International Federation of Accountants

Small and Medium Practices Task Force

April 2003

Controlling Computers in Business: Physical Security

The second 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 second 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: +1 212-286-9570
Email: SMPpubs@ifac.org

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

ISBN: 1-931949-01-X

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.

Often under-valued, the existence of sound physical security around computing equipment is one of the key factors in preventing loss or damage to that equipment and to the information it may contain. This guidance document examines the threats posed by inadequate physical security and suggests how these threats can be countered.

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 second in 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.

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' 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 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. Sound physical security for computing and communications equipment is one of the key factors in preventing loss or damage to that equipment and the information it contains. This guidance note uses the terms "computing equipment" to cover both IT and communications equipment.

9. Your computing equipment may be exposed to a wide variety of threats, both accidental and deliberate, caused by factors inside or outside your business. There are, however, appropriate precautions you can take to prevent accidental, deliberate, internal or external threats from causing losses.

10. A physical event affecting your computer equipment has the potential to interrupt processing for a long time. Yet, often, you would have been able to predict such events had you only taken the time to consider what can happen and the potential impact on your business. Ironically, the precautions against such events are inexpensive and easy to implement.

11. Consider the following threats and whether your business can prevent damage to its computer resources:

    - Natural disaster—fire, flood, storm damage, etc.;
    - Disruption to essential services—power cut, water shortage;
    - Withdrawal of facilities—strikes, disputes with business partners;
    - Malicious damage—sabotage or vandalism;
    - Criminal acts—theft or fraud; and
    - Unauthorized use of facilities.

12. The potential losses include:

    - Loss of equipment, either permanent or temporary;
    - Loss of processing capability;
    - Loss of data;
    - Inability to communicate with the outside world;
    - Inability to link with external computer systems;
    - Financial loss;
    - Reduction in financial control; and
    - Poor market perception.

13. Although the first five types of loss are obvious consequences of destruction or damage to computer and communications equipment, the remaining three are also worthy of further explanation.

14. Financial loss can involve both direct and indirect costs. Direct costs are incurred where insurance policies do not fully cover the cost of replacement hardware and the hire of temporary facilities. Even if they do, there may be a delay in obtaining settlement, triggering an adverse cash flow situation. Indirect costs are potentially more serious and could include reduced sales, loss of market share, loss of goodwill, overtime costs to resolve problems and many other consequential factors that can result from a business's inability to operate.

15. Financial control might be impaired because the loss of computer equipment might well undermine segregation of duties and because sensitive equipment and information might be more freely available than was previously the case.

16. A business's image in the marketplace might be tarnished when a seemingly simple physical event causes a major disruption to its operations. A quick recovery can restore this loss of image but the fact that the business was exposed in the first place reduces overall market confidence.

17. There are three main types of physical threats to your computing resources:

    - Physical security weaknesses;
    - Environmental threats; and
    - Administrative inadequacies.

18. Physical security weaknesses involve control deficiencies that allow unauthorized individuals access to computer equipment. Such unauthorized access can then lead to the theft, damage or destruction of that equipment.

19. Environmental threats include fire, flood, earthquake and other interruptions to power supplies.

20. Administrative inadequacies stem from inadequate procedural or documentary controls over computer equipment; the controls may be incomplete, inaccurate or not performed on a timely basis. An example of an administrative weakness would be the failure to maintain an adequate hardware register of all of a business's computer equipment.

21. The main objective of physical security is to prevent threats of any kind from materializing, thereby preventing disruption to computer processing, communications and damage to computer equipment and data. It is equally important to implement controls aimed at limiting damage should, despite your best efforts, some kind of incident damage your computing resources.

22. For example, good physical security controls should not only seek to reduce the risk of fire breaking out near a computer, but should also serve to limit damage that any fire may cause.

23. No matter how good your physical security is, it is impossible to prevent every potential threat from occurring. For that reason, you must carefully review your arrangements for recovering from potential disasters and so minimize the effects of such events. Computer disaster recovery planning will be covered in a later guidance note.

