INTOSAI

Information System Security Review Methodology

A Guide for Reviewing Information System Security in Government Organisations

Issued by
EDP Audit Committee
International Organisation of Supreme Audit Institutions
October 1995

Contents

APPENDICES

Volume 3 - A Detailed Information System Security Method

Information System Security Review Methodology

A Guide for Reviewing Information System Security in Government Organisations

Volume 1 : Overview

Overview

Users should read this overview before referring to the other volumes of the INTOSAI Information System Security (ISS) Review Methodology Guide. The purpose of this overview is to explain how this methodology is organised and in what circumstances to use it.

The ISS Review Methodology Guide is applicable to any environment (mainframe, microcomputer or local network of microcomputers).

The ISS Review Methodology Guide proposes a two-tier approach. Tier 1 offers Supreme Audit Institutions (SAI) a method to do a simple manual information system review, especially when resources are limited or reporting needs do not require otherwise (Volume 2) . Tier 2 is a more sophisticated method based on the monetary value of information security exposures (Volume 3).

The main objective of this guide is to assist Supreme Audit Institutions that have such a mandate to review information system security programmes put in place by various government organisations. It can also be used by SAIs to set up comprehensive and cost effective security programmes covering key information systems in their own office. This is not a detailed security audit guide: it is a description of a structured approach to assessing and managing risk in information systems.

What Is Information System Security

The objective of an information system security programme is to protect an organisation's information by reducing the risk of loss of confidentiality, integrity and availability of that information to an acceptable level.

A good information security programme involves two major elements, risk analysis and risk management.

In the risk analysis phase, an inventory of all information systems is taken. For each system, its value to the organisation is established and the degree to which the organisation is exposed to risk is determined. Risk management, on the other hand, involves selecting the controls and security measures that reduce the organisation's exposure to risk to an acceptable level. To be effective, efficient and reflect common sense, risk management must be done within a security framework where information security measures are complemented by computer, administrative, personnel and physical security measures (see Table I).

Risk management becomes a senior management issue. A balance has to be reached between the value of the information to the organisation on the one hand and the cost of the personnel, administrative and technological security measures on the other hand. The security measures put in place need to be less expensive than the potential damage caused by the loss of confidentiality, integrity and availability of the information.

Many formal risk analysis methodologies on the market require technical expertise in the area of information technology and relevant controls and availability of precise threat frequencies that may be beyond the reach of many audit offices, at least initially. The objective is to build up over time the necessary expertise and resources.

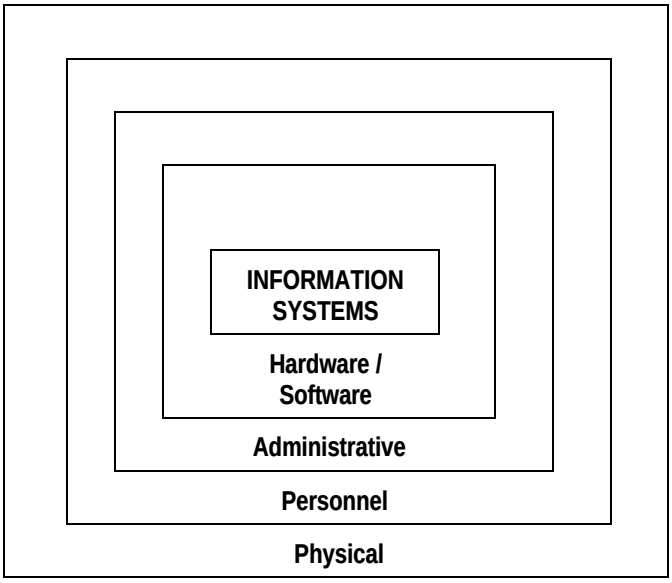


Table I Complementary Layers of Information Security

Information Security Framework

Information security is one element of a security infrastructure and, as such, should not be examined in a vacuum. There should be a framework of security policies dealing with all aspects of physical security, personnel security and information security. There should be clear roles and responsibilities for users, security officers and the Information Systems Steering Committee. An information security programme should include all aspects of the sensitivity of corporate information, including confidentiality, integrity and availability. A programme of security awareness should be in place reminding all staff of the possible risks and exposures and of their responsibilities as custodians of corporate information.

Referring to Table I, information security is a set of measures at the physical, personnel, administrative, computer and information system levels. They must all work together. Information security is good management control and shortcomings at any level can threaten the security at other levels. If personnel security policies, for instance, are not well designed and implemented, information security could become very costly or almost impossible to support. On the other hand, minimal measures at all levels should ensure a minimum of protection to the information, provided the security risk is reasonable and accepted by management. There are also situations where security measures at one level may compensate for security weaknesses elsewhere. Encryption, for instance, adds an extra layer of protection for data confidentiality and integrity even in cases where physical, personnel or administrative security measures may be weak. Encryption remains one last defence to help prevent a breach of confidentiality or of integrity.

In planning for information security, the value of the information to management and the volume of that information relative to other types of information have to be balanced against the basic security limitations of the medium. In many government departments, unless there are extreme requirements for carrying top secret information on a suitably protected laptop, the information should simply be created and carried otherwise. For those departments, the cost and the constraints of the appropriate security controls and measures may just not be acceptable, given the small volume of information that needs such protection.

Two-Tier Approach to Information System Security Reviews[1]

[1] This two-tier approach is the result of a joint effort by the National Audit Office of the United Kingdom and the Office of the Auditor General of Canada.

The guide introduces a two-tier approach to information system security reviews. The emphasis is on the use of common sense to always balance the cost of security to be built into a system to the value of the information carried by that system [2].

Given the limited resources of many Supreme Audit Institutions, it is proposed that SAIs first use a top-down, manual, management view of information security. SAIs should proceed to the second phase, a very detailed analysis aimed at a monetary valuation of information exposure to risk, only if management needs the monetary precision to support its decisions or if specific technical exposures are being examined. Both methods incorporate the elements of risk analysis and risk management (See Table II).

[2] Security is largely preventive in nature, like car insurance. Even though most people have never been in a serious car accident, they still have car insurance. The benefits are never fully realised until there is an accident. Security "is a legitimate and necessary expense of managing information, and (government) departments should consider both the cost of implementing controls and the potential cost of failing to do so. The costs of security should be commensurate with the need, and built into the life cycle costs of any computer system". (Office of the Auditor General of Canada, Annual Report, 1990, chapter 9, Information Security Audit)

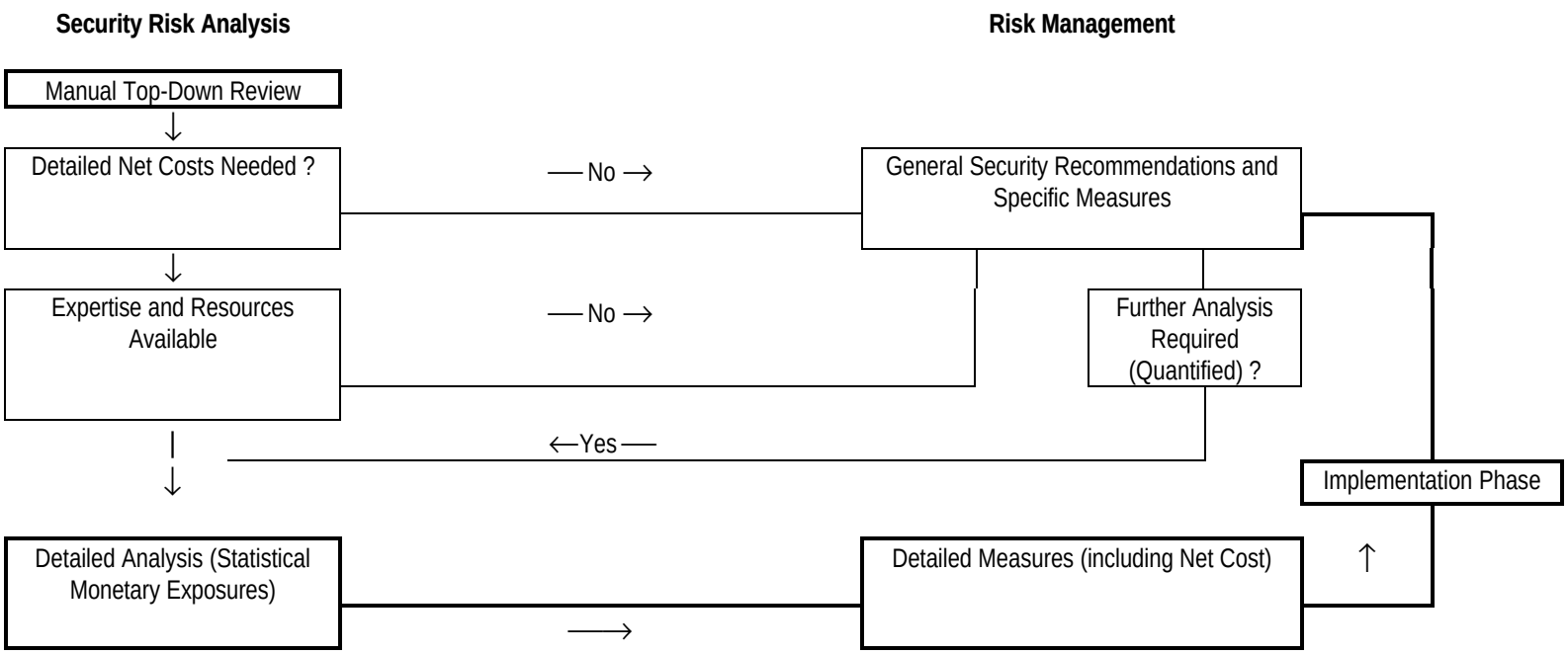


Table II **Two Tier Approach to Security Risk Analysis and Management**

This two-tier approach provides Supreme Audit Institutions with options in the choice of methodologies and with a gradual migration path from a less sophisticated methodology to a very formalised and resource intensive methodology.

The Top-down Information Security Review Approach - Volume 2

The top-down method is simple but complete and can help Supreme Audit Institutions reach conclusions on the security exposures of the information system under review. It takes a top-down perspective of information security as it attempts to take a senior management perspective of what information is of value to the organisation, what are the risks and the security exposures and what recommendations should be made. This approach allows auditors to focus their attention on key information systems, especially those presenting special security concerns.

The top-down method relies on qualitative assessments of the risk for threats to occur and of the degree of their impact if they did occur. The focus is on assessing the value to management of the information or the data carried by the information systems, not so much the value of the technology itself [3]. For each information system, the value of the information to the organisation, the threats and the possible impacts are evaluated first individually, then globally to determine a global degree of exposure to risk. These evaluations are subjective and usually expressed in terms of high, medium or low risk, impact and exposure.

Based on these evaluations, recommendations are made to management on the course of action to take or on the type of specific controls and security measures to put in place. These recommendations are part of risk management.

The top-down method has several advantages. It is easy and cheap to use. It is manual and can be used by any SAI with staff knowledgeable in matters of management controls and of information and computer systems in general. Internal staff resources may be sufficient. There is no need for sophisticated software packages to collect data about the information systems being reviewed, to obtain up-to-date and pertinent statistics and to produce very sophisticated analyses and reports. If a microcomputer is used, a word processing package is usually sufficient. Spreadsheets can help in producing summary tables. The more adventurous may want to use packages that offer database functionality to collect information and later produce analysis reports.

[3] Contrary to the top-down method, the detailed methodologies used in the second tier of the approach proposed by this Guide quantify in a very detailed manner the threats to the computer platforms on which information systems are running.

In the proposed Two-Tier Approach to Information System Security Review, the Top-Down Method is seen as a decision point in the overall method. Depending on the circumstances of the review, SAIs may satisfy themselves with the results of the review or may decide to pursue the review with more sophisticated procedures in areas of special concern or where very technical or costly security measures may need to be justified to management.

Detailed Information System Security Method - Volume 3

The detailed methodologies used in the second tier of the approach proposed to Supreme Audit Institutions are a well known type of risk analysis and management based on a detailed and quantitative analysis of information system assets. They attempt to measure the net monetary impact of security exposures and of the countermeasures put in place. Vendors around the world sell various security analysis packages that support such an approach.

