International
Federation of
Accountants

Small and Medium
Practices
Task Force

March 2003

Controlling Computers in Business: Backup, Archive and Restore

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

PRICEWATERHOUSECOOPERS

IFAC

The Mission of the International Federation of Accountants (IFAC) is the worldwide development and enhancement of an accountancy profession with harmonized standards, able to provide services of consistently high quality in the public interest.

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 first 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
535 Fifth Avenue, 26th Floor
New York, NY 10017 USA
Fax: 212-286-9570
Email: EDComments@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 the International Federation of Accountants or 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: 1-931949-03-4

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.

The existence of suitable backup procedures is one of the most fundamental controls that all businesses must implement, regardless of their size or the extent of their computer use. Because it is all too common to find inadequate procedures in this area, this guidance document addresses good practice.

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, SMP Task Force

Introduction

1. This is the first of a series of guidance notes on computing controls for Small and Medium Practitioners/Enterprises (SMPs/ SMEs) that the International Federation of Accountants will produce in association with PricewaterhouseCoopers LLP.

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 the current level of control in the area discussed. Accordingly, the notes are organized to allow readers to choose which sections they wish to read.

4. Each note has the following sections:

   - Background
   - Key Terms
   - Cost-Benefit Consideration
   - Risk Indicators
   - Practical Considerations
   - Good Practice Checklist and Appendices

How to Use These Notes

5. If you have only a short amount of time:

   - Read the background;
   - Read as many of the "Key Terms" as you need; and
   - 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, risk and practical considerations.

Background

8. The existence of a suitable backup procedure is one of the most fundamental controls that all businesses using computers, regardless of their size or extent of computer use, must implement.

9. Imagine a situation where you can no longer access the data in one of your computers. Consider the following situations:

   - Due to a power cut, important files are lost.
   - Due to user error, files are accidentally deleted from your computer.
   - A disgruntled employee deliberately destroys important files.
   - Your computer is stolen.
   - Your computer malfunctions so that you can longer access the data and files stored on it.

10. Your ability to recover from each of these situations depends to a large extent on whether you have adequate backup procedures.

11. Situations where files are lost can normally be easily resolved by reverting to backup copies of the lost files. Situations where a computer crashes or is stolen will require a disaster recovery plan, but one of the basic requirements of any recovery plan is the availability of adequate backups.

12. If computer files have not been backed up, those files may be lost forever. Depending on the data lost, a business could suffer a number of serious consequences, potentially including the failure of the business itself.

13. In trying to recreate files, a business could incur operator time to recreate files, programmer time to reconstruct spreadsheets or replacement costs for packaged software. The continued smooth running of operations might be affected, project time scales might be thrown off course and premium labor changes may be incurred to resolve problems.

14. If the data in question are essential, you might consider using online backup services available via the Internet. Because the Internet is not secure, any data sent have to be encrypted (rendered unintelligible) before transmission to the service provider, who then becomes contractually bound to provide you with backup services. This guidance note is primarily concerned with small and medium sized businesses that, alone, are responsible for their own data. Sound practices with regard to making backup copies of files, storing those backup copies off-site and regularly testing the ability to recover information from those backups are an essential aspect of computer system control.

Key Terms

15. Save

When you save a file, you copy it from the computer's working memory (the RAM) to its storage area (e.g., hard disk, floppy disk or network drive). Information in the computer's working memory is lost when the computer is switched off. The saved copy in its storage area can be accessed once the machine is switched back on. Saving makes one copy of a file.

16. Backup

(a) noun

A secure copy of data or programs held in case anything goes wrong with the originals. Thus, more than one copy of each file exists: one in the working environment and one in a separate off-site environment.

(b) verb

To create a second copy of data or programs for storage outside the working environment.

You can either create a backup yourself or program the system to perform backups at a pre-set time using automatic scheduling backup software.

17. Archive

A secure copy of data or programs no longer in regular use but retained for reference. The original programs or data are then deleted from computer storage.

18. Restore

Recovery of one or more files from backup copies in secure storage onto a computer, following damage or loss of the original. It also covers the retrieval of files from archival files.

19. Backup media

A general term used for the physical devices (e.g., tapes or disks) used for storing data. Different media are discussed later in the section on practical consideration.

20. Backup type

There are three main types of backup: Full, Incremental and Differential. These are methods for selecting which files should be included in a backup operation.

21. Full backup

Saves all files to the selected backup medium.

22. Incremental backup Saves all files that have changed (or been created) since the last backup (of any kind) outside the working environment. If incremental backups are used, the restoring of all files will require the last full backup plus all incremental backups since then.

23. Differential backup Saves all files that have changed (or been created) since the last full backup outside the working environment. If differential backups are used, the restoring of all files will require the last full backup plus the most recent differential backup.

24. Backup time Time taken to perform a backup, considered as either user time or machine time.

25. User time Period of time a user or operator has to attend to a computer to make the backup happen.

26. Machine time Period of time the computer requires for the backup. Many automated backup routines run unattended, particularly if high-volume backup media are used. Backup programs can be set to start outside normal working hours. Therefore, user time is generally much less than machine time.

27. Files All information on computers is held in files. The files can be categorized as files containing instructions (program files) and files containing information (data files). Typically, program files do not change regularly while data files are updated constantly.

28. Standalone PC A PC that operates with files on its own (floppy or hard) disk drives independent of a network. PCs that are not connected to any network will always operate as standalone. A PC attached to a network might sometimes work with files on its own disk drives and so be temporarily operating as standalone.

Cost-Benefit Considerations

29. You should do a cost-benefit analysis before making any important business decisions. Sometimes, this might be a formal process, particularly where the decision involves a significant investment. At other times, particularly in smaller businesses, it may be an informal procedure.