Key Terms

24.	Physical access	Physical access governs the security for the tangible, physical elements of your computer system, including computers, printers, backup media, communication devices and other physical equipment. A simple example of a physical access control is the use of locks (e.g., swipe cards or number keypads) to prevent access to computing equipment.
25.	Logical access	Logical access governs the security for intangible, logical elements of computer systems, including computer programs, operating systems and data. A simple example of a logical access control is the use of user names and passwords to prevent unauthorized access to computer programs.
26.	UPS	An Uninterruptible Power Supply (UPS) comprises battery power that can allow a computer to continue to operate in the event of a power failure. Often, a UPS will provide power to allow the computer to continue for a period of approximately 30 minutes, allowing a controlled shut-down of operations. Software is available that automatically backs up any data being worked on when the UPS becomes activated. A UPS should also provide protection from power surges.
27.	Modem	A MOdulator/DEmodulator (modem) is a hardware device that allows computers to communicate with each other across analogue telephone lines. When transmitting, a modem modulates the digital signal from a computer to an analogue signal for transmission over telephone wires; when receiving, a modem performs the reverse process to demodulate the analogue signal into digital form.

28.	EDI	Electronic Data Interchange (EDI) is a mechanism whereby a computer application in one organization can communicate with a computer application in another organization, eliminating the need for paper documents. An example of the use of EDI is where the purchase order processing system in Company A transmits order details to the sales order processing application in Company B using standard formatting messages. These EDI messages can also be encrypted to make the information more secure.
29.	EFT	Electronic Funds Transfer (EFT) is the term used for the electronic transmission of payment information. EFT covers payment systems such as BACS and is generally used by companies to pay employees and suppliers.
30.	LAN	A Local Area Network (LAN) is a collection of PCs linked together to allow them to share storage space (network drives), printers and other network facilities. LANs also allow the individual PCs to communicate with each other through the use of electronic mail packages.
31.	WAN	Wide Area Network (WAN) is the term used for a network of computers located in a number of physically distinct locations. WANs generally use different communication technologies from LANs and are intended to speed up communications across greater distances.

Cost-Benefit Considerations

32. You should do a cost-benefit analysis before making any important business decision. 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.

33. The implementation of a sound physical security framework is no different. A wide variety of physical access controls is now available throughout the business world, and the definition of an adequate control framework for your business should involve considering the costs and benefits of the different options.

General Benefits

34. The overall benefits of implementing sound physical access controls are the prevention of potential threats that might cause losses, the minimization of loss if a threat does materialize, and the peace of mind derived from knowing that your business has taken the appropriate level of precaution against such physical risks.

Cost of inadequate physical controls

35. Should disaster strike and your controls fail, or not exist in the first place, you will incur various costs, both direct and consequential (indirect):

36. Direct costs:

- Cost of replacement hardware, where insurance coverage is inadequate;
- Cost of funding replacement hardware, while waiting for settlement of the insurance claim;
- Cost of upgrading hardware and software where your insurance policy does not allow for any element of upgrade;
- Labor time to re-install system and re-enter data (including overtime premium).

37. Consequential or indirect costs:

- Orders lost while you recover your processing capability;
- Orders lost if customers cannot communicate with you electronically;
- Industrial action if you cannot process your payroll;
- Lost production due to lack of system or data;
- Penalty charges from customers, suppliers or banks due to late processing of income or receipts;
- Increased interest burden due to adverse cash flow;
- Loss of goodwill;
- Closure of a business division.

Cost of implementing physical security

38. The costs of implementing physical security access controls include:

- Purchase of control equipment, e.g., door locks, fire extinguishers, UPS, air conditioning, safes;
- Training of responsible staff; and
- Refurbishment to assist control, e.g., sealing unnecessary doors, installing partitions.

39. Fortunately, many physical controls are merely the application of common sense and good housekeeping that have little or no cost attached. Such controls include:

- General tidiness (no waste paper on floor, clear desk policy);
- Fire prevention (no smoking in sensitive areas, adequate storage of combustible materials);
- Barrier controls (locking doors when rooms and equipment are unattended); and

- Restricting public/customer access.