Quantitative security analysis methods are usually made available with a microcomputer software package for the benefit of the auditor as the task of entering data, calculating security exposures and reporting on the project may prove tedious and formidable. Such risk management packages come with expert help from the suppliers and training for the users of the method. **Volume 3** describes a manual version of a detailed information security method [4]. The objective is to provide SAIs with an overview of a method which is best used with the support of an automated software package.

In contrast to the top-down approach, quantitative security analysis attempts to evaluate in monetary terms, in a very detailed and structured way, all the assets and all the possible threats and impacts to the information systems carried by an organisation. Through interviews and questionnaires, the possible impacts to the information are evaluated by the users and given a rank, from one to ten, depending on their seriousness. Annual loss expectancies are calculated next by combining asset replacement costs, threat probabilities and impact weighting factors.

Most of the methods on the market are second-tier in nature and vary from one another in the way probabilities, costs and the cumulation of the annual loss expectancies are obtained. Other differences may be the user friendliness of the method and the kind of support provided by the vendor. These are some of the concerns this two-tier approach attempts to address.

The use of quantitative methods of risk analysis and management requires that tables of risk statistics and asset costs be modified for each country's own circumstances.

[4] Developed by the National Audit Office of the UK.

How To Use The Two-Tier Approach to Information System Reviews

Planning. Planning the security review is the key to success. It should cover the following main elements:

- Knowledge of the client and of the environment;
- Scope of the review: Which information systems, which logical, physical or geographical boundaries?
- Resources available: Qualified staff or consultants, budgets, timeframes;
- Availability of reliable threat statistics and cost figures, appropriate for the local conditions; adaptation of the default values, as necessary;
- Reporting requirements: Users of the report, context of the review (Annual Report, special report, internal, external, etc.), type of recommendations needed;
- Review method: Top-down approach, detailed analysis, or a combination of both.

When and How to Use the Top-Down Review Approach - Volume 2

The top-down approach is the preferred method to use, as it meets the needs and the capabilities of many Supreme Audit Institutions.

Volume 2 contains a description of the method, including the step by step completion of the security review. A series of forms is provided in appendices to the package. The forms can be used in printed form or on a microcomputer [5].

The two most important forms are the Information Sensitivity Statement and Security Classification form (Appendix C) and the Business Impact and Threat Assessment form (Appendix E). Depending on the circumstances of the security review, the hardcopy versions of these forms can be completed by the owners/users of the information systems under review and signed by a senior official. They become the permanent security assessment documentation for those systems. The availability of electronic forms simply makes it easier to adapt them to local needs.

[5] They were developed in WP 5.1 and in Lotus 123 version 2.01. The forms are available in electronic format and can easily be imported into a Windows environment.

The other forms, mostly spreadsheets, are used to summarise the results for several information systems on a master sheet. If Lotus 1-2-3 is not easily available, the security officer can use these forms and summarise the information from the individual security assessments on columnar pads .

When and How to Use Detailed Information Security Methods - Volume 3

There are circumstances where more detailed and quantified information security reviews will be the norm. This will be the case where Supreme Audit Institutions have the budgetary, technical and staff resources to conduct such detailed analyses or where reporting requirements dictate the approach to take.

Before attempting to use a detailed information security method, it is strongly recommended that SAIs take a closer look at the following issues:

- availability or easy access to expertise in information technology and information security;
- availability of a suitable methodology;
- availability of a good software supporting package: Quantitative risk methods are very comprehensive and involve detailed methodologies that almost beg the use of a microcomputer; on the other hand, the microcomputer package usually introduces complexities of its own, which makes detailed security reviews a formidable task;
- budgets to adapt or customise the package to the environment under review: Several months of effort are not unheard of;
- training budgets, as the learning curve can be quite steep and costly, especially if consultants have to be used;
- time and financial resources: Detailed or quantitative security reviews tend to be lengthy and resource intensive; and,
- the need for such a detailed review: It has been argued that detailed, quantitative security reviews cannot be justified for commercial or government information systems which are neither complex nor highly sensitive.

SAIs such as the National Audit Office in the UK and the Audit Office of New Zealand already have a long experience in the development and the use of

detailed security risk management methods. Other SAIs may want to consult them before moving in that direction.

To use those methods effectively, Supreme Audit Institutions need to have access to staff or consultants qualified in information technology AND in information security concepts. As commercial risk management packages are marketed world-wide by a number of consulting firms, training in the use of the underlying methodology is available from those firms with the purchase of the package.

There are several well known risk management packages. CRAMM, for instance, was developed for the British government and is now marketed around the world by various consulting firms. In the U.S.A., RiskWatch is a well established package that uses expert system software to carry out risk analysis and management. The US Department of Energy has developed the Los Alamos Vulnerability Assessment (LAVA) package. New Zealand is developing CATALYST in a Windows environment to respond to its own security analysis needs. The actual selection of a package may be a matter of local availability, cost, after sales support and amount of customisation needed to local conditions.

The cost of one of those commercial packages to a Supreme Audit Institution is approximately £ 6,000 or US$ 10,000. This may also include training for one or two persons.

In all cases, Supreme Audit Institutions have to ensure that the underlying statistics used by the selected package are appropriate for their local conditions. Otherwise, the results could reflect conditions found only in Europe or in North America.

A Guide for Reviewing Information System Security in Government Organisations

Volume 2 : **A Top-Down Approach**

Information Sensitivity Statement and Security Assessment for Computer Information Systems

I INTRODUCTION

The purpose of this guide is to provide a cost effective methodology to assist in reviewing or establishing appropriate security policies and measures within an organisation. Recognising that security requirements need to be updated on a regular basis, the guide also provides for simple documentation, updating and reporting.

The guide describes computer security assessment from the perspective of management in a government organisation [6] . Organisations can use this guide to assist in producing an "inventory" of computer applications used, assessing the sensitivity and security classification of the information, and completing a business impact threat risk security assessment. The person in charge of security [7] utilises this work as a foundation for overall assessment of security policies and measures and for making recommendations.

Supreme Audit Institutions (SAI) can use the guide in two ways: For internal purposes, to set up a security assessment process in their own organisation or, for external purposes, to help in reviewing the security assessment process in other government organisations.

This guide takes a top-down high level approach to information security. The emphasis is on the information carried on various electronic devices. In line with this high level approach, this guide categorises threats by general causes instead of their results, such as earthquakes instead of the destruction they may bring. A detailed bottom-up approach to information security, on the other hand, tends to examine every possible computer asset for weaknesses that may create loss exposures to the information generated or carried by those assets. The advantage of using the top-down approach is that it helps management to quickly target and focus on problem areas for further action. In some cases, this may point to the need for more detailed work to build a business case for extensive or costly security measures.

Because the method always takes a corporate or management view of information security, it remains flexible and can deal with issues of security policy as well as of security measures.

---

[6] "Organisation" refers to any government department, agency or state corporation. In this document, "computer application" and "information system" are used interchangeably.

[7] See Appendix I for details of a typical security infrastructure in government.

II COMPUTER SECURITY ASSESSMENT PROCESS

Evolution of Information Management

In managing information and applications, an organisation goes through four distinct stages, managing paper, managing automated technologies, managing corporate information resources, and finally, managing the strategic use of information (Appendix A). The technology and security challenges are to minimise the time and effort spent in each stage and to go through the stages as smoothly as possible.

At the managing automated technologies stage, the users are not significantly relying on computer applications but are achieving noticeable efficiencies. At the third stage, managing corporate information resources, computer security becomes a major concern due to significant reliance on computer based information and the exposures related to concentration of information at one place.

Security Management

One of the Organisation's key resources is its information. The first step to safe computing is adoption of information and administrative management policies and measures which embrace principles of good security management:

1. Security protection should be consistent with the value of the information being protected;

2. Security protection should remain with the information at all times as it is moved or processed; and

3. Security protection should be continuous in all situations.

The Security Team

Under the leadership of the person in charge of computer security, a security team is selected. Full commitment by senior management is important if the team is to achieve its objectives. Its responsibility is to implement the security policy set out by senior management and to identify changes made necessary by developments in the organisation's information systems or the threats that face them.

The Process

Security policies are designed to protect information according to the exposures of the information. Security measures (standards, procedures, and tools) are the building blocks for protecting the information.

In determining which specific measures are necessary, the Computer Security Assessment Process (Appendix B) is followed involving:

- **Sensitivity Statement:**

  Assessing the sensitivity of program and administrative applications (information systems) used in the Organisation, and determining the security classification.

  Confirming the Organisation's standard assessment of similar applications and, when appropriate, completing or updating an Information Sensitivity Statement & Security Classification form (Appendix C).

  Where desirable, rolling up individual sensitivity statements unto a Summary Description of Information Systems (Appendix D).

- **Business Impact Assessment:**

  Determining possible business impacts to the Organisation if the information were disclosed, integrity compromised or services disrupted.

- **Threat and Risk Assessment:**

  Determining the risk (the chance) that identified threats could occur.

- **Security Exposure Rating:**

  Evaluating the business impacts and the threats together to determine overall exposure to the Organisation.

  Confirming the Organisation's standard security assessment of similar applications and, when appropriate, confirming or updating a Business Impact and Threat Assessment form (Appendix E).

- **Security Decision and Recommended Actions:**

  Completing or updating a Summary of Security Assessments form (Appendix G).

Making security decisions and recommending management actions to minimise identified exposures, and highlighting any serious security policy deficiency.

III COMPLETION OF AN INFORMATION SENSITIVITY STATEMENT & SECURITY CLASSIFICATION FORM

It is important to establish a complete "inventory" of all operations and administrative applications (grouped or specific) in use and clearly establish the boundaries of the system(s) under review. Appendix I provides a definition of an application. **For security purposes, similar applications may be grouped together, such as word processing Letters, word processing Audit Memorandums, spreadsheet Financial Analysis, spreadsheet Planning Schedule, etc.**

Applications are owned by either a group or an individual. Where there is little interaction between applications, users of the output from the system can be readily identified. In highly integrated systems, an artificial boundary has to be agreed by all parties, including Senior Management.

A group may ask members to complete a User Information Sensitivity Statement and Security Classification form (Appendix C) in order to establish an "inventory" of applications in use and to collect the data required for consolidating similar applications. It is important that the form be reviewed and approved by a senior manager of the group. This ensures that all assessments reflect the true value of the information system to the organisation as a whole.

Through the completion of an Information Sensitivity Statement and Security Classification form (Appendix C), the owner assesses the sensitivity of information from the view of availability, integrity, and confidentiality, estimates replacement and opportunity costs, direct and indirect costs (hours @ an average dollar rate and expenses), and determines the required security classification.

The Information Sensitivity Statement and Security Classification form is formal documentation of the assessment. The form is also helpful to document specific integrity controls and procedures (completeness, accuracy and authorisation). It should be kept as permanent documentation and updated as necessary.

Where appropriate and once finalised, individual sensitivity statements are rolled up by management at the group level or at the organisation level unto a Summary Description of Information Systems (Appendix D). This provides management with an overview of the systems under their responsibility and of the value of the information they carry.

IV COMPLETION OF A BUSINESS IMPACT AND THREAT ASSESSMENT FORM

The Business Impact and Threat Assessment form (Appendix E) provides for a structured assessment of the Organisation's level of security exposures. The assessment has three distinct components, the risk (chance) of threat occurrence, the degree of seriousness of business impacts, and an exposure assessment rating. The first two components are independent of each other and can be assessed in any order. The business impacts and threats are then assessed together to arrive at an overall Organisation security exposure rating.

Threat and Risk Assessment

Threat. What could happen. Possible threats are listed in Appendix E. A more detailed list, along with suggestions for countermeasures, is also available in Appendix H. Security surveys report that over 80% of the threats experienced with computer information are from within the organisation (insiders) broken down between 24% due to inattention to procedures (carelessness), 26% due to inadequate training and 30% due to dishonest employees.

Care should be given to local conditions where the nature and importance of threats may differ considerably from country to country. In some cases, this may mean focusing more on certain types of threats, further defining some of the threats and adapting countermeasures to local conditions.

