GOVERNMENT COMMUNICATIONS SECURITY BUREAU

TE TIRA TIAKI

NZISM

New Zealand Information Security Manual

DECEMBER 2017 – Part 1

Chapters 1 - 13

www.gcsb.govt.nz

New Zealand Government

Contact us

Inquiries regarding any use of this document are welcome at:

The Government Communications Security Bureau
PO Box 12 209
Wellington 6144
Email: ism@gcsb.govt.nz

Foreword

The New Zealand Information Security Manual (NZISM) (December 2017, Version 2.7) is now publicly available and supersedes all previous versions of the manual. Changes include new paragraphs on Audit Evidence (Section 4.3) and Cable Trays (Section 10.1). Extensive work has also been done in updating Section 23.2 Glossary of Terms. A schedule of changes, additions and other amendments is also available to assist users in identifying additions and changes.

The NZISM is an integral part of the Protective Security Requirements (PSR) framework which sets out the New Zealand Government's expectations for the management of personnel, information and physical security as directed by Cabinet.

The safe and secure operation of information systems is essential to New Zealand's security and economic well-being. These systems are vital for the successful operation of government organisations and underpin public confidence by supporting privacy and security.

Chief executives and senior leaders in government agencies are ultimately accountable for the management of risk, including cyber risks, within their organisations. In the face of globally rising cyber threats, it is vital that agency executives, particularly those with information security governance responsibilities, keep abreast of technology challenges and threats and update their organisation's risk stance and security practices accordingly. This refreshed NZISM supports executives to discharge their risk management responsibilities.

The NZISM is a manual tailored to meet the needs of agency information security executives as well as practitioners, vendors, contractors and consultants who provide information and technology services within or to agencies. This version continues the regular update and enhancement of the technical and security guidance for government departments and agencies to support good information assurance practices. It is consistent with recognised international standards to support agencies' own approaches to risk management.

Andrew Hampton

Director-General
of the Government Communications Security Bureau

Table of Contents

1. About information security

1.1. Understanding and using this Manual

Objective

1.1.1. The New Zealand Information Security Manual details processes and controls essential for the protection of all New Zealand Government information and systems. Controls and processes representing good practice are also provided to enhance the essential, baseline controls. Baseline controls are minimum acceptable levels of controls. Essential controls are often described as "systems hygiene".

Context

Scope

1.1.2. This manual is intended for use by New Zealand Government departments, agencies and organisations. Crown entities, local government and private sector organisations are also encouraged to use this manual.

1.1.3. This section provides information on how to interpret the content and the layout of content within this manual.

1.1.4. Information that is Official Information or protectively marked UNCLASSIFIED, IN-CONFIDENCE, SENSITIVE or RESTRICTED is subject to a single set of controls in this NZISM. These are essential or minimum acceptable levels of controls (baseline controls) and have been consolidated into a single set for simplicity, effectiveness and efficiency.

1.1.5. All baseline controls will apply to all government systems, related services and information. In addition, information classified CONFIDENTIAL, SECRET or TOP SECRET has further controls specified in this NZISM.

1.1.6. Where the category "All Classifications" is used to define the scope of rationale and controls in the Manual, it includes any information that is Official Information, UNCLASSIFIED, IN-CONFIDENCE, SENSITIVE, RESTRICTED, CONFIDENTIAL, SECRET, TOP SECRET or any endorsements, releasability markings or other qualifications appended to these categories and classifications.

The purpose of this Manual

1.1.7. The purpose of this manual is to provide a set of essential or baseline controls and additional good and recommended practice controls for use by government agencies. The use or non-use of good practice controls MUST be based on an agency's assessment and determination of residual risk related to information security.

Target audience

1.1.8. The target audience for this manual is primarily security personnel and practitioners within, or contracted to, an agency. This includes, but is not limited to:

- security executives;
- security and information assurance practitioners;
- IT Security Managers;
- Departmental Security Officers; and
- service providers.

Structure of this Manual

1.1.9. This manual seeks to present information in a consistent manner. There are a number of headings within each section, described below.

- Objective – the desired outcome when controls within a section are implemented.
- Context – the scope, applicability and any exceptions for a section.
- References – references to external sources of information that can assist in the interpretation or implementation of controls.
- Rationale & Controls
  - Rationale – the reasoning behind controls and compliance requirements.
  - Control – risk reduction measures with associated compliance requirements.

1.1.10. This section provides a summary of key structural elements of this manual. The detail of processes and controls is provided in subsequent chapters. It is important that reference is made to the detailed processes and controls in order to fully understand key risks and appropriate mitigations.

The New Zealand Classification System

1.1.11. The requirements for classification of government documents and information are based on the **Cabinet Committee Minute EXG (00) M 20/7** and **CAB (00) M42/4G(4)**. The Protective Security Requirements (PSR) INFOSEC3 require agencies to use the NZ Government Classification System and the NZISM for the classification, protective marking and handling of information assets. For more information on classification, protective marking and handling instructions, refer to the Protective Security Requirements, NZ Government Classification system.

Key definitions

Accreditation Authority

1.1.12. The Agency Head is generally the Accreditation Authority for that agency for all systems and related services up to and including those classified RESTRICTED. See also Chapter 3 – Roles and Responsibilities and Section 4.4 – Accreditation Framework.

1.1.13. Agency heads may choose to delegate this authority to a member of the agency's executive. The Agency Head remains accountable for ICT risks accepted and the information security of their agency.

1.1.14. In all cases the Accreditation Authority will be at least a senior agency executive who has an appropriate level of understanding of the security risks they are accepting on behalf of the agency.

1.1.15. For multi-national and multi-agency systems the Accreditation Authority is determined by a formal agreement between the parties involved. Consultation with the Office of the Government Chief Information Officer (GCIO) may also be necessary.

1.1.16. For agencies with systems that process, store or communicate endorsed or compartmented information, the Director-General of the GCSB is the Accreditation Authority *irrespective of the classification level of the information*.

Certification and Accreditation Processes

1.1.17. Certification and accreditation of information systems is the fundamental governance process by which the risk owners and agency head derives assurance over the design, implementation and management of information systems and related services provided to government agencies. This process is described in detail in Chapter 4 – System Certification and Accreditation.

1.1.18. Certification and Accreditation are two distinct processes.

1.1.19. Certification is the formal assertion that an information system and related services comply with minimum standards and agreed design, including any security requirements.

1.1.20. *In all cases*, certification and the supporting documentation or summary of other evidence will be prepared by, or on behalf of, the host or lead agency. The certification is then provided to the Accreditation Authority.

1.1.21. Accreditation is the formal authority to operate an information system and related services, and requires the recognition and acceptance of associated risk and residual risks.

1.1.22. The requirements described above are summarised in the table below. Care MUST be taken when using this table as there are numerous endorsements, caveats and releasability instructions in the New Zealand information classification system that may change where the authority for accreditation lies.

Information Classification	MUST and MUST NOT controls	SHOULD and SHOULD NOT controls	Accreditation Authority
Information classified RESTRICTED and below, including UNCLASSIFIED and Official Information	Controls are baseline or "systems hygiene" controls and are essential for the secure use of a system or service. Non-use is high risk and mitigation is essential. If the control ***cannot*** be directly implemented, suitable compensating controls MUST be selected to manage identified risks. The Accreditation Authority ***may*** grant a Waiver or Exception ***if*** the level of residual risk is within the agency's risk appetite. Some baseline controls cannot be ***individually*** risk managed by agencies without jeopardising multi-agency, All-of-Government or international systems and related information.	Control represents good and recommended practice. Non-use may be medium to high risk. Non-use of controls is formally recorded, compensating controls selected as required and residual risk acknowledged to be within the agency's risk appetite and formally agreed and signed off by the Accreditation Authority.	Agency Head/Chief Executive/Director-General (or formal delegate)
All systems or services classified CONFIDENTIAL and above.	This is a baseline for any use of High Grade Cryptographic Equipment or the establishment of any compartments or the handling of any caveated information (see below). The Controls are baseline or "systems hygiene" controls and are essential for the secure use of a system or service. Non-use is high or very high risk and mitigation is essential. If the control ***cannot*** be directly implemented and suitable compensating controls MUST be selected to manage identified risks. The Accreditation Authority ***may*** grant a Waiver or Exception ***if*** the level of residual risk is within the agency's risk appetite. Some baseline controls cannot be ***individually*** risk managed by agencies without jeopardising multi-agency, All-of-Government or international systems and related information.	This is a baseline for any use of High Grade Cryptographic Equipment or the establishment of any compartments or the handling of any caveated information (See below). Control represents good and recommended practice. Non-use may be high risk Non-use of controls is formally recorded, compensating controls selected as required and residual risk formally acknowledged to be within the agency's risk appetite and agreed and signed off by the Accreditation Authority	Agency Head/Chief Executive/Director-General (or formal delegate)

Information Classification	MUST and MUST NOT controls	SHOULD and SHOULD NOT controls	Accreditation Authority
All use of High Grade Cryptographic Equipment (HGCE) **All systems or services with compartmented or caveated information classified CONFIDENTIAL and above.**	Accreditation based on work conducted by the agency and authority to operate by the Agency Head. Controls are baseline or "systems hygiene" controls and are essential for the secure use of a system or service. Non-use is high or very high risk and mitigation is essential. If the control ***cannot*** be directly implemented and suitable compensating controls MUST be selected to manage identified risks. The Accreditation Authority ***may*** grant a Waiver or Exception ***if*** the level of residual risk is within the agency's risk appetite. Some baseline controls cannot be ***individually*** risk managed by agencies without jeopardising multi-agency, All-of-Government or international systems and related information.	Accreditation based on work conducted by the agency and authority to operate by the Agency Head. Control represents good and recommended practice. Non-use may be high risk Non-use of controls is formally recorded, compensating controls selected as required and residual risk formally acknowledged to be within the agency's risk appetite and agreed and signed off by the Accreditation Authority.	Director-General of the GCSB (or formal delegate)

"All Classifications" category

1.1.23. The "All Classifications" category is used to describe the applicability of controls for any information that is Official Information or protectively marked UNCLASSIFIED, IN-CONFIDENCE, SENSITIVE, RESTRICTED, CONFIDENTIAL, SECRET or TOP SECRET, including any caveats or releasability endorsements associated with the respective document classification.