30. The creation of a backup procedure is no different. When you make the decision to buy, upgrade or outsource a computer or computerized system, you should include the backup process costs in your calculations. A wide variety of backup procedures are in use throughout the business world. Defining a procedure for your business should involve the identification and consideration of the costs and benefits of the different options available to you.

31. Basically, when you make any changes in the use of your computers, you should evaluate your procedures for saving business information off-site. There is very rarely a situation where a decision not to introduce a suitable backup procedure is justifiable. Very few computer users (businesses or individuals) can claim they have never lost data they would rather not have lost.

General benefits

32. The overall advantage of running an adequate backup procedure is the ability to recover data following a loss of that data from the computer's working storage.

33. The benefits of backups are two-fold. First, they provide peace of mind derived from knowing that your business can cope with unexpected disasters. Second, there is a potential future benefit in that you minimize future recovery costs, which might be significant, by incurring smaller costs at present.

Cost of an inadequate backup system

34. The types of costs that could be incurred in the event of a disaster where backups were not available include:

- Labor time to recreate programs or data (including overtime premium);
- Orders lost while data are being recovered);
- Industrial action if payroll cannot be completed;
- Lost production due to lack of systems or data;
- Penalty charges from customers, suppliers or banks due to inability to process information;
- Loss of goodwill (customers, supplier, banks, staff); and
- Closure of business due to lost production/sales/goodwill.

35. Appendix II provides some example scenarios discussing the costs of data recovery where backups are unavailable. This appendix also contains a template that allows you to perform an analysis for your own business.

Choices

36. You need to make a number of choices when designing a proper backup procedure, particularly:

- Frequency of backup — daily, every two days, weekly, other?
- Method of backup — manual or automatic?
- Type of backup — full, incremental or differential?
- Backup media used — disks (diskettes, DVD, CD-R/CD-RW), disk arrays (groups of hard disks acting as a single storage device), tapes?

37. These choices are discussed in more detail in the later section on “Practical Considerations.”

Costs of particular procedures

38. There are costs associated with implementing and running backup procedures. The extent of each type of cost will depend on the methods chosen. Cost can include:

- Purchase of backup media;
- Purchase of backup machinery (e.g., high-speed, high-volume tape streamers);
- Purchase of software to assist in backing up;
- Training in use of software;
- Purchase of on-site storage facilities (such as a fireproof safe);
- Purchase of off-site storage facilities;
- Rental of off-site storage locations (e.g., bank vault, third-party data-storage organization);
- Training in procedures;
- Time taken to perform backups (including data verification);
- Time to manage storage of backups (e.g., transport to and from off-site locations);
- Time taken to test backup procedures, including archive retrieval and recovery; and
- Monthly payments to a third party for storing data on a secure server.

Benefits of particular procedures

39. The benefits of each of the backup options as they relate to frequency, method, type and media are trade-offs between:

- User time taken to perform each backup;
- Machine time taken to perform each backup;
- Extent and choice of storage facilities;
- Time taken to perform recovery; and
- Interruption to normal work in performing backups.

40. Although some options offer benefits such as reduction in restructuring costs related to labor, time, media and storage space, sometimes the cost reductions are accompanied by increased risk. Do not try to achieve economies in recurring costs if that would result in inadequate protection from the risks presented by a loss of data.

Risk Indicators

41. You need to consider a number of factors when planning a backup procedure. These factors have a bearing on:

- The risk of problems from erroneous processing;
- The amount of processing that would have to be repeated if problems were encountered;
- The risk of significant interruption to processing caused by lost computer files; and
- The most suitable backup procedure.

Factors to consider when planning a backup procedure

42. Volume of processing:

- Daily use of files;
- Daily processing of transactions;
- Volume and significance of data updates; and
- Time on the system.

43. Use of purchased software:

- Extent of use;
- Customized/specialized nature of software; and
- Purchase/replacement cost of software.

44. In-house developed files:

- Programs;
- Spreadsheets;
- Databases;
- Word processing templates;
- Standard letters;
- Extent of use; and
- Development and redevelopment time.

Risks

45. Large volume of transactions:

- Increases importance of files;
- Increases time taken to reprocess any lost transactions;
- Increases extent of interruption to business while recovery is attempted.

46. Significant use of purchased software:

- Replacement cost of software;
- Interruption to business processes while replacement software is being obtained;
- Interruption while replacement software is being customized.

47. Significant use of in-house developed files:

- Interruption while files are redeveloped;
- Cost of time to redevelop.

Practical Considerations

48. The “Good practice Checklist” is divided into four parts:

Part A: What to back up

Part B: Making and storing backups

Part C: Recovery

Part D: Archiving

49. This section gives practical guidance in each of these parts in turn.

50. The guidance includes:

- A discussion of important issues in each area;
- A discussion on the merits of choices available; and
- Examples of things to consider.

Part A: What to Backup

General

51. A starting point in developing or analyzing a backup procedure for your business is the identification of what needs to be backed up. Only when you have a complete picture of your computer environment, the different computer programs its uses, the data it processes and all the files it needs to back up can you choose among different backup methods, media, equipment and frequency.

52. A common mistake in the management of computers in business is to concentrate effort on some systems and computers but ignore others. This can lead to an inconsistency of approach whereby some systems are well controlled while others are not. For example, companies often place great emphasis on backing up their financial systems but ignore their design systems. Yet, there may be a greater impact on the business if the design data were lost or not available.

53. It is important, therefore, to ensure that you consider all your computing resources in the development and analysis of your backup procedures. This means all computers, all systems, all data and all programs. By identifying how critical your data are to your business, you identify the computers and systems that need to be backed up and how frequently the backups need to be done.

54. The “Good Practice Checklist” gives some examples of what to consider in each of these areas. Further guidance and examples are given in the following notes. The examples are by no means an exhaustive list of considerations for every business.

