New Zealand Security of Information Technology Publication 104

RISK ANALYSIS OF GOVERNMENT COMPUTER SYSTEMS

CHAPTER 1

INTRODUCTION

The Need for Risk Analysis

101. Until the 1960s, most Government departments and agencies relied on well-established paper-based information systems and were familiar with the management of the associated risks. The confidentiality of information was provided by secure storage and availability was inherent in hard-copy systems. Integrity, if and when required, was managed through procedural controls such as spot checks and cross-referencing.

102. The high cost and stringent environmental requirements of early computer systems dictated that purpose-built, centralised facilities be established. The threats to information processed in these systems were easily recognised and managed, and an adequate measure of availability, confidentiality, and integrity could be assured through control mechanisms quite similar to those used in manual systems. New risks arising from equipment malfunction, operator error, and programming errors were evident but were easily countered. The architecture of mainframe systems provided adequate separation between the operating system and active applications, and, when remote terminal access became possible, additional software was incorporated to ensure that only authorised users could gain system access.

103. Modern computers do not require specialised environmental facilities, but their effective management does require new techniques. Microcomputers were initially designed as single user systems and did not incorporate the security measures provided in mainframes. They now, however, in many instances hold more information than early mainframe systems. Their use for decentralised processing of official information gives rise to a number of problems in the management of information security. Security is no longer the concern of Operations Management but is, in the more contemporary information systems, the responsibility of microcomputer users and LAN administrators.

104. The availability of cost-effective private and public networking facilities has encouraged the distribution of information processing. Microcomputers are commonly connected to servers on local area networks (LANs) and use wide area networks (WANs) to access remote facilities. The growth in network use has been accompanied by the introduction of network applications such as bulletin boards, electronic mail, and file transfer.

105. Increasingly, departments are obtaining information electronically from a variety of external sources, and providing their information electronically to

other departments. Information is increasingly at risk in this environment of diversified security responsibility, distributed processing, and widespread information exchange.

106. NZSIT103: *Security Evaluation Criteria* sets a security baseline for the protection of information systems, based on expected levels of risk. While appropriate in many applications, there are occasions where more focused protection is needed. Such protection can only be determined through detailed and formal analysis to identify specific risks. The function of this document is to provide Government IT managers with a common and structured methodology for the assessment of risks to departmental information systems.

Components of Risk

107. There are six principal components to be considered in risk analysis:

a. Assets. An asset is any item which may require protection, and may be tangible (premises, equipment) or intangible (information, goodwill).

b. Vulnerability . Vulnerability is an inherent weakness of an asset which may be exploited in an attack.

c. Safeguards . Safeguards are those system components and procedures which reduce vulnerabilities.

d. Threats . A threat is an event or a group of like events which may damage one or more assets.

e. Impact . Impact is an assessment of the level of damage that would be caused by a threat event (accident or attack) occurring.

108. The relationship between the components of risk is shown at Figure 1, which is based on the model of risk initially developed by Robin Moses of BIS Applied Systems.

Definition of Risk Analysis

109. Risk analysis is the process of formally identifying the assets incorporated in or associated with a computer system, the threats which may affect those assets, and the system's vulnerabilities, in order to assess the level of damage expected to the confidentiality, integrity, and availability of the information processed by the system.

Overview of Risk Analysis Methodology

110. There are six distinct phases in a risk analysis as follows:

a. Scoping. The Scoping phase is carried out to identify the boundaries of the system to be analysed, and establish the schedule for the risk analysis.

b. Information Gathering. The Information Gathering phase involves collecting details of the system, environment, and information processed through a series of interviews and analysis of available documentation.

c. Modelling. The Modelling phase is subdivided into:

(i). Information Modelling during which the nature and flows of information are documented;

(ii). Architecture Modelling to describe the physical equipment and communication links which support the information system; and

(iii). Valuation of the various tangible and intangible assets.