Compartmented Information

1.1.24. Compartmented information is information requiring special protection through separation or is "compartmented" from other information stored and processed by the agency.

Concept of Operations (ConOp) Document

1.1.25. Systems, operations, campaigns and other organisational activities are generally developed from an executive directive or organisational strategy. The ConOp is a document describing the characteristics of a proposed operation, process or system and how they may be employed to achieve particular objectives. It is used to communicate the essential features to all stakeholders and obtain agreement on objectives and methods. ConOps should be written in a non-technical language to facilitate agreement on understanding and knowledge and provide clarity of purpose. ConOp is a term widely used in the military, operational government agencies and other defence, military support and aerospace enterprises.

Information

1.1.26. The New Zealand Government requires information important to its functions, resources and classified equipment to be adequately safeguarded to protect public and national interests and to preserve personal privacy. Information is defined as any communication or representation of knowledge such as facts, data, and opinions in any medium or form, electronic as well as physical. Information includes any text, numerical, graphic, cartographic, narrative, or any audio or visual representation.

Information Asset

1.1.27. An information asset is any information or related equipment that has value to an agency or organisation. This includes equipment, facilities, patents, intellectual property, software and hardware. Information Assets also include services, information, and people, and characteristics such as reputation, brand, image, skills, capability and knowledge**.**

Information Assurance (IA)

1.1.28. Confidence in the governance of information systems and that effective measures are implemented to manage, protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

Information Security

1.1.29. Although sometimes described as cyber security, *Information* security is considered a higher level of abstraction than cyber security relating to the protection of information regardless of its form (electronic or physical). The accepted definition of information security within government is: "measures relating to the confidentiality, availability and integrity of information".

1.1.30. A number of specialised security areas contribute to information security within government; these include: physical security, personnel security, communications security and information and communications technology (ICT) security along with their associated governance and assurance measures.

Information Systems

1.1.31. The resources and assets for the collection, storage, processing, maintenance, use sharing, dissemination, disposition, display, and transmission of information. This includes necessary and related services provided as part of the information system, for example; Telecommunication or Cloud Services.

Information Systems Governance

1.1.32. An integral part of enterprise governance consists of the leadership and organisational structures and processes to ensure that the agency's information systems support and sustain the agency's and Government's strategies and objectives. Information Systems Governance is the responsibility of the Agency Head and the Executive team.

Secure Area

1.1.33. In the context of the NZISM a secure area is defined as any area, room, group of rooms, building or installation that processes, stores or communicates information classified CONFIDENTIAL, SECRET, TOP SECRET or any compartmented or caveated information at these classifications. A secure area may include a SCIF (see below). The physical security requirements for such areas are specified in the Protective Security Requirements (PSR) Security Zones and Risk Mitigation Control measures.

Security Posture

1.1.34. The Security Posture of an organisation describes and encapsulates the security status and overall approach to identification and management of the security of an organisation's networks, information, systems, processes and personnel. It includes risk assessment, threat identification, technical and non-technical policies, procedures, controls and resources that safeguard the organisation from internal and external threats.

Sensitive Compartmented Information Facility (SCIF)

1.1.35. Any accredited area, room, or group of rooms, buildings, or installation where Sensitive Compartmented Information (SCI) is stored, used, discussed, processed or communicated. The Accreditation Authority for a SCIF is the Director-General of the GCSB or formal delegate.

System Owner

1.1.36. A System Owner is the **person** within an agency responsible for the information resource and for the maintenance of system accreditation. This may include such outsourced services such as telecommunications or cloud. Their responsibilities are described in more detail in Section 3.4 – System Owners.

Interpretation of controls

Controls language

1.1.37. The definition of controls in this manual is based on language as defined by the Internet Engineering Task Force (IETF)'s Request For Comment (RFC) 2119 to indicate differing degrees of compliance.

Applicability of controls

1.1.38. Whilst this manual provides controls for specific technologies, not all systems will use all of these technologies. When a system is developed, the agency will determine the appropriate scope of the system and which controls within this manual are applicable.

1.1.39. If a control within this manual is outside the scope of the system then non-compliance processes *do not apply*. However, if a control is within the scope of the system yet the agency chooses *not to implement* the control, then they are required to follow the non-compliance procedures as outlined below in order to provide appropriate governance and assurance.

1.1.40. The procedures and controls described in the NZISM are designed, not only to counter or prevent known common attacks, but also to protect from emerging threats.

Identification and Selection of controls

1.1.41. In all cases controls have been selected as the most effective means of mitigating identified risks and threats. Each control has been carefully researched and risk assessed against a wide range of factors, including useability, threat levels, likelihood, rapid technology changes, sustainability, effectiveness and cost.

Controls with a "MUST" or "MUST NOT" requirement

1.1.42. A control with a "MUST" or "MUST NOT" requirement indicates that use, or non-use, of the control is essential in order to effectively manage the identified risk, unless the control is demonstrably not relevant to the respective system. These controls are baseline controls, sometimes described as systems hygiene controls.

1.1.43. The rationale for non-use of essential controls MUST be clearly demonstrated to the Accreditation Authority as part of the certification process, *before* approval for exceptions is granted. MUST and MUST NOT controls take precedence over SHOULD and SHOULD NOT controls.

Controls with a "SHOULD" or "SHOULD NOT" requirement

1.1.44. A control with a "SHOULD" or "SHOULD NOT" requirement indicates that use, or non-use, of the control is considered good and recommended practice. Valid reasons for not implementing a control could exist, including:

a. A control is not relevant in the agency;

b. A system or ICT capability does not exist in the agency; or

c. A process or control(s) of equal strength has been substituted.

1.1.45. While some cases may require a simple record of fact, agencies must recognise that non-use of any control, without due consideration, may increase residual risk for the agency. This residual risk needs to be agreed and acknowledged by the Accreditation Authority. In particular an agency should pose the following questions:

a. Is the agency willing to accept additional risk?

b. Have any implications for All-of-Government systems been considered?

c. If, so, what is the justification?

1.1.46. A formal auditable record of this consideration and decision is required as part of the IA governance and assurance processes within an agency.

Non-compliance

1.1.47. Non-compliance is a risk to the agency and may also pose risks to other agencies and organisations. Good governance requires these risks are clearly articulated, measures are implemented to manage and reduce the identified risks to acceptable levels, that the Accreditation Authority is fully briefed, acknowledges any residual and additional risk and approves the measures to reduce risk.

1.1.48. In some circumstances, full compliance with this manual may not be possible, for example some legacy systems may not support the configuration of particular controls. In such circumstances, a risk assessment should clearly identify *compensating* controls to reduce risks to an acceptable level. Acceptance of risk or residual risk, without due consideration is NOT adequate or acceptable.

1.1.49. It is recognised that agencies may not be able to immediately implement all controls described in the manual due to resource, budgetary, capability or other constraints. Good practice risk management processes will acknowledge this and prepare a timeline and process by which the agency can implement all appropriate controls described in this manual.

1.1.50. Simply acknowledging risks and not providing the means to implement controls *does not* represent effective risk management.

1.1.51. Where multiple controls are not relevant or an agency chooses not to implement multiple controls within this manual the system owner may choose to logically group and consolidate controls when following the processes for non-compliance.

Rationale Statements

1.1.52. A short rationale is provided with each group of controls. It is intended that this rationale is read in conjunction with the relevant controls in order to provide context and guidance.

Risk management

Risk Management Standards

1.1.53. For security risk management to be of true value to an agency it MUST relate to the specific circumstances of an agency and its systems, as well as being based on an industry recognised approach or risk management guidelines. For example, guidelines and standards produced by Standards New Zealand and the International Organization for Standardization (ISO).

1.1.54. The International Organization for Standardization has published an international risk management standard, including principles and guidelines on implementation, outlined in ISO 31000:2009 - Risk Management -- Principles and Guidelines. Refer to the tables below for additional reference materials.

The NZISM and Risk Management

1.1.55. The ISM encapsulates good and recommended best-practice in managing technology risks and mitigating or minimising threat to New Zealand government information systems.

1.1.56. Because there is a broad range of systems across government and the age and technological sophistication of these systems varies widely, there is no single governance, assurance, risk or controls model that will accommodate all agencies information and technology security needs.

1.1.57. The NZISM contains guidance on governance and assurance processes and technological controls based on comprehensive risk and threat assessments, research and environmental monitoring.

1.1.58. The NZISM encourages agencies to take a similar risk-based approach to information security. This approach enables the flexibility to allow agencies to conduct their business and maintain resilience in the face of a changing threat environment, while recognising the essential requirements and guidance provided by the NZISM.

References

1.1.59. This manual is updated regularly. It is therefore important that agencies ensure that they are using the latest version of this Manual.