Assess the hardware environment

55. Different businesses function using a variety of hardware environments. These environments may range from a single PC to a distributed network to a mainframe processor.

56. The number and location of your computers will have a bearing on the method you should use for backups. Consider the following examples.

- Centralized backup facilities might be appropriate for a single minicomputer accessed by terminals or for a PC network.
- For a large number of standalone PCs, it might be appropriate to use a portable storage device to perform backups.

- If PCs are attached to a network, it may be appropriate to perform scheduled backups of multiple servers or workstations in one central location.
- Peer-to-peer backups are a common solution for very small networks.
- If there are large volumes of critical data, it may be practical to compress data before transmitting it to a secure storage location, but this would require leased telephone lines or virtual private network software.
- If computers are spread out over various locations, it might be impractical to perform backups centrally on all machines each day. An appropriate backup cycle might involve backing up different computers on different days.
- If a business has two distinct locations, computers at one location could hold backup copies of files from the computers in the other location.

57. The location and use of computers might be organized to provide segregation of duties in important functions and to protect confidentiality of information. Backup procedures must not be organized in such a way as to undermine the segregation of duties or the confidentiality provided by location of the computers.

Identify critical systems and data

58. It is important to ensure that backup routines appropriately safeguard all your critical systems, programs and data against data loss.

59. The "Checklist" provides some examples of functional systems a business might have. As stated earlier, this list is not exhaustive but is intended to indicate some common areas that might be overlooked when identifying systems requiring backup protection.

60. Some further points to consider when preparing a list for your own business are given below.

    - Do not exclude systems that are being decommissioned. The decommissioning process might take longer than expected and the business could be vulnerable in the interim period.
    - Whenever you upgrade purchased or in-house developed application or operating software, you must ensure that the new systems can access current and archived files. This also applies when you upgrade storage devices and software.
    - If most PCs are networked, remember to consider significant systems running on standalone PCs and the data held on the PC hard disks. Often, the data on a standalone PC's hard disk may be more important than that on the network.
    - Remember to consider data already stored on storage media outside the working environment.
    - Understanding volumes of data held will allow you to make sensible decisions about the choice of backup media, backup methods and equipment and procedures to perform the backups.
    - To restrict unauthorized access, consider the confidentiality of data within your business, particularly where confidential data is stored in separate hardware. Be aware that the process

of backing up and restoring files can, in some circumstances, allow the person performing the backup to access information that he or she would not otherwise have access to.

Identify files developed in-house

61. Many larger businesses have a department of software developers producing software in-house within a formal framework. This framework should include regular backups of all work as it is being developed and the retention of master copies of programs at significant stages of development.

62. Smaller and medium-sized businesses will rarely have staff dedicated to program development. This does not mean that they may have no software developed for their specific needs. Any supplier of systems or dedicated software should be bound contractually to keep backups of application software available for the anticipated lifetime of that software. In addition, many small businesses still have significant resources invested in computer systems developed specifically for them, the loss of which could result in inconvenience or even financial loss.

63. Many PC software packages come with features that allow users to develop complex computer. Systems can be developed to automate or simplify manual tasks. The continued use of user-developed programs, templates and forms often enhances business performance. The danger is that such program files are not included in backup planning.

64. Consider the following types of files that are common to all businesses using computers.

    - Spreadsheets — Management accounting files, budgets, income and expenditure analyses, cash flow projections, templates for contract prices or loan repayments, fixed asset registers, VAT calculators.
    - Databases — Customer records, mailing lists, mail-merge files, product information, price lists.
    - Word processing (documents or templates) — Sales and purchase contracts, purchase orders, job applications, contracts of employment, delivery notes, invoices, letter templates, reports, fax headers, brochures, price lists, catalogues, newsletters.

65. If you can identify files of these types in your business, consider the following questions.

    - How long did it take to develop these files?
    - How much labor is invested in the cost of these files?
    - How much disruption would it cause your business if it lost some or all of these files? To operations? To management decisions? To personnel? To cash flow? To marketing? To staff/customer/supplier communication?
    - How long would it take to re-establish each of these files? (probably less than the original time taken, but possibly still significant)
    - How long would it take to re-establish all of these files at once?
    - Are the skills to redevelop these files still available in your business?

66. An analysis of in-house developed files (however formal the development procedure) will often lead to the conclusion that a business could suffer significant disruption, inconvenience or financial loss if backups of these files were not available.

Part B: Making and Storing Backups

Frequency

67. In determining the frequency of backups, you have to consider a number of factors as part of a cost-benefit analysis involved. Some of those factors are discussed below.

68. In most businesses with a significant degree of computerization, daily backups are desirable or even essential. Where less frequent backups are appropriate, a method must be defined that staff performing the backups can clearly follow. Such a scheme could, for example, dictate a full backup every Tuesday and Thursday, depending on the processing workload and the effect of any system failure at a critical processing time.

69. The frequency of backing up files is determined by the importance of the files, how often they are updated, the time required to recreate the files, the time to perform the backup, the ability to recover after restoring files and the resources required for recovery.

70. The more important the files and data are to your business, the more control you need to exercise over them. If a system is critical to the daily management and functioning of your business and is in constant use every day, a frequent backup cycle, possibly daily or twice daily, may be appropriate.

71. If files are changed only infrequently, daily backups could create multiple copies of identical files. In a small business, where almost all general ledger processing is performed at the end of each accounting month, backups may be necessary only immediately before and after the processing period. Daily backups over the three weeks of relative inactivity would probably be unjustifiable in terms of required backup time compared to the amount of time it would take to re-enter any transactions lost. If a large amount of data needed to be processed during the month-end closing period, however, and completion of processing were time-critical, daily backups during the month-end processing period would be appropriate.

72. It would be unwise to reduce control over computing resources merely because of inconvenience. It would be valid, however, to conclude that less frequent backups could be appropriate if the backups required several hours from a small system.