Probability of Occurrence. The chance that the threat will occur. As certain threats and risks may be common throughout the organisation, a general assessment should be completed by the person in charge of computer security and used as a yardstick for making individual assessments. The persons doing the individual assessments need only to concentrate on the risks which are relevant or could be different because of special circumstances. For each information system, the chance of individual threats to occur is rated as high, medium or low. After all possible threats to the application have been identified and assessed, a value judgement is made on the overall risk. For a given information system, the overall risk is not the result of a formula that

adds up the number of high and low ratings. A single high rating in a critical area may result in an overall high rating. On the other hand, several high ratings in non-critical areas may produce a medium to low overall rating.

Business Impact Assessment

Business decisions need to be made about the value of the information. For security purposes, these business values are expressed as business impacts on the Organisation if the information was disclosed, its integrity was compromised, or there was a disruption of services. Possible business impacts are listed in Appendix E. **Depending on local conditions, additional business impacts can be determined.** For each business impact, make decisions as to whether, if it occurred, the consequences would be very serious, serious, or less serious. Only those business impacts related to your information are assessed. After all possible impacts have been assessed, an overall business impact assessment is made for the application.

Each of those assessments is a subjective value judgement of the severity of each individual impact on the organisation as a whole. Similarly, after assessing the individual impacts on the organisation if the information were disclosed, compromised or made unavailable, an overall business impact assessment is made, not on the basis of a precise cumulation of those individual impacts, but on a value judgement of the overall effect on the organisation. These value judgements are built through consensus between the various key interested parties.

To be acceptable, it is important that assessments of business impacts and of threat risks be reviewed and approved by the senior executive of the organisational group and by the person in charge of computer security.

Security Exposure Rating

A security exposure assessment is the result of combining the overall threat risk rate or probability (high, medium, low) with the overall business impact rate (very serious, serious, or less serious). The Exposure Rating Chart, Appendix F, is used as a guide to rate exposures as high, medium, and low.

The first step is to assess the overall exposure for the application as a whole on the Business Impact and Threat Assessment form (Appendix E).

For instance, for a high overall threat risk assessment (vertical axis) but with a low overall business impact (horizontal axis), the Exposure Rating Chart would first make us select a "4" figure at the intersect. This is translated into a medium exposure rate. See the legend on the Exposure Rating Chart or the chart in Section VI below to see how exposure ratings can be regrouped as low, medium or high exposure rates.

As a second step and to identify which threat risk and business impact could be targeted for management action, an exposure rating is calculated for those business impacts that were assessed. This is done by using the Exposure Rating Chart to combine the individual business impact rate and the **overall** threat risk identified. The numbers obtained from the Exposure Rating Chart are posted to the relevant impact lines, in the exposure assessment area of Form E. For clarity, the numbers are posted in the appropriate Hi, Med or Lo column. Medium or high individual security exposure ratings could become the object of recommendations to management on the reassessment of the business impact or on the reduction of the overall threat risk, so as to reduce the security exposure to the organisation.

This assessment is the linkage between security exposures and what security decisions and actions are required.

V SUMMARY OF SECURITY ASSESSMENTS

The Summary of Security Assessments form (Appendix G) consolidates the information gathered and evaluated on the Information Sensitivity Statement & Security Classification forms (Appendix C) and the Business Impact and Threat Assessment forms (Appendix E). Group summaries, segregating program delivery operations and administrative work, are prepared. These forms and summaries should be kept as working papers and updated regularly. They should be reviewed and approved by the appropriate senior executive.

The summaries provide a senior management security overview of the applications in use. Based on these summaries, with the applications' assessments, the person in charge of computer security evaluates the Organisation security exposures and recommends actions required to minimise identified exposures. Given the changing nature of technology, the risk review process may also highlight security policies that are no longer adequate. All serious policy shortcomings are brought to the attention of senior management in the final report, along with other recommendations. Where, for a particular program or information system, the results indicate the need for more precise recommendations, a more detailed review using in-depth quantitative analysis may be recommended to determine what security countermeasures are required or to assess possible alternatives.

For security assessment and priority planning purposes, the threat and risk rating, the business impacts and rating if the threat occurred, and finally, the

overall organisational exposure assessment are very helpful in establishing acceptable long term security plans.

VI SECURITY DECISION AND RECOMMENDED ACTION

For each exposure assessment (Business Impact and Threat Assessment form), a security decision and a recommendation for management action is made. The relationship between an exposure and a security decision and recommended action is:

Exposure Rate	Security Decision	Recommended Action
HIGH (9,8,7)	Control the risk	Implement additional policies and measures (standards, procedures, tools)
MEDIUM (6,5,4)	Control the risk Avoid the risk	Implement additional policies and measures Change / improve operational procedures
LOW (3,2,1)	Avoid the risk Limit the risk Accept the risk	Change / improve operational procedures Obtain insurance coverage No change / continue as planned

Where specific measures need to be recommended, Appendix H provides a comprehensive list of possible actions to be taken. Used with professional judgement and an eye for costs, the list can provide the basis for recommending specific controls and security measures.

After review by the person in charge of computer security, the security report and recommendations are forwarded to senior management through the Information Systems Steering Committee for action.

VII COMPUTER SECURITY ASSESSMENT STEPS

The steps of a computer security assessment -- information sensitivity statement and security classification, business impacts assessment, threat risk assessment, security exposure assessment and security decision/recommended actions -- are outlined in Appendix B. The steps are:

1. For its applications, **each organisational group** assesses its information sensitivity and security classification,

   or alternatively,

   confirms the contents of the standard Information Sensitivity Statement and Security Classification form and, if appropriate, updates the form, including appropriate approval.

   Appendix C — Information Sensitivity Statement & Security Classification - Form

   Appendix D — Summary Description of Information Systems - Spreadsheet [8]

2. For its applications, **the organisational group** assesses the business impacts, and the threats and risks,

   or alternatively,

   confirms the contents of the standard Business Impact and Threat Assessment form and, if appropriate, updates the form, including appropriate approval.

   Appendix E — Business Impact and Threat Assessment - Spreadsheet

   Appendix F — Exposure Rating Chart

3. **The organisational group** prepares a summary of security assessments of applications in use in the format provided.

   Appendix G — Summary of Security Assessments - Spreadsheet

[8] Although developed as spreadsheet templates using Lotus 1-2-3, these forms can easily be used in hardcopy form (from photocopies) or done manually.

4. **The organisational group** sends a copy of the summary and the two forms to the **person in charge of computer security** for review and, if appropriate, meets with the person in charge of computer security to finalise the security assessment.

Appendix G	Summary of Security Assessments - Spreadsheet
Appendix C	Information Sensitivity Statement & Security Classification - Form
Appendix E	Business Impact and Threat Assessment - Spreadsheet

5. The summary is approved by the **person in charge of computer security** and, where appropriate, the summary is reviewed and approved by the Director of Security.

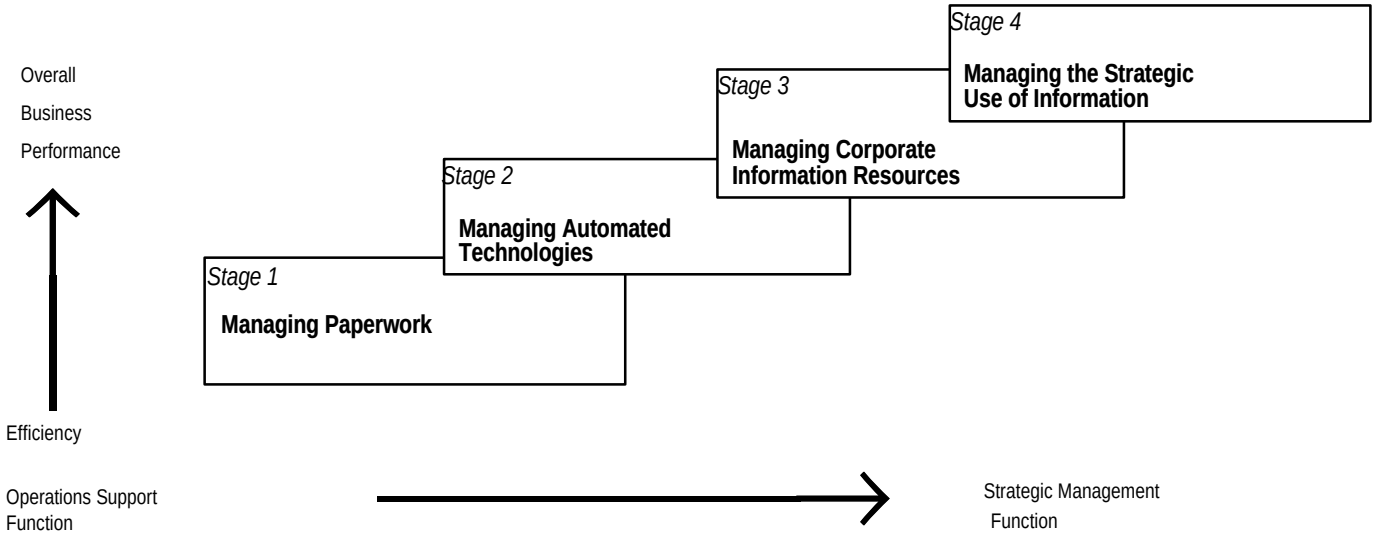
Appendix G	Summary of Security Assessments - Spreadsheet

6. The final summary is reviewed and approved by the **senior executive** responsible for the organisational group.

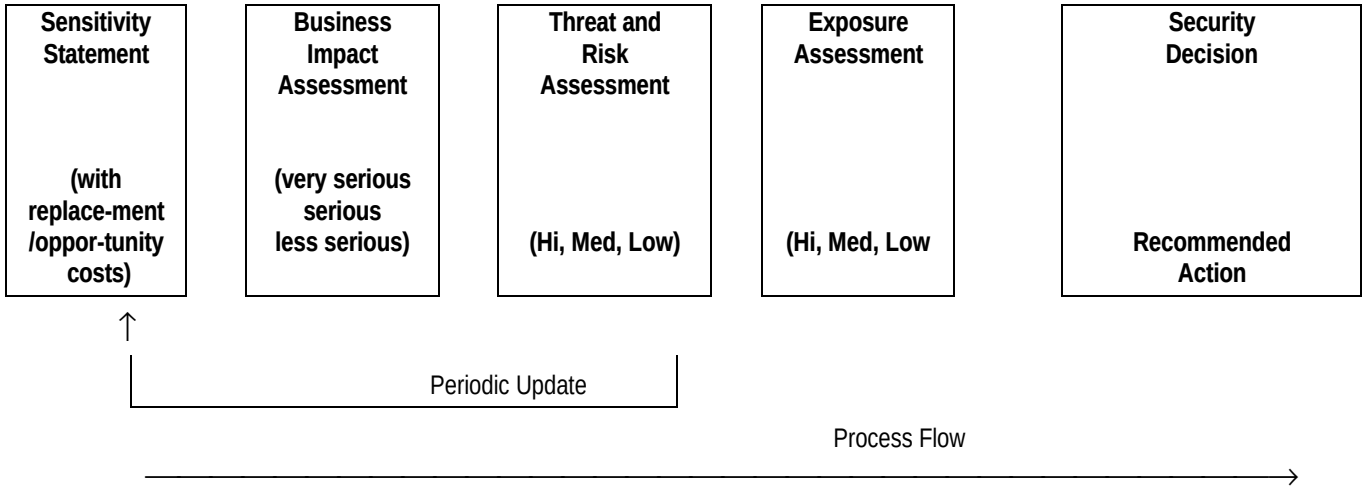
Appendix G	Summary of Security Assessments - Spreadsheet

7. The **person in charge of computer security** makes, if appropriate, security decisions with recommended management actions to minimise identified exposure(s) and reports to the Chief Security Officer.

APPENDIX A - EVOLUTION OF INFORMATION MANAGEMENT



APPENDIX B - INFORMATION SYSTEM SECURITY ASSESSMENT PROCESS



Appendix C - **Information Sensitivity Statement and Security Classification**

Introduction

This document can be used in hard copy form or as a WP 5.1 document, depending on local circumstances.

In the top-down information system security review, this document is used at the risk analysis phase, to document information systems. One document is completed per system.