References	Publisher	Source
The NZISM and additional information, tools and discussion topics can be accessed from the GCSB website	GCSB	http://www.gcsb.govt.nz.
Protective Security Requirements (PSR)	NZSIS	http://www.protectivesecurity.govt.nz
Another definitive reference is the ISO standard ISO/IEC 27000:2014 Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary (third edition)	ISO / IEC Standards NZ	http://www.iso27001security.com/html/27000.html http://www.standards.co.nz
CNSS Instruction No. 4009 26 April 2010 – National Information Assurance (IA) Glossary, (US),	Committee on National Security Systems (CNSS)	http://www.ncsc.gov/nittf/docs/CNSSI-4009_National_Information_Assurance.pdf
NISTIR 7298 Revision 2 – Glossary of Key Information Security Terms, May 2013	NIST	http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

1.1.60. Supplementary information to this manual can be found in the following documents.

Topic	Documentation	Source
Approved Products	Common Criteria ISO/IEC 15408, parts 1,2 & 3	ISO http://www.iso.org
	AISEP Evaluated Products List	ASD http://www.asd.gov.au
	Other Evaluated Products Lists	NSA http://www.nsa.gov CESG http://www.cesg.gov.uk CSEC http://www.cse-cst.gc.ca Common Criteria http://www.commoncriteriaportal.org
Archiving of information	Public Records Act 2005 (as amended)	Archives New Zealand or http://www.legislation.govt.nz
	Archives, Culture, and Heritage Reform Act 2000 (as amended)	Archives New Zealand or http://www.legislation.govt.nz
Business continuity	ISO 22301:2012, Business Continuity	Standards New Zealand http://www.standards.co.nz
Cable security	NZCSS 400: New Zealand Communications Security Standard No 400 (Document classified CONFIDENTIAL)	GCSB CONFIDENTIAL document available on application to authorised personnel
Emanation security	NZCSS 400: New Zealand Communications Security Standard No 400 (Document classified CONFIDENTIAL)	GCSB CONDFIDENTIAL document available on application to authorised personnel
Information classification	Protective Security Requirements (New Zealand Government Security Classification System Handling Requirements for protectively marked information and equipment)	NZSIS http://www.protectivesecurity.govt.nz
Information security management	ISO/IEC 27001:2013	ISO / IEC http://www.iso27001security.com/html/27001.html Standards New Zealand http://www.standards.co.nz
	ISO/IEC 27002:2013	ISO / IEC http://www.iso27001security.com/html/27001.html Standards New Zealand http://www.standards.co.nz
	Other standards and guidelines in the ISO/IEC 270xx series, as appropriate	ISO / IEC http://www.iso27001security.com/html/27001.html Standards New Zealand http://www.standards.co.nz

Topic	Documentation	Source
Key management – commercial grade	AS 11770.1:2003, Information Technology – Security Techniques – Key Management – Framework	Standards New Zealand http://www.standards.co.nz
Cryptographic Security	NZCSS 300: New Zealand Communications Security Standard No 300 (Document classified RESTRICTED)	GCSB RESTRICTED document available on application to authorised personnel
Management of electronic records that may be used as evidence	HB 171:2003, Guidelines for the Management of Information Technology Evidence	Standards New Zealand http://www.standards.co.nz
Personnel security	PSR, Protective Security Requirements	NZSIS http://www.protectivesecurity.govt.nz
Physical security	PSR, Protective Security Requirements	NZSIS http://www.protectivesecurity.govt.nz
Privacy requirements	Privacy Act 1993 (the Privacy Act)	Office of The Privacy Commissioner http://www.privacy.org.nz
Risk management	ISO 31000:2009 - Risk Management -- Principles and Guidelines	Standards New Zealand http://www.standards.co.nz
	ISO 27005:2011, Information Security Risk Management	Standards New Zealand http://www.standards.co.nz
	HB 436:2013, Risk Management Guidelines	Standards New Zealand http://www.standards.co.nz
	ISO/IEC Guide 73, Risk Management – Vocabulary – Guidelines for use in Standards	Standards New Zealand http://www.standards.co.nz
	NIST SP 800-30, Risk Management Guide for Information Technology Systems	http://www.nist.gov
Security Management	HB167, Security Risk Management	Standards New Zealand http://www.standards.co.nz
Security And Intelligence Legislation	Government Communications Security Bureau Act 2003 (as amended)	http://www.legislation.govt.nz
	New Zealand Security Intelligence Service Act 1969 (as amended)	http://www.legislation.govt.nz
	Telecommunications (Interception Capability and Security) Act 2013 (as amended)	http://www.legislation.govt.nz

Rationale & Controls

1.1.61. Non-compliance

1.1.61.R.01. Rationale

Controls for classified systems and information within this manual with a "MUST" or "MUST NOT" compliance caveat cannot be effectively *individually* risk managed by system owners without jeopardising their own, and in some cases, multi-agency or All-of-Government information assurance.

1.1.61.R.02. Rationale

Controls within this manual with a "SHOULD" and "SHOULD NOT" requirement may be risk managed by agencies. As the individual control security risk for non-compliance is not as high as those controls with a 'MUST' or 'MUST NOT' requirement, the Accreditation Authority can consider the justification for the acceptance of risks, consider any mitigations then acknowledge and accept any residual risks.

1.1.61.R.03. Rationale

Deviations from the procedures and controls in the NZISM may represent risks in themselves. It is important that governance and assurance is supported by evidence, especially where deviations from the procedures and controls in the NZISM are accepted. In this case a formal approval or signoff by the Accreditation Authority is essential. Ultimately the Agency Head remains accountable for the ICT risks and information security of their agency.

1.1.61.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

System owners seeking a dispensation for non-compliance with any essential controls in this manual MUST be granted a dispensation by their Accreditation Authority. Where High Grade Cryptographic Systems (HGCS) are implemented, the Accreditation Authority will be the Director-General of the GCSB or a formal delegate.

1.1.62. Justification for non-compliance

1.1.62.R.01. Rationale

Without sufficient justification and consideration of security risks by the system owner when seeking a dispensation, the agency head or their authorised delegate will lack the appropriate range of information to the make an informed decision on whether to accept the security risk and grant the dispensation or not.

1.1.62.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

System owners seeking a dispensation for non-compliance with essential controls MUST complete an agency risk assessment which documents:

- the reason(s) for not being able to comply with this manual;
- the effect on any of their own, multi-agency or All-of-Government system;
- the alternative mitigation measure(s) to be implemented;
- The strength and applicability of the alternative mitigations;
- an assessment of the residual security risk(s); and
- a date by which to review the decision.

1.1.63. Consultation on non-compliance

1.1.63.R.01. Rationale

When an agency stores information on their systems that belongs to a foreign government they have an obligation to inform and seek agreement from that third party when they do not apply all appropriate controls in this manual. These third parties will place reliance on the application of controls from the NZISM. If the agency fails to implement all appropriate controls, the third party will be unaware that their information may have been placed at a heightened risk of compromise. As such, the third party is denied the opportunity to consider their own additional risk mitigation measures for their information in light of the agency's desire to risk manage controls from this manual.

1.1.63.R.02. Rationale

Most New Zealand Government agencies will store or processes information on their systems that originates from another New Zealand Government Agency. The use of the Classification System, and implementation of its attendant handling instructions, provides assurance to the originating agency that the information is adequately safeguarded.

1.1.63.R.03. Rationale

Additional controls, not described or specified in this manual, are welcomed as a means of improving and strengthening security of information systems, provided there are no obvious conflicts or contradictions with the controls in this manual. A comprehensive risk assessment of the additional controls is a valuable means of determining the effectiveness of additional controls.

1.1.63.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

If a system processes, stores or communicates classified information from another agency, that agency MUST be consulted before a decision to be non-compliant with the Classification System is made.

1.1.63.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

If a system processes, stores or communicates classified information from a foreign government, that government MUST be consulted before a decision to be non-compliant with NZISM controls is made.

1.1.64. All-of-Government Systems

1.1.64.R.01. Rationale

All-of-Government systems, because they are connected to multiple agencies, have the potential to cause significant and widespread disruption should system failures, cyber-attacks or other incidents occur.

1.1.64.R.02. Rationale

Any deviation from the essential controls specified in the NZISM MUST necessarily be carefully considered and their implication and risk for all government systems understood and agreed by all interested parties.

1.1.64.R.03. Rationale

Interested parties may include the lead agency, the Government CIO and key service providers, such as with cloud services.

1.1.64.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

If a system processes, stores or communicates data and information with multiple agencies or forms part of an All-of-Government system, interested parties MUST be formally consulted before non-compliance with any essential controls.

1.1.65. Reviewing non-compliance

1.1.65.R.01. Rationale

As part of the process of providing justification for a dispensation to the Accreditation Authority, an assessment of the degree of compliance, identification of areas of non-compliance and determination of residual security risk is undertaken by the agency or lead agency. This assessment is based on the risk environment at the time the dispensation is sought. As the risk environment will continue to evolve over time it is important that agencies revisit the assessment on an annual basis and update it according to the current risk environment, and if necessary reverse any decisions to grant a dispensation if the security risk is no longer of an acceptable level.

1.1.65.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD review decisions to be non-compliant with any controls at least annually.

1.1.66. Recording non-compliance

1.1.66.R.01. Rationale

Without appropriate records of decisions to risk manage controls from this manual, agencies have no record of the status of information security within their agency. Furthermore, a lack of such records will hinder any governance, compliance or auditing activities that may be conducted.

1.1.66.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST retain a copy and maintain a record of the supporting risk assessment and decisions to be non-compliant with any essential controls from this manual.

1.1.66.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Where good and recommended practice controls are NOT implemented, agencies MUST record and formally recognise that non-use of any controls without due consideration may increase residual risk for the agency. This residual risk MUST be agreed and acknowledged by the Accreditation Authority.

1.2. Applicability, Authority and Compliance

Objective

1.2.1. Agencies understand and follow the requirements of the New Zealand Information Security Manual. Protection of government information and systems is a core accountability.

Context

Scope

1.2.2. The NZISM provides guidance and specific ICT controls that form part of a suite of requirements produced by GCSB relating to information security. Its role is to promote a consistent approach to information assurance and information security across all New Zealand Government agencies. It is based on security risk assessments for any information that is processed, stored or communicated by government systems with corresponding risk treatments (control sets) to reduce the level of security risk to an acceptable level.

Applicability

1.2.3. This manual applies to:

- New Zealand Government departments, agencies and organisations as listed in:
  - Parts 1 and 2 of Schedule 1 to the Ombudsmen Act 1975 (as amended); and
  - Schedule 1 to the Official Information Act 1982.
- any other organisations that have entered into a formal Agreement with the New Zealand Government to have access to classified information.

Authority

1.2.4. The Government Communications Security Bureau Act 2003, as amended ("the GCSB Act") provides that one of the functions of the GCSB is to co-operate with, and provide advice and assistance to, any public authority whether in New Zealand or overseas, or to any other entity authorised by the Minister responsible for the GCSB on any matters relating to the protections, security and integrity of communications; and information structures of importance to the Government of New Zealand. The NZISM is one aspect of the GCSB's advice and assistance to government agencies on information security.

1.2.5. This function furthers the objective of the GCSB to contribute to:

- The national security of New Zealand; and
- The international relations and well-being of New Zealand; and
- The economic well-being of New Zealand.