73. Where backup time is relatively long compared to the amount of time it would take to recreate the transactions for a day, there are three possibilities: (1) the volume of transactions dictates that daily backups are not appropriate; (2) the backup basis being used is inappropriate; or (3) the backup medium is not suitable for the volume of data being backed up.

74. An example of the first situation is a system that takes two hours to backup, but one day’s lost data would take two hours to recover.

75. An example of the second situation is where all files on a computer were being backed up each night but only a small proportion of the files had actually been changed. Time was, therefore, being spent on making additional identical backup copies of unchanged files.

76. An example of the third situation is where a full backup using floppy disks might take three hours but recovery of data might take 12 hours or more. In some businesses, the loss of 12 hours of data might be insignificant and the cost of backing up could outweigh the benefit of being able to recover the information. In other businesses, however, 12 hours of lost data would be a huge problem. In those cases, daily backups using different media could reduce the actual time required to perform backups and alter the cost-benefit equation.

77. In the cost-benefit analysis to determine frequency of backups, the time taken to perform and manage the backup procedure is the main cost, and it increases with more frequent backups. The costs that increase with less frequent backups relate to resources used to recover from the position stored on the most recent backup available after a disaster.

78. Recovery is discussed fully in Part C below, but the factors relevant to determining frequency of backup are discussed here. The resources include time taken to re-enter data and transactions to bring systems up to date. This is influenced by the availability of manual records of the data and transactions to be re-entered.

79. In some situations, comprehensive manual records exist to facilitate the re-input of data; in other cases, the manual information will not be readily available and the difficulty in recovering is correspondingly increased.

80. While the above comments relate to the time taken to recover, you need to be aware that some situations are not retrievable if too much time has passed since the last available backup. This could be because of practicalities of storage or retention of manual records, or because insufficient time was available to recover the data and transactions.

81. For example, consider a business that has used a computer package to maintain financial records and projections for bank lending, grant applications, VAT returns or income tax reporting. If the files containing data and transactions were lost the day before the application for funding or the tax returns are due to be submitted, it might be impossible to re-enter all relevant information before the deadline. In such a situation, the business may be denied vital funding or have penalties imposed for failing to submit returns on a timely basis.

82. You need to take all of the above factors into consideration when defining backup frequency.

83. Also bear in mind that it might be suitable to decide on different frequencies for different systems. It could also be appropriate to perform additional backups at critical times. To simplify the administration of backups, however, the overall backup routine for one piece of hardware is normally governed by the most sensitive and time critical-system residing on that hardware.

Bases for performing backups

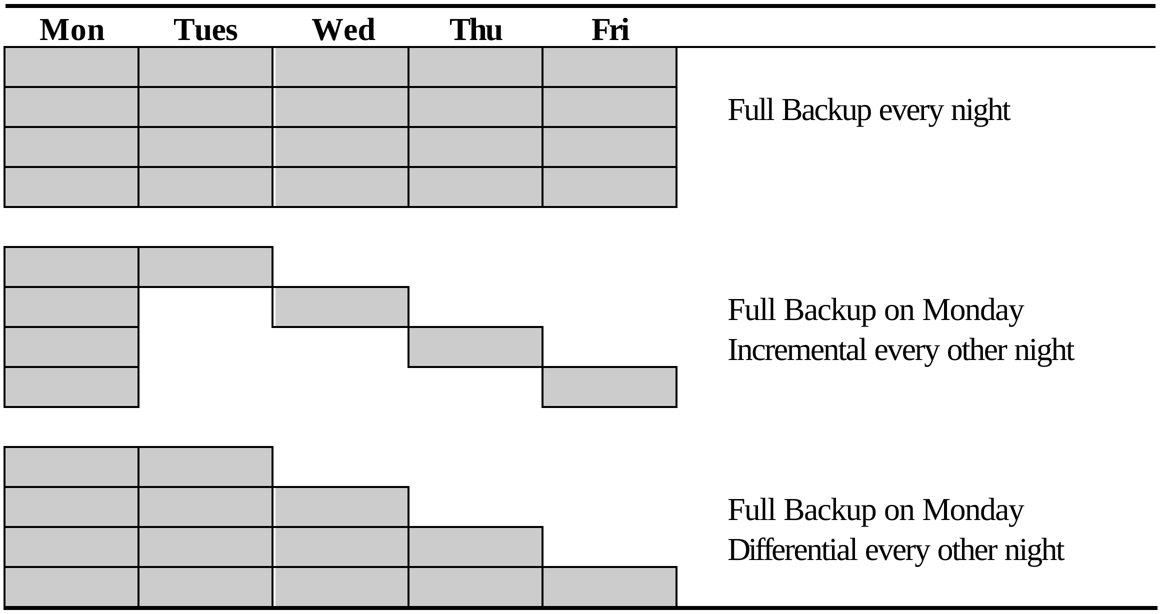
84. There are a number of different bases for performing backups. These are largely composed of a mixture of full, incremental or differential backups.

85. Full backups back up all files, incremental backups back up all files altered since the last backup of any type and differential backups back up all files that have been changed or created since the last full backup.

86. An illustration of the impact of these methods is given in Appendix IV. The general differences are given below.

87. A full backup will take longest to perform but recovery will require only one backup set. Using incremental backups saves backup time but increases the time taken to recover and the complexity of the recovery procedures. Backup time using differential backups falls between the other two bases, while recovery will require a maximum of two sets of backups.

88. An example of different backup bases is shown in the following diagram:



89. The full backup provides the maximum resilience but also requires the most space on the backup media and the longest time to perform. If a business uses online backup procedures, full backups may also be expensive as many providers of this service charge for the amount of space taken up on their server. The incremental backup takes the least space and time but a failure during Friday would require four backup sets to restore the system to its original position on Thursday night. The differential backup is a compromise between full and incremental since the space requirement increases as the week progresses but recovery requires two backup sets whenever a failure occurs.