Application :_____ Date: _____
(grouping of similar applications is acceptable)

New Statement _____ Amended Statement _____

Computer Environment :
Micro ____ Mini ____ Mainframe _____ Service Bureau _____

Software used : _____

1. Name of branch and, where appropriate, Group responsible for the information (i.e. the **OWNER**)

Branch : _____ Group : _____

2. If the applications have been "grouped", skip the "Total no. of transactions" question. Where applicable, provide a general description of the application including the source of the information, the volumes and any complexity in the processing.

Volumes		**Sources of information**	
% of total organisational information	_____	Client or external	_____
Total no. of transactions **or** monetary value of transactions	_____	Program / Operations	_____
File size		Administration	_____
No. of records	_____		
General description of application and complexity of processing			

3. Indicate the Primary Purpose and any Secondary Purposes of the Information :

Services to public _____ Admin. function _____
Decision making _____ Financial function _____

4. Indicate the Primary User and Secondary Users of the Information :

Program _____ Admin _____ Govt. _____ Public _____ Other _____

5. Are there manual and computerised procedures used before, during or after processing to ensure the completeness and accuracy of the information ? INTEGRITY

Procedure	Manual Yes / No	Compu-terised Yes / No	Comments (Nature of Main Procedures)

Before Processing			
During Processing			
After Processing			

6. What would be the consequences if the information were accidentally or deliberately disclosed ? CONFIDENTIALITY

Injury, loss or damage	**Yes / No**	**Injury, loss or damage**	**Yes / No**
1. Embarrassment to the organisation		5. Compromise of personal information	
2. Loss of credibility for the organisation		6. Compromise of national interest information	
3. Compromise of confidential organisation information			
4. Compromise of client or third party information			

7. What would be the consequences if the information were accidentally or deliberately modified and / or destroyed ? AVAILABILITY, INTEGRITY

Injury, loss or damage	**Yes / No**	**Injury, loss or damage**	**Yes / No**
Disclosure / Integrity of Information 1. Embarrassment to the organisation		**Disruption of services** 1. Late payment of bills / payroll	
2. Loss of credibility for the organisation		2. Inability to collect revenues	
3. Compromise of confidential organisation information		3. Disruption of service to the Government	
4. Compromise of client or third party information		4. Disruption of service to the public	
5. Compromise of personal information		5. Disruption of internal service	
6. Compromise of national interest information			
7. Legal implications / liability for compensatory and punitive damages			

Do contingency procedures exist to ensure recovery of the information ? AVAILABILITY, INTEGRITY

Recovery Procedures	Yes / No	Unknown	Comments
Backups			
Offsite Storage			
Other Method			

8. What is the maximum recovery period that the Organisation can tolerate without the availability of the application or service (if limited to specific period(s) indicate) ? AVAILABILITY

Hours _____ Days _____ Weeks _____ Months _____

Comment :

9. Indicate the sensitivity of the information
(5: Very critical; 4: Critical; 3: Sensitive; 2: Somewhat Sensitive; 1: Not Sensitive)
Availability _____ Integrity _____ Confidentiality _____

10. Estimate replacement and opportunity costs of the information, both direct and indirect (hours, expenses)

Replacement Costs	Staff Hours	Expenses
Direct (time spent restoring / recreating the information, hardware, software)		
Indirect (e.g. delays caused to other tasks, other parties involved in recovery, opportunities lost because of missing information etc.)		

11. Indicate the Security Classification / Designation of the information for this application / information system :

% of information	
_____	Basic Security Standards *(Undesignated)*
_____	Protected *(Designated)*
_____	Classified
100%	

Completed by : _____ Branch/Group : _____

Information Owner
(e.g. Executive Director) Approved by _____ Date : _____

Security Group Approved by _____ Date : _____

APPENDIX F - EXPOSURE RATING CHART

Impact / Probability	Very Serious	Serious	Less Serious
HIGH	9	8	4
MEDIUM	7	6	3
LOW	5	2	1

(Chart developed by Royal Canadian Mounted Police)

Exposure Rate : High (9,8,7) Medium (6,5,4) Low (3,2,1)

Appendix H - Baseline Threats and Security Measures

Introduction

This document gives a list of threats and countermeasures by asset. As presented, these threats often correspond to actual weaknesses as a result of specific threats. The countermeasures are controls or security measures that can be used to correct or minimise the security weakness.

In the text, the mention of disciplinary action as a possible countermeasure or deterrent to inappropriate staff action should be seen in a wider context. Disciplinary action should be envisaged or used only when other measures such as awareness and training have failed to prevent unacceptable actions or behaviour. Good security solutions are the ones where the staff buys in easily.

An index has been created at the end of the list for all the assets or topics for which threats and countermeasures have been presented.

In the text, for each asset :-

T = Threat
C = Countermeasure (control or security measure)

Table of Contents (Appendix - H)

Hardware

Communications

Telephone lines

T Telephone lines can be cut or lost.
C Set up alternative lines for key connections.

T Telephone lines can be intercepted.
C Use private lines where possible.
Avoid routing key lines through public areas.
Consider sealed cable conduits.
Ensure that cables leave the site underground.
Avoid making data cables conspicuous by separate routing or labelling.
If you do label telephone lines label them all and not just the key communications lines.
Consider encryption for the transmission of sensitive information. If you do use encryption consider the following:

- Encrypt keys as well as data.
- Use an encryption algorithm which complies with industry standards.
- Consider the use of "one time" keys to limit the usefulness of finding out any one key.
- Use non word keys of 6 characters or more.

Input / output ports

T Control over functions compromised by changing the port connections.
C Keep connection boxes in secure areas if you rely upon restricting functions to terminals connected to particular ports.

Modems

T Modems can be used to gain unauthorised access to the system.
C In general, do not attach modems to dial in lines. If there is a need for dial-in capability, provide access only to a central site that is protected with a bastion firewall. Restrict the caller to very specific applications within a bastion environment. Provide the caller with "terminal" sessions and not with "host" sessions or remote access sessions as these may provide open access to sensitive information on the microcomputer or on the network. Consider using encryption for the transfer and the storage of sensitive data.
Call-back features are usually too restrictive for auditors who are constantly moving in the field and may cause administrative headaches.

T Modems can be used for unauthorised transfer of information outside the organisation.

C Keep the number of modems to a minimum, monitor the usage of lines to which modems are attached, disable modem lines outside working hours.

Electronic mail

T Electronic mail can be used for the unauthorised transfer of information outside the organisation.

C Keep copies of all electronic mail sent out and keep records of sender and addressee.
Do spot checks on the contents of electronic mail.

Use searching programs to find key words in electronic mail.
Cross tabulate senders and addressees to establish any suspicious pattern.

[*Warning: In some countries, eavesdropping on electronic mail may be illegal or subject to special legislation.*]

Bulletin Boards

T Bulletin boards may be used as a means to pass information out of your organisation.

C Route all connections to bulletin boards through a central point. Use offline readers to extract messages and post replies. This will enable you to monitor traffic to and from the bulletin boards in much the same way as electronic mail.

T Malicious software containing viruses or Trojan Horses may be received from bulletin boards.

C All requests for the download of files from bulletin boards should be routed through a central specialist unit. Downloaded files should be checked thoroughly for viruses etc.

Postal Service

T Malicious software has been found on disks sent through the post.
C Introduce a procedure which makes it a disciplinary offence for anyone to use a disk before it has been tested by support staff.

T The postal service may be used to pass information out of your organisation.
C Register documents and disks that contain sensitive material and introduce procedures to control copying of them.

Network cabling

T Network cables can be tapped to steal information or introduce illicit messages.
C Do not route network cables through areas that are accessible to the public. Consider the use of locked cable trays. Always examine lengths of cable that have been maintained by engineers. Consider the use of encryption for parts of the network which carry sensitive information.

T Networks can be vulnerable to failure if one section of their cabling is broken.
C Design the network to minimise the impact of the failure of any one length of cable. Consider duplicate cabling for key links.

Computers

Terminals

T Unauthorised access to data can be gained from the keyboard of a microcomputer or any terminal on a network.
C The operating system and application software should use identification and authentication to ensure that access requests come from authorised individuals. All actions that could have a material effect on the business should be logged. The combination of identification, authentication and logging is the basis for accountability.
Where passwords are used for authentication they should be 6 or more characters in length and should be pronounceable non words. It is best for the computer to generate passwords to avoid the choice of trivial or duplicate passwords. If you do use machine generated passwords it is important that they are pronounceable so that people can remember them without writing them down.

Try to use a single password for each individual where possible. Multiple passwords are harder to remember and may lead to people writing them down which is a breach of security.

Passwords should be changed regularly. The more critical the functions to which passwords give access the more often the passwords should be changed. For key transactions the use of once only passwords may be justified. The reason for changing passwords / encryption keys frequently is to reduce the damage that would be caused by an unauthorised individual finding out a password.

T A terminal which is left logged in to a system is an invitation for someone to pretend to be the operator who logged on.

C Procedures should make it a disciplinary offence to leave an unlocked terminal logged in and unattended. The operating system / application software should log out terminals after a short period of inactivity or automatically lock the terminal so that any further activity will require reentry of identification and authentication details.

T Critical data may be modified through any local or modem connection to the information system.

C Identification and authentication controls go some way towards reducing the risk of unauthorised changes to critical data. Changes to key data should be subject to confirmation by a supervisor in addition to the normal checks.

Microcomputers

T Microcomputers are easily stolen.

C Mark all microcomputers and peripherals indelibly. Keep an inventory of all microcomputers and check it on a cyclical basis.

Buy microcomputers with a lock that disables the keyboard and removal of the case.

Introduce a system for logging computers into and out of the building. Security guards should be instructed to do spot checks to make sure that staff are not carrying computers, peripherals or consumables off the site without authorisation.

Position microcomputers so that they are not visible from public areas.

T Microcomputers may become unavailable due to the loss of their keys.

C Keep one of the keys to each microcomputer in a locked key cabinet in the support area.

T Microcomputers are particularly sensitive to malicious software such as viruses and Trojan Horses because the user can readily copy programs

onto the machine using floppy disks. Malicious software can also be introduced inadvertently from floppy disks from uncontrolled environments, and from distribution media such as shrink-wrapped software and CD-ROMs.

C Introduce procedures which make it a disciplinary offence to use any program on a microcomputer before it has been tested by the support staff. Make frequent backups of critical data and essential software. Support staff should keep records of software authorised for use on each machine and undertake spot checks to ensure that staff are not using unauthorised software.

Take special precautions with CD-ROMs as they can be virus-infected as any other media but can never be cleaned.

T Microcomputers are generally not fault tolerant.

C Prepare and test contingency plans to deal with the failure of any microcomputer which supports critical functions.

T Microcomputers are used and maintained by users rather than specialist staff. The result is that the need for backup and security is often overlooked.

C Buy tape streamers for machines which are used to store large quantities of volatile information.

Introduce procedures, awareness and training courses to make staff aware of the need for backup, proper handling of the equipment and security.

T Microcomputers can be used to introduce illicit software onto networks because they have floppy disks.

C Allow file transfer to the network only where it is essential.

Consider making it impossible to transfer "executable" files.

Introduce procedures which make it a disciplinary offence for users to transfer programs to or from the network.

Use diskless workstations unless floppy disks are essential.

Diskless workstations

T Workstations can be moved.

C If your access control system relies upon restricting functions to particular terminals then you will need to introduce procedures which ban users from moving their machines. Otherwise there is a risk that a machine will be moved from a secure area to a less secure area.

File servers

T Machine may fail making the system unavailable.

C Introduce backup procedures and a strategy for recovery in the event of the failure of a file server. Backup should allow for at least three generations on site and one off site. The nature and frequency of the backups will vary with the criticality of the applications supported by the file server. In many cases, weekly full backups and daily incremental backups are the norm. Automatic backups can be made in off hours, making full backups as easy as incremental ones.

Duplication of storage and processing may be necessary for file servers that support critical applications.

Mini and mainframe computers

T Machine failure can affect many users.
C Establish and test a backup strategy.
Consider duplication of storage and processing for key applications.

Input

Scanners

T Scanned images of sensitive documents may remain on shared scanner units.
C End a scanning session by scanning a blank page or a non sensitive document. Users should be familiar with the functions of the scanning software. Delete temporary files created during the scan process, e.g. hard disk files which have been copied out to diskette.

Output

General

T Output devices can radiate electromagnetic signals which can be decoded remotely.