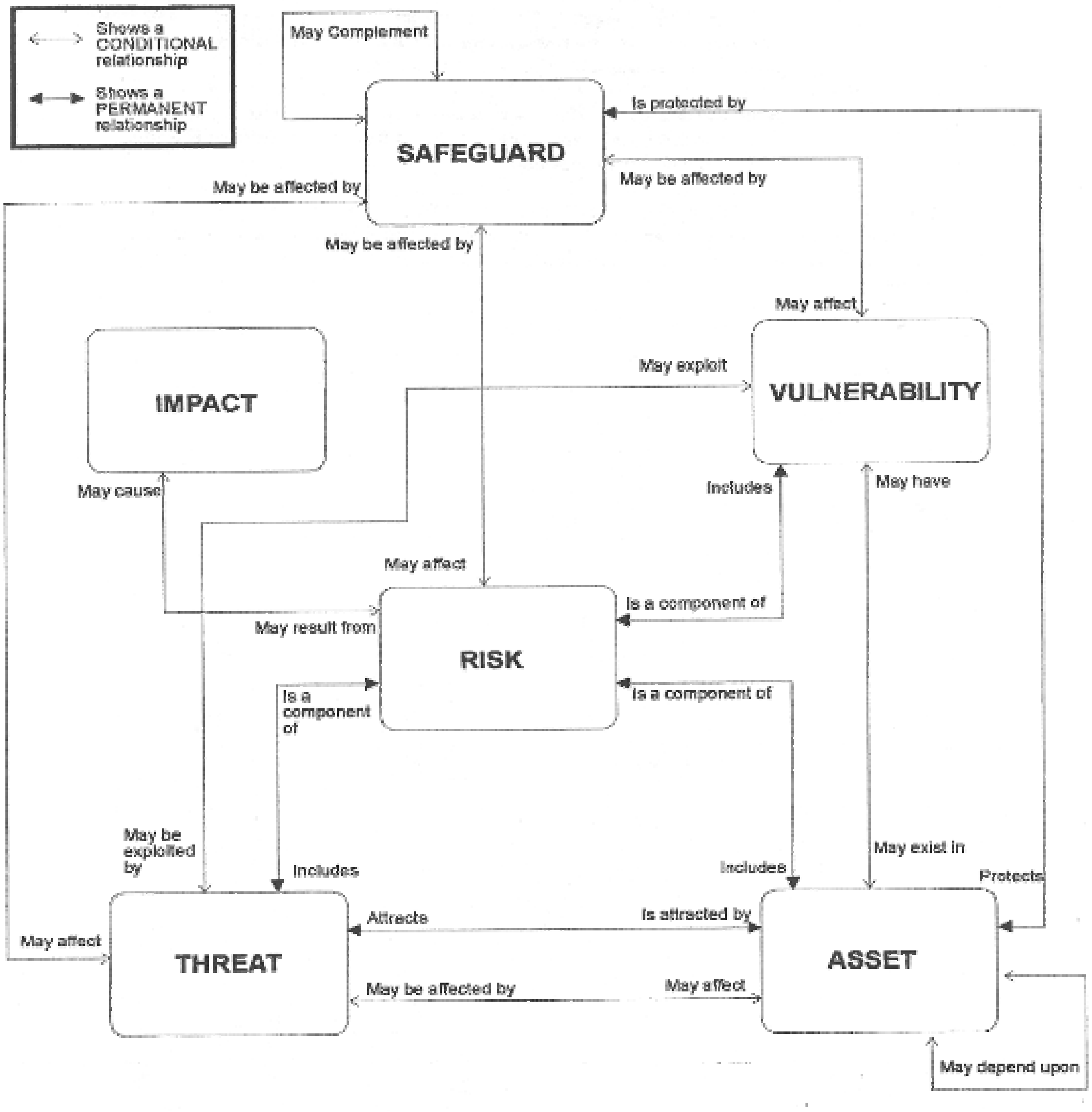

Figure 1: Components of Risk ('Moses' Model)

d. Threat Assessment. The Threat Assessment phase involves a review of threats to the system by considering the environment, information or physical assets, and potential attackers.

e. Vulnerability Analysis . The Vulnerability Analysis phase identifies information flows in the system and assesses weaknesses and any protection provided by existing safeguards.

f. Risk Assessment. The Risk Assessment phase is the part of the analysis where risk levels are calculated from the results of the threat and vulnerability assessments.

111. The risk assessment may establish a requirement for detailed security reviews of specific areas of the system. Where additional countermeasures are considered necessary to address identified risks, a Risk Management Plan may be required.

CHAPTER 2

SCOPING THE RISK ANALYSIS

Introduction

201. Scoping, the first step in a risk analysis project, identifies the boundaries of the system to be reviewed, defines the specific aspects of information security which are to be considered, and establishes a project timescale.

202. Scoping will normally be conducted through an initial interview with the project Sponsor. The Sponsor is the person for whom the analysis is being conducted, and to whom the final report will be submitted. It is essential that the scope of the analysis be formally agreed between the Sponsor and the Risk Analyst.