90. A disadvantage of incremental backups is that a failure in the incremental backup for Tuesday night would prevent full recovery for the remainder of that week. This is because the recoveries for Wednesday to Friday all rely on the earlier incremental backup being available.

Backup media

91. There are a number of different media types for backup storage, including floppy diskettes, CD-R/CD-RW, DVD, magnetic tape cartridges, DAT (Digital-Audio Tape) and DLT (Digital Linear Tape) tapes.

92. The decision on which media to use will be based on a consideration of what backup devices your computer supports, the amount of data you need to back up, how often it needs to be backed up and how long it will take to perform the required backup.

93. Although backup programs will normally give an estimate of the time required to back up a selection of files, that estimate will be in terms of machine time only. It does not take account of the time it takes users to swap disks or tapes, nor does it include the time the machine has to wait for the next disk to be inserted because the user has been distracted.

94. The ideal backup media for the task would be one where all the data from a backup run would fit onto that one item (e.g., a disk, tape or magazine of cartridges). This would allow an operator to set up the procedure, then leave the machine to do the work, knowing that the job could be completed without any further intervention.

95. It is not always possible to achieve that ideal, particularly where a move to higher volume media would involve a large investment.

96. Consider a situation where a backup program requires 10 minutes of machine time and four floppy disks to back up all files. Since the whole operation will be completed in less than 15 minutes, it would be reasonable to expect the user to stay by the machine to insert disks after the routine has started. When the backup requires 30 minutes of machine time and 12 disks, however, the user would be unproductive for most of an hour merely to ensure the program runs successfully. In this case, it would be worthwhile considering the use of higher-volume media as the investment in, say, tape streamers would quickly be recovered in reduced labor costs and machine time. This is particularly true if backups are performed very frequently and the personnel involved in operating the system are highly paid.

97. The cost of the backup media itself has to be considered. Because magnetic media are reasonably cheap and can be re-used many times, the labor cost of operating a backup routine that is inefficient due to the choice of media will often outweigh the extra cost of purchasing disks or tapes.

98. Machinery to operate the media should also be considered. Floppy diskettes require no hardware other than a floppy drive that is standard on the vast majority of computers. Cartridges, DAT tapes and DLT tapes will require additional streamers. Prices of these will vary with developments in technology and the competition for particular hardware types. You can, however, now acquire streamers that can back up all data from the hard disk of a large PC for just a few hundred dollars. As a one-off cost, this aspect should not be a restriction in choosing a time-efficient media type.

99. Because technology changes constantly, it is impossible to give definitive comparisons of capacities of each medium, and you ought to contact hardware suppliers to obtain advice on the latest technologies and capacities before committing yourself to a particular backup strategy.

Method

100. There are two different levels of sophistication in backup methods — simple copy functions and specific backup programs.

101. The simplest method of creating backup files is to use the copy function in your standard computer operating system. This will involve selecting the files to be backed up and copying each of them onto some portable storage media, such as floppy disks, an external hard disk or perhaps a portable computer. The only significant advantage of this method is simplicity.

102. The main disadvantage of the simple copy method is the administrative overhead. The user has to decide which files are to be copied. There is a risk that some files could be missed. If more than one disk is required for the backup, the user will have to document which files are on which disk. The organization of files might be disrupted so that the structure of file groups will have to be rebuilt manually when recovery is required.

103. As an alternative to manual file copying, you can use a backup program. These are commonly available and most PCs now have built-in backup programs. Backup programs provide options to back up data, compare backups to originals and restore backup files.

104. Backup programs assist with the administrative overhead of backing up. Generally, they allow a user to select the files to be backed up using sophisticated search functions. The programs provide the option to save the search criteria for future use, manage the allocation of the files onto the storage medium, create a catalogue of the files backed up and can automatically verify that the information has been correctly copied as the backup takes place.

105. Backup programs usually compress the files they are backing up. A compressed file will require less storage space than the original (compressed files often require less than half the storage capacity of the original, and some data files can be reduced to as much as 10% of the original size). Therefore, more files can be stored on a disk or tape, which in turn reduces the number of disks or tapes

required. A compressed file cannot be used directly but must be restored using the same backup program that made the original backup.

106. If the backup program is run using low-volume media (such as floppy disks), the program will prompt the user when the next disk is required. Therefore, if more than one disk or tape will be required for the backup, the program must not run unattended.

107. The majority of dedicated backup programs provide options whereby the backup process can take place at a specified time, often during the night, when the system is not likely to be in use.

108. Manual copying is suitable for only a very few files. It is an appropriate method for small systems or for small projects where backup protection in addition to the general method is required. In all other scenarios, a dedicated backup program should be used.

Decide on storage environment

109. Whether on tape or disk, backups provide access to files in the event of accidental or deliberate destruction of the original information. Therefore, it is essential that storage of backups allows the following:

- Reasonable certainty that a backup is available;
- Prompt access to backups should the original files be destroyed.

Guidance

110. You should store your backups in at least two distinct locations — one in the same general location as your computer equipment for prompt access, and the other physically removed from your computer equipment, i.e., off-site, so that the same physical event cannot affect both original and backup files.

111. On-site backups should be stored in a fireproof safe that is locked when not in use. A fireproof safe provides protection against fire but it should also be secure from water damage.

112. Access to on-site storage should be restricted to personnel who perform backups and who need to perform recovery procedures. The total number of people with access to the backups should be as small as possible, but no less than two.

- Backups should not be stored along with other items if the other items need to be accessed by personnel who are denied access to backups.
- Where separate systems are used for confidential or sensitive processing that should not be accessed by staff responsible for backing up other systems, the backups for the sensitive systems should be stored separately.
- If only one person has access to the backups, the business runs the risk of being unable to use the backups if that person is absent at the time when access is required.

