International
Federation of
Accountants

Small and Medium
Practices
Task Force

December 2003

Controlling Computers in Business: Logical Access Security

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

PRICEWATERHOUSECOOPERS

IFAC

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

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

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

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

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

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

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

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

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

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

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

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

ISBN: 1-931949-14x

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.

It is obviously important to prevent inappropriate access to programs and data. This guidance document examines the threats posed by inadequate logical access controls and suggests ways in which 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 third in a series of guidance notes on computing controls for Small and Medium Practitioners/Enterprises (SMPs/SMEs) that the International Federation of Accountants has produced in association with PricewaterhouseCoopers.

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

3. The readers of these notes will undoubtedly have a wide variety of needs, stemming from two factors. Their level of awareness of the issues discussed will affect how much or how little of each note they will have to use, as will 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.

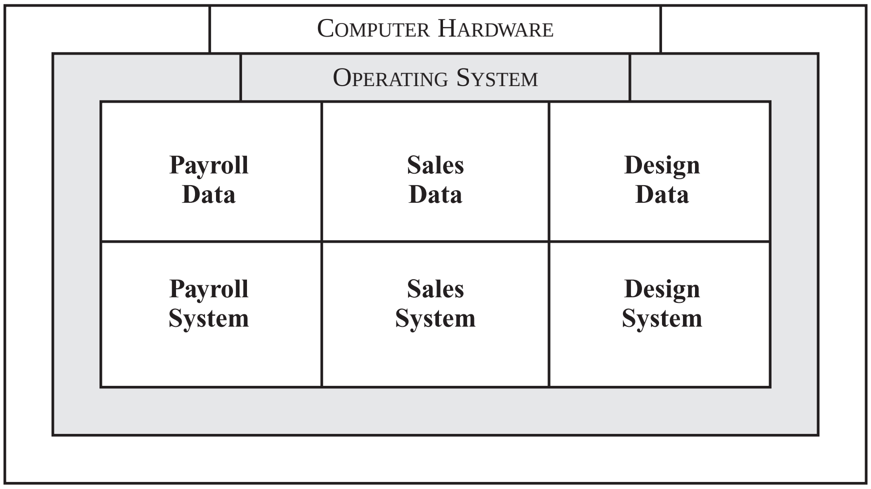
7. If you have more time, or the checklist results suggest that you need to perform a more detailed review of the issue, consider the other sections on costs and benefits, risks and practical considerations.

Background

What do we mean by “logical access security”?

8. At the outset of this guidance note, we should define what the term “logical access security” actually means. Simply put, it is the framework of controls that ultimately stops anyone from accessing your programs and data in a way that you believe is inappropriate. Logical access security is, therefore, concerned as much with preventing someone outside your company from gaining access to your systems as it is with preventing your purchase clerk from accessing your payroll system.

9. You will not be able to achieve total security for your programs and data if the physical security around your computer systems is inadequate and there is a low level of security awareness within your business. The following graph, which will be used throughout this guidance note to illustrate various logical access security scenarios, shows the relationship between different parts of your computer system:



10. Each computer system has hardware, an operating system, application systems and the data processed by those applications systems. Here is an explanation of each element:

Hardware The physical elements of a computer system, such as the processing unit, keyboard and monitor.

Operating system The collection of programs that allows users and application programs to interact with computer hardware; for example, Windows is an operating system.

Application system The programs that perform specific business functions, such as process payroll or produce sales invoices. Each application will be composed of a number of individual programs but they are not generally visible to those using the application.

Data

The individual units of information application programs use in their operations. This can include permanent payroll data, such as annual gross salary, as well as transitory information, such as the tax deduction for employee 100 for October.

11. To achieve and maintain sound security around your programs and data, you must have:
    - sound physical access security to protect the physical computer hardware;
    - security protection through layered defenses;
    - continual education and awareness of security on the part of your staff;
    - appropriate classification of data according to sensitivity and importance;
    - good security within your operating system to restrict access to sensitive operating system facilities;
    - good security administration of the systems, from monitoring security events to maintaining a secure environment through to well-managed configuration controls;
    - proper segregation of duties for each individual computer application.

12. Although it is never possible to achieve 100% computer security in any environment, it is possible to reduce the risks to a realistic level.

What are we trying to protect?

13. Ultimately, computer security is concerned with protecting two things:
    1) the data you use to operate your business; and
    2) the programs and business processes that perform operations with that data.

14. Although your physical computer equipment is valuable, the data and programs stored on it would almost always be worth more to you in economic terms than the equipment itself.

15. Computer systems today, even in the smallest organization, are becoming increasingly complex. The advent of Local Area Networks (LANs), Wide Area Networks (WANs), dial-up connections, Intranets, Extranets, the Internet and Electronic Data Interchange (EDI) all increase the difficulty of introducing proper computer security, and each new technology has its own specific security concerns. Detailed treatment of each of these areas is outside the scope of this guidance note; rather, we have concentrated on the fundamental principles associated with computer security so that you will be able to identify potential risks and seek expert guidance wherever it may be needed.

How can we achieve protection?

16. As we alluded to earlier, the logical access controls of a computer system have four objectives:

    - to allow access to authorized users;
    - to deny access to unauthorized users;
    - to restrict the access of authorized users; and
    - to monitor the activities of authorized users.

17. For the purpose of this guide, we have defined four mechanisms you can use to achieve logical access security. A good logical access framework will normally involve aspects of all four of these mechanisms, and the extent to which you will need to use them depends on the characteristics of your underlying computer systems. The four mechanisms are:

    - Hardware Security

      This is the control that prevents someone from gaining access to a system and is the security implemented by hardware rather than software. An example of such a control would be a power-on password.

    - Operating System Security

      This governs what access a user has to the data and programs once a PC or terminal has been activated. An element of this security could be a User ID and password that the user would have to enter before being presented with a menu screen.

    - Application Security

      This governs what a user can do within each application. An example of this security would be a User ID for a general ledger that lets the user view, but not edit, the data in the general ledger.