203. The analyst should seek in the scoping interview to determine the boundaries of the analysis, identify those areas which are of particular concern to the Sponsor and those which are to be excluded from the analysis. It is useful during scoping for the analyst to identify and obtain any previous audit or security-related reports. The Sponsor should be able to identify key personnel to be interviewed during the Information Gathering phase of the analysis.

Scoping Report Contents

204. A scoping report should be drawn up and formally agreed at the completion of the scoping exercise. The report should fully define the systems to be reviewed, the expected deliverables, and the timetable for completion. It should contain the following sections:

a. **References.** All documentary material referenced during scoping, typically correspondence and earlier reports, should be identified.

b. **Background.** The activities and events leading up to the analysis, including previous correspondence and any earlier project work, should be described.

c. **Objectives.** The specific objectives of the risk analysis should be clearly and concisely stated.

d. **System Description.** This section should briefly describe each computer system to be included in the risk analysis, and those which are to be excluded.

e. **Timetable.** A tentative timetable should be developed identifying proposed completion dates for the ensuing phases of the analysis, namely:

(i). information gathering;

(ii). information and system modelling;

(iii). model analysis; and

(iv). reporting.

f. **Personnel.** The report should identify those persons who are to be involved in the Risk Analysis, including:

(i). the Sponsor;

(ii). the analyst(s); and

(iii). personnel to be interviewed, e.g. information custodians, principal users, and key IT management and development staff.

g. **Visits.** A plan of site visits should be included where these are contemplated.

h. **Deliverables.** Tangible outputs of the analysis should be specified, typically:

(i). an information flow model;

(ii). a systems architecture model; and

(iii). the risk analysis report.

205. It is important that the contents of the scoping report are formally agreed. A signature block should be included for this purpose.

CHAPTER 3

INFORMATION GATHERING

Introduction

301. The purpose of the Information Gathering phase is to provide the raw material for the subsequent modelling of system architectures and data flows. Information may be gathered through interviews, system demonstrations,

previous security-related reports, departmental policies, and system design documentation.

302. The Information Gathering and Modelling phases overlap to some extent. The need for further or more detailed information will often become evident during modelling, and models may change throughout the analysis as new information is received. However, it is essential to acquire as much information as possible during the initial interviews to maximise the effectiveness of the modelling process and minimise any disruption of departmental activities.

Interviews

303. The formal Information Gathering process requires structured interviews during which the characteristics of each information system are established, and the significance of the information being processed is determined in terms of departmental objectives, policies, and requirements. Relationships between various departmental systems and between the department and external organisations should be identified in order to facilitate modelling of processing domains and information flows.

304. Interview planning will help to ensure that interviews are effective. It may be appropriate to arrange for a checklist of specific topics to be provided to interview subjects prior to interviews. Typical areas to be discussed during interviews are outlined below, and the checklists at Annex A may be useful in guiding the interview process. It is strongly recommended that interview notes are formally written up and retained as part of the analysis documentation.

Departmental Overview

305. The boundaries of the information systems under review need to be defined so that the high level flow of information into and out of the department can be determined. External entities, organisations, and systems should be identified and their role in relation to the department described. The physical and logical links to these entities should be determined and the data flows across them detailed. The information gained during this process should be sufficiently comprehensive to gain a complete understanding of the major information processes covered by the scope of the analysis, the external and internal information flows, and the computer systems and networks which process departmental information. Information gained during this phase will be used for high-level data flow and systems architecture modelling.

Security Domains

306. During the Information Gathering phase, the analyst must gain a clear understanding of the security domains within a department. A security domain is a location or set of locations operating under a common security regime. It may be physically delimited (for example a building) or logically delimited (for example, a group of systems handling information at the same level or subject to a common security policy). A security domain will typically contain one or more information systems, and may have external links to other domains. Security domains form the environment within which information exists and define the boundaries across which information flows.

Information Systems

307. Each information system within the scope of the analysis should be analysed. Information managed in each system should be reviewed and the following information obtained:

a. the owner and custodian of the data;

b. the classification of the data;

c. the relationship between data entities, and between data entities and processes;

d. the form in which information is held and transmitted; and

e. the paths over which the data flows.

308. For automated information systems, the following system configuration details need to be determined:

a. the hardware supporting the system;

b. the operating system supporting the applications programs;

c. the applications programs;

d. the subsystems supporting access control and security processes; and

e. any security measures incorporated within the applications programs.