113. Off-site backups should be performed according to a specified procedure:

- Haphazard off-site storage is difficult to control.
- A common procedure for daily backups is to make one person responsible for taking the backed-up media to the place of storage.

114. The decision about which backup media to store off-site and which to keep on-site should be based on the following factors:

- The need to recover from a backup in a very short time scale.
- The backup basis used — do you need the last full backup or must you also obtain the last four incremental backups?
- How easy is it to access the off-site location?

115. Disks and tapes used for backups have a finite life. Factors you should consider in managing backup media include:

- The life of the media will be a combination of the number of times the media have been used, how old the media are and the period of time since the data was last used.
- The manufacturer's guaranteed lifetime of the backup media used.
- Where files are archived, media will deteriorate after a long period in storage. To extend the life of archived data, it may be necessary to restore and then re-archive the files using new media.

Part C: Recovery

116. An essential component in a backup procedure is the ability to recover in the event of a disaster. The main considerations in this area are discussed below.

Verification of backups

117. Verification of backups immediately after they are done gives assurance that the backup has been performed correctly and that all selected files have been backed up.

118. Backup programs normally come with verification options that can be run immediately after a backup.

Restoring data

119. The order in which files are restored onto a system can be important.

120. The file grouping into which files are restored is also important. Certain programs may have to be in specific locations in named computer directories. Therefore, if the files are not restored into the same directory as the program calls for, the program might fail.

121. Where backup files have been compressed to save backup media space and time, the files must be decompressed before use.

122. Backup programs come with restore options that will manage the grouping of files as they are restored. If the program has compression options, then it will also have decompression options.

123. It is good practice to perform a practice restoration occasionally. This provides a number of benefits including ensuring that the backup program works properly, the methods used to back up and restore are sound and the backup media is reliable. It also provides training and experience for staff who will be required to perform the restoration when a disaster happens.

Which backup disks to use

124. The identification of backup disks (or tapes) is essential. Mark your disks should and store them methodically.

125. The number and selection of backup sets required will be determined by the backup basis (full, incremental or differential).

126. Maintain a register of backups. It should record the date of the backup, the backup set identification, the type of backup, etc. A potential format for a backup log is included in Appendix V.

Recovery of data from manual records

127. Regular backups will ensure that, in the event of a disaster, data has to be recovered only from the time of the last available backup. Manual records must be in place to allow that recovery to take place. This includes the retention of original vouchers and the availability of procedures to recapture that data.

128. For example, in a purchase ledger processing system, retention of purchase invoices will allow the data to be re-entered. Annotation of account codes and other information on the vouchers will assist in the data recapture.

129. Should a data loss interrupt processing, it may be inappropriate to continue with normal processing until all prior data is recaptured. This might require using alternative manual procedures for the current transactions while recovery of previous transactions takes place.

130. Consider a sales invoicing system that automatically allocated invoices numbers sequentially. New invoices could not be posted immediately as that would have resulted in the use of numbers already issued. In this case, perhaps, manual invoices could be issued to keep credit control procedures up to date, and those invoices entered into the system once it has been fully restored.

Part D: Archiving

Introduction

131. As previously noted, archiving differs from backup in that the original data being archived is normally destroyed after archiving has taken place. Normally, the purpose of archiving electronic information is to free up computer resources so that current processing requirements can be fully met. Archiving frees up hard disk space for current data and may reduce the time taken to produce reports from data files.

132. You should think about archiving when:

- Hard disk space is running low.
- More than two years' transaction data is held on file.
- New computer hardware or software is being implemented and previous files will no longer be accessible.

133. As with backup procedures, archival procedures should cover data and important in-house developed software.

Purchased software and data

134. Installation disks for purchased software often store programs in compressed format. The files are decompressed when installed. Therefore, storing installation disks in a safe place is often more space efficient than backing up from decompressed files.

135. In all recovery situations, it is desirable to have a backup copy of files in a known state. Installation disks provide an instance of this. The known state is the unaltered state as purchased.

136. If you have invested a significant amount of work in customizing the set-up of purchased software, store a backup copy of the customized version in a safe place. This is not an alternative to storing the original disks. The originals may be the only way to reinstate the system if the customization has had unexpected detrimental effects on the programs.

137. Purchased data can take a variety of forms, including:

- Business databases (e.g., trade price lists, tax rates, exchange rates, company information);
- Administration forms (e.g., templates for invoices, order forms, memos); and
- Design aids (e.g., general clip art, industry logos).

138. Where possible, do not keep using the original disks. Instead, install data and programs onto the computers and keep the original disks in a safe place to provide access to unaltered masters when required.

In-house developed files (spreadsheets, databases, work processing templates and master files)

139. Your should implement controls over master copies of in-house developed files in the same way as for original disks for purchased software and data. Archives of in-house developed information ensures that a full trail of the development of any in-house systems is available.

Develop archiving procedures

140. As with retention of master files, separate procedures are required to control copies of archive material. Similar factors should be considered as for the development of backup procedures.

141. The first stage will be identification of archiving requirements. This will depend on the nature of the business, but might include plans and proposals for explanation, lending or grant applications, historical data and resources for occasional projects. Other requirements that might affect a variety of businesses include legal, tax and employment matters.

142. Once you identify the purpose of archiving (system performance contracts, tax, etc.), you need to analyze your business resources.

This includes:

- Identification of the computers that might hold information that needs to be archived;
- Identification of systems that need to be archived (to access archived data); and
- Identification of data to be archived.