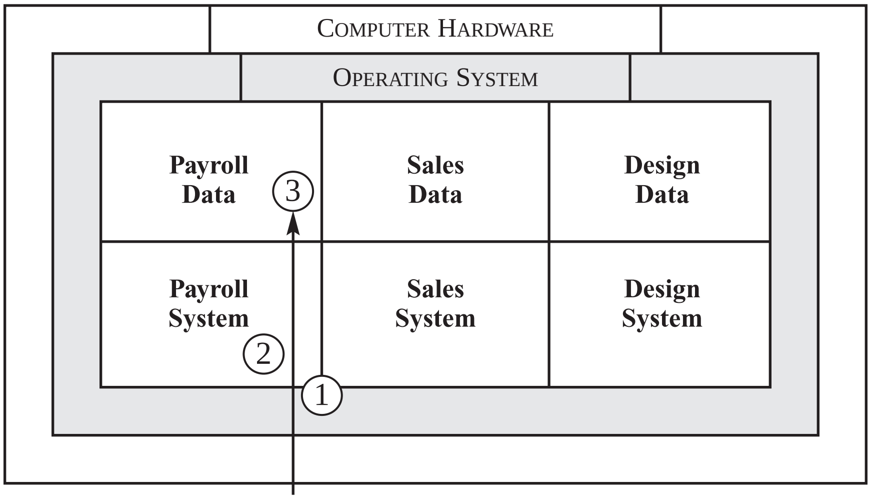
    - Network Security

      This is the control that prevents penetration into a business network. An example of this security could be implementing appropriate interfaces between an organization's network and networks owned by other organizations or public networks.

18. User IDs, passwords, PIN numbers, digital certificates, hardware tokens (see definition on page 7) and biometrics (fingerprint or retinal scans) form a fundamental — but not the only — part of logical access controls. They do not, in themselves, provide complete protection from security risks. Depending on other circumstances, User ID and password controls may be defeated or evaded, and physical security around computer systems (dealt with in the previous guideline in this series) is an important precursor to adequate all-round computer security.

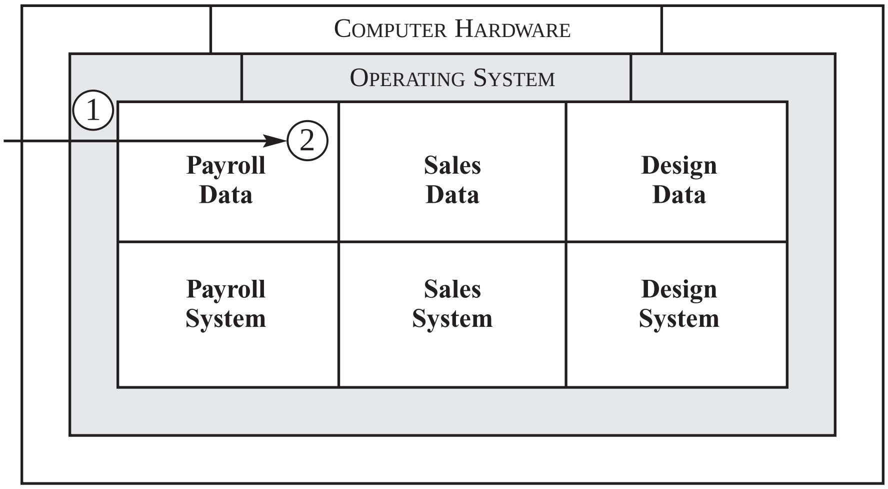
19. The interaction between the layers of security is also extremely important as weaknesses in one security layer can undermine the controls in another. For example, it is possible for weak operating system access controls to allow someone to have direct access to the files used by an application even if the application itself is password-protected. Similarly, weak controls within an application can lead to users gaining high-level access to the operating system.

20. To illustrate the interaction between operating system and application system security, the following diagram shows the access route a user follows to get into a typical payroll application.



21. The user turns on his or her PC or terminal and is prompted by the operating system to enter a User ID and password; this occurs at point 1. The start-up routine for the system may then present the user with a menu or selection of icons from which to choose the applications that user is permitted to access. The user selects the payroll application from this menu, which then asks the user to enter another User ID and password — point 2. From within this application, the user has been defined as a payroll clerk and can update the payroll data in accordance with those access rights — point 3.

22. The above diagram illustrates how different aspects of logical access security operate together to provide overall security for the payroll functions and data. The next diagram illustrates the situation where operating system security has not been properly configured and a user can gain access to payroll data without having access to the payroll application itself.



23. The user, John Jones, accesses the computer in the same way as noted above — providing his User ID and password to the operating system at point 1. This user is not permitted to access the payroll application since he is a purchase ledger clerk. The operating system security was, however, not properly set up and, therefore, the payroll data is not properly

protected. Using standard facilities available within the operating system, such as file viewers and editors, the purchase ledger clerk finds the payroll data files, can view details of other employees' salaries and can even change his gross salary figure — point 2. Since John Jones did not use the payroll application to change his salary, no audit trail was produced and the change may go undetected for a considerable period of time.

24. Such security weaknesses are not uncommon and can often be exploited with minimal knowledge.

25. The threats to the electronic information stored within your computer systems fall into four categories:

- disclosure — information becomes known outside its proper audience;
- alteration — data is changed in an unauthorized fashion;
- destruction — data is destroyed before it has reached the end of its life;
- inaccessibility — access to data is removed when such access is still required.

26. In the example given above, information was both improperly disclosed — the discovery of salary information — and altered — the changing of gross salary details.

27. The risks you are vulnerable to if your computer security is inadequate are obvious: theft, disclosure of information and public embarrassment, to name but a few.

Key Terms

28. Application

An application is a computer program (or suite of programs) that automates a range of business functions. Examples of applications include payroll, sales ledger and general ledger systems. An application can also represent business automation software, such as spreadsheet and word processing packages.

29. Extranet

Extranets are external Intranets. By setting up an Extranet, companies can allow trusted customers or partners to connect via the Web to view certain private Intranet information stored behind the firewall while, at the same time, restricting access to sensitive information.

30. Firewall

A computer situated between a company's internal network and the Internet whose purpose is to prevent unauthorized communications traffic entering the internal network.

31. Hardware security

A hardware mechanism that restricts access to a computer system's programs and data. An example would be a PC power-on password.

32. Hardware token

A device used to provide a means of authenticating a system's users. Hardware tokens can take various forms but generally either physically connect to the computer being authenticated or generate random numbers that only the computer being accessed can verify.

32. IDS An Intrusion Detection System (IDS) is an automated tool or set of tools designed to detect security violations by analyzing the data source and responding with appropriate actions.

33. Internet The Internet is a public network — anyone with an Internet connection can share and view information over the Internet.

34. Intranet An Intranet is a private network that is limited to a certain group of people.

For example, companies set up Intranets for employees to access while they are at work. Intranets reside inside a "firewall," which blocks access by anyone outside the company.

35. 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 individual PCs to communicate with each other through the use of electronic mail packages.

