to quickly identify if they have any problems. More detailed guidance is provided to assist in the resolution of those problems.

All organizations are required to assess the risks to the business should either physical or logical events cause serious harm to the operation of their computer systems. This guidance document highlights the importance of disaster recovery planning to increase the chances of your business surviving a catastrophic event.

PwC LLP is heavily involved in organizations within the middle-market and hosts a dedicated website that deals with many of the issues affecting the owners of such enterprises as they try to drive their businesses forward. The address of this website is www.driving-ambition.com, while the main PwC LLP website can be found at www.pwcglobal.com.

Finally, my thanks in particular to Colin Campbell and Victoria Fox of the Glasgow Office of PwC LLP, and to members of the SMP Task Force of IFAC, who are:

Paul Chan, Hong Kong
Ashok Chandak, India
Mohamed Ali Elaouani Cherif, Tunisia
Alex Hilman, Israel
Robin Jarvis, UK
Dawn McGeachy, Canada
Harold Monk, USA
Bernard Scicluna, Malta

ANGELO CASÓ
Chairman, IFAC SMP Task Force

Introduction

1. This is the fifth in a series of guidance notes on computing controls for small and medium-sized enterprises that the International Federation of Accountants has produced in association with PricewaterhouseCoopers.

2. Each note discusses an issue relating to computing controls and shows how best practice can be applied to the smaller organization. These notes give information on the issue, including definitions of key terms, costs and benefits, risks and practicalities. Each note then provides a good practice checklist. You should use the checklist to see how well controlled your business's use of computers is against the risks discussed in the note.

3. The readers of these notes will undoubtedly have a wide variety of needs, stemming from two factors. Their level of awareness of the issues discussed will affect how much or how little of each note they will have to use, as will their current level of control in the area discussed. Accordingly, the notes are organized to allow readers to choose the sections they wish to read.

4. Each note has the following sections:
   - Background
   - Key Terms
   - Cost-Benefit Considerations
   - Risk Indicators
   - Practical Considerations
   - Good Practice Checklist and Appendices.

How to Use These Notes

5. If you only have a short amount of time:
   - Read the background.
   - Read as many of the “Key Terms” as you need.
   - Then complete the “Good Practice Checklist,” consider the examples raised in the appendices and complete any appropriate schedules.

6. Read the other sections as required to resolve any issues that might be highlighted by your completion of the checklist.

7. If you have more time, or the checklist results suggest that you need to perform a more detailed review of the issue, consider the other sections on costs and benefits, risks and practical considerations.

Background

8. The purpose of disaster recovery planning is to increase the chances that your business will survive a catastrophic event. Studies have shown that 80% of businesses that suffered a catastrophic event and did not have a disaster recovery plan in place went out of business within 18 months. Disaster recovery planning reduces the risk that your company becomes part of that 80%.

9. There are two main types of disaster recovery planning:

Computer Disaster Recovery (CDR)
CDR addresses the risks that specifically affect the continued availability of your computer systems, for example, how to recover from a fire in the computer room.

Business Recovery Planning (BRP)
BRP is wider in scope than CDR and addresses the impact of a catastrophic failure in any part of your operations. For example, BRP would consider the impact and necessary recovery steps for a printing business if a fire destroyed its printing machines.

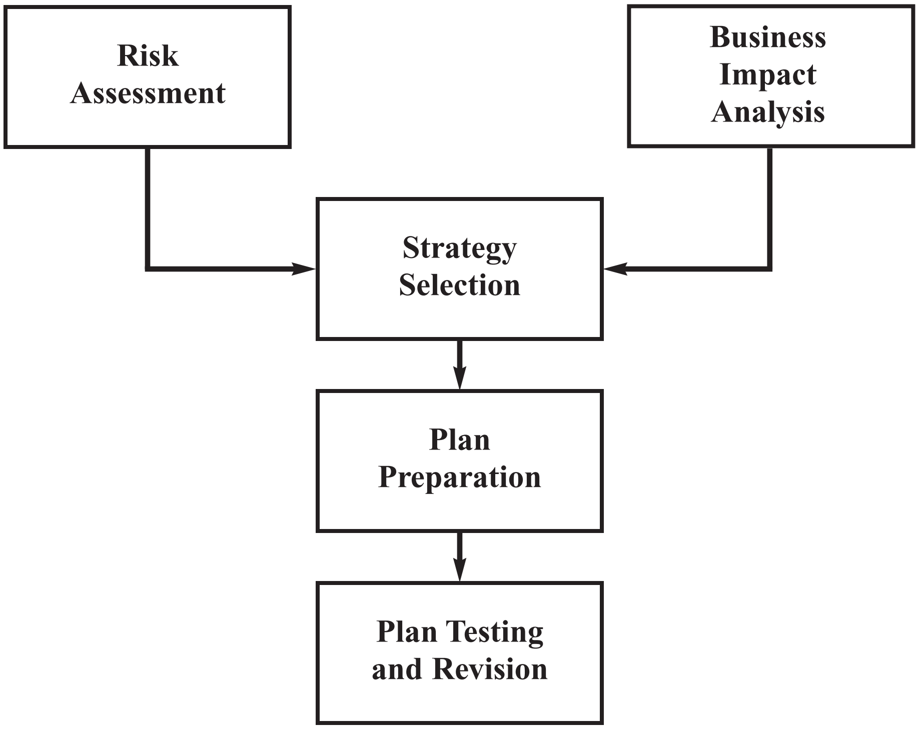
This guidance note focuses solely on CDR although the approach discussed and principles provided can equally be applied to a business recovery planning exercise. CDR is often the first area of concern for management and, when completed, can form the basis for a fuller BRP project.

10. Good contingency planning is made up of 10 simple components:

- executive management commitment;
- establishment of a service resumption planning team;
- assessment of the existing infrastructure;
- risk analysis;
- system prioritization;
- definition of recovery operations;
- preparation of a recovery operations plan;
- training;
- testing; and
- maintenance and update of the plan.

