New Zealand Security of Information Technology Publication 102

THE CERTIFICATION OF GOVERNMENT COMPUTER SYSTEMS

CHAPTER 1

INTRODUCTION

General

101. Proper implementation of appropriate security measures is an essential part of the life cycle of any computer system. Security needs to be specified, designed, implemented, and tested in the same way as any other component of the system.

102. The formal validation of system security is achieved through a process of certification and accreditation. As a general rule only those systems handling classified information, or those which are particularly critical to a department's operations, will require accreditation. The establishment of departmental computer security policy and the conduct of informal system reviews should provide sufficient assurance of security for other systems.

Certification

103. Certification is the term used to describe the development and maintenance of security documentation for a computer system. Certification is carried out by project staff to provide assurance to higher management that the confidentiality, availability, and integrity of the system are adequately protected.

104. For several reasons, certification should be carried out during system development rather than afterwards. These include:

a. **Resistance to Change**. People resist change. Changes to an operational system might add procedural steps, restrict existing capabilities or flexibility, or increase response time. Introducing security features during development is substantially easier than changing a system with which users are familiar.

b. **Costs**. The financial and technical resources required to make security changes to an operational system are in general greater than those required to design or make similar changes during development.

c. **Lack of Evidence**. The need to install increased security features in an operational system is often refuted on the basis that a potential breach has not yet occurred.

d. **Development Process**. Certification during development provides the opportunity to enhance the development process so as to inherently provide a more secure system before certification and to produce certification documentation as part of the development process.

Responsibilities

105. Certification and accreditation of departmental computer systems are respectively the responsibility of a Certification Officer and an Accreditation Authority. The Accreditation Authority, normally the Chief Executive or a senior departmental executive, will generally appoint an Accreditation Agent to carry out accreditation on his or her behalf. Their individual responsibilities are as follows:

a. **Certification Officer**. The Certification Officer is appointed by and responsible to the manager of the system being certified. The Certification Officer is responsible for producing the documentation required for accreditation and for carrying out a security evaluation to confirm the suitability of the implemented security measures.

b. **Accreditation Authority**. The Accreditation Authority is responsible for approving the system for operational use.

c. **Accreditation Agent**. The Accreditation Agent, a person independent of the system development team, is responsible to the Accreditation Authority for reviewing the documentation produced from the certification process, conducting site inspections, and recommending the accreditation decision.

106. Certification and accreditation do not need to be carried out by just the two nominated officers. It may be advantageous to use other staff members or external consultants to assist with the documentation of technical areas such as operating systems or data communications. All personnel involved in certification and accreditation tasks should be adequately trained in application of the procedures detailed in this publication.

Certification Planning

107. Certification of more complex, networked systems generally requires some level of pre-planning to ensure that adequate funding is available for site visits and any additional costs such as training, contracting in specialised skills, and purchasing any support tools that may be required. Planning requires expertise in, and knowledge of, both the system under evaluation and the evaluation process. Certification plans should, therefore, identify appropriate timings for any training, consultancy, and site visits that may be required, and coordination of the certification with any operational schedules that may be in place. General administrative support needs, specialist reference documents,

and technical support tools should also be identified. The plan should be formally agreed and promulgated before data collection commences.

108. One of the two major results of the planning phase will be an estimate of the time required to carry out the certification. The factors to be taken into account when estimating the time are:

a. the sensitivity of information in the system,

b. the size and complexity of the system,

c. the quality of existing documentation,

d. the amount of detailed evaluation necessary, and

e. the geographic dispersion of the system.

109. The second result of certification planning is a definition of the boundaries of the system to be certified. In general, the boundaries will be the human interfaces for information being entered and output from the system, although in more complex systems a boundary can occur at a trusted electronic interface.

Data Collection

110. Certification involves reviewing comprehensive system documentation, in particular covering the security subsystems. The Certification Officer will need access to any previous audit reports or assessments, and all statutes, regulations and policies relevant to the system. The Certification Officer may also need system flow or structure charts and source code for the system. Data can also be collected through interviews with application development and support personnel.

111. The documentation collected will allow the Certification Officer, and later the Accreditation Agent, to understand what the system does and how it works in order to assess the system's security posture. Application documentation, if accurate and up to date, is a good source of system information. A risk analysis, if one has been carried out for the system, will be a good source of information on system vulnerabilities and protective measures.