36. Logical access Logical access control restricts access to the intangible, logical elements control of computer systems, including computer programs, operating systems, data, electronic communications and networks. A simple example of a logical access control is the use of user names and passwords to prevent access to computer programs.

37. Modem A MOdulator/DEModulator (modem) is a hardware device that allows computers to communicate with each other across analogue telephone lines. A modem translates the digital signal from a computer to an analogue signal for transmission over telephone wires, and vice versa.

38. Operating system A computer’s operating system is the resident software that enables application programs and/or users to interact with the computer hardware itself. One of the most common operating systems is Windows. Other operating systems that you may encounter include Windows NT, Windows 2000, Windows XP, AIX, and Linux. Most operating systems are hardware specific and are provided by the vendor of the hardware.

39. Physical access Physical access controls restrict access to the tangible, physical controls elements of computer systems, including computers, printers, backup media, communications devices and documentation. A simple example of a physical access control is the use of locks to prevent access to computing equipment.

40. Resources Within a computer environment, a resource can be a file containing data, a file containing program instructions, a printer or any other physical or logical device that the computer is a capable of identifying.

41. Resource security Resource security is the term given to the access restrictions the operating system puts in place around resources. Preventing certain users from printing with a color printer would be an example of resource security. Original versions of the Windows operating system did not provide the facility to secure individual files and directories but later versions include this facility. In addition, the security management tools in these later versions are more powerful and easier to use.

42. Smart cards A plastic card with a microprocessor sealed inside it. Special card readers can communicate with the microprocessor on the card, allowing data to be securely stored and accessed. A smart card can be used to ensure that a user is authorized to perform particular actions by the use of various security checks.

43. WAN Wide Area Network (WAN) is the term used for the 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

44. 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 where expenditures tend to be smaller and control structures are less rigid, it may be an informal procedure.

45. The approach to creating logical access controls requires a careful balancing of the costs and benefits involved. You need to design a logical access security structure that balances the need to permit your users some level of access to your system against the ability to restrict access to everything. The security structure balances financial costs and benefits with practical administration concerns.

General benefits

46. The overall benefits of operating sound logical access controls are the prevention of potential threats that might cause losses, the minimization of loss if a security breach does occur and peace of mind derived from knowing that all practical steps have been taken to reduce the risks facing the business.

Cost of inadequate logical access controls

47. If your logical access security is breached because controls either failed or did not exist in the first place, you will incur various costs, either direct or consequential:

Direct costs:

- cost of lost business;
- cost of penalties imposed;
- labor time to re-enter data (including overtime premium).

Consequential costs:

- industrial action if you cannot process your payroll;
- lost production due to lack of systems data;
- loss of goodwill (customers, suppliers, bank, staff);
- closure of a business unit due to lost production/sales/goodwill.

Cost of implementing logical access controls

48. The main types of costs of implementing logical access controls include:
    - purchase of access control software;
    - staff training;
    - resource and staff time to implement controls;
    - administration, i.e., issuing and controlling smart cards;
    - maintaining a secure environment;
    - additional equipment, i.e., smart token readers.

49. Many systems come with some access controls built in, but you may find it necessary to supplement them with additional controls.

50. Staff training covers two areas — training the system administrator in the use of the system's control functions and making all users aware of security issues.

Risk Indicators

51. You need to consider a number of factors when developing a logical access security policy. These factors have a bearing on:
    - the risk of unauthorized access;
    - the risk of theft, loss, corruption and disclosure of business information;

- damage to business reputation;
- the extent of business disruption.

Factors

52. The following factors indicate that your business is at increased risk in the area of logical access security:
    - security issues lack senior management support;
    - business has a number of different computers;
    - business has several different operating systems;
    - a number of different applications are being used;
    - the existence of local or wide area networks;
    - easy public access to premises, PCs or central computers;
    - low awareness or appreciation of computer security issues;
    - lack of clearly defined security administrator responsibilities;
    - small staff, leading to inadequate segregation of duties;
    - high staff turnover;
    - systems contain highly sensitive or confidential data;
    - communication links with third parties;
    - lack of an IT security officer.

Practical Considerations

53. The Good Practice Checklist shows the questions you should be asking about logical access security for your computing resources. This section provides information and practical guidance on each of those areas in turn.

Physical security

54. As mentioned in the background section of this guidance note, computer environments tend to have two main types of access security: physical access security, which governs the tangible, physical elements of your computer system; and logical access security, which governs the use of intangible, logical elements of computer systems.

55. Adequate physical access controls are an essential prerequisite for sound overall security. The absence of physical controls will undermine even excellent logical access controls. For example, if you restart some computer systems, they give you an option that allows you to take full control of that computer — bypassing all logical access security controls you might have implemented. If you do not restrict access to your physical hardware, you can never enforce adequate security.

56. Volume 2 of this guidance series covers physical access security. Be sure to refer to that volume for guidance on how to establish effective physical access security procedures.

Expert guidance

57. This series of notes aims to give guidance on a number of computer-related issues and on how to implement best practice in a small or medium sized business.

58. The issue of logical access is more complex than many of the others discussed in the series. Therefore, the guidance cannot provide comprehensive details of every combination of hardware, operating system and application that might exist within your company.

Information Security Policy and Procedures

59. To be effective, most business activities and controls have to be planned and managed. This is certainly true of the use of computers and computerized systems, but is no less true of the logical access security for those computers and systems. Good logical access security does not just happen, it has to be planned and managed, just like any other aspect of business. A security policy requires the support of senior management, as that is the group that will be held liable if security issues are neglected.

60. To implement effective logical access security, you must have a clear idea of what you are trying to achieve. This will involve specifying general objectives and requirements for how your systems should be set up, the form of control to be used in various areas and who can access your systems.

61. Although an adequate logical access security framework is generally built on a foundation of automated access controls built into the computer system itself, manual intervention is also required to administer security and investigate exceptions.

Information security policy

62. You should document your logical access security aims in your information security policy. This has the advantage of:

    - allowing you to monitor actual security against planned objectives;
    - enforcing a consistency of approach across all systems within the organization;
    - improving user awareness.

Information security procedures

64. Once you have put together an information security policy that establishes your overall objectives for security, you can then develop the information security procedures required to support that policy.

65. These procedures will give guidance and instructions to those responsible for information security tasks, specifying what has to be done to achieve and maintain security. This will include detailed instructions specific to the system or application involved.

66. For example, one overall security objective might be to change user passwords at least every 90 days, and that the passwords cannot be changed to any of the last five used. The procedures would contain the necessary information to allow administrators to enforce the policies for the particular operating system they are responsible for.