309. All data communications systems within the scope of the analysis or which are used to connect automated information systems within the scope of the analysis should be reviewed to determine:

a. the network topology and location;

b. the ownership of the network;

c. the software used to access the network;

d. the protocols used;

e. the use of dial-in and remote diagnostic or operating facilities;

f. any protective measures employed; and

g. the presence of network applications such as electronic mail and file transfer.

Personnel

310. Key personnel information which is of significance to the risk analysis includes:

a. employee security clearance and reference checking policies; and

b. use of employee agreements to define responsibility for computer user codes or information protection.

Policies and Procedures

311. Departmental security policies are of fundamental significance to the risk analysis. These may be explicitly expressed as formal departmental policy statements or may be embodied in legislation relevant to a department.

312. In many cases, procedures include security relevant actions. A careful review of all procedures may therefore be necessary to identify those relevant to security.

313. Departmental security marking procedures are particularly relevant, and should be reviewed to ascertain:

a. the definition of any information sensitivity grading systems employed;

b. the rules and procedures for marking hard copy documents;

c. any protection afforded to documents at various levels of sensitivity; and

d. the nature of any security marking schemes implemented.

System Demonstrations

314. A demonstration of the various aspects of the system is often useful to consolidate information obtained through interviews, and identify aspects of the system not covered in the interviews. This is particularly useful to gain an understanding of the operation of the security subsystem. Demonstrations may be provided at interview, or on a separate visit or visits.

CHAPTER 4

MODELLING

Introduction

401. The modelling phase of the risk analysis should incorporate **Information Modelling** during which the nature and flows of information are documented, **Architecture Modelling** during which the physical equipment and communication links which support an information system are described, and **Asset Valuation** during which the value or significance of assets is assessed.

402. In the modelling process, the analyst consolidates and records information acquired during the Information Gathering phase. Key characteristics of departmental and external information systems and information flows can be represented effectively in diagrammatic form.

403. The object of modelling a system is to record, in an easily understood format, the domains and component parts of a departmental system, and the channels (logical or physical links) through which information is exchanged between domains. There are two main diagramming techniques used during risk analysis: Data Flow Diagrams (DFDs) and System Architecture Diagrams (SADs). DFDs can be used to show the logical relationship of information and the processes and entities which create and use it. SADs describe the computer and network architectures which support the information processes and flows. Once completed, the models should be reviewed by departmental staff to verify their accuracy and completeness. The validated models can then be used during the risk assessment phase to assist in the identification of areas where information may be at risk.

Information Modelling

404. DFDs represent information flows and stores, processes, and entities which provide or make use of information. DFDs are not concerned with the sequence in which processes take place within an information processing system. A sample DFD is shown at Annex B, Figure 1.

405. DFDs use combinations and repetitions of the following basic symbols:

a. **Entity**. An entity symbol represents an information provider or consumer. The symbol is usually annotated with the entity name but may also show other attributes such as the entity's security clearance.

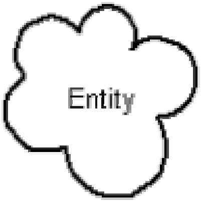

Figure 1: DFD Entity symbol.

b. **Process**. The process symbol is used to describe any manual or automated function which takes information in and/or produces information outputs. The symbol is annotated with the process name and, if automated, the location or host system identifier. An optional process number (n) may be shown.

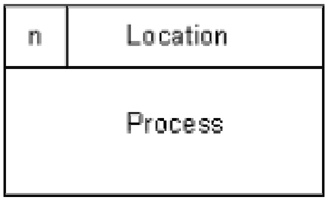

Figure 2: DFD Process symbol.

c. **Information Store**. An information store may be a manual store such as a registry or, more typically, a computer file or database. The symbol should show the information name and may be further annotated with significant information attributes such as sensitivity, classification, and value. An optional information store number (d) may be shown.

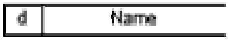

Figure 3: DFD Information Store symbol.

d. **Information Flow**. Information can flow between entities and processes, between two processes, and between processes and information stores. The information flow symbol connects the source and destination points and shows the direction of information flow. Solid lines are used to represent electronic data flows, and dotted lines to indicate manual data exchange.

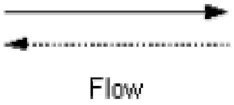

Figure 4: DFD Information Flow symbol.

Architecture Modelling

406. SADs are used to show the type and location of equipment within security domains and the hardware which supports the storage, processing, and transmission of information. SADs may also show information sensitivity or classification and any related protective measures. Premises, processing equipment, peripheral devices, and network connections may be included in these diagrams. A sample SAD is given at Annex B, Figure 2.