11. The five-stage approach to developing a computer disaster recovery plan discussed in this guidance note primarily deals with the second and ninth component: the establishment of a service resumption planning team and testing. Without the first component — executive management commitment — it is unlikely, however, that the other stages will deliver a workable plan for you to use to recover from a disaster situation. Your senior management must understand the need for, and the benefits of, a contingency planning exercise.

12. The following diagram shows the five key phases in developing a computer disaster recovery plan:



13. The key objectives of each phase are as follows:

Phase	Objectives
Risk Assessment	To assess the risks currently facing your computer systems, to identify steps for reducing those risks and to implement the steps considered to be cost-effective. See the notes below on the timing of the "Risk Assessment" phase.
Business Impact Analysis	To assess both the financial and non-financial impact on your business if your computer systems were unusable for various periods of time and to arrive at an appropriate time frame for recovery.
Strategy Selection	To identify which disaster recovery strategy is most appropriate for your business, bearing in mind the need to recover within the "target recovery time frame" (defined under "Key Terms" below.
Plan Preparation	To map out the necessary steps, actions and responsibilities for recovering your computer systems after a disaster has occurred.

Testing and Revision — To prove that the disaster recovery plan is workable and that it achieves the necessary level of recovery within the target recovery time frame.

14. The risk assessment phase is the one part of the disaster recovery planning process that does not need to be carried out in any particular sequence. If your prime objective is to develop a recovery plan, without first minimizing the risks that may be inherent in your current environment, the risk assessment work can be carried out later, even during the plan testing phase.

15. As previously mentioned, before starting a CDR planning exercise, you need to obtain buy-in from your entire management team since the project will require input from them or their staff. It is also important that the project team consists of not just computer staff but also general business people who have an appreciation of wider business matters.

16. It may be useful to employ consultants to assist in the initial phases of the project. These consultants should work with your staff to ensure that there is a transfer of knowledge and that your business takes ownership of the plan during the process. A computer disaster recovery plan, with its associated contractual arrangements, should be a living document that changes as your business evolves. Although it must be kept up to date with factual changes, such as employee home contact numbers, it must also be objectively assessed periodically to ensure that it still provides the level of protection your business needs.

Key Terms

17. BRP — Business Recovery Planning. Disaster recovery planning that examines the risks associated with the whole business process. You can purchase disaster recovery toolkits to help create such a plan. These toolkits normally comprise business continuity guidelines, a plan template and various questionnaires and checklists. The templates should cover everything from initial business impact analysis through to return to business as usual following an incident.

18. CDR — Computer Disaster Recovery planning. Disaster recovery planning that focuses only on the risks that affect the continued availability of your computer systems and data processing facilities.

19. Target Recovery Time Frame — The time within which your computer systems (or just some of them) must be recovered to avoid unacceptable business impacts.

Cost-Benefit Considerations

20. Computer disaster recovery is a form of insurance cover. You'll have to pay out some amount of money to protect yourself against the possibility of much higher losses should a disaster occur. The purpose of the Business Impact Analysis is to quantify, in both

financial and non-financial terms, just what impact a disaster would have on your business. A later stage, Strategy Selection, balances the potential costs of a disaster against the cost of adopting various recovery strategies.

21. Since the performance of a cost-benefit analysis is implicit within each of these phases, this issue will not be discussed further in this section.

Risk Indicators

22. Every company using computers depends on them to a greater or lesser extent. The following use of computer technology represent areas of higher risk:

- high level of computer use throughout your business;
- all financial information is stored only on your computer systems;
- production processes depend on your computer systems;
- complicated processes that make the use of manual procedures untenable;
- you use on-line, real-time systems;
- you need to provide quick responses to customer queries or risk losing business;
- computerization has been in place for a long time and manual methods of processing data have been forgotten;
- you have computer equipment and processes spread throughout your business in different sites;
- you depend on data communication links to process information;
- a financially unstable hardware or software supplier.

23. In addition to these factors, which indicate increased reliance on computer technology, other factors indicate an increased risk of a disaster occurring. These factors include:

- poor or non-existent security surrounding your physical computer equipment;
- lack of software and hardware maintenance contracts;
- software or hardware maintenance contracts specifying supplier response times that do not meet the needs of your business;
- inappropriate location of computer equipment, for example, over a store selling oil;
- inappropriate siting of business premises, for example, in a known flood plain;
- business processes are inherently risky, e.g., handling of explosives.

24. You face the most risk, of course, if you rely heavily on your computer equipment but have not taken appropriate measures to reduce the physical risk factors that affect that equipment. Some of the risk reduction measures you should consider include establishing adequate backup procedures and proper security measures. Both of these topics have been covered in earlier guidance notes within this series.

Practical Considerations

Scoping the Project

25. It is essential that you carefully define the scope of your disaster recovery planning project at the outset. CDR is directed towards physical computer equipment, the associated infrastructure, such as networks, and the applications that run on that equipment. When scoping out a CDR project, you must decide which:

    - locations you wish to cover;
    - business functions are to be included.

26. Perhaps, before you start any detailed work, you know that one of your outlying offices consists of one salesperson with a PC and a modem. Not only is this particular sales office unlikely to be an essential component of your business as a whole, but the salesperson may well be able to perform equally efficiently from a hotel room in the area. You can, therefore, exclude this location from the planning project.

27. Although this guidance note deals with CDR for a disaster recovery planning project, you should consider how you can emphasize wider recovery to your management. To reiterate an earlier example, a CDR exercise at a printing business identified in passing that the lead time for getting the company's four-color printing press back into operation after a disaster would be 18 months and that 75% of all of the company's income came from that one press. Emphasizing that fact to management enabled the company to obtain assurances from the press suppliers that, in the event of a disaster, it would obtain the next press off of the production line, potentially safeguarding its future viability.