67. If your business uses mobile computing equipment (e.g., palmtops, laptops and mobile phones), you need to ensure that your business information cannot be compromised. One way is to implement a policy detailing requirements for physical protection, access controls, backups and protection. This policy should also include guidelines on connecting mobile facilities to networks and on the use of this equipment in public places.

68. Although it is often larger organizations that have formal security polices and procedures, smaller to medium sized businesses should also consider what level of formality is appropriate for their security documentation. The policy and procedures could take the form of a few pages highlighting what your management considers to be the minimum standard for security within your business.

Identification of Systems

69. An important initial step in considering logical access security is to identify the computer systems within your business. The maxim that a chain is only as strong as its weakest link is particularly pertinent in the area of logical access security.

70. Your business may have one application that has very strong controls to prevent unauthorized users from running the program or gaining access to the files it uses. There may be another application running on the same computer, however, that allows its users to break out of the constraints of the application and access all the files of any application on the computer. For example, the logical access security of a payroll application may be adequate to restrict access to payroll files, but the security of the general ledger system running on the same computer may be inadequate. Users could break out of the general ledger application and obtain access to facilities within the underlying operating system. Depending on the facilities they had access to within the operating system, they could potentially view and edit payroll files.

71. Therefore, when you are considering implementing access controls for your systems and applications, you must first identify all access points to the systems.

72. It is also important at this stage to ensure that you identify all the different types of computer systems your business uses. While accountants often focus on financial systems, your most important system might be the computer aided design system containing information on the company's latest products. Security must be established over all systems to protect the entire business — not just the financial data.

Hardware Access Controls

73. Hardware access controls help to ensure that only authorized individuals are able to access the programs and data stored within your hardware. Hardware access security is distinct from physical access security in that the latter seeks to protect the physical, tangible assets and the former seeks to protect the intangible assets of data and programs.

74. Hardware access controls come in a variety of guises — ranging from simple power-on passwords to sophisticated smart card readers and, more recently, biometric devices. The use of the more sophisticated devices is outside the scope of this guidance, but you may find their use appropriate for particular systems, e.g., Electronic Funds Transfer (EFT) applications.

75. Power-on passwords discourage people from attempting to access a computer system by simply turning on the machine. Although such devices are generally not very sophisticated, and are certainly not foolproof, they are a good first line of defense against unauthorized access.

76. If your business uses power-on passwords, you need to ensure that any staff members leaving your company, for example, to work elsewhere, give the system administrator their power-on password before their departure.

77. Most PCs now come with two power-on passwords. One is an administrative password that lets the user change hardware settings while the other merely restricts access to the PC. It may be possible to use a standard administrative password for all your PCs while allowing individual users to set their own user password. Should anyone leave your company, the administrative password can still be used to access the PC. Obviously, you need to know who has access to this level of password and where it is stored.

78. Device locks are another type of access control and can take the form of key switches with a number of settings. The different key settings can disable input devices, such as keyboards, prevent certain operations from being carried out on highly privileged operating system facilities, or they can disable the device altogether. For example, check-printing machines often have a lock that prevents the machine from being used, even though it may be connected to an appropriate computer.

79. The use of hardware access controls, which are often standard accessories for computer systems, is often the simplest way to improve logical access security.

Operating System Security

80. A computer's operating system forms the bridge between the user and the hardware, and between individual applications and the hardware. One of today's most common operating systems is Windows, which provides PC users with graphical tools to perform a wide variety of tasks. These tasks include, but are not restricted to, listing files on the computer's hard drive, displaying the contents of files, editing the contents of files and controlling how different hardware devices operate.

81. A PC's application programs, such as spreadsheet and word processing packages, rely on facilities within Windows to provide them with access to the computer's hardware. If an application needs to open a file, the application sends an instruction to the operating system, which then retrieves the relevant file on the application's behalf. This interaction is invisible to the user.

82. More sophisticated operating systems provide additional facilities, such as the ability to communicate among computers, to share information between a number of users, to distribute processing tasks among a number of separate computers and to enforce security over programs and data.

83. You should consider automatic terminal identification to authenticate your computer's connections to specific locations or to portable equipment. This technique is useful if it is important that a session can be initiated from only a particular location or computer terminal.

84. In addition, inactive terminals in high-risk locations, i.e., areas outside the scope of your security management, should automatically shut down after a defined period of inactivity to prevent access by an unauthorized person.

85. The extent to which adequate logical access security can be established depends largely on the capabilities of the operating system running on the computer where the data is stored. For some transitory data created by your word processing package, such as normal correspondence, security might not be an issue but it might be paramount for other data created by the same package, such as a customer mailing list. The extent to which logical access security needs to be implemented is, therefore, driven by the business value of the underlying data.

86. A standard minicomputer or local area network operating system should provide the following logical access security features:

Feature	Purpose
User IDs	To identify uniquely each user to the system
Passwords	To confirm the user's identity
User Groups	To group together users with similar responsibilities, thereby reducing the administrative burden

Feature	Purpose
Audit trails	To record various user activities on the system and provide a means to investigate security breaches should they occur
Resource security	To restrict access to data files and other resources to only those staff who have a need to access them
Log-in security	To limit the number of times that an incorrect combination of User ID and password can be entered before further attempts are prevented.

87. The absence of some of these features does not mean that it is impossible to establish adequate logical access security. It does make it more important, however, to have good physical access security in place and to implement other logical access security features.

88. It is often difficult to implement sound operating system security. Any security established is also easily circumvented. Whoever is given the task of implementing operating system security should be properly trained and have an adequate understanding of your business, so that this person can identify the critical business processes and data to be protected and then translate that knowledge into a workable security framework. It is not enough to have technical knowledge since the security efforts may be valid but their focus might be misplaced. Providing detailed security standards, guidelines and procedures to administrators can introduce a consistent approach to managing security.

89. Operating system security is not only concerned with preventing or restricting access to the computer, it is also concerned with regulating access once a user has logged onto the system. The mechanisms for regulating access generally fall into two different areas:

1) resource security; and

2) user privileges

90. You may want to permit one user to update a file in your computer system but let another user only read the contents of that file. An operating system that supports resource security would allow you to set flags on the file that define which User IDs could read the file and which could update it. The extent to which these resource security facilities need to be used depends on which users have access to the operating system and what capabilities they have when they have gained access.