112. Interviews, though time-consuming, can sometimes produce information not available through other means. When interviewing it is important to assess the subject competence and bias, and independently to verify important facts. Subjective judgements can be faulty or represent extreme scenarios, and care should be taken when interpreting such information.

Certification Reporting

113. The documentation developed during certification must be provided to a level of detail sufficient to confirm that the security policy defines appropriate protection and that the security measures used are able to satisfy the requirements of the security policy. The following items of documentation, each described in the following chapters, should be submitted for accreditation:

a. Top Level Specification

b. Detailed System Description, if required

c. System Security Policy

d. System Security Plan

e. Product Evaluation Reports, if any

f. Standard Operating Procedures

Certificates

114. Once the system is installed and all certification documents have been written, the Certification Officer will need to raise up to five certificates which confirm that, on the basis of review and evaluation of the security requirements and mechanisms of the system, the system is secure (see Annex A). Certificates are produced for:

a. physical security,

b. personnel security,

c. emission security, where required,

d. communications security, where required, and

e. computer security.

Accreditation

115. The Certification Officer will submit on completion the certification documentation and certificates for accreditation, the process of verifying the system's security and formally authorising the system for operation. Accreditation involves an independent review of each of the certification documents to ensure that the security measures implemented in the system meet the required level of security for the information being processed. It also

involves site and system inspections to ensure that security has been implemented according to the documentation.

System Life Cycle

116. Figure 1 depicts the overall phases in the development of a departmental computer system and identifies the security related tasks. However, if certification is being undertaken retrospectively, the security related tasks can be carried out independently.

117. The security related tasks shown in figure 1 are an integral part of the system life cycle: development of a system security policy is one aspect of systems analysis; development of a system security plan is one aspect of system design; security evaluation is system testing of security functionality; and accreditation is the acceptance of security functionality.

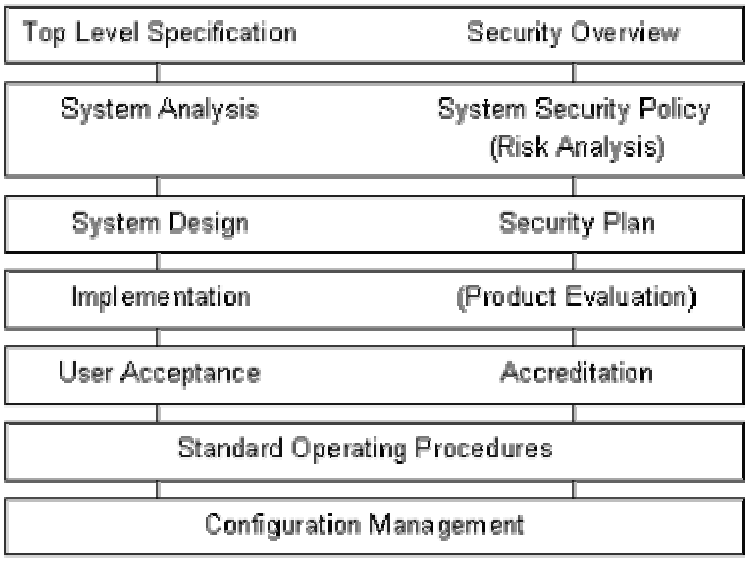

Figure 1: Security Tasks in System Development

CHAPTER 2

TOP LEVEL SPECIFICATION

Introduction

201. The first item of documentation to be produced as part of certification is the Top Level Specification (TLS). This provides a general description of the system and its security requirements in simple, non-technical terms and

provides a basis for the remaining accreditation documentation. The TLS is primarily a system design document, not a security document; ideally, it should be developed from the original proposal for system acquisition.

202. It is advisable to have the draft TLS reviewed by the Accreditation Agent while development continues on further certification documentation. This allows feedback at an early stage on any areas of particular concern, enables the Accreditation Agent to acquire familiarity with the system concepts, and provides some assurance that the TLS will be appropriate to the accreditation process.