143. Then you have to decide on methods and storage facilities. This should recognize the fact that, often, the archived information will not be needed for a long time but might have to be located quickly when it is needed. Two emerging storage architectures are the Storage Area Network “SAN” and the Network Attached Storage “NAS.” In different ways, these two architectures provide access to data by more than one application or user. Both NAS and SAN exploit the availability of high-speed networking. SAN architectures address the need to consolidate large amounts of data by designing high-speed fiber optic networks. NAS products plug into existing local area networks to provide convenient, low-cost additional storage. Both NAS and SAN provide scaleable storage capacity and performance, a clean separation between server and storage purchasing decisions, the ability to serve multiple users in multiple operating environments and support for high availability.

144. Archival procedures should document what data has been archived, when the archive was created, how many copies of the archived material are in existence, where those copies are stored, the software used to create the archive and any special procedures needed to recreate the data files.

Good Practice Checklist

	Yes	No	N/A	Reference
A. WHAT TO BACKUP				
Assess the hardware environment				
Do you know how many computers your business has?				
Do you know where all the computers are?				
Do you know what the computers are used for?				
Identify critical systems and data				
Do you know what systems run on those computers? Consider: Financial Design Manufacturing Contract management Asset management Personnel Correspondence Other				
Do you know how may networks operate in your business?				
Do you know what systems operate on individual PCs?				
Do you know what systems operate at remote sites?				
Do you know what systems operate on portable computers?				
Do you know what data are stored on the computers in your business? Consider: Purpose Volume Frequency of change Commercial significance Confidentiality				
Do you know what data are stored on the network(s)?				
Do you know what data are stored on the hard disks of PCs connected to networks?				
Do you know what data are stored on the hard disks of PCs not connected to networks?				

	Yes	No	N/A	Reference
Do you know what data are stored at remote sites?				
Do you know what data are stored on portable computers?				
Do you know what data are stored on floppy disks?				
Do you know what data files you need to back up to protect your business records? Consider: Financial Design Manufacturing Contract management Asset management Personnel Correspondence Other				
Do you know what data files you need to back up to continue business operations? Consider: Financial Design Manufacturing Contract management Asset management Personnel Correspondence Other				
Identify in-house developed files				
Are in-house developed programs included in backup procedures?				
Are in-house developed word processing templates, standard documents and forms included in the backup procedures?				
B. MAKING & STORING BACKUPS				
Determine backup method and frequency				
Do you know how often you need to back up your data files?				
Are the correct data files being backed up on a sufficiently regular basis?				
Is the correct method being used to perform backups?				

	Yes	No	N/A	Reference

Are all backups logged?				
Does someone check the backup logs to ensure that backups are taking place correctly?				
Is every backup verified?				
Is the backup medium used the most appropriate?				
Decide on storage environment				
Are backups kept securely off-site on a rotational basis?				
Are on-site backups kept securely and in a fireproof safe?				
Are backup media regularly tested to ensure that they are still viable?				
Do you know how often your backup media should be replaced?				
C. RECOVERY				
Check recovery procedures				
Are the backups checked to ensure that data have been correctly copied?				
Do you know how to restore data from backups?				
Do you know which generation of the backup media to use when restoring data?				
Are manual records sufficient to allow full recovery of data?				
Are recovery procedures regularly tested to prove that they work?				
D. ARCHIVING				
Master copies of source files				
Are installation disks for purchased software held securely?				
Are installation disks for purchased data held securely?				
Consider: Databases Document templates Forms Clipart Other				

	Yes	**No**	**N/A**	**Reference**
Are master copies of in-house developed programs held				

securely?				
Are master copies of in-house developed spreadsheets and databases held securely?				
Are master copies of in-house developed word processing templates, standard documents and forms held securely?				
Develop archival procedures				
Do you know what data files you need access to for legal, tax and Customs & Excise investigations?				
Do you know how far back you can recover employee details?				
Do you know how long data needs to be held for legal purposes?				

APPENDIX I — DATA LOSS CASES

Case 1

Business: A charity

Event: The premises of a charity were broken into and the computer equipment was stolen.

Effect: The charity hoped that the equipment might be replaced by donation. It lost all its data (including accounts, contact names and addresses and standard document templates), however, as no backup copies of files had been made.

Summary: Lack of routine backups led to severe interruption in the operations of the charity and, potentially, to the permanent loss of charitable income from donors whose information was lost.

Case 2

Business: Self-employed publisher who also used his computers to maintain membership records for a social club

Event: A fire occurred in premises three floors above the publisher. The water damage caused by putting out the fire destroyed the hard disks of the publisher's computers and also the floppy disks, containing membership data that he kept beside the computers.

Effect: Business data were irretrievable lost. The permanent records of statistics and archived information for publishing were lost. Document templates had to be redeveloped. Historical and statistical data had to be re-entered.

Financial models were lost and had to be recreated.

The membership data were irretrievably lost. New memberships could not be issued for some time, and the interruption threatened the viability of the social club and reduced membership income.

Summary: Lack of off-site backups caused disruption to the maintenance of social club membership files, and the club was unable to prove which of its members had paid their membership subscriptions.

Business data had to be re-entered over a period of three months. Staff time used in data capture reduced productivity capacity in the business and income was lost as a result.

APPENDIX II — COST-BENEFIT CASES

The purpose of the following examples is to illustrate the costs and benefits that might be considered when establishing a backup routine.

Example 1

Business:	A graphic design business using desktop publishing technology on a network
Computers:	Eight PCs (six for client work and two for secretarial work)

The following table shows the use made of each of the computers over an average working week and the cost-benefit considerations that could be taken into account when deciding on a backup strategy.

	Design Activities	**Admin Activities**
Number of users	6 designers	2 secretaries
Average daily productive processing time per user	3 hours/day	5 hours/day
Reprocessing time required if one day's input were lost	18 hours	5 hours
Working days in week	5 days	5 days
Reprocessing time required if one week's input were lost	90 hours	25 hours
Total Reprocessing Required		
Per day	23 hours	
Per week	115 hours	

This table provides an indication of the amount of reprocessing required in the event of a major data loss. If no backups were made, it might be possible to recreate the work for one day or one week, but the recovery of information might be impossible over a longer time scale.