Risk Indicators

40. You need to look at a number of factors when developing a physical security policy. These factors have a bearing on:

    - The risk of malicious damage;
    - The risk of accidental damage; and
    - The extent of loss as a consequence of a physical disaster.

Risk factors to consider

41. The following factors increase the risks associated with physical security:

    - Large number of pcs spread throughout your business;
    - Extensive use of electronic communications to deal with customers and suppliers;
    - A lot of portable computing (e.g., laptop) equipment;
    - Easy public access to premises, pcs and main computers (e.g., servers);
    - Inadequate physical segregation of staff in incompatible roles (e.g., staff responsible for handling cash and for maintaining accounting records);
    - Inadequate procedures to restrict the access of departed or departing employees to your computing resources;
    - Systems include sensitive or commercially confidential data;
    - Use of systems with immediate cash implications (e.g., BACS, EDI, EFT);
    - Backup data held on floppy disks; and
    - PC equipment fitted with removable hard drives.

Practical Considerations

42. The "Good Practice Checklist" near the end of this document sets out the questions you or your managers should ask about the physical security for your computing resources.

43. This section gives practical guidance on the areas covered in that checklist.

44. Before physical access controls can be implemented or evaluated, you must have a complete picture of the computer systems and peripheral equipment your business uses. Once you have put together an exhaustive list, you can consider the physical, environmental and administrative issues relating to each item of equipment in turn.

45. These practical notes are split into four parts.

    - A: Identification of computer systems and resources

- B: Physical security measures
- C: Environmental protection
- D: Necessary administrative procedures and controls

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

Part A: Identification of Computing Systems and Resources

47. The identification and analysis of your computer equipment will indicate where you need to place greater emphasis on introducing or improving physical security controls.

48. It is important to completely identify all your computing equipment. Damage to a minor part of a network or to an essential peripheral may have a significant impact on your business overall. A simple example is the damage a spilled cup of coffee can do to an electronic scanner. Although you can probably replace the equipment within a few days, if the damage occurs at a critical point in the delivery of some service to a client, those few days of delay could have a significant ripple effect.

49. When identifying the computer equipment within your business, you must also consider:

- Specific tailoring or configuration of equipment; and
- Old hardware that might not easily be replaced.

50. You will need to implement a greater degree of control for your specialized or more valuable systems than for your standard systems, as the cost of losing them would probably be greater in terms of length of time to replace or repair. Some older systems with functions tailored to a specific business may be impossible to replace due to lack of availability of equipment or programming skills.

51. Another factor to consider when analyzing your physical environment is the availability of comprehensive and up-to-date documentation. Although the configuration of a specialized printer might not be important on an ongoing basis, the configuration information might become essential if the equipment has to be replaced within a short time scale. Detailed documentation reduces reliance on key individuals and therefore reduces the adverse consequences of a physical event affecting computer equipment.

Part B: Physical Security Measures

52. You should implement physical security measures not only for your main computing equipment, but also over peripheral equipment, communications equipment, distributed computing resources and documentation.

Computer room

53. Normally, your main computer hardware will reside in a dedicated computer room. The advantage of a dedicated area is that physical security and environmental controls are easier and cheaper to implement.

54. The computer room should be made as secure as possible from all physical threats. The threat of theft will be reduced if the room has no windows into public areas, is situated away from public access and is higher than ground level.

55. Access to the computer room should be restricted to a small number of people, each of whom should have a role in computer management or operations. The room should be separate from other work areas to minimize the number of people who access it. The area should also be locked at all times to discourage casual access.

56. To preserve the sanctity of the computer room, do not put other office equipment, such as photocopiers and printers, in it.

57. Where it is not possible to put computer equipment into a dedicated room, figure out how to best secure your important equipment, such as network file servers. You can purchase lockable cabinets and fireproof safes to prevent unauthorized physical access to such important equipment. Although not as secure as a dedicated room, these cabinets will provide valuable protection against accidental damage.