C Ban parking of vehicles in areas adjacent to rooms used for the output of sensitive data.
Consider the need for "Tempest proofed" equipment.
Consider installing white noise generators to mask signals from equipment used for the output of sensitive material.

T If output devices are visible from a public area then information may be disclosed.

C Avoid positioning output devices in such a way that unauthorised staff / outsiders could read the output.

Burster

T Spoiled stationery may be used for financial gain or as a means of passing sensitive information to outsiders.

C Introduce a system for accounting for sensitive stationery. Spoilage should be signed off by the supervisor and sent for shredding / secure disposal.

T Bursters contain a lot of moving parts which are prone to failure.

C Ensure that bursters are maintained regularly.
Establish procedures for critical applications to be supported in some other way if a particular burster fails.

Enveloper

T Envelopers need to be set up at the start of each run. There is a risk that spoiled stationery could be used for financial gain or to pass information to outsiders.

C Establish an accounting system for sensitive stationery. Spoiled output should be signed off by a supervisor and shredded. Requests for duplication of spoiled output should be signed by the supervisor.

Laser printer

T Laser printer output can be rubbed out if the fusing assembly is not working properly.
C Introduce regular checks of output to ensure that toner is bound to the paper.

T Laser printers can be set to print duplicate copies. This may be undesirable if the output is sensitive.
C Ensure that software sets the number of copies before printing each page.

Impact printer

T Ribbons can retain the image of the characters that were printed
C Send ribbons used for sensitive applications for incineration.

Plotter

T Plotters may produce misleading information if the pens are worn, missing or loaded incorrectly.
C Make designated staff responsible for setting up and maintaining plotters. The designated staff should be responsible for quality control of the output.

Output queues

T On local area networks and in minicomputer environments, print jobs of sensitive documents can remain in output queues for a variety of reasons.
C In the event of aborted or incomplete printouts, ensure that the print queue is cleared.

Visual Display Unit

T Unattended visual display units can reveal sensitive information to unauthorised personnel / outsiders.
C Introduce procedures to blank screens when they are not in use. Staff should also lock the keyboard when they leave the machine. Some software combine the functions of blanking the screen and locking the keyboard.

Photocopier

T Photocopiers make it easy for staff / outsiders to make unauthorised copies of sensitive information.

C Introduce procedures making it a disciplinary offence to copy sensitive output without authorisation.
Restrict the number and location of "casual" copiers so that usage can be monitored. They should not be located in areas where sensitive information is held. They should be in an area where anyone using the copier would be visible to other staff.

Typewriter

T Typewriter ribbons can retain an image of what was typed.

C Use only designated typewriters for sensitive material and send ribbons for incineration.

Storage

Paper files

T Paper files can be burned or damaged by water.

C Keep copies of essential documents in fire / water proof storage cabinets and / or off site.

T Paper files can be used to remove sensitive information from the site.

C Paper files that contain sensitive information should be registered. Sensitive files should be copied only by authorised staff in a secure area. Introduce procedures which make unauthorised copying of sensitive files a disciplinary offence.

Removable magnetic media

T Magnetic media can be used to transfer large amounts of data out of the organisation.

C Use magnetic media which bear the corporate logo. Introduce procedures for all magnetic media to be signed into and out of the site.
The handling and storage of tapes, diskettes and removable hard disks should be subject to procedures similar to that of paper documents.
Introduce procedures which make it a disciplinary offence to remove magnetic media from the site or introduce magnetic media to the site without authority.

T Floppy disks are one of the main media for the transmission of viruses from one computer to another.

C Check all formatted magnetic media for viruses on entry to the site.
Check disks carried by engineers and students particularly carefully. All disks that are checked should have a label attached with the corporate logo and the signature of the tester and date.
Introduce procedures which make it a disciplinary offence for staff to use floppy disks that have not been tested.

T Used floppy disks retain information even when files are deleted or the disks reformatted.

C If floppy disks or tape cartridges are used to store sensitive information then they should be marked accordingly and treated like a registered paper file. Magnetic media that have been used to hold sensitive information should be "degaussed" / security erased before being used for other work. If magnetic media fail whilst holding sensitive data then they should be treated as confidential waste and shredded or burned.

Fixed magnetic media

T Hard disks can hold very large quantities of information. It is easy to forget sensitive files.

C When a hard disk is first used to hold sensitive information it should be registered. It should not be deregistered until it has been inspected by a member of the support staff. All sensitive files should be security erased.

T Access control to microcomputers is much less rigorous than a network system. If microcomputer hard disks are used to store sensitive information there is a considerable risk of unauthorised modification or disclosure.

C Lock microcomputers when they are not in use. Maintain site level security to restrict access to rooms with microcomputers.
Consider installing access control packages and data encryption packages on machines used to hold particularly sensitive information.
Consider using exchangeable hard disks that can be locked away when the machine is not in use.

T Defective hard disks cannot always be security erased

C If a hard disk which holds sensitive information fails then it should be destroyed if it cannot be security erased.

T Fixed disks do fail. If they store large quantities of volatile data the loss can be very serious.

C Backing up a large hard disk to floppy disks is so time consuming that staff are unlikely to do it regularly. Tape streamers make backup quick and

easy. Install tape streamers on machines with a lot of volatile information on hard disks. Backup tapes / disks should be held for three generations. At least one backup should be held off site. This should be renewed cyclically.

Backup tapes should be stored securely and security marked to reflect their content.

Removable optical media

T Optical disks are easily concealed and can hold very large amounts of information.

C Optical disks that hold sensitive information should be serially numbered and registered. The only safe way to dispose of them is incineration.

T Partial or total loss of data on optical disks can occur if either surface of the disk is scratched.

C All optical disks should be handled with extreme care to prevent scratches that may damage the reflective quality of the disk and "hide" major portions of the data. When the file allocation table of the disk is affected, the whole disk may become unreadable.

Fixed optical media

T Optical disks hold a lot of information and often cannot be erased.

C If an optical disk does fail it should be destroyed.

T The large volumes of data held on optical disks can pose problems for backup.

C Unless optical disks hold mission-critical data not found elsewhere, they need not be duplicated or backed-up. Optical disks usually hold static information such as reference materials or software programs that are already duplicates or backups of existing data. If this is not the case and the information is mission-critical, duplicate copies can be obtained or made on write-once-read-many-times (WORM) optical disks. Copies can also be made on tape in the usual way. Modern tape backup systems can now offer reliable gigabyte backups. Normal backup strategies apply for off-site storage.

Microfilm / fiche

T Film and fiche can be easily destroyed by fire and may be lost or stolen.

C Never rely on a single fiche film copy of key data. Keep archival copies at a remote site.

Treat fiche film like registered files. Keep them stored securely and register date, time and name for issues.

People

Staff

General

T Staff may be dishonest or subjected to blackmail.

C When new staff join the organisation, make routine enquiries to ensure that their employment and educational history can be verified.
Staff with access to key information should be investigated more thoroughly to ascertain any criminal or social history that could lead them to be dishonest or subject to blackmail. Pay particular attention to financial history, involvement in subversive organisations, family circumstances, psychological history and any evidence of drug abuse / dependency. Checks should be repeated at regular intervals.
Security awareness programmes should stress the need for staff to be vigilant and stress the positive advantages of seeking help for themselves or others.

T Inadequate separation of duties makes the compromise of any one individual more damaging, may tempt staff to be dishonest and can lead to high data entry / update error rates.

C Ensure that there is adequate separation of duties between staff responsible for authorisation, data entry, receipts, bill paying, custody of financial instruments, audit, systems analysts, programmers, change control staff, access control staff and information librarians.

T Staff will be more likely to make errors or exceed their authority if accountability is inadequate.

C Ensure that your information systems provide for sufficient identification, authentication and logging for accountability to be maintained.

T Inadequate training in operational and emergency procedures is an important source of errors and system malfunctions.

C Ensure that all persons dealing with information systems receive sufficient training in operational and emergency procedures to meet the requirements of their responsibilities and duties.

T Persons in position of authority may leave authorisation of transactions in a computerised environment to clerical subordinates, in instances when they would never do so in a manual system.

C Set up adequate authorisation schemes for electronic documents. Improve the general control environment with education and programs that enhance awareness, management involvement and supervision.

Key personnel

T Key personnel who play an important role because of their duties or special skills may be absent for a long period of time.

C Consider alternative or backup personnel to replace key personnel should the need arise.

Data entry

T Data may be deleted, amended or created incorrectly.

C Software should incorporate validation checks for all key fields, identification and authentication checks.
Consider the introduction of authorisation and batching where possible.

Enquiries

T Anyone who gains enquiry rights within the system could become a source of unauthorised disclosure of information.

C Accountability and supervision are the main defence against unauthorised disclosure. The system can help by clearly marking printed output with appropriate privacy markings and ensuring that it is routed through an output control section who can log any sensitive output.

Individuals should have the minimum access rights consistent with their jobs.

Any failed access attempts should be logged and investigated by internal audit. Where 100% check is impracticable a statistical sample should be selected to ensure that testing is evenly spread over time. Internal audit or the systems audit team should undertake the checks.

Output handling

T There is a risk that output handling staff could copy output, lose it or route it to unauthorised staff / outsiders.

C All sensitive output should be routed through independent output handling sections but the staff in output handling should have no access to copiers and no rights to initiate output. Their sole role should be to record the production of sensitive output and route it to the correct recipient.

Programmers

T Programmers could compromise the controls of live information systems.

C Programmers should not have access to live information systems. Change control staff should be responsible for copying new software from the development environment to the live system.

T Programmers could introduce covert functionality into their software such as time bombs or logic bombs.

C Programming should be modularised. Each unit should be subjected to peer review to guard against the introduction of unintended functions.

T Programs may compromise the integrity or availability of information systems if they are not thoroughly tested.

C All programs should be subjected to unit testing to ensure that expected outputs result from expected inputs. Testing should be undertaken by staff independent of the programmer and should be formally documented as part of the quality control procedures. Once a unit has been tested the programmer should have no further access to it.

T Poorly documented programs can be difficult to maintain which may compromise the availability or integrity of dependent information systems.

C Documentation should be included in the quality control procedures. No unit should be passed to change control until the documentation is complete.

T Availability of information systems could be compromised if user instructions get out of step with the live information system programs.

C Completion of changes to user documentation should be a necessary prerequisite of a new unit being copied to the live system.

Analysts

T Availability and integrity may be compromised if analysts make design errors.

C Design documentation should include specifications that are intelligible to the clients. Clients should be required to sign off each stage in the design process. Prototypes may be a useful means of firming up client requirements before proceeding to a full functional design.

T Analysts have a broader perspective on the interaction of information systems than programmers. There is a risk that they might exploit their understanding to circumvent controls.

C Analysts should not have any write access to source code. They should not have access to compilers or assemblers that would enable them to develop their own applications.

Analysts should have no authority to initiate or authorise sensitive transactions.

System support

T Support staff act as custodians of information which belongs to others. There is a risk that they could initiate changes to the information or programs or produce unauthorised output.

C Support staff should not have access to compilers or assemblers that would enable them to develop their own programs. They should have no access to the source code of the live information systems.

Powerful amendment facilities are often provided by operating system vendors to directly amend programs or data. Seek advice from the vendors about utilities that can be used to circumvent system controls and store them offline. Use of system amendment utilities should require the entry of a password known only to the shift leader. The media librarian should keep note of occasions when the restricted utilities are issued. All usage of restricted utilities should be logged and the internal / systems audit staff should review the logs kept by the operations supervisor and the media librarian.

If the operating system access control package is sophisticated enough to impose access, copy and execute controls over named utilities then this mechanism can be relied upon rather than keeping the utilities offline. If this course is adopted, the internal / systems audit staff should review access rights at regular intervals and insist that privileged users have their passwords changed frequently. Every time system amendment facilities are used the execute password should be changed.

Systems Programmers

T System programmers are responsible for maintaining the operating system environment. This will include the operating system and may additionally include network management software, database management systems, transaction processing software and storage management software. The work of systems programmers is often poorly understood which may lead to poor control over their activities. Systems programmers could accidentally or deliberately destroy the entire system.

C Systems programmers should not have access to the source code or data structures of any live information systems. They should not have access to compilers or assemblers in the live environment.