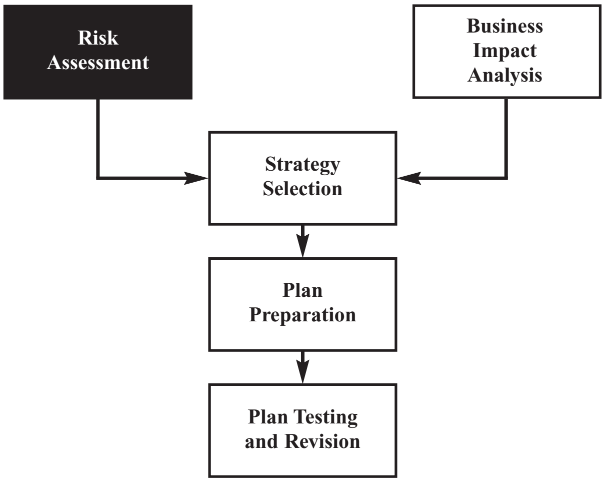
28. To scope out your CDR project, you first need to determine what types of disaster situations could have a serious impact on your business. Most CDR projects consider the loss of:

    - main computer;
    - communications equipment;
    - computer room;
    - local area networks;
    - wide area networks;
    - file servers;
    - electronic mail servers;
    - PCs running essential systems on a standalone basis;
    - real-time information feeds;
    - point-of-sale terminals.

29. They stop short of considering the implications of other risks, such as loss of the whole building or key members of staff. Defining potential disaster situations allows you to not

only identify the deliverables from each stage of the project but also to alert management to any potential wider business recovery problems.

Risk Assessment



30. Normally, the first phase of a computer disaster recovery planning exercise is to assess the risks currently facing your computer systems, to identify the steps you can take to reduce those risks and to implement the most cost-effective steps. Risks are physical or logical events that can harm your computer systems.

31. The types of risk to consider include:

- flood;
- fire;
- service failure due to, say, loss of power;
- mechanical breakdown, including hardware failure;
- software failure, including virus attacks;
- accidental or deliberate damage to equipment or facilities, including terrorism;
- personnel problems.

32. Power failures or power surges that damage equipment are the most common causes of interruption to computer processing. One study found this problem accounted for 50% of all data losses. The next most common cause was fire or explosion, followed by earthquakes, hardware errors, network failures and storm damage.

33. The risk assessment phase considers the risks facing the particular environment your company operates in and the counter measures you can take to address those threats. When you are identifying appropriate counter measures, be sure to do an informal cost-benefit calculation first.

34. For example, a company located on the top of a hill might not be susceptible to flooding but may suffer other storm damage. It should take precautions such as covering its computer room windows with a film that prevents the glass from shattering should a roof tile strike them.

35. A company situated in an area with a known flooding problem might permanently surround the building with sandbags, although a more cost-effective option might be to put its computer equipment in an upper floor of the building.

36. A company situated at the end of an airport runway will recognize the possibility of being hit by an aircraft, but there really is no realistic counter measure it can put in place to prevent that from happening.

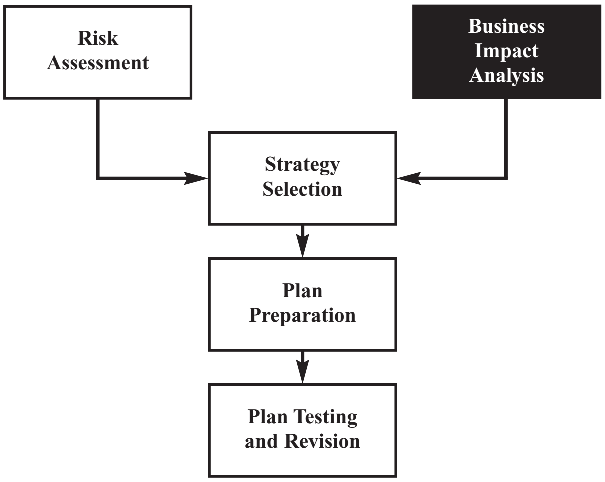
37. When you are working on the risk assessment phase, you should review whether your insurance policies deal with issues such as consequential loss. A disaster could interrupt your cash flow, cause a dip in your profitability and incur additional costs during the recovery stage. Insurance is not a substitute for proper disaster recovery arrangements, but it can alleviate the financial burden at a difficult time.

38. As noted earlier, the risk assessment phase is the one stage in disaster recovery planning that does not need to be carried out in any particular sequence. You can do a risk assessment before you develop your disaster recovery plan or even after you have fully developed and tested such a plan. The most effective time to carry it out is, however, before the strategy selection phase. Certain strategic options may appear more or less favorable once you have assessed the likelihood of certain events occurring and have taken cost-effective measures to reduce that likelihood.

Business Impact Analysis

39. The purpose of the business impact analysis (BIA) phase is to assess the impact of the loss of, or serious disruption to, your data-processing facilities. The BIA seeks to answer a number of questions:

- What systems do I need to recover?
- When do I need to recover them?
- In what order do I need to recover them?
- What will be the effect on my business if I cannot recover my systems when I want them?



40. You begin the BIA process by figuring out what the likely impact of losing your data-processing facilities might be over different periods of time. The disruption could have financial and non-financial implications. Factors to consider are:

(a) direct loss of profits;

(b) indirect costs;

(c) loss of life;

(d) operating efficiency;

(e) market reputation;

(f) public perception;

(g) legal requirements.

(a) Direct loss of profits — This might occur if you could not provide a particular service or deliver a product and your customers decide to go elsewhere. The value here is purely monetary, based on the best estimate of the managers supervising your different business functions.

(b) Indirect costs — These may be incurred for a number of reasons, including:

- hire of temporary staff;
- overtime;
- fines;
- lost discounts;
- punitive payments (e.g., late payment of supplier invoices incurring interest charges);
- interest earned/paid;
- opportunity cost.