Distributed Computer Equipment

58. The growth in the use of standalone PCs and networks of PCs means that, inevitably, your computing equipment is spread throughout your business. Although the physical security of that distributed equipment is no less important than the equipment in the computer room, its distributed nature makes it more difficult to secure.

59. Any distributed PCs should be located in areas that are not accessible by the public.

60. Desktop PC equipment should be locked to the desk wherever possible. Most computer equipment now comes with a facility whereby you can attach the computer case to a desk using steel cables. Portable equipment should also be securely locked when not in use, and it should be securely stored at night. Additionally, most computer equipment now comes with a power-on password that can be used to prevent people with physical access to equipment from being able to access any of the data it contains. Although they are not foolproof, such passwords should be used wherever possible.

61. You must learn to avoid common mistakes, such as storing a file server under a desk where it is easy to inadvertently kick the on/off switch or to spill coffee onto it.

Portable computer equipment

62. The physical security of portable computer equipment (e.g., laptops) presents a specific problem in that the owner/user cannot always control the computer's physical environment, either when it is being used or when it is being transported.

63. When you transport a portable PC, physical control of the equipment is important. When you travel by air, take your PC on board as hand baggage. This reduces the risk of damage in transit and ensures that the PC is never out of your sight. Security scanners are designed so they will not damage PCs, including the data stored on their hard and floppy disks.

64. Should you travel by car, never leave the PC unattended in full view, for example, on the back seat and, wherever possible, take it with you when leaving the car.

65. Although it is unlikely that your PC will be stolen from your hotel room, it is possible that hotel staff may start the computer to see what programs and data it contains. There have been known cases of industrial espionage involving PCs left in hotel rooms, although it is more likely that data could be damaged or destroyed through unauthorized use. The best protection is to keep the PC with you whenever possible and secure it when it has to be left somewhere.

66. Be sure also to secure floppy disks when you are traveling. A disk can be copied in a matter of minutes and, unless the data has been encrypted, the information can then be easily read by whoever has copied the file.

Communications Equipment

67. Communications equipment for local and wide area networks requires as much physical protection as the main computer equipment itself. It is important to keep such equipment in a secure area, inaccessible to staff not needing access to it as part of their duties.

68. Because communications equipment is so important, you should think about housing it within the main computer room or establishing a separate communications room subject to the same physical and environmental controls as the main computer room.

Biometrics

69. Biometric recognition systems are fast becoming a standard solution for physical access controls. Biometric systems verify an individual's identity based on unique physical or behavioral characteristics rather than on the use of a password or keycode. The idea behind biometric systems is that you always display or exhibit the characteristic that the system uses to verify your identity rather than having you remember a particular access code.

70. Although the most widely available biometric identification systems are based on fingerprint recognition, hand recognition, retina scanning and iris scanning systems are also available. In addition, voice and signature recognition systems utilize behavioral characteristics to verify an individual's identity.

71. Because fingerprint recognition systems can now be purchased at a reasonable price, you might want to consider their use for protecting high security applications, either through physical door access systems or application access systems.

Backups and Data Storage

72. The existence and availability of backup data is a fundamental prerequisite to recovery from disaster situations. To ensure that backups are available when required, you need to implement adequate physical restrictions over access to such backups.

73. Keep all your backup copies of data and programs in a physically secure location to which only computer operators and management have access. This backup storage location should be physically separate from the computer equipment the backup is protecting.

Documentation

74. Always store documentation about your physical computing environment in a safe location. The loss of, or damage to, such documentation, coupled with the loss of, or damage to, the equipment it relates to, can seriously impair your ability to recreate that physical environment within a reasonable time scale. To reduce the risk of one physical event affecting both the documentation and equipment it relates to, keep copies of documentation in more than one location.

75. System documentation includes but is not restricted to:

    - The hardware register;
    - Hardware maintenance agreements;
    - The software register;
    - Software license agreements;
    - Software maintenance agreements;
    - Network diagrams;
    - Detailed technical configuration documents;
    - Insurance policies; and
    - A disaster recovery plan.