1.2.6. The NZISM is intended to structure and assist the implementation of government policy that requires departments and agencies to protect the privacy, integrity and confidentiality of the information they collect, process, store and archive. While these overarching requirements are mandatory for departments and agencies, compliance with the NZISM is not required as a matter of law. The controls in the NZISM could be made binding on departments and agencies, either by legislation, or Cabinet direction.

1.2.7. The Protective Security Requirements Framework provides a specific authority and mandate through a Cabinet Directive **CAB MIN (14) 39/38**.

Compliance by smaller agencies

1.2.8. As smaller agencies may not always have sufficient staffing or budgets to comply with all the requirements of this manual, they may choose to consolidate their resources with another larger host agency to undertake a joint approach.

1.2.9. In such circumstances smaller agencies may choose to either operate on systems fully hosted by another agency using their information security policies and information security resources or share information security resources to jointly develop information security policies and systems for use by both agencies. The requirements within this manual can be interpreted as either relating to the host agency or to both agencies, depending on the approach taken.

1.2.10. In situations where agencies choose a joint approach to compliance, especially when an agency agrees to fully host another agency, the agency heads may choose to seek a memorandum of understanding regarding their information security responsibilities.

Legislation and other government policy

1.2.11. While this manual does contain examples of relevant legislation (see Tables 1.1.59 and 1.1.60), there is no comprehensive consideration of such issues. Accordingly, agencies should rely on their own inquiries in that regard.

1.2.12. All controls within this manual may be used as the basis for internal and external annual audit programmes, any review or investigation by the Controller and Auditor-General or referenced for assurance purposes by the Government Chief Information Officer (GCIO).

Rationale & Controls

1.2.13. Compliance

1.2.13.R.01. Rationale

In complying with the latest version of this manual agencies awareness of the current threat environment for government systems and the associated acceptable level of security risk is vital. Furthermore, if a system is designed to an out-dated standard, agencies may need additional effort to obtain accreditation for their systems.

1.2.13.R.02. Rationale

GCSB continuously monitors technology developments in order to identify business risks, technology risks and security threats. If a significant risk is identified, research may be undertaken, additional controls identified and implementation timeframes specified.

1.2.13.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies undertaking system design activities for in-house or out-sourced projects MUST use the latest version of this manual for information security requirements.

1.2.13.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

When GCSB makes a determination that newly introduced standard, policy or guideline within this manual, or any additional information security policy, is of particular importance, agencies MUST comply with any new specified requirements and implementation timeframes.

2. Information Security within Government

2.1. Government Engagement

Objective

2.1.1. Security personnel are aware of and use information security services offered within the New Zealand Government.

Context

Scope

2.1.2. This section covers information on organisations involved in providing information security advice to agencies.

Government Communications Security Bureau

2.1.3. GCSB is required to perform various functions, including the provision of material, advice and other assistance to New Zealand government departments on matters relating to the security of classified information that is processed, stored or communicated by electronic or similar means. GCSB also provides assistance to New Zealand government departments in relation to cryptography, communications and computer technologies.

2.1.4. An agency can contact GCSB for advice and assistance relating to the implementation of the NZISM by emailing ism@gcsb.govt.nz or phone the GCSB's Information Assurance Directorate on (04) 472-6881.

2.1.5. An agency can contact GCSB to provide feedback on the NZISM via email as above.

2.1.6. Agencies can also contact GCSB for advice and assistance on the reporting and management of information security incidents. GCSB's response will be commensurate with the nature and urgency of the information security incident. There is a 24 hour, seven day a week service available if necessary.

2.1.7. Finally, agencies can contact GCSB for advice and assistance on the purchasing, provision, deployment, operation and disposal of High Grade Cryptographic Equipment (HGCE). The cryptographic liaison can be contacted by email at products.systems@gcsb.govt.nz.

Other organisations

2.1.8. The table below contains a brief description of the other organisations which have a role in relating to information security within government.

Organisation	Services
Archives New Zealand	Provides information on the archival of government information.
Auditor General	Independent assurance over the performance and accountability of public sector organisations.
Audit New Zealand	Performance audits and better practice guides for areas including information security.
Department of Internal Affairs	Guidance on risk management, Authentication Standards, One.govt and i-govt services.
Department of Prime Minister and Cabinet	National security advice to government.
Ministry of Business, Innovation & Employment (MBIE)	Development, coordination and oversight of New Zealand Government policy on electronic commerce, online services and the Internet.
Ministry of Foreign Affairs and Trade	Policy and advice for security overseas.
National Cyber Security Centre (NCSC)	Provides enhanced services to government agencies and critical infrastructure providers to assist them to defend against cyber-borne threats.
New Zealand Police	Law enforcement in relation to electronic crime and other high tech crime.
New Zealand Security Intelligence Service	Personnel and Physical security advice Maintenance of the New Zealand Government Security Classification System.
Office of the Government Chief Information Officer (DIA)	Advice, guidance and management for sector and All-of-Government systems and ICT processes. ICT assurance (including privacy and security).
Privacy Commissioner	Advice on how to comply with the Privacy Act and related legislation.
State Services Commission	Monitoring of Public Service organisations and Chief Executives' performance.
DIA	Government Chief Privacy Office (GCPO)
NZCERT	General reporting of Cyber Security problems.

References

2.1.9. The following websites can be used to obtain additional information about the security of government systems:

Organisation		Source
Government Communications Security Bureau		http://www.gcsb.govt.nz
Archives New Zealand		http://www.archives.govt.nz
Audit New Zealand		http://www.auditnz.govt.nz
Auditor General		http://www.oag.govt.nz
Department of Internal Affairs		http://www.dia.govt.nz http://www.ict.govt.nz
Department of Prime Minister and Cabinet		http://www.dpmc.govt.nz
Ministry of Business, Innovation & Employment (MBIE)		http://www.mbie.govt.nz
Ministry of Foreign Affairs and Trade		http://www.mfat.govt.nz
National Cyber Security Centre (NCSC)		http://www.ncsc.govt.nz
New Zealand Security Intelligence Service		http://www.security.govt.nz
New Zealand Police		http://www.police.govt.nz
Privacy Commissioner		http://www.privacy.org.nz
Protective Security Requirements		http://www.protectivesecurity.govt.nz
Standards NZ		http://www.standards.co.nz
State Services Commission		http://www.ssc.govt.nz

Rationale & Controls

2.1.10. Organisations providing information security services

2.1.10.R.01. Rationale

If security personnel are unaware of the role government organisations play with regards to information security they could be missing out on valuable insight and assistance in developing an effective information security posture for their agency.

2.1.10.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Security personnel SHOULD familiarise themselves with the information security roles and services provided by New Zealand Government organisations.

2.2. Industry Engagement and Outsourcing

Objective

2.2.1. Industry handling classified information implements the same security measures as government agencies.

Context

Scope

2.2.2. This section covers information on outsourcing information technology services and functions to contractors as well as providing those partners with classified information in order to undertake their contracted duties.

Cloud computing

2.2.3. Cloud computing is a form of outsourcing information technology services and functions usually over the Internet. The requirements within this section for outsourcing equally apply to providers of cloud computing services.

PSR References

2.2.4. Additional information on third party providers is provided in the PSR.

Reference	Title	Source
PSR Mandatory Requirements	GOV6, GOV8, GOV9, PERSEC1, PERSEC3, and PERSEC6	http://www.protectivesecurity.govt.nz
PSR content protocols and requirements sections	Security Requirements of Outsourced Services and Functions New Zealand Government Information in Outsourced or Offshore ICT Arrangements	http://www.protectivesecurity.govt.nz
Support Resources	Non-Disclosure Agreement	http://www.protectivesecurity.govt.nz

Rationale & Controls

2.2.5. Outsourcing information technology services and functions

2.2.5.R.01. Rationale

In the context of this section, outsourcing is defined as contracting an outside entity to provide essential business functions and processes that could be undertaken by the Agency itself.

Outsourcing may present elevated levels of risk and additional risks. Outsourcing therefore, requires greater consideration, demonstrable governance, and higher levels of assurance before committing to such contracts.

2.2.5.R.02. Rationale

A distinction is drawn between important business functions and the purchase of services such as power, water, building maintenance, stationery and telecommunications. These services are not usually provided by the agency itself.

Purchased services, as identified above, do NOT require accreditation or a third party review as defined in the NZISM. However, normal contract due diligence should be exercised before committing to these supply contracts.

2.2.5.R.03. Rationale

Contractors can be provided with classified information as long as their systems are accredited to an appropriate classification in order to process, store and communicate that information. Contractors and all staff with access to the classified systems must also be cleared to the level of the information being processed. This ensures that when they are provided with classified information that it receives an appropriate level of protection.

2.2.5.R.04. Rationale

New Zealand, in common with most developed countries, has agreements with other nations on information exchange on a variety of topics, including arms control, border control, biosecurity, policing and national security. The lead agency in each sector will usually be the controlling agency for each agreement. While the detail and nature of these agreements is sometimes classified, the agreements invariably require the protection of any information provided, to the level determined by the originator. Agencies that receive such information will be fully briefed by the relevant controlling agency or authority, *before* information is provided. It is important to note that there is no single list or source of such agreements.

2.2.5.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies engaging industry for the provision of off-site information technology services and functions MUST accredit the systems used by the contractor to at least the same minimum standard as the agency's systems. This may be achieved through a third party review report utilising the ISAE 3402 Assurance Reports on Controls at a Third Party Service Organisation.

2.2.5.C.02. **Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT engage industry for the provision of off-site information technology services and functions in countries that New Zealand does not have a multilateral or bilateral security agreement with for the protection of classified information of the government of New Zealand. If there is any doubt, the agency's CISO should be consulted.

2.2.6. Independence of ITSMs from outsourced companies

2.2.6.R.01. **Rationale**

If an agency engages an organisation for the provision of information technology services and functions, and where that organisation also provides the services of an Information Technology Security Manager, they need to ensure that there is no actual or perceived conflict of interest (See also Section 3.3 - Information Technology Security Manager).

2.2.6.R.02. **Rationale**

When an agency engages a company for the provision of information technology services and functions having a central point of contact for information security matters within the company will greatly assist with incident response and reporting procedures.