The next five categories are all consequential losses that cannot easily be quantified in financial terms. You need to attach a probability to such events to assess how likely they are to happen, on a scale of 0 to 9, with 9 being the highest. For example, one of your systems might be essential to your business even though it is not worth much financially.

(c) Loss of life — This category also includes the risk of serious injury. Loss of life might occur where a computer system used for safety purposes, for example, to monitor exposure to hazardous substances, was not functioning properly and a staff member was exposed to those substances.

(d) Operating efficiency — This may be affected if a computer system is not functioning as it should. Your staff might have to manually perform processes that were automated; you might have to replace links to on-line reference sources with references to printed material. You might be able to operate with amended procedures for a while, but there may come a point when the volume or complexity of transactions makes processing without a computer impossible. The payment of staff and suppliers is another area where bad feeling can arise very quickly. Most people will be try to be understanding, but there are industries where a failure to pay on a due date could lead to industrial action or non-delivery of supplies.

(e) Market reputation — This will be affected when your general marketplace learns of the disaster affecting your computer systems and watches to see how quickly and professionally "normal service is restored." A successful recovery will give the market confidence in your overall business acumen, whereas a fragmented approach and extended recovery process could have an adverse impact on your customer's perception of your overall management ability. Within this category of impact, you should also consider the perception of your shareholders.

(f) Public perception — This is linked to market perception. It is the impression that the outside world — which may know nothing about you — gets during your recovery efforts. Public perception is important as it can affect potential future customers and the wider business world, including financial institutions.

(g) Legal requirements — These are important because you may be bound by law to hold certain records, operate certain processes or submit regulatory returns. You can incur indirect costs if, for example, you file a tax return late. Worse, some regulators have the power to stop you operating if you do not meet certain criteria.

41. The last factor to consider when performing a BIA is the impact of time. Many systems can be lost for short periods of time with no adverse effect — witness normal computer downtime when a moderate amount of overtime catches up with processing and no one outside your company knows that the system was not functioning.

42. It might be another story altogether if that same system were down for an entire week. It would be important, therefore, that the particular system was up and running again in less than one week.

43. To assess the impact of different time frames, you might use a questionnaire, such as that shown in Appendix II, to gather information and quantify the potential effect of a disaster.

44. Collation and comparison of this information will provide the answers to the questions posed at the beginning of the BIA phase.

45. When gathering the required information, think about who is to complete the questionnaire. Senior management is likely to be too distant from the details to know which individual computer systems are used, while system users may be too close to the details to understand where their activities fit into the wider business activities. Middle management and supervisory staff are likely to have the most informative view of what is important to their own department while still keeping such issues in overall perspective.

46. Appendix I looks at a number of different scenarios where computer systems may or may not be essential to the survival of a business.

47. When assessing the business impact, you should consider the worst possible scenario, within reason, that could occur. For example, a financial ledger might not be essential at any time except at the month end when third parties, such as shareholders, are waiting for a set of accounts. Although they might find a delay of an hour or a day acceptable, they would probably frown on a delay of a whole week.

48. When you have collected the information for all of your computer systems, you can rank the systems according to the financial or consequential impact their loss would have on your business. The ranking shows in which order the systems need to be recovered and the necessary recovery time for each.

49. The size of your business will determine how much detail is necessary to assess the impact of a disaster. Smaller companies might bypass a lot of the formal BIA steps by substituting a workshop where managers consider and discuss the implications of a disaster. If you decide on this approach, ensure that the following key factors are addressed:

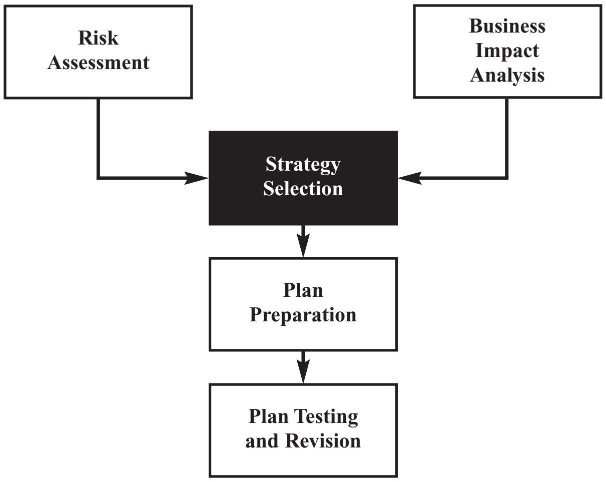
    - You need to prepare a comprehensive list of your systems before the workshop. Your senior management probably doesn't know about every small system in your company.
    - The participants in the workshop should have a broad enough business knowledge to recognize implications but should also have a grasp on the detail of business processes.
    - Ensure that everyone's views are considered and that information is not lost in the heat of discussion.
    - Keep notes on any decisions reached so that, if questions are raised later, you can justify those decisions.

50. Effectively, you are still dealing with the BIA phase, but a workshop may be a more appropriate environment for gathering the necessary information.

Strategy Selection

51. Strategy selection is where the cost-benefit analysis comes in. Your company might adopt various recovery strategies, such as:

    - You might purchase additional hardware and use it as standby for your existing configuration.
    - You might enter into an agreement with a computer supplier for the provision of alternative equipment, including peripherals and communications devices.
    - You might enter into a reciprocal agreement with someone who has the same type of computers as you do, promising to help each other out in the event of a disaster.



52. Each of these strategies will carry a different price tag and can provide recovery within different time frames. A bank's mainframe that runs its auto-teller machines may be duplicated by another mainframe in another part of the country. If the first mainframe goes down, it might only be a matter of seconds before the second mainframe takes up the mantle and starts to process auto-teller transactions. The switchover may be so smooth that users believe all that happened was a glitch in the telephone line.

53. A small company that relies on one PC for processing its accounts may be quite content to live without the computer until the end of the month. In this case, the appropriate recovery strategy may simply be to buy a replacement PC from any computer store.