407. There is no standard for system architecture diagram symbols. Icon-style symbols can be used to provide a clear representation of items, and minor variations in the symbol will allow different categories of items to be distinguished.

408. Modelling should adopt a top-down approach starting with security domains, and providing an increasing level of detail down to specific information assets. The diagrams should be developed in an electronic form where possible to allow additional material to be included throughout the risk analysis.

409. The top level of modelling will show the department as a single entity with links to external organisations. The attributes of the external links, particularly the nature and sensitivity of the information moving across them, are also modelled at this level.

410. The second level of modelling will identify the relevant security domains within the department. A domain may be delimited physically, for example, a self-contained processing centre; or logically, such as all remote users. At this level, links between domains, and any links into or out of a domain, are shown. Each link may be annotated with the information flow it supports, referenced back to the DFDs.

411. A third level model is developed for each security domain identified at the second level. A domain may contain entities such as IT equipment and personnel. All entities within a security domain, by definition, are subject to a common security policy. Links between systems within the domain and paths over which information is transferred in or out of the domain should also be shown. It may be necessary, depending on the scale of the system, to show the relationships between individual equipment items (as, for example, in the case of a LAN). Alternatively, it may be acceptable to model only a single typical or notional item to represent all such items collectively. Various entity attributes will be associated at this level: equipment value, software assurance, hardware reliability, personnel clearance levels, and information access rights. Security containers such as safes, cabinets, and vaults should also be shown.

412. A fourth level diagram is required for each security container or computer storage subsystem shown at the third level. Each fourth level diagram describes the individual information stores located within the computer storage subsystem, or the hard copy or media stored within each

security container. Associated with each information store are its classification and value. Figures 3a to 3d in Annex B show an example of a four-level model.

Asset Valuation

413. Assets are the various tangible and intangible components of an information system. These may include:

a. premises and plant;

b. hardware, peripherals, and ancillary equipment;

c. storage media;

d. software; and

e. information.

414. An assessment of each asset's value is an important part of the modelling phase. Asset values identify the relative importance of model components and allow the cost-effectiveness of a proposed or existing countermeasure to be calculated. Where assets are tangible (e.g. computer hardware, commercial software packages) it is easy to assign a book or depreciated value, or a replacement cost. This value can then be input to an Annualised Loss Expectancy formula to enable the cost-effectiveness of a particular countermeasure to be determined. The valuation process is more difficult where the asset is intangible. Departmental information is an intangible asset and may constitute an investment more valuable than the system within which it is processed.

415. While the classification of information is well understood, its value is difficult to ascertain and may be highly variable. Information may be rendered obsolete within a short time, or it may retain a value indefinitely. It may lose value through being copied or corrupted, or gain value through association with other information.

Valuation Options

416. It is necessary for risk analysis purposes to assign at least a notional value to information assets. The following options may be used individually or in combination:

a. **Cost of Collection.** This considers the original cost to the department of acquiring, entering, and validating a body of information. In some cases information may have been purchased, in which case a direct dollar value can be assigned. The cost of collection may be discounted by any perceived depreciation in the value of the information since it was initially collected.

b. **Cost of Restoration.** This approach assesses the cost to restore a given unit of information if it were to be corrupted or rendered unavailable. Where tested backup and restoration procedures are in place this may be a relatively small cost, but where such measures are weak or absent the cost may be considerably higher. The valuation should take into account the availability of the original information, and whether it would be necessary to recreate some or all if it were to be lost or corrupted.

c. **Unavailability Cost.** The cost to the department is estimated in terms of lost opportunity if the information were to be unavailable for an extended period.

d. **Embarrassment Cost.** As its name suggests, this approach assesses the potential damage to the department arising from legal actions, complaints to Members of Parliament, approaches to the Ombudsman, and the like. The embarrassment cost will vary depending on the nature of the department's activities and the sensitivity of the information handled. As a dollar value may not be easily derived, it may be necessary to categorise value on a scale from 'very low' to 'very high' for the purposes of the risk analysis.

e. **Legal Damages.** Disclosure of information may result in a financial penalty to an individual, or the imposition of damages or fines upon a department or its personnel. This may occur as a result of negligence or breach of statutory requirements. The cost of legal damages may include any legal costs incurred in defending such an action whatever the outcome or verdict.

f. **Classification.** Classification of information represents a form of value, but is expressed in terms of the impact on national interests if information passes into unauthorised hands, rather than a financial value. Classified information generally requires a specific level of protection rather than a risk based assessment.