The access control software should restrict systems programmers to files which they have a legitimate reason to change. All activities by systems programmers should be logged.

Systems programmers should not have any access to the access control software or data files.

All changes to operating system software should be undertaken in a development environment and should be subjected to peer review.

In the rare event that emergency changes have to be made without formal quality control the review process should take place after the event.

Change control

T Change control staff are responsible for copying programs and data from the development environment to the live environment. There is a risk that they could abuse their access to the live environment by altering live programs or data.

C Change control staff should not have access to program development tools that would enable them to compile their own programs.
Their activities should be carefully monitored by internal / systems audit staff.

Media librarian

T Media librarians are responsible for maintaining and issuing offline data and programs. If they have access to the system there is a risk that they will alter the information that they control.

C Media librarians should not have access to any software that would enable them to manipulate the contents of the media in their charge.

Logical access control

T The access control staff are responsible for maintaining user profiles which determine who has access to what. There is a risk that they will give themselves rights that are inconsistent with their functions.

C Changes to access profiles should be logged and the access control staff should be unable to switch the log off or to alter its contents.
Internal / systems audit staff should review access profiles paying particular attention to access rights of knowledgeable users and the users who have access to particularly sensitive programs / data.

Physical access control

T Security guards necessarily have access to secure areas during quiet hours. There is a risk that they will abuse the privilege.

C Security staff should have no access rights to information systems. Sensitive output should be locked away during quiet hours and all terminals logged out and switched off.

Auditors

T Auditors require extensive access to information systems and to logs. There is a danger that auditors could compromise system integrity either deliberately or accidentally.

C Auditors should not need write access to any areas other than their own. They should be given read only access to other areas on a need to know basis.

Data owners

T The owners of a set of information should be the staff who are responsible for maintaining it. Owners should be primarily responsible for the security of their own data. There is a risk that owners will abuse their privileges.

C Separation of duties within the staff comprising the owners should ensure that alteration, destruction, creation or output of sensitive information requires the co-operation of more than one person.

Data users

T Data users are given access rights to information by data owners. There is a risk that they will exceed the authority conferred on them by the owners.

C Data users should be given the minimum rights consistent with their legitimate need to access information. Access to sensitive information should be logged and any unusual patterns investigated.

Data custodians

T Data custodians are those responsible for maintaining the infrastructure which supports access to information and the security measures specified by the owners. There is a risk that they will exceed their authority by accidentally or deliberately destroying, disclosing or modifying the information in their care.

C Custodians should have minimal access rights to the information in their care. Operations staff do not need to be able to read or modify information in order to maintain access to it. They only need to know that process X requires data sets A, B and **C** which are stored on device Q. It is not necessary or desirable for them to know the details of the function of the processes they support. Special classes of custodians such as systems programmers, data administrators and network administrators may need read or write access to live data. Particularly sensitive information should be encrypted so that it is not revealed to support staff in the course of monitoring the network or maintaining the system.

It is wise to avoid employing staff in the operations area who have a knowledge of systems or applications programming. Individuals with knowledge of machine code are particularly dangerous because they could develop small programs without using an assembler or compiler.

Where possible, make it impossible for operations staff to create an executable file. This is only an option where the operating system can distinguish executable from other files and the access control system can control the ability of users to change the status of files that they create or modify.

Contractors

Maintenance

T Maintenance engineers often have an intimate knowledge of the operating system as well as the hardware. This can enable then to exploit "trap doors" to compromise security.

C Maintenance engineers should not be left to work unattended and should not be allowed to take any files containing sensitive information off site.

T Many systems have "maintenance users" with a default password. This can be used to gain unauthorised access to the system.

C Seek the vendor's advice on default users and passwords and change them regularly and, in particular, after every visit by an engineer.

Consultants

T Consultants will inevitably gain inside knowledge of your organisation.

C Consultants should be required to sign a non disclosure agreement. If they need to access particularly sensitive systems, then get them to submit to "vetting".

Change any passwords / user identities that are known to the consultant when their contract ceases.

Outsiders

Visitors

T If visitors are allowed to see areas where sensitive information or processing takes place this may compromise security.

C Visitors should be required to wear identity badges and staff should be instructed to challenge anyone whom they do not recognise or who is not wearing a badge. In secure environments visitors should be escorted at all times.

Keep visitors away from sensitive areas. If they do need to see sensitive information then require them to sign non disclosure agreements and make sure that they do not see more than is necessary.

Intruders

T Intruders can compromise information system confidentiality, integrity and availability.

C Multiple layers of security offer the best protection. Avoid publicity. Make penetration of the perimeter difficult. Install intruder detection equipment. Lock rooms that give access to sensitive facilities. Use access control to make it difficult to make use of information systems even if an intruder gains access to a terminal.

Physical

Buildings

Site

T There is a risk that the site will be physically damaged. The specific risks that affect your site will depend upon local circumstances.
C Contingency plans should be developed, which include a plan for the continuation of critical functions in the event of damage to or destruction of the site. Contingency plans should be tested annually.

T Intruders may penetrate your site which could compromise availability, integrity or confidentiality of your information systems.
C Site level physical security should be consistent with the average value of your information systems. Particularly sensitive applications can be further secured by providing higher levels of security for the locations necessary to support them. Basic site security should include security guards who monitor people entering and leaving the site. Ground floor windows should be kept locked when rooms are unattended and fitted with intruder alarms. Public parking should not be allowed in areas adjacent to critical facilities. Fire doors should open outward and be fitted with glass bolts and alarms linked to a central control panel in the security guards office.

T Sites which are used to support well publicised critical functions are particularly vulnerable.
C Keep the location of assets which support critical functions vague. Try to avoid unnecessary publicity. If the details of the site do become widely known then more extensive security measures will be required to compensate for the increased risks.

T Sites near to areas of dense population are more likely to suffer from the effects of civil disturbance.
C Key information system support sites should be situated away form conurbations if possible.

T Educational sites are particularly vulnerable to theft and attempted system penetration.
C Physical and logical access controls are often weak in educational sites. Ensure that areas which contain assets that are attractive and portable are secured to higher than base level. Accountability controls should be given a high priority for key systems accessible from educational sites.

Key rooms

Data entry / update

T Areas where information is entered or maintained are focal points for threats to the confidentiality and integrity of your information systems.

C Data entry areas should, where possible, be inaccessible to staff without a legitimate need to go there.

Terminals with access to facilities for updating critical information should not be visible from public areas. They should not be left logged in and unattended.

Applications which update key information should close down sessions where there has been no keyboard activity for more than a few minutes. Where the information has critical implications for key information systems the application should repeat identification and authentication checks at regular intervals and log all changes that are made. For particularly sensitive information, consider setting up applications so that changes cannot be finalised until confirmed by an authorising officer.

Processing

T Areas where information is processed may provide extensive opportunities to corrupt, disrupt or gain access to information systems.

C Restrict access to enforce separation of duties where possible.

T Mainframe computers often have exacting environmental requirements. This led to a natural isolation of key machines from staff who were not involved in operating them. As small machines have become more powerful so key applications have been moved onto them. Small machines can usually operate in a normal office environment. The use of distributed processing has in some cases led to information systems becoming reliant on a large number of geographically dispersed small machines. Down-sizing has led to a neglect of the need to protect key machines leaving them vulnerable to physical abuse and environmental failure.

C Machines which support key functions should be physically isolated from the general office environment.

Consider the need to protect the power supply of any machines that play an essential part in critical information systems.

Printing

T Sensitive output should be routed through secure areas so that it can be monitored and possibly logged. In the case of financial stationery material loss could arise from theft of output. Where the value of the output lies in

the need for confidentiality losses may be incurred by someone merely seeing the output without necessarily removing it.

C Access to rooms used for the output of valuable or sensitive information should be restricted to output handling staff. Physical and logical access control should enforce a separation of duties between those responsible for handling and registering output and those responsible for initiating or authorising it.

Storage

T Areas where information is stored may present an attractive target to someone trying to gain unauthorised access because a lot of information is gathered together.

C Sensitive information should be stored in secure archives / libraries. Access should be restricted to librarians who should check the clearance of staff who request access and log information which is issued.

T Reliance upon unique archived copies of information renders you vulnerable to losses of the integrity and availability of your information.

C Adopt a backup policy which ensures that at least two copies of key information are held at geographically dispersed locations. The integrity of machine readable archives should be checked at regular intervals and any magnetic media archives should be copied at least every three years.

Enquiries

T Rooms that handle enquiries are particularly vulnerable to threats which could compromise availability or integrity of the information systems.

C Consider contingency plans that would enable staff who deal with enquiries to continue to satisfy critical requirements if the information systems, or the hardware supporting them, failed.

T Rooms that are used as centres for handling enquiries may be particularly vulnerable to threats to confidentiality of information.

C Procedures should set out the conditions for providing each class of information and any need to register the issue of information. Access to areas which deal with sensitive enquiries should be restricted.

Software should automatically log off staff if there is no keyboard activity within a specified period. Accountability is an essential aspect of controlling enquiries. It can be just as important to be able to ascertain what individuals did as to restrict the activities that they can undertake.

It may reduce threats to confidentiality if enquiry facilities are physically dispersed. For example, make one group of staff responsible for answering all enquiries about individuals whose surnames began with the letters A through D and other groups responsible for other letters. Fragmenting the ability to access and collate information can reduce vulnerability to abuse.

Particularly sensitive information should require authorisation from a second operator / supervisor before it is revealed.

Enquiry terminals should be situated so that they cannot be looked over from public areas and so that operators cannot read each others' screens.

Communications

T Rooms which house network junction boxes, modem racks, telephone branch exchanges, or patch boxes provide an opportunity for unauthorised staff to identify equipment associated with sensitive facilities and disrupt the service or tap into it.

C Information systems cables and communications equipment should not be labelled in human readable form. Coded cable labels are preferable. The key to the cabling coding system should be locked away. If any cables are labelled they should all be labelled to make it more difficult to spot the route taken by key connections.

Junction boxes, modem racks and telephone exchanges should be secured. Access should be restricted to maintenance staff and network administrators.

Application live system operations

T Access to machines which are running live applications can facilitate the circumvention of measures designed to maintain the integrity, availability and confidentiality of the systems.

C Rooms which house machines which are key parts of live information systems should be accessible only to operations staff.

Separation of duties should ensure that operations staff are unable to originate transactions, design or develop programs or access sensitive output produced by the systems that they operate. The latter is made easier if secure output is possible only to devices outside of the operations area and operations staff are barred from entry to it.

Application development

T Application software is potentially the most powerful means of compromising the integrity of information systems. Programmers or others with access to the development environment can introduce covert actions into the system.

C Programmers should be assigned work on a modular basis. Each module should have defined inputs and outputs. Peer review and unit testing should guard against the introduction of covert functionality. Change control staff should be separate from application programmers both physically and managerially.

Access to rooms which are used for application development of secure systems should be limited to the programmers. Analysts and change control staff should not be allowed access.

Strict accountability controls and a strong version control system should ensure that there is always a record of who did what and when.

Development tools should be made unavailable during quiet hours.

Systems functions

T Systems diagnostics and management tools can be used to intercept network traffic and to circumvent controls.

C Access should be restricted to designated terminals and accountability controls used to monitor usage in much the same way as for application programmers. Physical access to systems terminals should be restricted to systems support staff and they should preferably work in pairs.

Plant

T Power supply is a key resource for information systems. Disruption to the power supply could destroy information and, in the case of power surges, the hardware that supports the system.

C All information system assets should have smoothed power supplies capable of eliminating harmful surges in the supply.
Key machinery such as file servers will need an uninterruptible power supply unit to ensure that they can at least close down gracefully in the event of disruption of the supply.
Access to plant rooms should be restricted to maintenance personnel.

Stationery

T Blank forms may be essential for the continued operations of some systems. Licenses and certificates are two examples. Destruction of stocks would disrupt the service.

C Backup supplies of essential forms should be held at any remote processing site and at an alternative location within the main site. Stocks should be held to the same level of security as the main stock and the storeholder should regularly check the completeness / usability of backup stocks.

Cooking / smoking

T Cooking and smoking are the main sources of information system unavailability due to fire.