54. Your strategy must ensure that it will meet your required recovery time frame, as identified in the BIA phase. The other consideration is that the recovery should be achieved in the most efficient, effective and economic way possible.

55. Specialized companies offer disaster recovery services ranging from the provision of an alternative machine delivered to a specified site on a trailer to the use of their own disaster recovery standby site. The different recovery options have different cost implications, but most include the right to test the arrangements each year.

56. Disaster recovery suppliers offer different types of services commonly known as “hot site,” “warm site,” “cold site” and “trailer site.” The explanations for these terms are:

Hot site
The supplier has a recovery site ready to accept your backup tapes and can start processing immediately since the computer environment is running and operational. All accommodation, peripherals and communication links are provided.

Warm site
A recovery site with the same level of accommodation, peripherals and communication links as a hot site, but without the computers. The supplier will provide the computers, but they must be moved into the recovery area and powered up.

Cold site
This type of recovery site is basically a fully fitted computer room but with no equipment and with no provision in the contract to supply equipment. A cold site agreement would be used if you had your own backup machine but did not have an alternative location in which to site it.

Trailer site
The computer equipment is placed in a mobile trailer fitted out as a computer room. This mobile facility is taken to a designated recovery site, where the computer is linked back into the company's remaining network.

57. The cost of these different services varies enormously since a hot site must be kept fully manned and operating 24 hours a day, whereas a cold site requires minimal maintenance.

58. Your hardware largely dictates the choice of disaster recovery supplier. Certain hardware manufacturers also provide disaster recovery arrangements and it will be necessary to compare the costs and service levels of the different suppliers. The service differentiators for recovery suppliers include:

- the extent of recovery support included in the contract;
- the number and duration of tests permitted each year;
- the flexibility with which hardware configurations can be amended; and
- the subscription level.

59. The subscription level is the ratio of recovery arrangement subscribers to each machine available for recovery. The higher the ratio, the greater the risk that someone else will already be using the recovery machine when your own disaster occurs. In 1992, when a burst water main hit the business area of Chicago, the disaster recovery suppliers were so much in demand that processing was farmed out to all of their recovery sites throughout the US. Natural disasters tend not to affect only one organization at a time.

60. Beware of entering into a reciprocal arrangement with another company for mutual support in the event of a disaster. There are serious disadvantages of such an arrangement:

    - To provide an adequate level of service, should you suffer a disaster, your supporting company may need to run a computer that is twice the power and capacity it needs for its own business processes.
    - It is likely to be unenforceable in law — a "gentleman's agreement."
    - Computer needs grow and whatever excess capacity was available at the time of the agreement is unlikely to still be there when the need arises.
    - The perception that your processing could take place at quiet times, such as the middle of the night, may be false since the supporting company may be running a lot of system housekeeping tasks overnight.
    - A supporting company will always put its own needs at the top of its agenda. If it has an invoicing run to perform at the same time as your payroll run, its invoicing will always take priority.
    - Unless you have identical IT strategies, which is doubtful, sooner or later compatibility will become a problem. For instance, you may be forced into accepting a system upgrade that your business may not need or want.
    - To continue to process information, you may need to ask your staff to work a nightshift to continue processing. It is also possible that the same staff will be required during the day to help recover what has been lost.

61. Reciprocal arrangements should only ever be considered for businesses with an interest in helping each other survive, such as companies within the same family. The overall management of the group will recognize the benefits of keeping the recovery arrangements in-house and should provide the necessary financing to purchase the appropriately specified hardware.

62. Within the strategy selection phase, you also need to consider the level of service your staff will need should a disaster occur. It may not be necessary to provide a terminal for everyone in the company, since a large proportion of users may need them only occasionally. On the other hand, it may be necessary for all of your telesales staff to have constant access to a terminal.

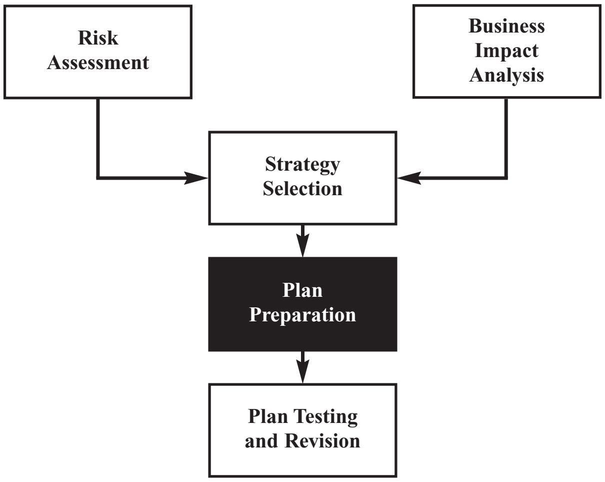
63. Your recovery needs must be worked through, bearing in mind that full operation is unlikely to be achievable in a disaster situation. The types of resources required to recover the computer systems must be considered in terms of:

- application software;
- communications, including voice and data;
- systems software;
- supplies;
- vital records;
- equipment;
- personnel;
- transport;
- utilities, including power and water;
- software licenses that permit the use of software on the recovery computer;
- office space.

64. Your choice of strategy may be restricted by your needs in each of these areas.

Plan Preparation

65. Plan preparation is the stage where you implement the agreed-on recovery strategy. As well, you begin to document the detailed requirements of the recovery process, together with information gathered during earlier stages. We say that information "begins to be documented" because the first pass of any disaster recovery plan can never be the final draft. Computer disaster recovery planning is too complex for that and, if you stop with an untested plan, you will not succeed in protecting your business.



66. The plan preparation stage doesn't require as much external help as may have been the case in the earlier stages of the project. A lot of work is required to pull together information and document the plan detail, and it is more efficient to have your internal staff carry out this stage of the project. It is also an effective way of ensuring that ownership of the plan resides in-house.