Part C: Environmental Protection

Computer Room

76. As the computer room normally houses your most important computing equipment, you should take adequate precautions to reduce the risk of environmental factors having an adverse impact on the operation of that equipment.

77. Your first consideration should always be the sitting of a computer room. Is it well away from inherent physical hazards such as fuel tanks, water tanks, pipes, etc.?

78. Specific environmental threats include fire, flood, storm damage, earthquakes, etc., and the provision of an exhaustive list of potential countermeasures to all such threats is outside the scope of this document. The factors pertaining to fire and flood are relevant to most small and medium enterprises, however, and are discussed here.

79. Fire and smoke detectors should be installed in the computer room and in any other location where significant computing equipment (such as local servers, communications links or data stores) is located.

80. Fire extinguishers should be readily accessible in all computer environments. In larger computer environments, or where a building is likely to be unoccupied overnight or on weekends, consider installing an automatic fire detection and suppression system in the computer room. The use of such a system minimizes the risk of fire damage at times when the building is unoccupied. Check your fire extinguishers and automated fire suppression equipment regularly to ensure that they still operate correctly.

81. Do not purchase fire suppression equipment that uses halon gas because halon is a CFC gas and, therefore, dangerous. The current alternatives are:

82. CO_2 — CO_2 works by removing all the oxygen in a room, thereby extinguishing the fire. The danger with this approach is that it can harm staff in the computer room when a fire breaks out. They must be able to get out very quickly when the automatic suppression system goes off. Failure to do so is life threatening.

83. Inergen — Inergen is a combination of gases that work by lowering the percentage of oxygen in the air to a level that will not support combustion but will still support life. Inergen is, therefore, safer than CO_2 but is more costly, as it is a proprietary product and requires a large storage area since the gas cannot be compressed. Other similar gases are available that remove oxygen from the atmosphere but are not life threatening.

84. Water — Water suppression systems work by dispersing a fine mist of water droplets to quench the fire. They must be linked to the power supply so that the power to the computer room is cut before the water suppression starts. Although

these systems will not damage computer equipment, the water must be removed before processing can restart.

85. To reduce the risk of physical events, such as fire, damaging your computer equipment, you should implement a no-smoking policy for rooms housing computer and communications equipment. In addition, to reduce the risk of damage by spillage, do not allow food or drink in those rooms.

86. False floors can provide protection from flooding but can also hide pools of water and vermin damage. Carry out regular inspections to ensure that any false floors are not hiding a potential problem. A sensible approach to the location of the computer room and other equipment should significantly reduce such risks.

87. All important computing equipment should have their own dedicated power supply to eradicate problems of power surges caused by other machinery. A UPS system should protect critical systems.

88. Air conditioning may be necessary for the effective running of larger or older computing equipment. But do not allow the need for air conditioning to compromise your physical access controls. Do not open external doors and windows to allow air flow if this would increase the risk of unauthorized public access to the computing equipment.

89. Should you be planning any kind of local construction work, be aware of the impact such work might have on your computer equipment. Because dust and vibration can cause serious problems for your equipment, take appropriate precautions such as temporarily relocating the computers, installing dust filtration equipment or limiting the times the construction work is performed.

Distributed Computer Equipment

90. Normally, you would implement the same types of environmental controls for your distributed computer equipment as those applied to the environment it is located in. PCs do not require specific air conditioning or power supplies and, therefore, the majority of them do not receive any special treatment.

91. As UPS systems are available for PC equipment at a cost of a few hundred dollars, you might consider purchasing them for your important distributed PCs.

92. The same situation is true of precautions against fire or flood. A conventional office sprinkler system could severely damage a PC, either through direct water damage or the effect of a combination of water and electricity. The difficulty of protecting your equipment in such situations serves to emphasize the need for proper backup procedures so that data can be recreated should such an event occur.

93. Although specialist firms have the technology and facilities to retrieve data from damaged PCs, their services are expensive and do not guarantee success.