2.2.6.C.01. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

Where an agency has outsourced information technology services and functions, any ITSMs within the agency SHOULD be independent of the company providing the information technology services and functions.

2.2.6.C.02. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

Where an agency has outsourced information technology services and functions, they SHOULD ensure that the outsourced organisation provides a single point of contact within the organisation for all information assurance and security matters.

2.2.7. Developing a contractor management program

2.2.7.R.01. **Rationale**

The development of a contractor management program will assist the agency in undertaking a coordinated approach to the engagement and use of contractors for outsourcing and provision of information technology services and functions.

2.2.7.C.01. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD develop a program to manage contractors that have been accredited for the provision of off-site information technology services and functions.

2.3. Approach to Cloud Services

Objective

2.3.1. Agencies understand and manage their approach to cloud services securely, effectively and efficiently.

Context

Scope

2.3.2. This section provides guidance on approaches to cloud services.

2.3.3. It is important that agencies identify cloud systems risks and that Official Information and agency information systems are protected in accordance with Cabinet Directives, the PSR, the NZISM, the New Zealand Classification System and with other government security requirements and guidance.

2.3.4. Reference should also be made to the following sections in the NZISM:

- Chapter 4 – System Certification and Accreditation
- Chapter 5 – Information Security Documentation
- Chapter 13 – Decommissioning and Disposal
- Chapter 16 – Access Control
- Chapter 17 – Cryptography
- Chapter 19 – Gateway Security
- Chapter 20 – Data Management
- Chapter 22 – Enterprise Systems Security

2.3.5. Detailed controls for Cloud Computing are provided in Section 22.1 – Cloud Computing.

Mandates, Directives and Requirements

2.3.6. In 2012, Cabinet directed government agencies to adopt public cloud services in preference to traditional IT systems. Offshore-hosted office productivity services were excluded **[CAB Min (12) 29/8A]**

2.3.7. In August 2013, the Government introduced their approach to cloud computing, establishing a 'cloud first' policy and an All-of-Government direction to cloud services development and deployment. This is enabled by the Cabinet Minute **[CAB Min (13) 37/6B]**. Under the 'cloud first' policy state service agencies are expected to adopt approved cloud services either when faced with new procurements, or a contract extension decision.

2.3.8. Cabinet also incorporated the cloud risk assessment process into the system-wide ICT assurance framework **[CAB Min (13) 20/13]**.

2.3.9. The New Zealand Government ICT Strategy released in October 2015 requires agencies to outsource their IT functions using common capabilities and public cloud services where this was feasible and practical.

2.3.10. In 2014 The Government Chief Information Officer published Cloud Computing Information Security and Privacy Considerations. This guidance is designed to assist agencies systematically identify, analyse, and evaluate information security and privacy risks related to individual public cloud services.

2.3.11. In July 2016, new measures were confirmed to accelerate the adoption of public cloud services by New Zealand's government agencies. The new measures complement existing policies and risk assessment processes and provide appropriate checks and balances.

Background

2.3.12. The adoption of cloud technologies and services, the hosting of critical data in the cloud and the risk environment requires that agencies exercise caution. Many cloud users are driven by the need for performance, scalability, resource sharing and cost saving so a comprehensive risk assessment is essential in identifying and managing jurisdictional, sovereignty, governance, assurance, technical and security risks.

2.3.13. Security requirements and drivers in the cloud differ significantly from traditional data centre environments requiring new security models and architectures. Key factors include:

- The dynamic nature of the cloud and its related infrastructure;
- No customer ownership or control of infrastructure;
- Limited visibility of architectures and transparency of operations;
- Shared (multi-tenanted) physical and virtual environments; and
- May require re-architecting of agency system to optimise use of cloud services.

2.3.14. While there is potential for significant benefit, flexibility and cost saving, any use of cloud services carries risk. All cloud computing decisions should be made on a case-by-case basis after a proper risk assessment, the agency technology architecture is developed and security is properly considered and incorporated.

2.3.15. There is also likely to be a significant mismatch in service-level agreements (SLAs) between existing systems and outsourcing arrangements and those of cloud-based services.

2.3.16. It is important to note that although agencies can outsource operational **responsibilities** to a service provider for implementing, managing and maintaining security controls, they cannot outsource their **accountability** for ensuring their data is appropriately protected, including any system or service decommissioning or termination.

2.3.17. The GCIO has developed a risk and assurance framework for cloud computing, which agencies are required to follow when they are considering using cloud services.

References

Reference/Title	Publisher	Source
CAB Min (12_ 29/8A Managing The Government's Adoption of Cloud Computing	Cabinet Office	https://www.ict.govt.nz/assets/Uploads/Documents/CabMin12-cloud-computing.pdf
CAB Min (13) 20/13 Improving Government Information and Communications Technology Assurance	Cabinet Office	https://www.ict.govt.nz/assets/Cabinet-Papers/Cab-Minute-Improving-Govt-ICT-Assurance-June-2013.pdf
Cloud Computing – Information Security and Privacy Considerations April 2014	DIA	https://www.ict.govt.nz/assets/ICT-System-Assurance/Cloud-Computing-Information-Security-and-Privacy-Considerations-FINAL2.pdf
Government ICT Strategy 2015	DIA	https://www.ict.govt.nz/strategy-and-action-plan/strategy/
Accelerating the Adoption of Public Cloud Services	DIA	https://www.ict.govt.nz/assets/Cloud-computing/Accelerating-the-Adoption-of-Public-Cloud-Services-Redacted.pdf
Cloud Risk Assessment Tool [Excel Spreadsheet]	DIA	https://www.ict.govt.nz/assets/Guidance-and-Resources/Cloud-ICT-Assurance/Cloud-Risk-Assessment-Tool-v1-1-1.xlsx
Risk Assessment Process	DIA	https://www.ict.govt.nz/assets/ICT-System-Assurance/Risk-Assessment-Process-Information-Security.pdf

PSR References

2.3.18. Additional information on third party providers is provided in the PSR.

Reference	**Title**	**Source**
PSR Mandatory Requirements	GOV6, GOV8, GOV9, PERSEC1, PERSEC3, and PERSEC6	http://www.protectivesecurity.govt.nz
PSR content protocols and requirements sections	Security Requirements of Outsourced Services and Functions New Zealand Government Information in Outsourced or Offshore ICT Arrangements	http://www.protectivesecurity.govt.nz
Support Resources	Non-Disclosure Agreement	http://www.protectivesecurity.govt.nz

Rationale & Controls

2.3.19. Risk Assessment

2.3.19.R.01. Rationale

The adoption of cloud technologies will introduce a wide range of technology and information system risks *in addition* to the risks that already exist for agency systems. It is vital that these additional risks are identified and assessed in order to select appropriate controls and countermeasures. Trust boundaries must be defined to assist in determining effective controls and where these controls can best be applied. The geographic location of agency data should be identified as this may include offshore data centres.

2.3.19.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies intending to adopt cloud technologies or services MUST conduct a comprehensive risk assessment, in accordance with the guidance provided by the GCIO *before* implementation or adoption.

2.3.19.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure cloud risks for any cloud service adopted are identified, understood and formally accepted by the Agency Head or Chief Executive and the agency's Accreditation Authority.

2.3.20. Security Architecture

2.3.20.R.01. Rationale

The adoption of cloud technologies will introduce a wide range of technology and information system risks *in addition* to the risks that already exist for agency systems. It is vital that these additional risks are identified and assessed in order to select appropriate controls and countermeasures.

2.3.20.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies intending to adopt cloud services SHOULD review and enhance existing security architectures and systems design to prudently manage the changed risk, technology and security environment in adopting cloud services.

2.3.21. Selection of Services

2.3.21.R.01. Rationale

A number of cloud related service, contracts and other arrangements have been negotiated on behalf of the New Zealand Government with a number of cloud service providers. Agencies must consider these services before negotiating individual contracts or supply contract with cloud service providers.

2.3.21.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST consider the use of any All of Government contracts with cloud service providers before negotiating individual contracts.

2.3.22. System Decommissioning and Contract Termination

2.3.22.R.01. Rationale

It is important that agencies understand how and where their data is processed, managed, stored, backed up and archived within the cloud service provider's environment. This may result in multiple copies of agency data in several data centres, possibly also in several countries.

2.3.22.R.02. Rationale

When an agency system or service is decommissioned or a service provider's contract terminated, it is important that agencies ensure data is returned to the agency and no copies are retained by the service provider.

2.3.22.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agency system architectures and supply arrangements and contracts SHOULD include provision for the safe return of agency data in the event of system or service termination or contract termination.

3. Information security governance - roles and responsibilities

3.1. The Agency Head

Objective

3.1.1. The agency head endorses and is accountable for information security within their agency.

Context

Scope

3.1.2. This section covers the role of an agency head with respect to information security.

Chief executive officer /or other title

3.1.3. In some agencies and bodies, the person responsible for the agency or body may also be referred to as the CEO, Director-General, Director or similar title specific to that agency. In such cases the policy for the agency head is equally applicable.

Devolving authority

3.1.4. When the agency head's authority in this area has been devolved to a board, committee or panel, the requirements of this section relate to the chair or head of that body.

3.1.5. The Agency Head is also the Accreditation Authority for that agency. See also Section 4.4 – Accreditation Framework.

3.1.6. Smaller agencies may not be able to satisfy all segregation of duty requirements because of scalability and small personnel numbers. In such cases, potential conflicts of interest should be clearly identified, declared and actively managed for the protection of the individual and of the agency.

3.1.7. Refer also to *Compliance By Smaller Agencies* in 1.2.8 for information on joint approaches and resource pooling.

Rationale & Controls

3.1.8. Delegation of authority

3.1.8.R.01. Rationale

When an agency head chooses to delegate their authority as the Agency's Accreditation Authority they should do so with careful consideration of all the associated risks, as they remain responsible for the decisions made by their delegate.

3.1.8.R.02. Rationale

The CISO is the most appropriate choice for delegated authority as they should be a senior executive and hold specialised knowledge in information security and security risk management.

3.1.8.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Where the agency head devolves their authority the delegate MUST be at least a member of the Senior Executive Team or an equivalent management position.