67. Before you begin to draft a plan, you will have:

- identified the impact that a disaster would have on your business;
- established measures to reduce the chance of a disaster happening in the first place; and
- selected an appropriate recovery strategy.

68. It is important now to document, publish and distribute the detailed plans necessary for full recovery of your systems.

69. The potential contents list for a disaster recovery plan, and the anticipated plan contents themselves, could include:

SECTION	CONTENTS
Assumptions	The assumptions used in the development of the plan.
Scope	Defines the situations in which the plan is to be used.
Disaster definition	Defines what a disaster is and prevents the plan being invoked either too early or too late.
Distribution list	Records who has copies of the plan and where those copies are kept. At least one copy should be kept off-site.
Disaster recovery teams	Various teams of people will be required to enable recovery, dealing with different topics such as: • Disaster recovery control • Recovery and restoration of off-site backup tapes • Initialization of alternative hardware • Liaison with the media The different teams should be documented with team membership details.
Notification procedures	The people who have to be informed of the disaster situation and how that information is to be disseminated throughout your business.
Assembly instructions	Where staff should assemble in the event of a disaster.
Damage assessment	Procedures to assess whether or not a disaster has occurred and, therefore, whether the plan should be invoked.
Contact information	Essential contact information for emergency services, disaster recovery services and key members of the disaster recovery teams.

Section	Contents
Public relations information	Prepared PR material suitable for distribution to the media and customers. Preparedness in this area helps restore confidence in your ability to recover.
Recovery procedures	This is a very detailed section that will contain sub-sections for each of the disaster recovery teams. For example, the team responsible for obtaining the backup materials from the off-site storage location will have detailed procedures detailing whom to contact, where the materials are stored, what versions of the materials will have been used, where to take the materials and the time frame in which these activities should be carried out. The recovery steps will include all the details necessary for recovering key hardware and communication facilities.
Disaster prevention measures	The steps that have been taken to minimize the possibility of a disaster should be documented. This section could include information on: • Insurance cover • Backup strategies • Recovery site contracts • Hardware and software maintenance agreements
Plan testing and maintenance	The procedures for maintaining and updating the plan should be recorded within the plan itself so that all key team members are aware of the need to keep the maintainers of the plan up to date on developments within their area and current contact details, etc.
Training	Arrangements and minimum requirements for training should be recorded to ensure that all recovery participants are aware of their responsibilities and the opportunities for training that are available to them.

Be aware that the above list cannot be comprehensive, since every business is different, nor should you feel that your plan needs to have to have all of the above sections.

70. Your CDR plan should be developed in accordance with defined documentation standards to reduce the chance of confusion in a disaster situation. These standards should consider:

- numbering and naming conventions;
- format of text and appendices;
- stationery, binding and page size;

- word processing/graphics/desktop publishing/disaster recovery software output;
- responsibility for ongoing publishing.

71. The suggested disaster recovery teams for a typical SME could include:

TEAM	**FUNCTION**
Business recovery	Overall control and coordination of recovery efforts.
Facilities	Assesses damage to existing facilities, arranges alternative accommodation and leads repair efforts.
Hardware	Assesses damage to existing computer infrastructure, arranges alternative equipment and eventually obtains replacements.
Off-site storage	Retrieves off-site backups and takes them to the recovery site.
Computer recovery	Manages the hardware, software and communications at the recovery site and aims to restore service within the required recovery time frame.
User recovery	Coordinates the transport of users to the recovery site and organizes the peripheral equipment that users will need, such as phones, photocopiers, faxes, etc.

Note, however, that one team, or even a few individuals, may be able to carry out all of these functions. What is important is that you consider all of the areas and allocate appropriate responsibility.

72. A CDR plan should be as explicit as possible and should be written in clear language. The aim of any plan must be to provide sufficient information for a reasonably educated layperson to effect recovery of the systems. A mistake that many companies make is to use experts to develop the disaster recovery plan and then find, at the time of a disaster, that there is not enough information to permit non-experts to recover the processing.

73. A plan can be viewed as management's decisions on how to cope with a disaster situation made before a disaster actually occurs. When viewed like this, the plan serves to reduce the amount of crisis management required in a disaster situation and reduces the risk of making incorrect or inappropriate decisions.

74. Specialist software packages are available to assist with the documentation of disaster recovery plans. These packages normally consist of a database with word processing functionality. Permanent data is stored only once in the database and links are used to pull that information into the text that is the plan. Whenever a change is made to the data within the database, that change will be automatically propagated to the plan the next time it is printed. Such packages facilitate the production of disaster recovery plans but are normally appropriate only where the organization and recovery procedures are extremely complex.

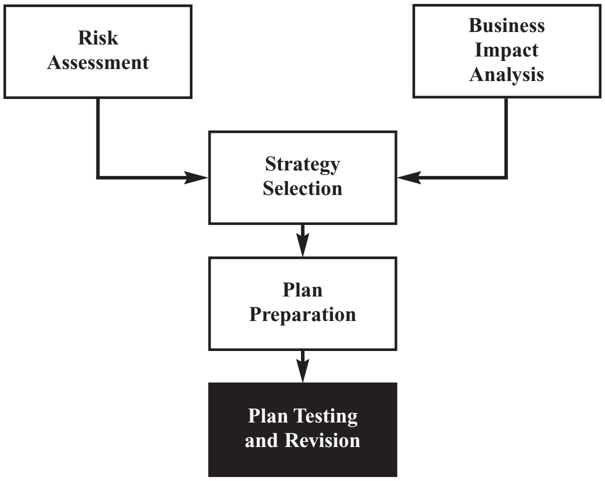
75. Sometimes, disaster recovery suppliers will provide plan preparation software as part of the standard recovery package. In this case, it could be beneficial to use the software, especially if consulting support is available in developing the plan.