91. Generally, when defining resource security parameters within an operating system, you have to define which user, or group of users, should access the resource and the mode of access they should have. The use of data classification to define how the data should be protected, who can access the data and what can be performed with the data is required to define the type of access. The typical types of access and how they relate to files on the system are categorized as follows:

Access Type	Capabilities
Read	Users can view the information
Write	Users can view and change the information
Execute	Users can run the file if it is a program
Delete	Users can delete the file

92. Sound resource security must consider the types of access that are appropriate for staff so that they carry out their normal business functions.

93. Most sophisticated operating systems support the concept of user privileges. These operate in a similar manner to resource security in that there are flags set on a User ID which define what that user can do at the operating system level. Certain privileges allow users to bypass resource security, others might allow them to back up and restore information, while still others might allow them to shut down the computer from a remote terminal. You should restrict such privileges to a few key members of your staff and monitor their use wherever possible.

94. Each operating system has a number of programs, known as utilities, which allow users to perform actions, for example, to edit a file. Because some of these utilities themselves bypass operating system security, it is important to identify such utilities and restrict access to them. As each sensitive utility is specific to a particular operating system, a complete list of such utilities is outside the scope of this guidance note.

95. Another potential danger to operating system security is the existence of freely available password cracking and security weakness detection programs. These programs can be downloaded from the Internet and used legitimately to identify weaknesses in the operating system security of several different operating system versions. Unfortunately, if an unauthorized individual gains access to such a program, he or she can use it to exploit any existing weaknesses in your operating system security. Be sure to prohibit staff form loading extraneous and unauthorized software onto any of your computers.

96. You ought to consider additional security controls for your business-critical systems and for systems with a high threat value. The definition of a business critical system will depend on the specifics of each business, but examples could include a computer-aided design system, a database of customers, a patient database or a manufacturing system. Controls such as intrusion detection systems, coupled with a good monitoring practice, can provide a high level of security. If managed correctly, these measures can be of good forensic value to help companies recover from security incidents and may even provide evidence for prosecution.

Segregation of duties

97. In any computer department, as in a finance department, a number of different roles have to be carried out. Typically, these roles fall into the following common categories:

Category	Typical Functions Performed
Developers and programmers	Develop new computer programs, enhance existing programs, resolve application program problems.
Operators	Take backups of programs and data, schedule batch jobs, monitor computer performance.
System administrators	Administer operating system security.
System programmers	Resolve operating system problems, introduce new versions of the operating system.

98. Most of these duties involve the use of sensitive operating system commands and utilities and it is important to properly segregate access to different parts of the computer system. For example, development staff should not normally have access to the area of the system that contains live programs and data. This is because they know how to change the programs and data. Operations staff, however, will require such access because they must perform backups of those programs and data.

99. A key role mentioned above is that of the system administrator. Effectively, this individual, or group of individuals, can access anything on the system and can alter any audit trail that might be created. Such powerful capabilities should be appropriately restricted to only a small number of trusted individuals and reviewed at regular intervals.

Application System Security

100. Generally, your business will have a number of applications that generate the data that, in turn, are used to manage the business. Examples of common applications include payroll, sales ledger and general ledger applications, but they also include office automation tools such as word processing and spreadsheet packages.

An application system should provide the following security features:

Feature	Purpose
User IDs	To identify uniquely each user to the application
Passwords	To confirm the user’s identity
User Groups	To group together users with similar responsibilities, thereby reducing the administrative burden

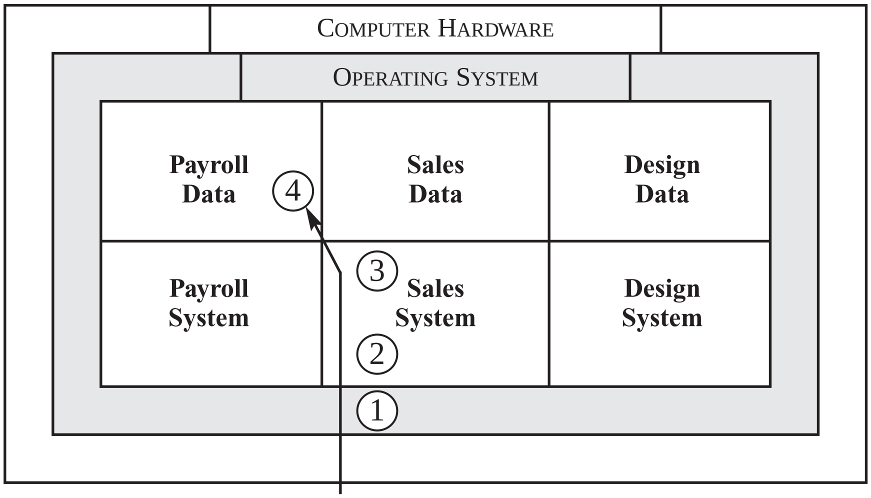
Audit trails — To record various user activities on the system and provide a means to investigate security breaches should they occur.

101. When a user has logged onto a computer's operating system, he or she will often be presented with a choice of applications to access. This choice may be presented through either a menu structure or icons on the screen. When a user selects an application, that application should provide security features to restrict what the user can do with it.

102. For example, after a user has logged onto a local area network, that user may want to run the payroll application. The user double clicks on the payroll icon and the payroll application starts. The first level of security is the requirement to enter a valid User ID. The user enters the ID for that application and is then asked to enter a password to prove that he, or she, is in fact the owner of that ID.

103. Rather than typing in a second User ID, some applications may be sophisticated enough to pick up the User ID from the operating system, thereby reducing the risk of error and improving security by directly linking the operating system with application system security.

104. Some applications have security loopholes or "back doors" that permit application users to exit temporarily from an application and issue an operating system command. The following diagram illustrates how such back doors work.



105. The user logs into the operating system and provides his/her User ID and password — point 1. The user, who is not permitted to access any payroll information or operating system facilities, then enters the sales ledger application, providing his/her user ID and password — point 2. The sales ledger application has an option entitled "Exit to operating system," which the user selects — point 3 — and is then able to use operating system facilities to view and edit payroll data files — point 4. If applications do provide this back door facility, they normally provide a way of turning it off.

106. To implement application system security properly, it is important that the application provides administration facilities, such as the ability to group a number of users together and administer them as one unit, and also to report on the security settings within the application.

Configuration Management

107. To maintain a secure environment, computer systems require a formal method for updating to new configurations of the latest software. System bugs are prevalent in any modern computing environment and can lead to an attacker compromising a system. Software suppliers provide regular patches to address these bugs. Patching these systems to remove system vulnerabilities should be a continual process along with system hardening (removing unnecessary network services, software, etc), testing new updates and maintaining documentation.