C Both smoking and cooking should be banned in areas adjacent to key assets. Rooms where either are allowed should be provided with fire fighting equipment. In particular flame proof ash trays and bins should be used in rooms where smoking is allowed.

Valuable stationery

T Stationery which can be used for financial gain or as the basis for gaining rights, such as blank passes, payable orders or cheques, is an attractive target for theft.

C Sensitive stationery should be serially numbered and kept in locked storage. The storekeeper(s) should account for issues including any wastage. Endeavour to ensure that a reconciliation can be undertaken which can account for all usage in terms of authorised issues and spoilage. Store rooms holding valuable stationery should be secured and accessible only to designated accountable staff.

Documentation

Software

T Documentation is essential if software is to be maintained. There is a risk that it will be lost, destroyed or stolen. There may be a strong motivation for theft where the software performs functions which have a commercial value or disclose proprietary or sensitive information.

C Documentation should be examined as part of the quality control procedures. Once it has been approved registered copies should be filed by change control staff.

Backup copies of the documentation of the live system should be held at a remote site.

Documentation of sensitive systems should be treated like a registered file. Copies should be numbered, copying banned and issues should be on a need to know basis. Copies should be locked away when not in use.

Hardware

T Information systems assets are often both attractive, portable and easily damaged.

C A full inventory of all material information system assets should be kept, maintained and audited.

T Manuals for hardware are infrequently required but essential on the occasions that they are required. They are often difficult to replace and may contain information that would be of use to a system infiltrator.

C Keep hardware manuals in locked libraries or within secure areas. Issues of manuals should be registered especially where approval is granted to take the manual away from the room that houses the equipment. Keep copies of essential hardware manuals at a remote site.

Procedures

T Office manuals provide staff with essential information and may provide others with an undesirable insight into the way that your systems work.

C Procedures guides should be issued to named individuals, registered and kept securely. All manuals should be privacy marked on each page and sensitive manuals should have instructions on each page which make it clear that copying is not allowed.

Keep copies of procedure manuals off site.

Contingency plan

T By their nature contingency plans are needed infrequently and at a time when the organisation is under stress. There is a risk that they will become out of date or be unavailable when an emergency arises. In addition they may be of use to someone who intends to disrupt the service.

C Contingency plans should be reviewed and tested at regular intervals, every year in most situations but more frequently where availability is very critical. Copies of relevant sections should be held securely at backup sites.

Floor plans

T Floor plans are extremely useful documents for a potential intruder.

C Keep architectural drawings locked away. This is particularly important where the drawings have functional information overlaid.

Cabling diagrams

T Cabling diagrams are essential to the maintenance of networked systems. Loss could compromise the ability to maintain information systems or diagnose network faults. The diagrams are also very useful to anyone with an interest in infiltrating or disrupting the information services provided by the network.

C Network diagrams should be prepared and updated whenever a new routing or connection is introduced.

Copies of cabling diagrams should be kept at backup sites to facilitate recovery if the main site is damaged.

Access to cabling diagrams should be restricted to staff with a legitimate interest in cabling management / network administration.

Data dictionary

T The data dictionary should provide an index to the structure of all permanent information systems. It is an essential tool for the development of new information systems. It can be an invaluable aid to anyone wishing to infiltrate your information systems.

C Integrate the maintenance of the data dictionary with the change control procedures to ensure that it reflects the current structure of data held by your information systems.
Keep copies at remote sites.
Maintain a register of copies of documents which are derived from the data dictionary and treat sensitive extracts like registered files.

Environment

Air conditioning

T Large computers and their peripherals often have exacting environmental requirements. Failing to comply with the environmental conditions specified by the manufacturer may lead to machine failure and disputes over maintenance.

C Set up a regular maintenance programme for essential air conditioning equipment.
Consider the need for backup of air conditioning equipment where key assets would be affected by failure.

Power

T Information systems assets can be affected adversely by reduction or increase in the voltage or frequency of power supplies.

C All computers should be protected by surge suppressing power supplies. Key assets should be protected by uninterruptible supplies.

Water

T Some mainframe computers require supplies of cooled water. Failure of the water supply can lead to serious damage to the computer.

C Ensure that the continuation of the water supply is under the control of operations staff and not building maintenance staff. It is not unknown for maintenance staff to inadvertently switch off chilled water supplies during holiday / quiet periods. Consider backup supplies of chilled water or automatic, orderly, shutdown of dependent computers in the event of the failure of the supply.

Lighting

T Darkness can seriously disrupt plans for dealing with emergencies.

C Consider the need for backup lighting.

Waste

Paper

T Information systems often produce prodigious quantities of waste paper. This can be a source of leakage of information from the organisation.

C All paper output should be security marked as appropriate. Consider shredding material of particular sensitivity. "Confidential waste" sacks should be used for material awaiting incineration. The security of waste is often overlooked. A waste sack containing material that would have been put on a registered file should be subject to the same level of security as would have been applied to the file.

Magnetic media

T Magnetic media retain fragments of the files that have been copied to them even after the files have been erased.

C Waste magnetic media should be security erased, degaussed or destroyed.

Optical media

T Optical media cannot usually be effectively erased.
C Incineration is the best way to destroy waste optical storage devices.

Stationery

T Waste financial stationery may be used illicitly.
C Obsolete financial stationery should be formally written off and disposed of as confidential waste.
Make sure that accounting records take account of the disposal of prenumbered stationery.

Index

Appendix I - A Few Definitions

Classification of information:

Undesignated information: information not otherwise designated or classified where safeguards of normal good management practices are sufficient. Information that is publicly available. **For example:** Time Reporting, Staff Scheduling, Manuals and Publications, General Administration, released Chapters, released Positions, released Opinions, etc.

Designated information: information related to other than the national interest that is designated as needing protection.

Classified information: information related to the national interest.

Information System / Application:

"The application of specific software to complete specific work. Any set of steps followed in doing financial, administrative, or program work", for instance an Accounts Payable System.

In a microcomputer environment, applications may be very simple, such as a WordPerfect report - keying, setting format, and printing, **or** complex, a CAAT - down loading client data, extracting samples, analysing the results, and printing samples or results.

The software used, such as CAAT programs, Lotus, or WP, should not be confused with the application of the software, audit sampling or annual chapter. An application's name is usually a combination of the software used and the application developed, such as CAAT Audit Sample, Lotus Financial Analysis, WP Audit Chapter.

For security assessment purposes, similar applications may be grouped together.

"Logical" Access Control and Accountability as part of a Security System

"Logical" access control using IDs and passwords enforces restricted access to **data** on an individual user basis. This is achieved through a security system which determines what the user can access and do, and maintains **accountability** through the creation of an **audit trail** which records the user's use of the computer.

Access control, as any other control, is not considered effective and reliable unless the control can be demonstrated to be working as intended and can be monitored. An **audit trail** serves as evidence that the access control measure is working as intended and provides the means to investigate irregularities and to identify areas where controls could be improved. Within a computer security system, the **audit trail** is a history file created and protected by the system through password and encryption controls. The use of an **audit trail** is transparent to the user. Under many security systems, the security administrator has access to all users' **audit trail** history files. Individual users have read access to their own **audit trail**.

Need to Know Principle

A fundamental principle of security policy is to restrict access to **data** and **assets** to those who need such access, which involves defining the specifications of sharing the data and assets. Within a computer environment this involves physically and/or logically (Security System) controlling access to **data** and **assets**. For example, in an Audit Office, users protect client, audit and administrative **information** to keep others from accidentally reading, modifying or erasing the **information**.

Sensitivity of information:

> **Availability:** the quality or condition of information, services, systems, and programs being available in a timely manner ("at the Organisation level").
>
> **Confidentiality:** the quality or condition of being sensitive ("may cause injury if information is disclosed").
>
> **Integrity:** the quality or condition of being accurate and complete ("may cause injury if information is modified, incorrect, or incomplete").

Security Exposure Assessment

A security exposure assessment is the result of combining a business impact assessment with a threat risk/probability assessment. A security exposure assessment is rated as:

> **High:** Dramatic impact - reasonable probability. Those events that have enough probability of occurrence and such strong business impact that it is prudent to take preventive and recovery steps. The expectation of damage is high enough that you don't have to agonise over precise predictions of probability.
>
> **Medium:** Significant impact - unknown probability. The business impact is such that steps should be taken. A review of the threats and their probability is required to reduce the threats to a manageable level.
>
> **Low:** Low impact - any probability. The so-what category. If it happens, it won't hurt that much. If you feel comfortable that the potential for damage is low, these are the threats you accept. There is no need to undertake detail probability analysis.

Security Infrastructure

Typically, in many government organisations, under similar or different titles, security administration is delegated in the following manner:

- **Chief Security Officer:** A Senior Executive, who has overall responsibility for security in the organisation. He is the liaison with all other government entities and is fully accountable for all matters of security within his own organisation.

- **Director of Security:** A senior manager, with delegated authority from the Chief Security Officer, who has the day to day responsibility for the administration of all security matters within the organisation.

- **Person in charge of computer security:** A senior manager, with delegated authority from the Chief Security Officer and reporting to the Director of Security, who has the day to day responsibility for the administration of computer and technology security matters within the organisation.

- **Security Team:** A team of individuals built from as wide a cross section of the organisation as possible. The team needs the full support and commitment of senior management to perform the security review and gain the acceptance of its results. For instance, it is preferable that the user

representative be an influential member of the user community and be the team leader. Users and senior management are more likely to accept security recommendations from the team as they are usually suspicious of reports produced by "technical specialists".

A corporate security policy, approved by senior management, is put in place to support the information system strategy which, itself, is based upon the mission and objectives identified in the statement of corporate policy.

Typically also, an **I**nformation **S**ystems **S**teering **C**ommittee (**ISSC**), chaired by a senior executive, plays an important role to ensure that all information systems in the organisation are developed and used in line with corporate objectives and strategies. ISSC oversees the implementation of the information systems policy and of the security policy.

Security Management Principles

1. Security protection should be consistent with the sensitivity of the **data** being protected;

2. Security protection should remain with the **data** at all times as it is moved or processed; and

3. Security protection should be continuous in all situations.

These principles are implemented by determining **data** sensitivity from the view of integrity, confidentiality & availability and the application of specific elements of a **Security Scheme** which includes people, physical, practice & procedures, hardware, software, applications, and back up elements of protection.

Information System Security Review Methodology

A Guide for Reviewing Information System Security in Government Organisations

Volume 3 : **A Detailed Information System Security Method**

A Manual Quantitative Approach to Information System Security [9]

1. Overview

1.1 The objective of an information system security programme is to reduce the risk of loss of confidentiality, integrity and availability of information to an acceptable level.

1.2 The aim of an information system security method is to facilitate the establishment of a comprehensive, cost effective, security programme covering all key information systems. The method should assist users to establish a level of security commensurate with their requirements. Finding an appropriate level of security involves risk analysis and risk management.

1.3 **Risk analysis** is used to establish the degree to which information systems are exposed to risks. It entails examining the threats facing information systems, estimating the frequency with which they are expected to occur and then evaluating the impact that the organisation would suffer if threats do occur. "Exposure" is calculated by combining the valuation of impact and the estimated frequency of threats.

1.4 **Risk management** involves the choice of the cheapest countermeasures which reduce the organisation's exposure to risk to an acceptable level. Countermeasures are steps taken by the organisation to reduce the frequency of a threats or to reduce the impact when threats do occur.

1.5 Valuation is the key to establishing an appropriate level of security and users are the key to valuation. It follows that groups of users must be established at an early stage. Each system can be valued by reference to its users. A system with no users or one where the users place no value on the information received is worthless and should not be maintained let alone secured.

1.6 If systems faced no threats then security would not be required. The method should help identify threats to the confidentiality, integrity or availability of information systems. This involves identifying all of the

[9] Adapted from a methodology developed by the National Audit Office, UK. This document aims only at providing a general description of a detailed and quantitative risk analysis method which is used in various ways by most commercial risk analysis packages. It is strongly recommended that a microcomputer software package be used with this detailed risk analysis method.

components that must be in place if the users are to continue to receive a reliable service and then looking at events which would adversely affect each component. It also involves the identification of ways that information can leak from each component of the information system.