76. If you use a normal word processor to document the recovery plan, the document should be structured so that changeable data, such as contact numbers, are recorded in a separate section. This avoids having to reissue the entire plan if one employee moves house.

77. The documentation of a detailed computer disaster recovery plan can be quite time consuming, both to produce initially and to maintain. There has to be a trade-off between developing and maintaining a perfect plan that leaves nothing to chance and developing a plan that enables recovery but perhaps contains less detail.

Plan Testing and Revision

78. Once you have completed the documented plan, you need to test it and reflect any subsequent revisions in all versions of the plan produced.



79. The overall objective of any disaster recovery plan test is to ensure that the plan itself will be workable in a disaster situation. The testing of the plan must therefore concentrate on:

- confirming the accuracy of documented procedures;
- verifying that the recovery requirements specified are comprehensive;
- training team members in the necessary recovery tasks;
- developing team members' familiarity with reactions during crisis situations;
- developing plan testing procedures for ongoing use;
- revising the plan where inadequacies or errors are discovered;
- developing plan maintenance procedures for ongoing use.

80. It is extremely unlikely that a new disaster recovery plan will be successfully tested the first time. There are so many complications and implicit assumptions in the processing of information that a workable plan comes only with the passing of time and a number of reviews.

81. Testing can take the form of:

- a conference room pilot where you talk everyone on the team through a recovery exercise;
- limited testing of certain key areas, e.g., the restoration of tapes onto the backup machine to ensure that key procedures within the overall recovery plan operate as they should;
- a passive test of the recovery procedures where you assume that the disaster has occurred and assign designated staff to recover processing at the off-site location;
- full testing, including invoking the disaster recovery arrangements with the supplier of the replacement machine.

82. If the test produces unsatisfactory results, the necessary changes must be made to the plan and the changes disseminated.

83. The different methods of testing can be used at different stages of a plan's development. When the plan has first been completed, it would be unwise to attempt a full test, since there will inevitably be inconsistencies and inaccuracies. The first test should be either a conference room pilot involving the recovery team or a limited testing of specific areas. Both will confirm the factual accuracy of the plan and ensure that it can be carried out in the anticipated order.

84. A passive test would follow when all members of the recovery team were satisfied that the plan was robust enough to cope with an off-site test. A passive test will normally highlight technical errors where the plan assumes a particular hardware or software configuration that turns out to be incorrect.

85. Full testing is the final step when all other methods have been used and have delivered a satisfactory outcome.

86. A final approach to testing a disaster recovery plan is to deliberately cause a disaster, the so-called "kick the plug" test. In these circumstances, an individual may deliberately instigate a disaster situation by turning off power, removing data tapes, etc., to see how well the business can recover. This form of testing is not recommended because it is possible that the plan might not work smoothly and could actually trigger the failure of your business.

87. As with all test systems, it is extremely important that you correctly record and assess the test results. All tests should have known outcomes and the results should be measured against them.

88. Maintain your business continuity plans by regular reviews and updates to ensure their continuing effectiveness. Assign responsibility for regular reviews of each business continuity plan and for appropriate updates. Procedures for updating the plan should be included in the change management program.

89. Examples of situations that may require plans to be updated include the acquisition of new equipment, or upgrading of operational systems changes in personnel, business strategy, legislation, contractors, suppliers and key customers, facilities and resources.

Good Practice Checklist

	Yes	No	N/A	Reference
A. GENERAL				
Does your company have a computer disaster recovery plan?				
Have you got arrangements in place to replace equipment that might be lost in the event of a disaster?				
Is your communications infrastructure resilient enough to enable recovery at another site?				
Have you got adequate insurance to cover for consequential loss in the event of a disaster?				
B. PLANNING				
Have you clearly scoped the project in terms of: organizational units? physical locations?				
Have you identified key staff to form part of the recovery planning project team?				
Has senior management given approval to the project and does it recognize that costs will be incurred in establishing recovery arrangements?				
Have you established a realistic timetable for each stage of the project?				

	Yes	No	N/A	Reference
C. Risk Assessment				
Have you identified the risk to your computer equipment from: flood? fire? service failure (electricity, water, etc)? mechanical breakdown (including hardware failure)? intermittent fault of hardware or software? software failure (consider a virus attack)? accidental or deliberate damage (including terrorism)? personnel problems?				
Have you considered any other risks that particularly affect your site? Consider nearby construction activity, location of dangerous premises, etc.				
Have all of the identified risks been addressed by cost-effective risk reduction measures?				
Do the risk reduction measures also cover voice and data communications?				
D. Business Impact Analysis (BIA)				
Have all of the relevant business units been consulted?				
Have the results of the analysis been shared and agreed on with senior management?				
Has a list of systems to be recovered been drawn up in the order in which they will be required?				
Have any dependencies between systems been identified? (E.g., that the sales order processing system must be recovered before the sales ledger.)				
Do you know in what time frame the systems will be required to be up and running?				
Do you know what level of service needs to be delivered from each system in a disaster situation?				

	Yes	No	N/A	Reference
E. Strategy Selection				
Have you prepared an appropriate recovery strategy that will allow critical systems to be recovered in the necessary time frame?				
Have you made appropriate contractual arrangements with third parties?				
Does your strategy address the use of communications within your business?				
Did you obtain appropriate competitive bids for the provision of recovery arrangements?				
Does your strategy maximize the use of duplicate in-house equipment?				
Are your strategy and recovery arrangements flexible enough to cope with future business expansion?				
F. Plan Preparation				
Have documentation standards been agreed on so that the plan is consistently formatted and its contents unambiguous?				
Has an adequate, but not excessive, level of detail been included to facilitate recovery?				
Has the plan been structured to allow volatile information (such as contact telephone numbers) to be updated without requiring the reissue of the entire plan?				
Have other qualified staff members validated the contents of the plan?				