TLS Contents

203. The TLS consists of six sections:

a. **User Requirements**. This section summarises the user requirements of the system from a business rather than technical point of view. It will cover the basic business functions of the system and the means of interfacing with each class of user.

b. **Information**. This section outlines the types of information being processed by the system, and shows the flow of information through the system from entry to destruction.

c. **Environment**. This section describes the physical environment for the system. In particular it defines the central system site, if there is one, and each remote site at which components of the system are located.

d. **System Design**. This section provides an overview of the system design. It specifies the configuration of hardware, software, firmware and procedural components. Any interconnections beyond the scope of the system design (such as links to other systems or public networks) should be highlighted. It may be appropriate to provide detailed system design in a separate document and just provide reference to it in this section.

e. **System Management**. This section details the overall principles of system management and support. Where the system spans a number of sites, an appreciation of the coordination procedures should be included.

f. **Security Overview**. The security overview summarises the principles of security for the system. In particular, this section should provide an appreciation of the relative emphasis on physical vs technical security measures and identify the means by which the specific security requirements will be defined (ie, through minimum doctrinal standards or risk analysis).

204. It is often useful to include a diagram of the system architecture as an annex to the TLS. This should show the interconnection of system components and any external electrical connections. The diagram should also highlight the placement of individual software components of the system.

CHAPTER 3

DETAILED SYSTEM DESCRIPTION

General

301. Where the system under certification is particularly complex and the system cannot be adequately described within the TLS, a comprehensive description of the system architecture and functionality can be separately submitted as part of the accreditation documentation. Alternatively, the TLS may reference the existing system design documentation produced during systems analysis and development. In the latter case, however, any referenced material must be fully up to date and incorporate all changes made since the system was documented.

302. The Detailed System Description would typically describe the system configuration down to individual functional elements (hardware, software and firmware), including communications devices and interfaces to users and other systems. It should also include data flows between system components.

303. The system functionality should be detailed by flow charts, structure charts, or pseudocode. In addition the system as a whole, and each module individually, should be described in plain language. Where the system architecture incorporates a proprietary software package, a summary of the features of the packages and its interface to the rest of the system should be described.

CHAPTER 4

SYSTEM SECURITY POLICY

Introduction

401. The System Security Policy provides a consolidated statement of the security requirements for the system. The policy documents the basic information regarding system security, and identifies the relevant national and departmental doctrine containing security directions. A threat analysis is carried out and the results used to determine the level of security assurance required. If minimum standards of security for the system cannot be clearly identified, or if more focused protective measures are required, then a risk analysis should be conducted to identify specific security requirements.

402. The System Security Policy consists of five sections, each described in more detail in this chapter. The sections are:

a. Basic Facts,

b. Security Domains,

c. Security Functionality

d. Security Assurance, and

e. Configuration Management.

Basic Facts

403. The Basic Facts section of the System Security Policy details individual responsibilities for each security aspect of the system and the categories of users on the system. It also defines the classification policy of the system and all associated system and certification documentation.

404. The recommended layout for Basic Facts is:

a. **Responsibilities**.

This subsection details the responsibilities for:

(i) Project/System Management

(ii) System Administration

(iii) System Security/Certification

(iv) Accreditation

b. **Classification Policy**. This subsection details the classification policy for the existence and purpose of the system. This classification policy should then apply to all documentation regarding the system. Documentation produced during certification should be marked at least at the level of classification for the purpose of the system, but may be higher.

c. **System Users**. This subsection identifies each category of system user. In this document the users will be categorised according to their security clearances rather than the tasks they undertake.

d. **Information**. This subsection summarises the type of information processed on the system in terms of usage and classification. It may be useful to present this as a matrix showing information groups against classification levels.

Security Domains

405. The Security Domains section of the System Security Policy provides full details of each environment within which components of the system will operate. The electronic environment within which the system will operate is described, and the threat levels and protective measures in each physically discrete site (the local security domains) are detailed. A common threat and security description may be provided for a number of physically separate areas for which all security-relevant details are the same.

406. **Electronic Security Domain**. The Electronic Security Domain describes the computer and communications environment outside the boundaries of the system under certification. This subsection is required only if the scope of the certification does not include the network through which the system host will communicate with user sites or if certification is for an application rather than a complete computer system. All threats to the system from the electronic security domain should be detailed. Any protective measures provided by the electronic environment should be described, such as identification and authentication measures, security partitioning, audit logs, file access controls, reliability enhancements, and data integrity features.

407. **Local Security Domain**. A Local Security Domain is a separate physical environment in which some part of the system being certified is located and for which the department exerts access control. A system will typically have multiple local security domains. The Local Security Domain will describe the threat level and any physical or personnel protection provided to the system at the local site. The threat level is assessed by considering both the attractiveness and the exposure to attack of the system and its information. The GCSB may be consulted for advice on threat levels, although a very low threat can be assumed for systems that are:

a. located in New Zealand,

b. not accessible by the public or through a public network,

c. handling only CONFIDENTIAL or lower grade information, and

d. sited in departmental premises.