Communications Equipment

94. As mentioned in the section on physical controls, your communications equipment is worthy of the same level of environmental protection as your main computer equipment enjoys. For this reason, you might want to consider locating your communications equipment within your main computer room.

Backups and Data Storage

95. As magnetic media is extremely flammable, the storage for backup media should be fire resistant, for example, a fireproof safe. If the volume of such media requires a dedicated data storage room, that room should have the same protection as your computer room. That is, install fire detection and suppression equipment and take appropriate measures to reduce the risk of flooding.

Documentation

96. Documentation, by its very nature, is extremely vulnerable to physical events such as fire or flood. The best precaution to prevent the destruction of such documentation is to have multiple copies, perhaps in both electronic and paper form, distributed throughout your business.

Part D: Necessary Administrative Procedures and Controls

97. To improve the physical control over your computing equipment, you need to ensure that certain administrative functions are carried out.

Hardware Inventory Register

98. The first is to establish and maintain a register that records the details of all your computing equipment. You can use this register to:

- Verify the continued existence of each piece of equipment;
- Ensure equipment is adequately insured;
- Better manage hardware maintenance programs;
- Allow management to assess the extent and type of equipment the business owns; and
- Plan a hardware replacement program.

99. The hardware inventory should include a full description of each asset, including manufacturer, model, serial number, data capacity, processing capacity, cost and location.

100. Ensure that the inventory is updated regularly, which will require the development of procedures for making additions to, and disposals from, the register. The accuracy of the register should be regularly checked by an asset count.

101. Example inventory forms for hardware and software registers are included as appendices to this document.

102. If your business uses a lot of PCs, or the allocation of your PCs changes frequently, it will not be practical to maintain annual records. As an alternative, you might want to store the necessary information in a spreadsheet, database or dedicated fixed asset/hardware inventory software package. The responsibility for maintaining accurate records should ideally be allocated to one nominated individual within your business.

Insurance Coverage

103. Insurance coverage is essential to any business, not just to provide the funds for the replacement of hardware and software in the event of a disaster, but also to compensate for the consequences that the loss of computer equipment has on operations.

104. Insurance should provide for the prompt replacement of damaged computer equipment and, if necessary, the hire of equipment in the interim period. When you negotiate your insurance policies, ensure that the level of coverage includes all the PC equipment, peripherals and communications equipment purchased over time. Although each individual purchase might not have been material, the total value of all such equipment is likely to be significant. The coverage should also provide for the costs of third-party assistance in re-establishing the computing environment.

105. A complication of "new for old" policies applying to computer equipment is that an equivalent to old computer equipment may no longer be available. Ensure that your policy will pay out for any inherent upgrade of hardware and software that may be required.

106. Although consequential loss policies compensate for some of the losses incurred by a business interruption, some consequences are normally not covered:

- The failure to recover debts due to the destruction of accounting records;
- Fines, damages or penalties incurred as a result of not being able to meet contractual or legal obligations; and
- Loss of goodwill.

GOOD PRACTICE CHECKLIST

	Yes	No	N/A	Reference
A. WHAT TO SECURE				
Physical equipment				
Do you know how many computers your business has? Consider not just mainframes or minicomputers but also PCs and portable equipment.				
Do you know where the computers are located?				
Do you know what the computers are used for?				
Consider: key business activities, e.g., design, personnel financial planning, etc. sensitivity of systems confidentiality				
Do you know what peripheral equipment your business has?				
Consider: printers scanners plotters CD-ROM drives tape drives or streamers others				
Do you know where the peripheral equipment is located?				
Do you know what communications equipment is used in your business?				
Consider: LAN equipment WAN equipment EDI links BACS links reference databases others				
Do you know where the communications equipment is located?				
Data storage				
Do you know where backup media is stored?				
Do you know where master copies of files are kept?				
Do you know where working data disks/or tapes are held?				
Documentation of the physical environment				
Do you have a comprehensive hardware inventory?				
Do you have a comprehensive software inventory?				
Do you know where system documentation is stored?				
Do you know where source code listings are stored?				