In this situation, the level of computer use is such that a daily backup routine would appear to be prudent.

Example 2

Business: A small publishing company using desktop publishing technology to produce copy for a weekly magazine. The magazine must be printed on Friday and loss of copy after Wednesday would be critical to the business.

Computers: A single PC

Use of the PC:

Monday	1 hour
Tuesday	2 hours
Wednesday	3 hours
Thursday	6 hours
Friday	1 hour

Backup time: It takes 30 minutes to back up all data onto floppy disks by a manual routine.

Suggested backup procedure:

(1) Performs a backup after processing on Wednesday

(2) Perform a backup on Thursday evening

(3) Perform a backup on Friday once the edition is complete

This procedure recognized the critical processing pattern of the business while acknowledging that not all data need to be backed up all the time.

Analysis sheet for your own business

The purpose of the following schedule is to provide you with a framework for identifying and considering the necessary backup routine for your own business.

Business: ....

Computers: ....

Usage

		Business Activities		Admin Activities	
Number of users	A				
Average daily processing time per user	B		hours/day		hours/day
Percentage of processing that would not have to be repeated, for example, because it is experimental or non-productive	C		%		%
Reprocessing time required if one day's input were lost (A × B × (100 – C))	D		hours		hours
Working days in week	E		days		days
Reprocessing time required if one week's input were lost (D × E)	F		hours		hours

Total Reprocessing Required

Per day (D Business + D Admin)	hours
Per week (F Business + F Admin)	hours

Now consider the costs and disruption involved in reprocessing, with particular reference to:

- The cost of labor (including overtime premiums, sub-contractors' fees, etc);
- The capacity to re-perform work without falling behind in the current workload;
- The ability/willingness of staff to perform extra work at short notice.

The frequency of backup will be determined by the volume of reprocessing required, the time needed to make backups (be they full, incremental or differential) and by any fluctuations in processing volumes throughout the business cycle.

APPENDIX III — FLAWED BACKUP CASES

This Appendix contains two examples of businesses performing regular backup routines that appeared to be sensible but that, after further probing, turned out to exclude large areas of processing.

Example 1

Business sector:	Education
First systems details:	Customer recording system and accounting package
Hardware:	Network linking 24 PCs
Backup:	Full backup made daily
Second system details:	Personnel system
Hardware:	Standalone PC
Backup:	None
Conclusion:	In the event of data loss, there would be no records to allow historical data to be recaptured. No manual personnel records were maintained and no backups existed. The financial systems had been adequately catered for but the needs of the personnel department had been overlooked.

Example 2

Business sector:	Education
First system details:	Database systems maintaining mailing lists, customer credit agreements, course details
Hardware:	One minicomputer accessed by around 50 PCs and terminals
Backup:	Full backup made daily
Second system details:	Accounting ledger
Hardware:	Minicomputer, the use of which was being wound down in preparation for disposal
Backup:	None made for 15 months.
Conclusion:	There was no backup routine for the minicomputer because of proposals to replace the current accounting systems. A significant failure of the minicomputer, which was becoming increasingly unreliable, would prevent the preparation of accurate accounting records and management information. Records could be restored only if all financial transactions for the last 15 months were to be re-entered.

APPENDIX IV — COMPARISON OF BACKUP BASES

The following tables compare three different backup methods working over a five-day period. The times taken for each backup are assumed and are used to illustrate potential time saving and costs.

KEY:			
	F1, F2, F3, F4, F5	=	Full backup sets 1, 2, 3, 4 and 5.
	I1, I2, I3, I4	=	Incremental backup sets 1, 2, 3 and 4.
	D1, D2, D3, D4	=	Differential backup sets 1, 2, 3 and 4.

Method 1 Full backups

The following table illustrates the use of a full backup made every night.

	Day 1	**Day 2**	**Day 3**	**Day 4**	**Day 5**	**Max**	**Ave**
Backup							
Set(s) used	F1	F2	F3	F4	F5		
Time take (Mins)	100	100	100	100	100	100	100
Recovery							
Sets used	F1	F2	F3	F4	F5		
Number of sets	1	1	1	1	1	1	1

Method 2 Incremental backups

	Day 1	**Day 2**	**Day 3**	**Day 4**	**Day 5**	**Max**	**Ave**
Backup							
Sets used	F1	I1	I2	I3	I4		
Time take (Mins)	100	20	20	20	20	100	36
Recovery							
F1 + I1 + I2 + I3 + I4	F1	F1 + I1	F1 + I1 +I2	F1 + I1 +I2 +I3			
Number of sets	1	2	3	4	5	5	3

Method 3 Differential backups

The following table shows the situation where a full backup is performed at the end of day one and differential backups are made at the end of days two to five.

	Day 1	Day 2	Day 3	Day 4	Day 5	Max	Ave
Backup							
Set(s) used	F1	D1	D2	D3	D4		
Time take (Mins)	100	20	40	60	80	100	60
Recovery							
Sets used	F1	F1 + D1	F1 + D2	F1 + D3	F1 + D4		
Number of sets	1	2	2	2	2	2	2

APPENDIX V — BACKUP LOG

The following table is a suggested format for a manual backup log that could be kept to record which backups were made, what data was backed up, and when the backup was actually made:

Date	Tapes used	Type of backup	Event	Any additional comments	Initials
Records the date on the backup was performed	Records the labels(s) of the disk(s) or tape(s) used to carry out the backup	Was the backup: F Full I Incremental D Differential?	Why was the backup performed? End of day, end of week, end of month, before a new software upgrade?	Space to note any problems experienced	Initials of the person carrying out the backup.