3.1.8.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

When the agency head devolves their authority the delegate SHOULD be the CISO.

3.1.8.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Where the head of a smaller agency is not able to satisfy all segregation of duty requirements because of scalability and small personnel numbers, all, potential conflicts of interest SHOULD be clearly identified, declared and actively managed.

3.1.9. Support for information security

3.1.9.R.01. Rationale

Without the full support of the agency head, security personnel are less likely to have access to sufficient resources and authority to successfully implement information security within their agency.

3.1.9.R.02. Rationale

If an incident, breach or disclosure of classified information occurs in preventable circumstances, the relevant agency head will ultimately be held accountable.

3.1.9.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

The agency head MUST provide support for the development, implementation and ongoing maintenance of information security processes within their agency.

3.2. The Chief Information Security Officer

Objective

3.2.1. The Chief Information Security Officer (CISO) sets the strategic direction for information security within their agency.

Context

Scope

3.2.2. This section covers the role of a CISO with respect to information security within an agency.

Appointing a CISO

3.2.3. The requirement to appoint a member of the Senior Executive Team or an equivalent management position, to the role of CISO does not require a new dedicated position be created in each agency.

3.2.4. The introduction of the CISO role and associated responsibilities is aimed at providing a more meaningful title for a subset of the security executive's responsibilities that relate to information security within their agency.

3.2.5. The CISO should bring accountability and credibility to information security management and appointees should be suitably qualified and experienced.

3.2.6. Where multiple roles are held by the CISO, for example CIO, or manager of a business unit, conflicts of interest may occur where operational imperatives conflict with security requirements. Good practice separates these roles. Where multiple roles are held by an individual, potential conflicts of interest should be clearly identified and a mechanism implemented to allow independent decision making in areas where conflict may occur.

PSR references

Reference	Title	Source
PSR Mandatory Requirements	GOV5, GOV6, INFOSEC2 and INFOSEC4	http://www.protectivesecurity.govt.nz
PSR content protocols and requirements sections	Security Awareness Training Compliance Reporting	http://www.protectivesecurity.govt.nz

Rationale & Controls

3.2.7. Requirement for a CISO

3.2.7.R.01. Rationale

The role of the CISO is based on industry and governance good practice and has been introduced to ensure that information security is managed at the senior executive level within agencies. Without a CISO there is a risk that an agency may not be resourced to effectively manage information security.

3.2.7.R.02. Rationale

The CISO within an agency is responsible predominately for facilitating communications between security personnel, ICT personnel and business personnel to ensure alignment of business and security objectives within the agency.

3.2.7.R.03. Rationale

The CISO is also responsible for providing strategic level guidance for the agency security program and ensuring compliance with national policy, standards, regulations and legislation.

3.2.7.R.04. Rationale

Some agencies may outsource the CISO function. In such cases conflicts of interest, availability and response times should be identified and carefully managed so the agency is not disadvantaged. Conflicts of interest may also be apparent where the outsourced CISO deals with other vendors.

3.2.7.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

The CISO MUST be:

- cleared for access to all classified information processed by the agency's systems, and
- able to be briefed into any compartmented information on the agency's systems.

3.2.7.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD appoint a person to the role of CISO or have the role undertaken by an existing person within the agency.

3.2.7.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

The CISO role SHOULD be undertaken by a member of the Senior Executive Team or an equivalent management position.

3.2.7.C.04. Control: System Classification(s): All Classifications; Compliance: SHOULD

The CISO SHOULD be responsible for overseeing the management of security personnel within the agency.

3.2.7.C.05. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

Where the role of the CISO is outsourced, potential conflicts of interest in availability, response times or working with vendors SHOULD be identified and carefully managed.

3.2.8. Responsibilities – Reporting

3.2.8.R.01. **Rationale**

As the CISO is responsible for the overall management of information security within an agency it is important that they report directly to the agency head on any information security issues.

3.2.8.C.01. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

The CISO SHOULD report directly to the agency head on matters of information security within the agency.

3.2.9. Responsibilities – Security programs

3.2.9.R.01. **Rationale**

Without a comprehensive strategic level information security and security risk management program an agency will lack high-level direction on information security issues and may expose the agency to unnecessary risk.

3.2.9.C.01. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

The CISO SHOULD develop and maintain a comprehensive strategic level information security and security risk management program within the agency aimed at protecting the agency's official and classified information.

3.2.9.C.02. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

The CISO SHOULD be responsible for the development of an information security communications plan.

3.2.9.C.03. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

The CISO SHOULD create and facilitate the agency security risk management process.

3.2.10. Responsibilities – Ensuring compliance

3.2.10.R.01. Rationale

Without having a person responsible for ensuring compliance with the information security policies and standards within the agency, security measures of the agency are unlikely to meet minimum government requirements and may expose the agency to unnecessary risk.

3.2.10.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

The CISO SHOULD be responsible for ensuring compliance with the information security policies and standards within the agency.

3.2.10.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

The CISO SHOULD be responsible for ensuring agency compliance with the NZISM through facilitating a continuous program of certification and accreditation based on security risk management.

3.2.10.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

The CISO SHOULD be responsible for the implementation of information security measurement metrics and key performance indicators within the agency.

3.2.11. Responsibilities – Coordinating security

3.2.11.R.01. Rationale

One of the core roles of the CISO is to ensure appropriate communication between business and information security teams within their agency. This includes interpreting information security concepts and language into business concepts and language as well as ensuring that business teams consult with information security teams to determine appropriate security measures when planning new business projects for the agency.

3.2.11.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

The CISO SHOULD facilitate information security and business alignment and communication through an information security steering committee or advisory board which meets formally and on a regular basis, and comprises key business and ICT executives.

3.2.11.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

The CISO SHOULD be responsible for coordinating information security and security risk management projects between business and information security teams.

3.2.11.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

The CISO SHOULD work with business teams to facilitate security risk analysis and security risk management processes, including the identification of acceptable levels of risk consistently across the agency.

3.2.12. Responsibilities – Working with ICT projects

3.2.12.R.01. Rationale

As the CISO is responsible for the development of the strategic level information security program within an agency they are best placed to advise ICT projects on the strategic direction of information security within the agency.

3.2.12.R.02. Rationale

As the CISO is responsible for the overall management of information security within an agency, they are best placed to recommend to the accreditation authority the acceptance of residual security risks associated with the operation of agency systems.

3.2.12.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

The CISO SHOULD provide strategic level guidance for agency ICT projects and operations.

3.2.12.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

The CISO SHOULD liaise with agency architecture teams to ensure alignment between security and agency architectures.

3.2.13. Responsibilities – Working with vendors

3.2.13.R.01. Rationale

Having the CISO coordinate the use of external information security resources will ensure that a consistent approach is being applied across the agency.

3.2.13.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

The CISO SHOULD coordinate the use of external information security resources to the agency including contracting and managing the resources.

3.2.14. Responsibilities – Budgeting

3.2.14.R.01. Rationale

Controlling the information security budget will ensure that the CISO has sufficient access to funding to support information security projects and initiatives.

3.2.14.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

The CISO SHOULD be responsible for controlling the information security budget.

3.2.15. Responsibilities – Information security incidents

3.2.15.R.01. Rationale

To ensure that the CISO is able to accurately report to the agency head on information security issues within their agency it is important that they remain fully aware of all information security incidents within their agency.

3.2.15.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

The CISO SHOULD be fully aware of all information security incidents within the agency.

3.2.16. Responsibilities – Disaster recovery

3.2.16.R.01. Rationale

Restoring business-critical services to an operational state after a disaster is an important function of business continuity. As such it will need high level support from the CISO.

3.2.16.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

The CISO SHOULD coordinate the development of disaster recovery policies and standards within the agency to ensure that business-critical services are supported appropriately and that information security is maintained in the event of a disaster.

3.2.17. Responsibilities – Training

3.2.17.R.01. Rationale

To ensure personnel within an agency are actively contributing to the information security posture of the agency, an information security awareness and training program will need to be developed. As the CISO is responsible for information security within the agency they will need to oversee the development and operation of the program.

3.2.17.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

The CISO SHOULD be responsible for overseeing the development and operation of information security awareness and training programs within the agency.

3.2.18. Responsibilities – Providing security knowledge

3.2.18.R.01. Rationale

The CISO is not expected to be a technical expert on information security matters; however, knowledge of national and international standards and good practice will assist in communicating with technical experts within their agency on information security matters.

3.2.18.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

The CISO SHOULD provide authoritative security advice and have familiarity with a range of national and international standards and good practice.

3.3. Information Technology Security Managers

Objective

3.3.1. Information Technology Security Managers (ITSM) provide information security leadership and management within their agency.

Context

Scope

3.3.2. This section covers the role of an ITSM with respect to information security within an agency.

Information technology security managers

3.3.3. ITSMs are executives within an agency that act as a conduit between the strategic directions provided by the CISO and the technical efforts of systems administrators. The main area of responsibility of an ITSM is that of the administrative and process controls relating to information security within the agency.

Rationale & Controls

3.3.4. Requirement for ITSMs

3.3.4.R.01. **Rationale**

When agencies outsource their ICT services, ITSMs should be independent of any company providing ICT services. This will prevent any conflict of interest for an ITSM in conducting their duties.

3.3.4.R.02. **Rationale**

Ensure that the agency has a point of presence at sites to assist with monitoring information security for systems and responding to any information security incidents.

3.3.4.C.01. **Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST appoint at least one ITSM within their agency.

3.3.4.C.02. **Control:** System Classification(s): All Classifications; Compliance: MUST

ITSMs MUST be:

- cleared for access to all classified information processed by the agency's systems; and
- able to be briefed into any compartmented information on the agency's systems.

3.3.4.C.03. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

Where an agency is spread across a number of geographical sites, it is recommended that the agency SHOULD appoint a local ITSM at each major site.

3.3.4.C.04. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

The ITSM role SHOULD be undertaken by personnel with an appropriate level of authority and training based on the size of the agency or their area of responsibility within the agency.

3.3.4.C.05. **Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

ITSMs SHOULD NOT have additional responsibilities beyond those needed to fulfil the role as outlined within this manual.