Network Security

108. Network security is becoming more and more dependent on preventative controls, i.e., physical and logical access controls and hindsight reporting on user activities. There are a number of factors you should consider in the deployment of an access control system.

Network planning

109. Key factors to consider when planning network services include:

1) Whether you require only internal services or whether you will need external services to communicate and exchange data with other organizations. Internal services are more secure in that all operations will be contained within your business. External services bring the threat of interception or alteration of data and the possibility of data loss over longer routes.

2) Whether privately managed services or dedicated links are adequate or whether you will need access to public domain services. Privately managed services offer less likelihood of unauthorized parties gaining access to your network. Public services, such as the Internet, require you to take protective measures to ensure unauthorized parties do not gain access to your network.

3) Whether you need to integrate new networks with existing networks. Networks that employ different protocols — the agreed on formal procedures for transmitting data between different devices — and mixtures of networking schemes are more complex to administer and maintain.

4) Determining the best manner in applying layered security to a network infrastructure not only to limit access to networks from external sources but also internally.

5) How the security administration of network devices and security appliances is to be managed. Networks require continual monitoring against attacks and you need to develop and test procedures to configure your systems in a secure manner.

110. A detailed network plan should be in place to take account of cost, volume and security of the network.

Network applications

111. Networked applications need capabilities that set them apart from other applications. A networked application may have to support a large number of users in real time. It is essential that the application can distinguish one user from another to ensure that transmissions do not get confused.

112. Most modern operating systems have been designed to provide ease of use functionally. This, unfortunately, can compromise security unless adequate countermeasures are developed. For example, all system should go through a level of "hardening" to remove unnecessary network services and applications. The degree of hardening will depend on how high the threat level is perceived to be. For example, a firewall to the Internet would require extensive hardening, as it will be under constant attack from Internet threats.

113. You should implement a logging mechanism to log events that have taken place, who has initiated them and when. The logs and security events will require continual monitoring to detect any threats or system compromises.

Network hardware

114. Additional hardware will be required for network services. Physical security for this hardware must be considered because uncontrolled access to network hardware can lead to risks such as:

- equipment may be damaged or stolen, resulting in a loss of service;
- bugs or taps could be installed, affecting the confidentiality of the data;
- transmissions could be intercepted.

Network access

115. You need to control access to both internal and external networks to ensure:

- appropriate interfaces are in place between your network and networks owned by other organizations or public networks. You will need to monitor those interface systems on a regular basis;
- appropriate authentication mechanisms are in place for users and equipment;
- user access to information services is controlled.

116. You need to develop a policy on the use of network services. This policy should cover the networks and network services allowed to be accessed, authorization procedures to determine who is allowed to access which networks and, finally, management controls and procedures to protect the access to network connections and network services.

117. External connections provide a potential for unauthorized access to business information, by dial-up methods, for example. Access by remote users should be subject to authentication, i.e., methods based on the use of cryptographic techniques, which are methods of protecting information by transferring it into an unreadable format. Hardware tokens are also common and provide good authentication.

118. Networks are being extended beyond traditional organizational boundaries. For example, if you enter a new business partnership, you may find it necessary to arrange for interconnection or sharing of information processing and networking facilities. Extensions in the network may increase the risk of unauthorized access to systems already on the network. You may, therefore, want to consider the introduction of controls within your networks to segregate groups of users and information services.

119. An alternative to providing and administering User IDs and passwords for each system, platform and network is to introduce identity management. An integrated identity management system identifies users, determines what they can do, determines the level of trust they should receive, protects your information and alerts you if that information has been compromised. To date, the cost of identity management systems has been high and, as a result, they have generally been implemented in large organizations.

Internet and Remote Access Security

120. With the proliferation of access to the Internet from within businesses, it important to properly protect your internal computer networks from external influences.

121. You should install a firewall to prevent unauthorized Internet users from accessing any of your private networks connected to the Internet. Firewalls provide a single point where it is possible to block unwanted traffic and logging traffic to and from the private network. This ensures security and allows you to audit the activity. It can also hide information such as system names, network topology, network device types and internal User IDs from the Internet.

122. You can purchase various types of firewalls offering varying degrees of security and cost. You should consider the level of threat your business faces and the consequences of security being breached. Then implement the appropriate level of firewall protection and configure firewalls as required. Where firewalls have been breached, it is not normally a failing in the firewall technology, rather, it is a consequence of poor configuration.

123. A firewall requires a secure network design, which may require other devices, such as proxies, which effectively hide the true network devices to provide greater security. Administration of the firewall infrastructure is also an important concern with event monitoring, incident escalation, etc.

124. Firewalls are often supplemented with intrusion detection systems that offer greater levels of security monitoring.

125. If you have a web site, the server hosting the site should be physically isolated from your other internal computer equipment. Alternatively, if your web site is hosted externally, ask your sever for appropriate assurance on the adequacy of the built-in security.

126. Increasingly, businesses require remote access to their information systems, with commercial telephone lines most commonly providing this access. Appropriate security should be in place to protect this connection. This may include controlling knowledge of the dial-in access number, setting up a dial-back facility and setting strong User IDs and passwords.

127. You might consider the use of Virtual Private Networks (VPNs) to allow a trusted network to communicate with another trusted network over the Internet. A secure point-to-point connection is established and communication between these points is encrypted. You might want to use a VPN for connecting remote offices or to allow remote users to gain secure access to your system.

128. Some companies are now offering a managed security service so that you can outsource many of your security management and monitoring needs to dedicated security professionals. For example, an external company can manage your firewalls, anti-virus protection, virtual private networks and intrusion detection systems. This would have the added benefit of having someone monitor and manage your systems on a 24x7 basis, which even some large multinational companies have not yet achieved.

Security Administration

129. Your should assign a system administrator to manage each operating system and application within your organization.

130. Depending on the size and nature of your business, the administration of all systems may be the responsibility of one person or of a number of people. Administrators might be dedicated to the task or they might perform their administration role along with some other staff role.

131. In all cases, the person or persons responsible for each system must be identified as such. If you don’t clearly identify who is managing your system security and operations, there is an increased risk of inadequate logical access security.

132. It is important that security administrators have sufficient knowledge and training to allow them to:

- understand the risks involved in operating the system;
- understand the facilities available in the system to manage those risks;
- carry out the necessary security tasks.