Security Functionality

408. Various Government legislation contains principles of protection that must be met by departmental information systems. Protection must be provided for a range of official information relating to national security, commercial dealings, and individuals. In addition, departments may have established their own specific departmental policies in which further protection for departmental information is mandated. This may be in the form of specific departmental security policy, departmental IT policy, or policy regarding functional activities within the department. This section should identify the relevant government legislation, national doctrine, and departmental doctrine for the system being certified and list the mandated security requirements for

the system. These requirements will often be extracted from doctrine in a conceptual form, for instance *user authentication is required,* and will need to be reviewed and stated in terms of specific security functionality, for instance *a userid and password mechanism will be used to authenticate users* . The System Security Policy should not include reference to specific products.

409. Each item of security functionality should be stated in its own paragraph, with a specific reference number in the format SFR-1, SFR-2, etc. The requirement should also have a reference back to the source document, for instance (SIGD 5.12). Each SFR should be independently inspectable.

410. In some cases the minimum standards laid down for the system may be considered too coarse and a finer assessment of security requirements may be appropriate. This can be achieved, albeit at some additional cost in time and resources, by carrying out a full risk analysis. The conceptual security requirements resulting from the risk analysis should be extracted and listed in this section of the policy together with a reference to the full risk analysis report.

411. Consideration must be given to any special protection required for information provided to the department by an external agency. In addition, all special security requirements imposed by external agencies to which the system is interconnected should be listed.

412. The relative emphasis of physical and technical security will need to be taken into account in order to identify the security requirements that will be met through computer security mechanisms. The security standards defined in the NZSIT 103: Security Evaluation Criteria should be reviewed and, where possible, one or more selected to satisfy the computer security requirements. Use of pre-defined standards will allow subsequent selection of preferred products in the security plan, thus avoiding the need to conduct full product evaluations as part of certification. If none of the pre-defined security standards are appropriate, then the computer security functionality can be defined as a specific list of security functions.

Security Assurance

413. Assurance defines how strong and how correct security functions need to be, and is directly related to the level of threat under which the system will operate. As the requirement for strength and correctness in a security function increases, so does the effort required to evaluate that function and therefore the cost of products at that level of assurance. Selecting the assurance level therefore involves balancing cost against security needs.

414. Assurance is expressed as one of the levels E1 to E6 ("Evaluation", refering to ITSEC evaluation standards) or EAL1 to EAL7 ("Evaluation Assurance Level", refering to the more recent Common Criteria standards), with each higher level meeting all of the lower level criteria. The major features of each of the assurance levels are as follows:

a. **E1/EAL2 (Vendor Assured)**. This level of evaluation is an independent confirmation by an approved evaluation facility that the security functions claimed by the vendor exist and operate according to the vendor's documentation.

b. **E2/EAL3 (Independently Tested)**. This level of assurance incorporates a review of system design documentation and detailed system testing by an approved evaluation facility.

c. **E3/EAL4 (Independently Assured)**. This level requires that source code and/or hardware schematics be independently reviewed by an approved evaluation facility.

d. **E4/EAL5 (Structured Design)**. The main new requirement at this level is that a formal model of the security policy and a semi-formal design description have been reviewed by an independent evaluation facility.

e. **E5/EAL6 (Rigorous Design)**. These evaluations include a review of all run time library source code and extends the requirement for configuration management.

f. **E6/EAL7 (Formal Design)**. The toughest evaluation. All security functions must be formally specified and proven in an approved notation. Formal notations are typically based on predicate calculus or defined within a theorem prover such as VDM, Z, Gypsy or LOTOS.

415. The minimum assurance levels recommended for computer systems are included in the specification of minimum security standards (see NZSIT 103: Security Evaluation Criteria Part 3). These should be considered in conjunction with the assessed threats as follows:

a. **E1-2 (EAL2-3).** Basic strength measures to provide protection against accident and low threat attack.

b. **E3-4 (EAL4-5).** Medium strength measures to provide protection against directed but medium threat attacks.

c. **E5-6 (EAL6-7).** High strength measures to provide protection against high intensity, long term attacks and to provide assurance of correct design.

Configuration Management

416. The last section of the System Security Policy consists of the required procedures for configuration management. While accreditation provides a statement of the status of computer system security relative to the stated security policy at the time of the accreditation, configuration management provides the control process for maintaining the required level of security throughout the life of the operational system.