	Yes	No	N/A	Reference
G. Plan Revision and Testing				
Have you identified one individual (with a deputy) to maintain the plan on an ongoing basis?				
Has a testing program been defined to keep the plan up to date?				
Have maintenance procedures been established and published that maximize the chance of picking up changes to the plan?				
Have key recovery team members validated the plan by means of a walkthrough test?				
Have key aspects of the plan been tested, e.g., that backup tapes can be restored onto replacement hardware?				
Has a full recovery plan test been carried out to verify that all the necessary recovery resources will be available when required?				

APPENDIX I

BUSINESS IMPACT ANALYSIS SCENARIOS

Background

A company has an automated billing system that produces invoices based on customer standing data and pre-set charging rates. The business produces a high volume of invoices, submission of which is time critical.

Scenario

The billing system became inoperable in the middle of one afternoon. Staff started to prepare bills manually by reference to printed customer contracts and price lists. By working overtime, all the afternoon's bills were processed and dispatched by the end of that day. Because the system was not operational by the following morning, manual billing was used again. By the end of the third day, however, there was a significant backlog that could not be cleared by having staff work overtime. Assuming that the billing process requires skilled labor and that temporary staff could not carry it out, the billing system would need to be operational by the beginning of the third day if the business is to keep functioning properly.

Background

A company uses a treasury system to move liquid funds on and off deposit and to limit its exposure to exchange rate fluctuations.

Scenario

The treasury system became inoperable. Immediately, the company had to contact all the banks it deals with to obtain a note of bank account balances and currency positions. Instead of having access to on-line exchange rate information, treasury staff had to refer to other, less timely, sources of information. The exchange rate moved against the company over the course of the day but, because of the disorganized nature of the manual information, the trend was not spotted and the company lost $20,000. The highly volatile nature of the company's treasury activities means that it should consider attempting to recover the system within a few hours of any failure.

Background

A company operates in a highly regulated industry where engineers are not allowed to work in the plant unless it can be proved that they have received the appropriate training. Training records are stored within the human resources system.

Scenario

The plant within the factory was taken out of action for maintenance purposes. In addition, the HR system was inoperable due to a power failure triggered by the maintenance work being carried out. Legislation prevented the maintenance work from continuing, as the training authorization could not be obtained without the HR system. The maintenance period was, therefore, extended by the length of time the HR system was out of action; this resulted in direct financial loss.

APPENDIX II

BUSINESS IMPACT ANALYSIS QUESTIONNAIRE

Background Information

Department	
Manager	
Location	

Please list the main business processes carried out within the department, detailing the computer applications used and the key individuals involved in each process.

Business Process	Computer Applications	Key Individuals

For each of the processes identified above, please complete an impact analysis questionnaire.

Impact Analysis Questionnaire

Name of process:	
Description of process:	

Financial Impact

What is the expected profit impact on your business if data processing facilities were not available following a disaster for:

		Justification
One day	$	
One week	$	
One month	$	

Estimate what additional costs (fines, lost leases, cancelled contracts, lost discounts, etc.) you would incur if data processing facilities were not available following a disaster for:

		Justification
One day	$	
One week	$	
One month	$	

Non-Financial Impact

RANK THE IMPORTANCE OF THE FOLLOWING STATEMENTS ON A SCALE OF 0 TO 9. (9 BEING THE HIGHEST)

Human life would be put in jeopardy if key data processing facilities were not available following a disaster for:

	Ranking	Justification
One day		
One week		
One month		

Your organization will incur ill will if key data processing facilities were not available following a disaster for:

	Ranking	Justification
One day		
One week		
One month		

Your operating efficiency would be affected if key data processing facilities were not available following a disaster for:

	Ranking	Justification
One day		
One week		
One month		

Customer service would be affected if key data processing facilities were not available following a disaster for:

	Ranking	Justification
One day		
One week		
One month		

Legal requirements would not be met if key data processing facilities were not available following a disaster for:

	Ranking	Justification
One day		
One week		
One month		

APPENDIX III

PROBLEMS WITH DISASTER RECOVERY PLANNING

Inadequate Plan Maintenance

A company developed a comprehensive computer disaster recovery plan that was regularly tested. The main computer covered by the plan was upgraded in tandem with an upgrade to the operating system. Although the factual detail within the plan was changed to reflect the new hardware and software in use, no testing was done to ensure that the detailed recovery instructions were still valid for the enhanced operating system.

The company had a disaster situation and needed to recover systems in accordance with the recovery plan. When the detailed steps were followed, they actually made the problem worse since the operating system commands had subtly changed and the previous instructions now had a different effect. Following the plan exacerbated the problems to such an extent that the detail of the plan was abandoned in favor of following its main recovery principles. The company recovered but incurred additional cost, in the form of software support and lost business, because the plan did not work as documented.

What is a Disaster?

A small professional office faithfully maintained backup copies of data and programs, keeping them remote from its local area network but still within the same building. One Monday morning, the partners arrived to find that the offices two floors below them had had a fire and that the fire service was preventing any access to the office block on safety grounds.

As some of this partnership's activities were time sensitive, it was unable to meet legal deadlines and some clients incurred direct financial losses. Although a disaster recovery plan existed, it had not anticipated the situation where the office was unharmed but access was prevented because of someone else's disaster.

Identify Essential Systems, not Financial Ones

A firm of architects was in the process of developing computer disaster recovery plans for its financial systems, since it was the finance staff who recognized the need for disaster recovery arrangements. When asked to review the progress made in developing the plan, an independent consultant noticed that the computer aided design (CAD) systems had not been included within the scope of the project.

Further investigation revealed that the CAD equipment was not being backed up properly and a loss of the data at a critical time could lose the firm hundreds of thousands of dollars. The impact of losing the financial systems was comparatively negligible.

The project was refocused to protect the business rather than the finance department.

International Federation of Accountants

545 Fifth Avenue, 14th Floor, New York, NY 10017 USA

Tel +1 (212) 286-9344 Fax +1 (212) 286-9570 www.ifac.org