	Yes	No	N/A	Reference
Do you know where software licenses are held?				
Do you know where guarantees and service level agreements for software and hardware are held?				
Do you know where the disaster recovery plan is stored?				
B. PHYSICAL SECURITY MEASURES				
Computer room				
Are the main business computers located in a dedicated computer room?				
Is access to the computer room restricted to people who operate the computers?				
Is the computer room dedicated to computing?				
Consider: photocopiers, storage of cleaning equipment, non-computing staff, non-computing machinery				
Is entry to the computer room controlled by lockable doors?				
Are computer room doors locked as standard?				
Are report printers for confidential output located in the computer room?				
Can the computer room be accessed by use of force?				
Is the computer room out of public view?				
Are visitors to the computer room supervised at all times?				
Computer equipment outside a computer room				
Are computers located in areas where the public or customers cannot gain access to them?				
Are computers used for confidential purposes kept in the areas to which they relate?				
Are power-up passwords used on all PCs?				
Is all computer equipment visibly marked with an asset number and a company name?				
Are all desktop PCs attached to the desk?				
Is portable equipment securely stored at night?				
External communication				
Are telephone numbers for dial-in modems hidden from view?				
Are security devices (such as BACS safe devices) held securely, with access restricted to a small number of people?				

Documentation				
Is system documentation stored in a way that prevents: unauthorized access? unauthorized removal? unauthorized alteration?				
Are source code listings stored in a way that prevents: unauthorized access? unauthorized removal? unauthorized alteration?				
Are all software licenses accessible when required?				
Are all software licenses filed in an organized, controlled manner?				
Are all guarantees and service level agreements filed in an organized, controlled manner?				
Is the disaster recovery plan stored in a place that prevents: unauthorized access? unauthorized removal? unauthorized alteration?				
C. ENVIRONMENTAL PROTECTION				
Computer room				
Is the computer room sensibly located away from environmental hazards?				
Consider the location of fuel tanks, loading bays, other physical risks.				
Fire				
Have fire and/or smoke detectors been installed in the computer room?				
Are suitable fire extinguishers located in the computer room?				
If the building is unattended at any time, has an automatic fire detection and extinguishing system been installed in the computer room?				
Have fire and/or smoke detectors been installed near your other computing equipment? Consider: sensitive PCs peripherals disk/tape storage areas communications equipment				
Are combustible materials stored away from computing equipment? Consider: waste paper chemicals stationery cleaning fluids				

Are combustible materials excluded from the computer room?				
Flood				
Have you ensured that there are no water pipes near or in the computer room?				
Is the computer room fitted with a false floor to minimize the risk of water coming into contact with computer equipment?				
Is all other computing equipment kept away from any water sources? Consider: adjacent kitchens adjacent toilets overhanging water pipes				
Power supply				
Is computing equipment on a separate "clean" power circuit?				
Has a UPS system been installed?				
Air conditioning				
Is air temperature controlled to prevent computers from overheating?				
Is ventilation around computers sufficient?				
Is the environment around computers controlled to keep it clean and dust-free?				
D. ADMINISTRATION				
Insurance				
Is insurance coverage adequate to cover the replacement cost of all computer equipment damaged, lost or destroyed? Consider: total value of coverage mainframe computer mini-computer desktop PCs portable PCs coverage for any required upgrades printers storage media modems backup tapes training resources				
Does your insurance policy adequately cover replacement costs as opposed to purchase costs?				
Does your insurance policy cover all of the types of risk your computing equipment is exposed to?				
Is insurance coverage adequate to cover all direct and consequential (indirect) costs incurred?				
Are insurance policies filed in such a way as to make them easy to find when required?				

APPENDIX I:
HARDWARE INVENTORY

Asset Reference	Manufacturer	Model	Specification (RAM, Disk, Speed)	Serial Number	Date of Purchase	Supplier	Initial Cost	Physical Location	Network Address	Maintenance Details	Comments

APPENDIX II:
SOFTWARE INVENTORY

Package	Manufacturer	Serial Number	Date of Purchase	Supplier	Cost	Which PC is the software on?	Comments