417. The Configuration Management section should define change approval procedures, state the composition of the Configuration Management Board, and provide a reference to baseline configuration documentation.

CHAPTER 5

SECURITY PLAN

General

501. Just as the System Security Policy identifies the required security functions, so the Security Plan details the specific security measures and products selected to satisfy those functions. This document provides a description of each of the security functionality requirements (SFRs), and identifies the security procedure or countermeasure response that has been taken to satisfy the requirement. For example,

SFR.4

Where media has been used for storage of material classified SECRET and above, or when declassification through degaussing or overwriting is not possible, media must retain the highest classification of any information previously recorded. When no longer required, the media must be destroyed. (NZSIT 207 para 115)

Response

All media are marked with the highest classification allowed for storage. SOPs state that all media used for storage of classified material are to be destroyed when no longer required.

502. In many cases, a range of security measures will be available for the same security functionality. The appropriate measures should be selected on the basis of cost, assurance level, and suitability of the mechanism to the system.

Physical Security

503. This section provides full details of the physical security measures in place to provide protection for each local security domain. Such measures may include site and building access restrictions, security guard patrols, intruder detection systems, secure rooms, vaults, and safes.

Personnel Security

504. This section should cover the security vetting procedures and standards laid down for all personnel involved with management, development, maintenance, operation, or use of the system.

Communications Security

505. The communications security section should provide details of the products selected to meet the link encryption and TEMPEST requirements of the system. Any security measures applied within the terminal/computer software and used to encrypt transmissions should be detailed in the computer security section.

Computer Security

506. If protection for the system is not entirely managed through physical, procedural, and communications security, a computer security section should be included in the Security Plan with details of the specific products selected to meet the security requirements as detailed in the SSP.

507. For each product, the security plan should provide the following information:

a. **Functionality**. The security functionality of the product should either be identified by reference to a security standard or by detailed description.

b. **Assurance**. The assurance level of each product should be stated, and evidence provided to substantiate the assurance claim either through reference to the product entry in the NZCSIM 104: Preferred Products List or to a specific evaluation report.

c. **Failure Action**. Details of how the security measure behaves under failure conditions should be provided.

508. If the level of assurance required in the security policy cannot be met by a security measure, or if the security measure selected does not fully cover the required security functionality, the deficiencies must be highlighted and justification provided for continuing system certification.

Standard Operating Procedures

509. The final section of the Security Plan should contain all security relevant procedures used in the management, administration, and operation of the system. These will often be detailed under separate cover and referenced in the Plan.

510. The Standard Operating Procedures document will consist of a number of independent procedures and should include specific procedures designed to protect against known vulnerabilities in the system which are not otherwise protected. Other procedures may be security-relevant while not being written specifically for security reasons. Examples of security and security-relevant procedures would include:

a. hard copy and media storage procedures;

b. system startup, recovery, and closedown procedures;

c. user training and terminal usage procedures;

d. arrangements for supervision of visitors including maintenance personnel;

e. userid and password allocation;

f. control of file and peripheral access permissions;

g. monitoring of privileged accounts;

h. procedures for separation of development;

i. controls on the introduction of software;

j. procedures for hardware and software installation and delivery; and

k. security officer audit procedures.

CHAPTER 6

PRODUCT EVALUATION REPORTS

General

601. Products used to implement emission, communications, and computer security should be selected from *NZCSIM402: The Evaluated Product List*, or the Evaluated Products Lists of the Australasian Information Security Evaluation Programme(AISEP), the UK Government's ITSEC scheme or the US or Canadian Trusted Product Evaluation Programmes(TPEP). There will be occassions when a non-preferred product will be selected; in such cases a product evaluation should be carried out during certification and in accordance with the procedures detailed in *NZSIT 103: Security Evaluation Criteria.* Product evaluation reports for non-preferred products should be included in the documentation submitted for accreditation.

602. The level of assurance required for product evaluations should be determined by the threat level and the degree of protection provided in the local security domain (see Chapter 4).

603. Where a department has selected a non-preferred product for their use but considers it to be potentially useful for general government use, the Bureau may be requested to carry out the product evaluation. In such cases, the department will spponsor the evaluation and be responsible for submission of the required evaluation documentation. If the evaluation is successful, the product will be included in the Preferred Products List.