133. Security administration is best carried out as a regular routine. Such a routine will ensure that the regular administrative tasks, such as reviewing access logs, are not neglected as the administrator responds to more immediate ad-hoc tasks.

134. The types of tasks a security administrator should carry out on a regular basis include:

Task	Purpose
Daily	
Review the report of invalid access attempts	To identify and investigate any potential unauthorized access attempts
Create and remove user accounts	To maintain a secure environment that limits exposure
Weekly	
Scan user activity reports for any unusual activity	To identify suspicious user activity and thereby detect or prevent a security breach
Monthly	
Review the access history list for any IDs not used in the last three months	To identify and disable User IDs of staff who may have left the organization
Quarterly	
In tandem with user managers, review the list of User IDs within the operating system	To identify and disable the User IDs of staff who may have left your company and ensure that operating system access rights are still appropriate
In tandem with user managers, review the list of User IDs within significant application systems	To identify and disable the User IDs of staff who may have left your company and ensure that application access rights are still appropriate

135. You need to review the results of these monitoring activities regularly. The frequency of this review will depend on the associated risks, i.e., the importance of the application processes, the sensitivity of the information involved or the past experience of system misuse.

User Training and Awareness

136. Inadequate user training and awareness can undermine the effectiveness of the most comprehensive computer security framework. One of the commonest ways for professional hackers to gain access to a computer system is for them to call a user, pretend to be from his or her IT department or hardware supplier, and to ask for the User ID and password. Often, the unsophisticated user will provide the information and security is breached.

137. Other common user weaknesses include users shouting passwords across open plan offices, writing their passwords on sticky labels next to their computer screen or writing passwords in the back of desk diaries. Each of these weaknesses can only be addressed by the users themselves appreciating the need for proper computer security and taking their responsibilities seriously.

138. Larger organizations often include computer security as part of their induction procedures and make compliance with computer security procedures a condition of continued employment. While smaller businesses might not have the luxury of formal induction processes, they can address the issue by informal guidance or periodic communications with staff highlighting where current procedures are not adequate. As always, if senior management takes the issue seriously and leads by example, staff members are likely to comply.

Computer Viruses

139. A computer virus is a computer program that has two aims — to replicate itself and to cause damage. There are many different types of computer viruses and a number of different ways they can infect a computer, but such detail is beyond the scope of this guidance note.

140. The key points to remember with regard to viruses are that:

1) Viruses can be transmitted to computers through programs, data or communication links and even system vulnerabilities.
2) Every diskette or CD that comes into your company could contain a virus and should be checked on a dedicated, isolated PC before it is used.
3) New viruses are being developed all the time and you should install — and update — appropriate virus checking software on a regular basis.
4) All workstations and servers should be protected by anti-virus software.
5) You should develop procedures for dealing with virus attacks, such as getting alerts of new viruses, isolating infected systems, cleaning systems and recovering vital information, etc.
6) Make staff very aware of the risks of virus infection and tell them that disciplinary procedures will be taken against anyone introducing a virus into your company.

141. Most commercially available virus protection programs are able to detect the majority of known viruses and will often provide you with a dedicated program to disinfect any PCs that do become infected. As the destructive trigger for a virus is often a predetermined date, it is important that virus scanners are run automatically and regularly.

Other Issues

142. You may also consider using data encryption techniques to protect the confidentiality of your electronic mail messages. If you choose to do this, you should make it clear to your employees that you may access their electronic mail messages to ensure that they are for valid business purposes. Similarly, you want to know that, if an employee were to leave the company and his or her e-mail contained important business information, you were aware of this and were able to access it.

143. Now that your employees are accessing the Internet more and more, for various business and non-business reasons, it is important to protect your internal computer networks from external influences. If you have a web site, the server hosting the site should be physically isolated from your other internal computing equipment. If employees are permitted to access the Internet, perhaps through an Internet gateway, be sure to take suitable precautions, such as installing a firewall.

144. New technologies are continually exposing companies to security vulnerabilities. The emergence of technologies, such as wireless networks, the General Packet Radio Service (GPRS) and the Personal Digital Assistant (PDA), can offer you various benefits but they also pose security risks by making your systems more vulnerable to attacks and misuse.

Good Practice Checklist

	Yes	No	N/A	Reference
A. Information Security Policy and Procedures				
Have you considered how to best implement logical access security in your business?				
Has this been documented as a policy on information security?				
Do you have security procedures in place to ease the task of day-to-day security administration and to make sure that such administration is performed on a consistent basis?				
B. Identification of Systems				
Do you know what computer systems your business has? Consider: Financial Design Manufacturing Contract management Asset management Personnel Administration				
Do you know what access controls are used for the elements of each system? Consider: Physical access security Hardware access controls Operating system security Application security features Network security controls				
Do you know who is responsible for administering security for each of the systems at an: operating level application level?				
Do the system administrators fully understand the security risks facing the systems for which they are responsible?				
Do the system administrators fully understand the security features that they have available to counteract the identified risks?				

	Yes	No	N/A	Reference
C. HARDWARE ACCESS CONTROLS				
Are power-on passwords used for all computers that provide that facility?				
Are specialized hardware access controls used where greater risk demands greater protection, e.g., the use of BACS code generators?				
D. OPERATING SYSTEM SECURITY				
This section of the checklist must be completed for each hardware platform/operating system combination in use. Hardware platform: ____________________ Operating System: ____________________				
Security facilities				
Does the operating system support basic security features? Consider: User IDs password controls audit logs of user activity user groups controls to detect unauthorized access attempts resource security capabilities User IDs and User Groups				
Is each user allocated an individual User ID that only he/she uses to access the system?				
Have you assigned users with similar access requirements to user groups for ease of security administration?				
Are security administrators promptly informed of staff that leave or change positions?				
Do location and time of day restrict user access?				
Are normal users given only basic capabilities within the operating system?				
Can you identify all users with greater than normal capabilities and are their capabilities fully justified?				
Do you regularly review User IDs to identify users with excessive privileges or User IDs that are now redundant?				

	Yes	No	N/A	Reference
Have you renamed or disabled default User IDs delivered with the operating system?				
Password controls				
Do you force users to change their passwords frequently?				
Has the system been configured to encourage users to choose passwords that are difficult to guess?				
Do you maintain password histories to prevent users from reusing previous passwords?				
Are passwords hidden from view when entered with the keyboard?				
Do the procedures for setting up new users ensure that new users change their passwords as soon as they access the system?				
Are passwords stored securely and known only to the users themselves?				
Have you changed the passwords of default User IDs delivered with the operating system?				
Audit trails				
Have you established audit trails to track when users access the computer system?				
Have you established audit trails to record invalid attempts to access the computer system?				
Have you established audit trails to record other events that might compromise system security, e.g., access to certain files?				
Do you review audit trails regularly and take appropriate action?				
Control over unauthorized access attempts				
Are users locked out of the system after a number of failed attempts to log in?				