3.3.5. Responsibilities – Security programs

3.3.5.R.01. **Rationale**

As ITSMs undertake operational management of information security within an agency they can provide valuable input to the development of the information security program by the CISO.

3.3.5.C.01. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

ITSMs SHOULD work with the CISO to develop an information security program within the agency.

3.3.5.C.02. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

ITSMs SHOULD undertake and manage projects to address identified security risks.

3.3.6. Responsibilities – Working with ICT projects

3.3.6.R.01. **Rationale**

As ITSMs have knowledge of all aspects of information security they are best placed to work with ICT projects within the agency to identify and incorporate appropriate information security measures.

3.3.6.C.01. **Control:** System Classification(s): All Classifications; Compliance: MUST

ITSMs MUST be responsible for assisting system owners to obtain and maintain the accreditation of their systems.

3.3.6.C.02. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

ITSMs SHOULD identify systems that require security measures and assist in the selection of appropriate information security measures for such systems.

3.3.6.C.03. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

ITSMs SHOULD consult with ICT project personnel to ensure that information security is included in the evaluation, selection, installation, configuration and operation of IT equipment and software.

3.3.6.C.04. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

ITSMs SHOULD work with agency enterprise architecture teams to ensure that security risk assessments are incorporated into system architectures and to identify, evaluate and select information security solutions to meet the agency's security objectives.

3.3.6.C.05. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

ITSMs SHOULD work with system owners, systems certifiers and systems accreditors to determine appropriate information security policies for their systems and ensure consistency with the PSR and in particular the relevant NZISM components.

3.3.6.C.06. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

ITSMs SHOULD be included in the agency's change management and change control processes to ensure that risks are properly identified and controls are properly applied to manage those risks.

3.3.6.C.07. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

ITSMs SHOULD notify the Accreditation Authority of any significant change that may affect the accreditation of that system.

3.3.7. Responsibilities – Working with vendors

3.3.7.R.01. **Rationale**

The CISO will coordinate the use of external information security resources to the agency, whilst ITSMs will be responsible for establishing contracts and service-level agreements on behalf of the CISO.

3.3.7.C.01. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

ITSMs SHOULD liaise with vendors and agency purchasing and legal areas to establish mutually acceptable information security contracts and service-level agreements.

3.3.8. Responsibilities – Implementing security

3.3.8.R.01. **Rationale**

The CISO will set the strategic direction for information security within the agency, whereas ITSMs are responsible for managing the implementation of information security measures within the agency.

3.3.8.C.01. **Control:** System Classification(s): All Classifications; Compliance: MUST

ITSMs MUST be responsible for ensuring the development, maintenance, updating and implementation of Security Risk Management Plans (SRMPs), Systems Security Plans (SecPlan) and any Standard Operating Procedures (SOPs) for all agency systems.

3.3.8.C.02. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

ITSMs SHOULD conduct security risk assessments on the implementation of new or updated IT equipment or software in the existing environment and develop treatment strategies if necessary.

3.3.8.C.03. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

ITSMs SHOULD select and coordinate the implementation of controls to support and enforce information security policies.

3.3.8.C.04. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

ITSMs SHOULD provide leadership and direction for the integration of information security strategies and architecture with agency business and ICT strategies and architecture.

3.3.8.C.05. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

ITSMs SHOULD provide technical and managerial expertise for the administration of information security management tools.

3.3.9. Responsibilities – Budgeting

3.3.9.R.01. **Rationale**

As ITSMs are responsible for the operational management of information security projects and functions within their agency, they will be aware of their funding requirements and can assist the CISO to develop information security budget projections and resource allocations.

3.3.9.C.01. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

ITSMs SHOULD work with the CISO to develop information security budget projections and resource allocations based on short-term and long-term goals and objectives.

3.3.10. Responsibilities – Reporting

3.3.10.R.01. **Rationale**

To ensure the CISO remains aware of all information security issues within their agency, and can brief their agency head when necessary, ITSMs will need to provide regular reports on policy developments, proposed system changes and enhancements, information security incidents and other areas of particular concern to the CISO.

3.3.10.C.01. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

ITSMs SHOULD coordinate, measure and report on technical aspects of information security management.

3.3.10.C.02. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

ITSMs SHOULD monitor and report on compliance with information security policies, as well as the enforcement of information security policies within the agency.

3.3.10.C.03. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

ITSMs SHOULD provide regular reports on information security incidents and other areas of particular concern to the CISO.

3.3.10.C.04. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

ITSMs SHOULD assess and report on threats, vulnerabilities, and residual security risks and recommend remedial actions.

3.3.11. Responsibilities – Auditing

3.3.11.R.01. Rationale

As system owners may not understand the results of audits against their systems ITSMs will need to assist them in understanding and responding to reported audit failures. ITSM's should also refer to 5.8 Independent Assurance Reports.

3.3.11.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

ITSMs SHOULD assist system owners and security personnel in understanding and responding to audit failures reported by auditors.

3.3.12. Responsibilities – Disaster recovery

3.3.12.R.01. Rationale

Whilst the CISO will coordinate the development of disaster recovery policies and standards within the agency, ITSMs will need to guide the selection of appropriate strategies to achieve the direction set by the CISO.

3.3.12.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

ITSMs SHOULD assist and guide the disaster recovery planning team in the selection of recovery strategies and the development, testing and maintenance of disaster recovery plans.

3.3.13. Responsibilities – Training

3.3.13.R.01. Rationale

The CISO will oversee the development and operation of information security awareness and training programs within the agency. ITSMs will arrange delivery of that training to personnel within the agency.

3.3.13.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

ITSMs SHOULD provide or arrange for the provision of information security awareness and training for all agency personnel.

3.3.13.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

ITSMs SHOULD develop technical information materials and workshops on information security trends, threats, good practices and control mechanisms as appropriate.

3.3.14. Responsibilities – Providing security knowledge

3.3.14.R.01. Rationale

ITSMs will often have a strong knowledge of information security topics and can provide advice for the information security steering committee, change management committee and other agency and inter-agency committees.

3.3.14.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

ITSMs SHOULD maintain a current and up-to-date security knowledge base comprising of a technical reference library, security advisories and alerts, information on information security trends and practices, and relevant laws, regulations, standards and guidelines.

3.3.14.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

ITSMs SHOULD provide expert guidance on security matters for ICT projects.

3.3.14.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

ITSMs SHOULD provide technical advice for the information security steering committee, change management committee and other agency and inter-agency committees as required.

3.3.15. Responsibilities

3.3.15.R.01. Rationale

ITSMs are generally considered the information security experts within an agency and as such their contribution to improving the information security of systems, providing input to agency ICT projects, assisting other security personnel within the agency, contributing to information security training and responding to information security incidents is a core aspect of their work.

3.3.15.R.02. Rationale

An ITSM is likely to have the most up to date and accurate understanding of the threat environment relating to systems. As such, it is essential that this information is passed to system owners to ensure that it is considered during accreditation activities.

3.3.15.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

The ITSM SHOULD keep the CISO and system owners informed with up-to-date information on current threats.

3.4. System Owners

Objective

3.4.1. System owners obtain and maintain accreditation of their systems, including any directly related services such as cloud.

Context

Scope

3.4.2. This section covers the role that system owners undertake with respect to information security.

Assertions in Certification and Accreditation

3.4.3. Originating in financial auditing, assertions are now widely used as the basis for assurance processes covering a wide range of business activities and the related technology.

3.4.4. Assertions are formal statements by management or system owners. They are claims on the completeness, accuracy and validity of events, presentations, disclosure, transactions and related assurance, risk and governance aspects of certification and accreditation.

3.4.5. It is the responsibility of the management (or system owner) to prepare and validate assertions relating to the governance, assurance and security of information systems, in accordance with national policy and related standards.

3.4.6. When such assertions are made it means management (or system owners) have presented and disclosed information appropriately giving a true, fair and balanced view of the activities. In preparing assertions, implicit and explicit claims are made on the validity and completeness of the assertions.

3.4.7. Assertions are typically characterised as follows:

Transactions and events

- Occurrence — the activities recorded have actually taken place.
- Completeness — all aspects are properly recorded.
- Accuracy — the assets and activities are accurately allocated and recorded.
- Cutoff — the activities have been recorded in the correct time period.
- Classifications — are accurate and appropriate.

Position on project completion

- Existence — assets, liabilities and equity balances exist.
- Rights and Obligations — the entity legally controls rights to its assets and its liabilities and accurately records obligations.
- Completeness — all aspects are properly recorded.
- Valuation and Allocation — costs and assets appropriately valued and allocated.

Presentation and disclosure

- Occurrence — the events and implementations have actually occurred.
- Rights and Obligations — contracts, licences, support and supply agreements
- Completeness — all disclosures have been included in the statements.
- Classification — statements are clear and appropriately presented.
- Accuracy and Valuation — information is disclosed at the appropriate amounts.

Rationale & Controls

3.4.8. Requirement for system owners

3.4.8.R.01. Rationale

The system owner is responsible for the overall operation of the system, including any directly related support or outsourced service such as cloud. They may delegate the day-to-day management and operation of the system to a system manager or managers.

3.4.8.R.02. Rationale

All systems should have a system owner in order to ensure IT governance processes are followed and that business requirements are met.

3.4.8.R.03. Rationale

It is strongly recommended that a system owner be a member of the Senior Executive Team or in an equivalent management position, however this does not imply that the system manager(s) should also be at such a level.

3.4.8.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Each system MUST have a system owner who is responsible for the operation and maintenance of the system.

3.4.8.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

System owners SHOULD be a member of the Senior Executive Team or an equivalent management position, for large or critical agency systems.

3.4.9. Accreditation responsibilities

3.4.9.R.01. Rationale

The system owner is responsible for the operation of their system and as such they need to ensure that systems are accredited to meet the agency's operational requirements. If modifications are undertaken to a system the system owner will need to ensure that the changes are undertaken in an appropriate manner, documented adequately and that any necessary reaccreditation activities are completed.

3.4.9.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

System owners MUST obtain and maintain accreditation of their system(s).