Information Classification

417. The requirements for information confidentiality, availability, and integrity of each conceptual group of information must be assessed so that the importance and potential impacts from loss or damage can be estimated.

418. For confidentiality requirements *Security in Government Departments* (SIGD) defines nationally recognised classification labels and the protection requirements of them. (SIGD is produced by the Interdepartmental Committee on Security and is available from The Department of the Prime Minister and Cabinet.) To simplify the risk modelling and security management processes specific departmental classifications or handling caveats may also be defined to further group sensitive or critical information in regards to its protection requirements.

Application of Value to DFDs and SADs

419. Values may be annotated on the DFD or architecture diagrams. An asset valuation report could then be produced listing significant assets and, for each, a dollar value and an assessment of its significance to the organisation.

CHAPTER 5

THREAT ANALYSIS

Introduction

501. The risk of a security-relevant event occurring in an information system is determined by considering each of the threats to the information, and the vulnerabilities of the information technology used to support the system. This chapter describes how to analyse the various threats to an information system as the first phase in this risk assessment process.

502. Information systems are at threat from events that may affect the confidentiality, availability, or integrity of their information. The threats to availability have traditionally been covered through contingency planning procedures, while security procedures have focused primarily on confidentiality. Contemporary risk analysis can often require an assessment of risks in all three areas.

Accidents

503. The threats to departmental information can be considered as either deliberate or accidental. Accidents such as human error (including negligence), system error, and environmental disasters may result in disclosure of sensitive information, its unavailability, or its corruption. The impact of such incidents affecting departmental information may be as great as that of an attack. However, reducing the risk of accidents has traditionally been addressed through contingency planning procedures and is essentially a management issue. Inclusion of such threats in a risk analysis is entirely at the discretion of each department.

Deliberate Threats

504. A threat analysis should be carried out for each potential attack on the information system. Likely attackers and methods, specific targets and their attractiveness, and the potential impact of an attack or attacks should be taken into account during the analysis.

The Analysis Process

505. Threat analysis involves three steps: collation, refinement, and assessment.

506. **Collation**. The first step in the threat analysis is the development of a list of all threats that are relevant to the information technology used by the information system under consideration. A standard list including the most common attacks is given at Annex C as an initial threat list for any analysis.

507. **Refinement**. The threat list is then refined by considering the motivation, resources, and skills of each category of attacker. The type of information being processed and its value to the attacker will determine motivation. The kind of attack will determine the level of resource and skill needed by an attacker. The main categories of attackers considered for the purpose of risk analysis are:

a. foreign state-funded intelligence services,

b. business and organised crime,

c. news media and lobby groups, and

d. individuals acting alone.

508. Assessment. The assessment step considers, for each threat on the refined threat list, the opportunity an attacker has to access the system, by considering the physical location of the system, the building security measures (defined as the *Grade of Site* in the publication *Security in Government Departments*), and the opportunity for electronic access to the system.

509. The GCSB can provide on request standard threat levels for a range of different information categories and attacks, and can assist in defining threat levels for specific attack scenarios not covered in the standard threat list.

Threat Levels

510. The threat assessment should result in one of the following five threat levels:

a. **VERY LOW**. An attack is unlikely to occur.

b. **LOW**. Random subversion or attacks employing a low levels of expertise and resource are likely to occur.

c. **MEDIUM**. Attacks are likely to be limited by attacker expertise, resources, or opportunity.

d. **HIGH**. Frequent attacks, or attacks involving high levels of expertise, resources, and support, are likely to be mounted.

e. **VERY HIGH**. Continuous or intensive attacks are likely, and specialised security advice should be sought.

511. An example of threat assessment is included at Annex D.

CHAPTER 6

VULNERABILITY AND RISK ASSESSMENT

Introduction

601. As discussed in the previous section, the risk of a security-relevant event occurring in an information system is determined by considering each of the threats to the information and the vulnerabilities of the information technology used to support the system. Risk analysis is not a precise science and contains a substantial element of subjective judgement. The Bureau can provide expertise on request to support departmental risk analysis efforts.

602. The risks can then be ranked in priority order by factoring in the impact should the specific event be realised. This chapter describes how to assess the vulnerabilities and rank the resulting risks to an information system. For convenience, the risk assessments should be grouped under the following broad headings:

a. Physical Security and Technical Security;

b. Personnel Security and Procedural Security;

c. Compromising Emanations (TEMPEST);

d. Transmission Security;

e. Computer Systems Security; and

f. Media Security.