	Yes	No	N/A	Reference
Protection of files and other resources on the system				
Can resources be adequately secured? Consider: files directories printers peripherals operating system utilities				
Have you identified your sensitive system resources?				
Have you established appropriate resource security over your sensitive resources?				
E. APPLICATION SYSTEM SECURITY				
Each of these points should be considered for each significant application running on any of your computer systems. Hardware platform: ____________________ Operating system: ____________________ Application: ____________________				
Security facilities				
Does the application provide logical access security facilities? Consider: User IDs password controls audit logs of user activity user groups controls to detect unauthorized access attempts links to the operating system User IDs				
User access profiles				
Is each user allocated an individual User ID that only he/she uses to access the application?				
Has the application User ID been linked to the operating system User ID?				
Have you assigned users with similar access requirements to user groups for ease of security administration?				

	Yes	No	N/A	Reference
Are security administrators promptly informed of staff that leave or who change positions?				
Have all known “back doors” been documented?				
Have any “back doors” to the operating system been closed?				
Do you regularly review User IDs to identify users with excessive access or User IDs that are now redundant?				
Password controls				
Do you force users to change their passwords frequently?				
Are password histories maintained to prevent users from reusing previous passwords?				
Are passwords hidden from view when entered at the keyboard?				
Do the procedures for setting up new users ensure that new users change their passwords as soon as they access the system?				
Are passwords stored securely and known only to the users themselves?				
Audit trails				
Have you established audit trails to track when users access the application?				
Have you established audit trails to record invalid attempts to access the application?				
Have you established audit trials to record significant events within each application, e.g., when someone has made a change to the payroll rate file?				
Do you review audit trails regularly and take appropriate action?				

	Yes	No	N/A	Reference
F. Network Security				
Is a network plan in place?				
Is a logging mechanism in place to log events that take place by whom and when?				
Is physical security for network hardware adequate?				
Is a network policy in place?				
Are all connections with external connections adequately protected?				
G. Security Administration				
Have you assigned responsibility for the administration of the operating system security to someone with sufficient authority to demonstrate the importance management attaches to the issue? with the ability to perform the role? with adequate training? with adequate resources?				
Have you assigned responsibility for the security administration of each significant application to someone with sufficient authority to demonstrate the importance management attaches to the issue? with the ability to perform the role? with adequate training? with adequate resources?				
Have you assigned responsibility for monitoring operating system security to someone with sufficient authority to demonstrate the importance management attaches to the issue? with the ability to perform the role? with adequate training? with adequate resources?				

	Yes	No	N/A	Reference
Have you assigned responsibility for monitoring security on each application to someone with sufficient authority to demonstrate the importance management attaches to the issue? with the ability to perform the role? with adequate training? with adequate resources?				
Does management review the work of the system and security administrators?				
H. USER TRAINING AND AWARENESS				
Do all users of all systems appreciate the need for information security?				
Have you provided adequate training for existing staff on the minimum security procedures expected of them?				
Is information security part of the standard induction procedures for new staff?				
Are regular bulletins issued to staff to maintain general security awareness?				
I. COMPUTER VIRUSES				
Have you issued guidelines on the need for virus protection to all new staff?				
Do you prohibit staff from loading software onto company PCs?				
Are facilities available to virus check all diskettes being introduced into your company?				
Do you prohibit staff from downloading information from external data sources such as bulletin boards and the Internet?				
Has virus scanning software been installed on all PCs and does it run automatically and regularly?				

APPENDIX I

EXAMPLES OF PHYSICAL SECURITY WEAKNESSES

Inadequate physical security leading to unauthorized access to data

One version of a common operating system was particularly vulnerable to physical security weaknesses. When the company's computer was first switched on, users were allowed to choose which mode the computer should start in. One of the modes allowed the computer to start in single-user mode, with the user as "Superuser."

Effectively, this meant that, if an individual could gain physical access to the hardware, which in this case was stored in an open plan office, he or she could access every piece of information on the computer, with full edit capabilities, and no audit trail would remain.

Operator consoles

Some older operating systems require a "system console" to be present at all times. This system console is a terminal where system messages are displayed and where operator commands are entered. As such, any commands entered at the system console have full authority over all parts of the system.

The only way to restrict access to programs and data with this kind of system is to physically restrict who has access to the system console itself.

APPENDIX II

EXAMPLES OF OPERATING SYSTEM SECURITY WEAKNESSES

Default password left unchanged

A supplier who sold a computer to a company in the oil industry insisted that the password for the standard User ID used for hardware support be set to a certain value.

The IT manager of the site in question was not happy that she could not change the password and that it did not expire in line with all other passwords at the site. She investigated the supplier's instructions at other sites using the same hardware and found that the same User ID and password, with the highest level of access, was in place at all companies using that hardware throughout the region.

She promptly changed the User ID and password and informed the hardware supplier that it should contact her for all future access to the company's systems.

Excessive operating system capabilities

A large multi-national organization implemented a new electronic funds transfer system for making payments to its suppliers. These payments totaled billions of dollars a year and individual payments could be several million dollars each.

After the system went live, the access capabilities of the development team were not reviewed and revised to ensure that such access was appropriate. As a result, this team was left with full access to the underlying payment data files and had the opportunity to change the sort code, account number and amount of any fund transfers to be made. No resource security or audit trial had been established around these sensitive data files, nor were any changes identified for some considerable period of time.

APPENDIX III

EXAMPLES OF APPLICATION SYSTEM SECURITY WEAKNESSES

Inadequate purchase ledger security

A company within the beverage industry was in the process of reducing staff numbers and rationalizing staff responsibilities. As a result of the rationalization, a purchase ledger clerk was given excessive access capabilities within the purchase ledger system.

Investigations revealed that he could not only process invoices but could also set up new suppliers, order goods and make automated payments — all without the need for any subsequent management review or supervision. When the weakness was identified, the security settings within the purchase ledger were amended and responsibilities were allocated to re-establish adequate segregation of duties.

International Federation of Accountants
545 Fifth Avenue, 14th Floor, New York, NY 10017 USA
Tel +1 (212) 286-9344 Fax +1 (212) 286-9570 www.ifac.org