1.7 Once the value of a system and the threats that face it have been established a security requirement can be formulated. This will take the form of a list of measures that are necessary to reduce the risks faced by users to an acceptable level. Putting these measures in place and maintaining them is the job of the staff which make up the security infrastructure.

1.8 The stages of an information system security method are:

(1) Establish a security policy
(2) Build up the security infrastructure
(3) Identify information systems
(4) Identify threats / weaknesses
(5) Value the systems
(6) Assess the security requirement for each system
(7) Implement and maintain a security programme and procedures consistent with the security policy

2. Infrastructure

2.1 The security policy should reflect the information system strategy which should itself be based upon the mission and objectives identified in the statement of corporate policy. It is not appropriate to begin designing an information system security strategy before the corporate or information system strategy. The senior management board should devise a security policy. The policy should be endorsed by the head of the organisation. A **S**ecurity **O**fficer (**SO**) should be appointed to oversee the implementation of the security policy.

2.2 If you have, or plan to have, extensive information systems you should set up an **I**nformation **S**ystems **S**teering **C**ommittee (**ISSC**). A member of the senior management board should chair the ISSC. The role of the ISSC is to ensure that the information system strategy develops in line with corporate objectives and that the security strategy keeps up to date. You should appoint an **I**nformation **S**ystem **S**ecurity **O**fficer (**ISSO**) and consider establishing an **I**nformation **S**ystem **S**ecurity **G**roup (**ISSG**). Information system security is a speciality. The role of the security group is to act as a focus for information system security development work.

2.3 The security policy statement should provide a framework for the security programmes dealing with each major information system. Large organisations often produce security guidelines which set out security standards in great detail. The guidelines are intended to help staff translate the requirements of the security policy into a security programme for their systems.

2.4 **S**ecurity **O**perating **P**rocedures (**SOP**s) take the form of manuals which give details of the procedures necessary to support the security programme. The SOPs are particularly important as many security measures are ineffective unless staff both understand and comply with supporting procedures.

2.5 Staff training and awareness programmes are an essential part of the security infrastructure. You should include security awareness training as part of staff induction and follow this up with refresher courses at regular intervals. The use of posters, booklets and manuals can further reinforce the main elements of the security programme.

3. Boundary

3.1 The first stage in any information system security review is to establish the boundaries of the system under review. This can be achieved by identifying a community of users.

3.2 Where there is little interaction between information systems this is quite easy as users of the output from the system can be readily identified. In highly integrated systems an artificial boundary has to be agreed in order to keep the review to a reasonable scale.

3.3 It is important to gain Senior Management commitment to the review and, in particular, to ensure that they agree the boundaries of it.

3.4 Ideally you should start with a complete information model of the organisation in which the review is to take place. This should show the flow of information both within the organisation and between the organisation and others outside. This model can act as the basis for an information system security programme which will cover all key systems when completed.

4. The Team

4.1 The first manifestation of senior management commitment to information system security should be the establishment of an **I**nformation **S**ystem **S**ecurity **G**roup (**ISSG**). The security group should be responsible for the implementation of the security policy set out by senior management and identifying changes made necessary by developments in the organisation's information systems or the threats that face them.

4.2 If the findings of a review are to be accepted throughout the organisation it is important to ensure that the security team is built from as wide a cross section of the organisation as possible. This is particularly important if you are undertaking the review as an external consultant.

4.3 The internal audit team should have built up a deep understanding of the information systems within the organisation and will have a major part to play in ensuring that the security recommendations are implemented effectively. The security team may be able to use internal audit working papers to assist their understanding of the information systems in the organisation but it is unlikely that members

of the internal audit section will want to play an active role as this would compromise their independence at the review stage.

4.4 Users of an information system have a key role to play in explaining how the system works and in valuing the information gained from it. The co-operation of users is essential if the information security programme is to be implemented successfully. Users are much more likely to accept security recommendations if an influential member of the user community is a member of the team. The user representative often makes a good team leader as this reassures both senior management and users who are often deeply suspicious of reports produced by "technical specialists".

4.5 If the system is heavily computerised then a systems analyst should be included on the team to help explain how the computer system works and to advise on a clear and consistent method of documenting the flows of information.

4.6 Computer Security specialists may not be required at all if the system is simple but for complex computerised systems their help will be required both in evaluating the threats to the system and formulating countermeasures.

5. Threats / Vulnerability

5.1 The first stage in assessing the threats facing a system is to establish the chain of assets which are involved in the supply of information to each major user. Remember the information security objectives of confidentiality, integrity and availability and think of all of the points in the system where any one of these objectives could be compromised. The list of assets will be longer for a networked application than for a manual or stand alone one. A stand alone word processor will be vulnerable through the screen, printer, keyboard and via any storage device such as floppy disks, paper or tapes. A networked system may be vulnerable at many other points including terminals, printers, telecommunications equipment linked to the network, the network cabling and both central and local disks.

5.2 Create a form for each asset or group of assets that you identify and then make a list of all of the events which could compromise integrity, availability or confidentiality of information systems that are connected to the asset. For each event you will have to make an estimate of the likelihood of the event occurring in any one year. This can be very difficult if there have been no occurrences of the event in the history

of your information systems. Actuarial statistics from insurance companies may help you to make a realistic estimate of the frequency of unusual events. Whichever approach you adopt there will be an element of uncertainty. Records of past experience relate only to detected events; the security of the system may have been compromised but not detected. In addition there is no guarantee that events will occur with the same frequency that they have in the past.

5.3 The judgement of the expected frequency of events which could compromise security of your information systems plays an important part in the cost justification of measures to protect the system. If you do not gain senior management commitment to the strategy that you adopt for assessing the frequency of events you are unlikely to gain commitment to your recommendations.

5.4 If there are already measures in place to reduce the likelihood that the information system will be compromised you should note them and make an assessment of the annual cost of keeping them in place as well as the effect that they are judged to have on the frequency of events which could adversely affect the information systems. This information can be used later to decide whether the existing measures should be replaced with more effective ones.

6. Valuation

6.1 Analysis of the threats and vulnerabilities of the system results in a list of events that could adversely affect the information system. You should have agreed an expected frequency for each event. The next stage is to discuss the impact of each event with the users.

6.2 The values that users identify for the impact of each threat will be used as part of the cost justification for security measures. It is important that impacts can be expressed in monetary terms and that they are assessed on a consistent basis. Many impacts that can result from the compromise of an information system have no direct financial impact. In these cases it is necessary to construct scales which can be used to translate non financial impacts into monetary terms.

6.3 The key scale deals with financial loss and might look like the one shown below:

Loss [10]	**Points**
£10m+	10
£4m-£10m	9
£2m-£4m	8
£1m-£2m	7
£500,000-£1m	6
£250,000-£500,000	5
£100,000-£250,000	4
£50,000-£100,000	3
£10,000-£50,000	2
£1,000-£10,000	1

6.4 Another scale to apply might deal with personal safety:

Result	**Points**
Loss of 100+ lives	10
Loss of 50+ lives	9
Loss of 25+ lives	8
Loss of 10+ lives	7
Loss of 5+ lives	6
Loss of 1-5 lives	5
Loss of 1 life	4
Loss of sight or 2+ limbs	3
Loss of limb or hearing	2
Minor injury	1

6.5 The scales above are examples. Many more could be constructed such as legal liability, political embarrassment and organisational disruption. The scales that you construct should be consistent with each other and should cover all of the main impacts that could result from the loss of your information systems.

6.6 Once the scales have been agreed with Senior Management you can proceed to interview users of the information systems. You should ask them to consider the impact of each of the events identified during threat / vulnerability analysis. They may be able to identify impacts on more than one scale. Be careful to avoid double counting. If destruction of the information could lead to loss of a life and this could lead to a court case with damages of £100,000 being awarded but only £5,000 other expenses then you would score 4 on the personal safety scale, which would be equated to a mid-point value of

[10] In this document, the pound symbol (£) represents any national monetary unit. The scale ranges may need to be adapted to each country's currency and agreed levels of materiality.

£175,000 on the financial loss scale. Adding other expenses of £5000 to this figure results in a total loss in financial terms of £180,000, equivalent to a total score of 4 on the financial loss scale.

6.7 When you have interviewed the key users of the system you will have a series of scores. The scores may need to be adjusted by Senior Management if the impacts identified by the users are considered unreasonable. The score for an event can then be established by compiling a list of all of the impacts identified by the users for each event.

7. Security Requirement

7.1 The security requirement is a statement of how much it is worth spending on the protection of each asset in the system. This is derived from the valuation and frequency assessments for each adverse event. The user valuations should be converted to monetary values by using the mid points of the financial scale. Frequencies should be expressed in terms of the number of times that the event is expected to occur in any one year. This will be less than one where an event is rare. Collect together all of the impacts identified by users for each event and exclude any duplicates. If you then add the financial values of the impacts and multiply by the frequency of the event this will give the **A**nnual **L**oss **E**xpectancy (**ALE**) for one particular event affecting one particular asset.

7.2 The calculation of ALE has to be repeated for each event that could significantly adversely affect each asset that is connected to each of the information systems under review. When this job has been completed the assets can be sorted by ALE. The sorted list should form the basis for an action plan to develop the security programme.

8. Countermeasures

8.1 The security requirement will highlight assets that represent a significant risk to the confidentiality, integrity or availability of the information systems under review. Countermeasures are steps taken to reduce the frequency of threats to information system assets or the impact when the threats occur.

8.2 You should begin by installing countermeasures to protect the assets with the greatest ALE. Consider steps that could be taken to reduce the frequency or impact of events that would have the greatest impact. Find out their costs including any training, maintenance and

disruption that they would cause. Once you have evaluated the measures that could be introduced consider the reduction in ALE that they would be expected to achieve.

8.3 A single countermeasure, such as the introduction of a security guard at the entrance to the site, may reduce the ALE associated with many events affecting many assets. You will need to make sure that all of the benefits of the measure are reflected in the case for introducing each measure. For each countermeasure keep an **impact list** of the events / assets whose ALEs are affected and the magnitude of the expected change.

8.4 Once you have identified countermeasures that would reduce the largest ALE to the level of the next largest ALE you should switch your attention to the next event / asset in the list.

8.5 Each time you select a countermeasure you will have to adjust the ALEs of any other events / assets which are affected by the countermeasure. As you move down the list the remaining ALEs will get smaller. You should stop when the remaining ALEs are below the threshold that you think management will accept.

8.6 Recommendations to management should highlight those countermeasures which yield the greatest reduction in ALE at the least cost. Management may decide to accept the risk of any event affecting any asset in the information system but they should do this explicitly in the light of ALE analysis so that they are aware of the magnitude of the risks that they are accepting. If management do decide not to install a countermeasure then you will have to readjust the list of ALEs using the impact list for the countermeasure.

9. Security Administration

9.1 Once a list of countermeasures has been agreed these will have to be carried forward into the security programmes and the security operational procedures. The information system security group should be responsible for implementing the selected countermeasures.

9.2 Internal audit should review the risk assessment and risk management working papers and monitor the implementation and effectiveness of the countermeasures selected.

9.3 The security programme and procedures will need to be updated to take account of changes in the security environment and the information systems. The information system security group should keep themselves informed of developments in information system security and be informed of all significant developments in the organisation's information systems. They should continuously monitor the need for updating the security programme.

Security Risk Terminology [11]

- **Countermeasure (C):** A control which is designed to enhance security by either reducing the threat, reducing the impact, detecting a security breach or recovering from a security incident.

  Synonyms: Safeguard, security measure.

- **Impact:** The adverse effect or consequence of a threat occurring.

- **Probability:** The likelihood of a particular threat occurring.

- **Risk / Exposure:** A measure of the probability and magnitude of the impact of a particular threat on an information system. It is a function of a threat occurring and the possible loss that may result.

- **Risk Assessment:** A formal process to evaluate the chance of vulnerabilities being exploited, based on the effectiveness of existing or proposed security safeguards.

- **Threat (T):** Any potential event or act that is unwanted and can impact on an information system, such as a fire, natural disaster, unauthorised access, etc.

- **Vulnerability:** A measure of the likelihood of an asset succumbing to or being attacked by a particular threat.

[11] Security risk terminology may vary very much between different schools of thought. Similarly, depending on the methodology used, impacts and vulnerabilities may be assessed in the presence of existing safeguards or in the absence of any safeguard.