CHAPTER 7

ACCREDITATION

General

701. Accreditation is the process of verifying the documentation produced during certification and formally authorising the system for operation. Accreditation involves an independent review of each of the certification documents to ensure that the security measures implemented in the system are appropriate for the required level of security and the information being processed. Accreditation also involves site and system inspections to confirm security measures have been correctly implemented.

702. The accreditor will consider the system, and reason about its security, in terms of security assumptions and security assertions. A security assumption is some protective measure assumed to be provided within the electronic security domain or at the local site whereas a security assertion is a protective measure included as part of the system being certified. A security requirement is therefore typically met by one or more security assertions which are reliant upon some subset of the security assumptions.

703. Accreditation involves eight steps:

a. The security measures are confirmed as correct by reviewing the System Security Policy against the stated, and possibly other relevant, national and departmental security policies.

b. The Security Plan is validated as providing appropriate and consistent security mechanisms to implement the functionality required by the System Security Policy.

c. The Standard Operating Procedures are reviewed to ensure that sufficient procedural security exists to ensure the effectiveness of the security measures implemented and to provide adequate security where security requirements are not otherwise addressed.

d. The Top Level Specification is reviewed to ensure it adequately describes the system and that the security overview correctly reflects the posture identified in the System Security Policy and Plan.

e. The systems's security assumptions and assertions are extracted from the System Security Policy, the Security Plan, and the Standard Operating Procedures and security checklists created.

f. Each site is inspected to confirm adequate implementation of physical and personnel security, and to ensure communications and computer security measures have been correctly installed. Equipment will be verified against Configuration Management baseline documentation.

g. A security evaluation of the computer system will be carried out to confirm that the computer system adequately protects the information being processed and stored, and that the computer security measures implemented cooperate as required to provide a well integrated security environment.

h. An accreditation report is written and a recommendation made to the Accreditation Authority.

System Evaluation

704. System evaluation looks at the protective measures from the following three points of view:

a. **Functional Operation**. The system is reviewed to ensure that the controls acceptably perform the required functions as identified in the security policy and plan. This is achieved through testing the security mechanism's handling of parameters, error conditions, and configuration changes.

b. **Performance**. A number of qualitative factors related to security must be considered during the evaluation, including availability, survivability, accuracy, response time and throughput. Performance is normally evaluated by stress testing and monitoring system parameters while increasing system load.

c. **Penetration Testing**. Penetration testing is used to assess the ease of circumventing or breaking the system's security mechanisms, and is the most technically complex of the evaluation activities. While penetration testing is specific to each category of security mechanism, the following are common areas where flaws may be exploited:

(i). complex interfaces,

(ii). maintenance procedures,

(iii). error handling,

(iv). temporary security level changes,

(v). residual information,

(vi). new features and the interface between new and old, and

(vii). control of security information.

Pre-Accreditation

705. It is preferable that the Accreditation Agent reviews the system's Top Level Specification (TLS) as soon as it is developed in order to confirm the nature and scope of the certification. Early review of the TLS may avoid unnecessary work in the security policy and plan.

Accreditation Recommendation

706. The accreditation may be refused if major security deficiencies have been identified. Alternatively, if rectifiable deficiencies have been identified and an acceptable plan for the correction of those deficiencies has been presented, a *Qualified Accreditation* may be granted. In the latter case, a further target date will be stipulated for rectification of the deficiencies, and restrictions may be placed on operation of the system.

707. At successful completion of the accreditation process the Accreditation Authority is provided with a recommendation for accreditation. If he/she is satisfied that the certification and accreditation processes have been properly completed and the required level of security has been achieved, then the system will be authorised for full operation.

708. On executive approval of accreditation recommendations, an accreditation reference number will be allocated. This number should be simply constructed in the format *org-xxx-yy* where *org* is an organisational identifier, *xxx* is a sequential number, and *yy* is the year of accreditation, e.g., GCSB-021-97. A register of all accreditation reference numbers should be maintained. The certification and accreditation process is now complete.

Re-Accreditation

709. An accreditation may be given only for a specified period after which a re-certification and re-accreditation would be required. Also, during the life of the accredited system, changes in the environment or the system itself may justify a partial or full re-accreditation. Configuration management procedures, if properly applied, will ensure that much of the required documentation will be available to submit for a reaccreditation.

710. Where changes are made to any of the security documentation, amendments should be forwarded to the Accreditation Agent for review.

The related annex to this document is located at http://www.gcsb.govt.nz/nzsit/102/102nxa.htm.