Vulnerability Assessment

603. The vulnerability assessment is a subjective process of identifying any means, or vulnerabilities, by which each of the threats to the information system could be realised. Vulnerabilities result from both technical deficiencies, faulty procedures, and human fallibilities.

604. All known vulnerabilities of system components should be included in the assessment. These may be determined by local or external evidence of successful attack, as in the case of hacking or viruses. A range of vulnerabilities will also often be known to specialist departmental IT staff, particularly systems programmers, and should have been identified during interviews. As well as identifying known technical vulnerabilities, security procedures should be critically reviewed to identify potential loopholes. Documented cases of security breaches should also be reviewed to ensure that adequate countermeasures have been implemented. The GCSB holds information on system vulnerabilities which can be provided to departmental staff on request.

605. All existing countermeasures which may reduce the identified vulnerabilities should be included in the vulnerability assessment. A subjective assessment of the residual vulnerability should be made based on the identified vulnerabilities and the likely effectiveness of any countermeasures.

606. The vulnerability assessment should result for each threat in one of the following assessed vulnerability levels:

a. **VERY LOW**. There are no residual vulnerabilities that could be exploited by the most intensive attack.

b. **LOW**. Residual vulnerabilities have been identified, but would require a high level of resource and skill for any attack to succeed.

c. **MEDIUM**. Attackers with moderate levels of resource and skill could be expected to exploit the identified vulnerabilities.

d. **HIGH**. A limited opportunity and little specialised knowledge would be needed to succeed in an attack. For instance, a system connected to the Internet would normally be considered to have a HIGH vulnerability, unless rigorous security countermeasures are in place.

e. **VERY HIGH**. The system could be successfully attacked at any time. For example, plain text on a communications line is always rated as a VERY HIGH vulnerability.

Risk Assessment

607. The risk assessment can be carried out once the threat has been assessed and the system's vulnerabilities analysed. The risk assessment indicates the likelihood of someone attacking (a realised threat) and being able to penetrate (an exploited vulnerability) the system. If there are no potential attackers, none of the system's vulnerabilities constitute a risk; if there are no vulnerabilities, potential attackers do not constitute a risk. Where there is both a vulnerability and a threat, the risk level is normally calculated by selecting the lower of the threat and residual vulnerability levels. This assessment may need to be adjusted after subjective, expert review.

608. For example, consider an information system which is under a VERY HIGH threat of communications interception. The information is transmitted in encrypted form and the residual vulnerability is therefore considered to be VERY LOW. The assessment should indicate a VERY LOW risk of information compromise through communications interception.

609. The resulting risk levels can then be ranked according to their priority for countermeasure implementation. The ranking is made on the basis of the following impact levels:

a. **Serious Impact**. If a successful attack would result in serious impact to the Government or the Departmental mission, the countermeasure priority will be one step higher then the risk level. Thus a risk level of MEDIUM would result in a HIGH countermeasure priority.

b. **Significant Impact**. If a successful attack would result in some impact on a major Departmental operation, cause Departmental embarrassment, or result in substantial financial gain for any commercial organisation, the countermeasure priority will be the same as the risk level.

c. **Minimal Impact**. If a successful attack would cause some impact on the Department or result in minor financial gain for any commercial organisation, the countermeasure priority will be one step less than the risk level.

610. The actual order of countermeasure implementation is further discussed in Chapter 7, and depends on many factors including the cost of countermeasures. Nevertheless, the countermeasure priorities resulting from the risk assessment can be interpreted in the following way:

a. **VERY HIGH**. Risks in this category have a high probability of occurrence, are potentially highly damaging, and existing countermeasures are inadequate. Action should be taken immediately to counter the associated attack.

b. **HIGH**. Risks in this category are slightly less significant than the highest priority risks, and but action should be taken at an early opportunity to counter the associated attacks.

c. **MEDIUM**. Risks at this level indicate that routine corrective action should be scheduled.

d. **LOW**. A LOW level of countermeasure priority suggests that action may be desirable when convenient.

e. **VERY LOW**. VERY LOW countermeasure priorities should not be discounted entirely but require no further action.

611. A worked example of vulnerability and risk assessment is included in the example risk analysis at Annex D.

CHAPTER 7

RISK MANAGEMENT

Introduction

701. Once the risk analysis has been carried out, a Risk Management Plan may be developed to identify and schedule the implementation of countermeasures to avoid or transfer risk.

Countermeasures

702. A countermeasure is a process, procedure, or device which reduces risk. It may reduce the vulnerability of an asset, make a particular attack less probable, or minimise the impact of a realised threat.

703. There are four major countermeasure types:

a. **Hardware**. Some risks can be countered by the use of additional hardware such as link encryption devices, mirrored disk drives, and plug-in security subsystems. The *NZCSIM 402 Part 2: Evaluated Information System Security Products* includes hardware security products approved for Government use.

b. **Software**. A range of software countermeasures can be used to reduce the risks in computer systems. These include application security and controls, and access control subsystems or extensions to an operating system. A set of pre-defined countermeasure standards are detailed in the *NZSIT 103: Security Evaluation Criteria for Government Computer Systems* and the *NZCSIM 402 Part 2: Evaluated Information System Security Products* includes the software security products approved for Government use.

c. **Physical**. Physical countermeasures such as safes, locks, security guards and intruder detection systems can be used to reduce the need for computer security countermeasures.

d. **Procedural**. Procedural countermeasures may be appropriate where risk areas cannot be addressed through physical or computer security countermeasures.

Types of Risk Management

704. There are a number of ways in which risk can be managed:

a. **Risk Avoidance**. Risk may be avoided by eliminating or relocating an asset. For example, a decision may be made to discontinue processing a particular class of information on a system.

b. **Transfer of Risk**. Risk may be transferred where an asset is moved to a different security domain. For example, processing may be moved to a different site or outsourced. Insurance is both a transfer of financial risk and an impact reduction measure.

c. **Reduction of Vulnerability**. Countermeasures to reduce vulnerability can be viewed as barriers which increase the effort an attacker would have to expend to achieve a successful attack. In the case of risks arising from error, negligence, or accident vulnerabilities may be reduced by countermeasures such as improved staff training.

d. **Reduction of Impact**. It may be cost-effective to accept a certain level of risk where the impact of an incident can be reduced, for example through insurance. Countermeasures may reduce impact by reducing the cost of recovery through, for example, disaster recovery planning.

e. **Detection**. Detection countermeasures may reduce risk or facilitate the early detection of an incident and therefore reduce its impact. Examples include error logs, access control logs or journals, and recordings from security cameras.

Selection of Countermeasures

705. The most effective set of countermeasures should be selected, taking into account:

a. the need to achieve a balance between minimisation of risk and minimisation of impact on productivity;

b. the cost of each countermeasure against the potential loss arising from an incident;

c. any existing countermeasures; and

d. applicable constraints.

Constraints

706. There are a number of possible constraints which may affect the acceptability of a particular proposed countermeasure and which should be considered before a countermeasure is recommended:

a. **Organisational**. A countermeasure may be technically excellent but inappropriate due to the way a department works.

b. **Financial**. Implementation of a countermeasure, for example a PC security package, may be desirable but impracticable due to budgetary constraints.

c. **Environmental**. For example, Halon gas fire control systems may be an effective option for protection of computer equipment, but may not be environmentally acceptable.

d. **Personnel**. For example, hidden surveillance cameras might be considered an excellent measure for prevention of theft by employees, but staff may object.

e. **Time**. Countermeasures may be urgently required but rendered infeasible due to the time they would take to implement.

f. **Legal**. An organisation may be unable to implement a particular countermeasure due to legislative barriers.

g. **Technical**. For example, PC security hardware may only be available for IBM compatible PCs, but an organisation may also be using Macintosh equipment.

Risk Management Report

707. The conclusions of the risk management process should be presented in a Risk Management Report. This should identify recommended countermeasures, their cost, the assets being protected, and the extent to which risks are being reduced. It may also identify existing countermeasures which are ineffective or which are not cost-effective.

708. Countermeasures should be prioritised taking into account the assets to be protected, the extent to which risk is reduced by the countermeasure, and the number of risks mitigated by the countermeasure. This process will assist management in deciding whether a particular countermeasure should be implemented, particularly where budgetary constraints may prohibit the implementation of all recommended countermeasures.

709. Implementation of countermeasures should be planned. Where systems are under development, implementation should be an intrinsic part of the development life cycle. Where countermeasures are to be retrofitted to an existing system, planning should aim to implement countermeasures in a timescale commensurate with the degree of risk, while minimising the impact on system users. The report should provide an implementation plan and a suggested timetable, and may also include a follow-up plan identifying the requirement for further reviews and specifying any inspection or audit activities to be conducted once countermeasures have been implemented.

The annex documents related to this document are located at NZSIT 104 Annex A - Risk Analysis Checklists