3.4.10. Documentation responsibilities

3.4.10.R.01. Rationale

While the system owner is responsible for ensuring the development, maintenance and implementation of Systems Information Security documentation, in particular the Security Risk Management Plans (SRMPs), System Security Plans (SecPlans) and Standard Operating Procedures (SOPs), their exposure to information security issues can be too narrowly focused and restricted to the systems with which they are familiar. Involving security personnel in the process ensures that a holistic approach to information security can be mapped to the system owner's understanding of security risks for their specific system. Information Security documentation is detailed in Chapter 5. Refer also to Chapter 4 – System Certification & Accreditation.

3.4.10.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

System owners MUST ensure the development, maintenance and implementation of complete, accurate and up to date Information Security documentation for systems under their ownership. Such actions MUST be documented.

3.4.10.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

System Owners MUST involve the ITSM in the redevelopment and updates of the Information Security documentation.

3.5. System Users

Objective

3.5.1. System users comply with information security policies and procedures within their agency.

Context

Scope

3.5.2. This section covers the role that system users undertake with respect to information security.

Types of system users

3.5.3. This section covers responsibilities for all system users i.e. users with general access (general users), and users with privileged access (privileged users).

Rationale & Controls

3.5.4. Responsibilities of system users

3.5.4.R.01. Rationale

If agencies fail to develop and maintain a security culture where system users are complying with relevant security policies and procedures for the systems they are using, there is an increased security risk of a system user unwittingly assisting with an attack against a system.

3.5.4.R.02. Rationale

Security policies, procedures and mechanisms aim to cover all situations that may arise within an agency. However there may be legitimate reasons for a system user to bypass security policies, procedures or mechanisms. If this is the case, the system user MUST seek formal authorisations from the CISO or the ITSM (if this authority has been specifically delegated to the ITSM) before any actions are undertaken.

3.5.4.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

All system users MUST comply with the relevant security policies and procedures for the systems they use.

3.5.4.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

All system users MUST:

- protect account authenticators at the same classification of the system it secures;
- not share authenticators for accounts without approval;
- be responsible for all actions under their accounts; and
- use their access to only perform authorised tasks and functions.

3.5.4.C.03. Control: System Classification(s): All Classifications; Compliance: MUST

System users that need to bypass security policies, procedures or mechanisms for any reason MUST seek formal authorisation from the CISO or the ITSM if this authority has been specifically delegated to the ITSM.

4. System Certification and Accreditation

4.1. The Certification and Accreditation Process

Objective

4.1.1. Executives and Security Practitioners understand the Certification and Accreditation (C&A) process and its role in information security governance and assurance.

Context

Scope

4.1.2. This section provides a short, high-level description of the C&A process.

4.1.3. This section must be read in conjunction with the Roles and Responsibilities described in Chapter 3. Subsequent sections of this chapter describe elements of the C&A process in more detail.

The Process

4.1.4. Certification and Accreditation is a fundamental governance and assurance process, designed to provide the Board, Chief Executive and senior executives confidence that information and its associated technology are well-managed, that risks are properly identified and mitigated and that governance responsibilities can demonstrably be met. It is essential for credible and effective information assurance governance.

4.1.5. C&A has two important stages where certification must be completed *before* accreditation can take place. It is based on an assessment of risk, the application of controls described in the NZISM and determination of any residual risk.

4.1.6. Certification and Accreditation are separate and distinct elements, demonstrate segregation of duties and assist in managing any potential conflicts of interest. These are important attributes in good governance systems.

4.1.7. The acceptance of residual risk lies with the Chief Executive of each agency, or lead agency where sector, multi-agency or All-of-Government (AoG) systems are implemented.

4.1.8. An exception applies where high grade cryptographic equipment (HGCE) is required or endorsed or compartmented information is processed, stored or communicated. In this case the Director-General of the GCSB is the Accreditation Authority.

4.1.9. The complete C&A process has several elements and stages, illustrated in the Block Diagram at the end of this section.

Key Participants

4.1.10. There are four groups of participants:

- **System Owners**, responsible for the design, development, system documentation and system maintenance, including any requests for recertification or reaccreditation.
- The **Certification Authority**, responsible for the review of information and documentation provided by the system owner to ensure the ICT system complies with minimum standards and the agreed design.
- The **Assessor** or Auditor, who will conduct inspections, audits and review as instructed by the Certification Authority.
- The **Accreditation Authority** will consider the recommendation of the Certification Authority. If the level of residual risk is acceptable, the Accreditation Authority will issue the system accreditation (the formal authority to operate a system).

Certification

4.1.11. Certification is the assertion that an ICT system including any related or support services such as Telecommunications or cloud comply with the minimum standards and controls described in the NZISM, any relevant legislation and regulation and other relevant standards. It is based on a comprehensive evaluation or systems audit. This process is described in Section 4.2 – Conducting Certifications.

4.1.12. Certification is evidence that due consideration has been paid to risk, security, functionality, business requirements and is a fundamental part of information systems governance and assurance.

Certification Authorities

4.1.13. For all agency information systems the certification authority is the CISO unless otherwise delegated by the Agency Head.

4.1.14. For external organisations or service providers supporting agencies, the certification authority is the CISO of the agency.

4.1.15. For multi-national, multi-agency, and AoG systems the certification authority is determined by a formal agreement between the parties involved. Within NZ this is usually the lead agency.

Accreditation

4.1.16. Accreditation is the formal authority to operate a system, evidence that governance requirements have been addressed and that the Chief Executive has fulfilled the requirement to manage risk on behalf of the organisation and stakeholders. This element of the C&A process is described in Section 4.4 – Accreditation Framework.

4.1.17. Accreditation ensures that either sufficient security measures have been put in place to protect information that is processed, stored or communicated by the system or that deficiencies in such measures have been identified, assessed and acknowledged, including the acceptance of any residual risk.

Accreditation Authority

4.1.18. For agencies the Accreditation Authority is the agency head or their delegate.

4.1.19. For multi-national, multi-agency systems or AoG systems, the Accreditation Authority is determined by a formal agreement between the parties involved.

4.1.20. In all cases the Accreditation Authority will be at least a senior executive who has an appropriate level of understanding of the security risks they are accepting on behalf of the agency.

4.1.21. Depending on the circumstances and practices of an agency, the agency head could choose to delegate their authority to multiple senior executives who have the authority to accept security risks for the specific business functions within the agency, for example the CISO and the system owner.

Conflicts of Interest

4.1.22. A conflict of interest is a situation in which a person has duties or responsibilities to more than one person, organisation or elements of a process, but is placed in a position where they cannot do justice to all. This includes, for example, when an individual's vested interests or concerns are inconsistent with organisational outcomes, or when an official has conflicting responsibilities. In the context of the C&A process, a conflict of interest can occur when an individual has multiple roles, such as being both the system owner and the Accreditation Authority.

4.1.23. A conflict of interest has the potential to undermine impartiality and integrity of a process and the people involved in a process. It will also undermine the integrity of governance and information assurance derived from the C&A process.

4.1.24. Conflicts of interest are normally managed though segregation of duties, the division of **roles** and **responsibilities** in order to reduce the ability or opportunity for an individual to compromise a critical process. Segregation of duties also reduces errors of interpretation or judgement and better manages risk.

4.1.25. It is important to note that in the C&A process in the NZISM, the Certification Authority, System Owner and Accreditation Authority are *independent* of each other. In smaller agencies, the Assessor may also be the Certification Authority. Ideally this role will also be segregated.

Penetration Testing

4.1.26. Penetration tests are an effective method of identifying vulnerabilities that in a system or network testing existing security measures and testing the implementation of controls. Penetration testing is also very useful in validating the effectiveness of the defensive mechanisms. This testing provides an increased level of assurance when system certification and accreditation is undertaken. It also demonstrates prudent risk management.

4.1.27. A penetration test usually involves the use of intrusive methods or attacks conducted by trusted individuals, methods similar to those used by intruders or hackers. Care must be taken not to adversely affect normal operations while these tests are conducted.

4.1.28. Organisations may conduct their own tests and regular simple tests are effective in maintaining the organisation's security posture. Because of the level of expertise required to effectively conduct more complex testing, comprehensive penetration tests are often outsourced to specialist organisations.

4.1.29. Penetration tests can range from simple scans of IP addresses in order to identify devices or systems offering services with known vulnerabilities, to exploiting known vulnerabilities that exist in an unpatched operating system, applications or other software. The results of these tests or attacks are recorded, analysed, documented and presented to the owner of the system. Any deficiencies should then be addressed.

References

4.1.30. Additional information relating to systems governance, certification and accreditation can be found at:

Title	Publisher	Source
ISO/IEC 27000:2014 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary	ISO	http://www.standards.co.nz http://www.iso.org
ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements	ISO	http://www.standards.co.nz http://www.iso.org
ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls	ISO	http://www.standards.co.nz http://www.iso.org
ISO/IEC_27006:2011 Information Technology – Security Techniques - Requirements for bodies providing audit and certification of information security management systems	ISO	http://www.iso27001security.com/html/27006.html http://www.standards.co.nz
ISO/IEC_27007:2011 Information Technology – Security Techniques - Guidelines for information security management systems auditing	ISO	http://www.iso27001security.com/html/27007.html http://www.standards.co.nz
ISO 19011:2011 Guidelines for Auditing Management Systems	ISO	https://www.iso.org/standard/50675.html
NIST SP 800-37 Rev. 1, Feb 2010 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach	NIST	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf
NIST SP 800-171, June 2015 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations	NIST	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf
Mitre Engineering Guide - Create and Assess Certification and Accreditation Strategies	MITRE	http://www.mitre.org/publications/systems-engineering-guide/se-lifecycle-building-blocks/test-and-evaluation/create-and-assess-certification-and-accreditation-strategies
RAND National Defense Research Institute - Implications of Aggregated DoD Information Systems for Information Assurance Certification and Accreditation	RAND Corporation	http://www.rand.org/content/dam/rand/pubs/monographs/2010/RAND_MG951.pdf
An Introduction to Certification and Accreditation	SANS Institute	https://www.sans.org/reading-room/whitepapers/accreditation/introduction-certification-accreditation-1259

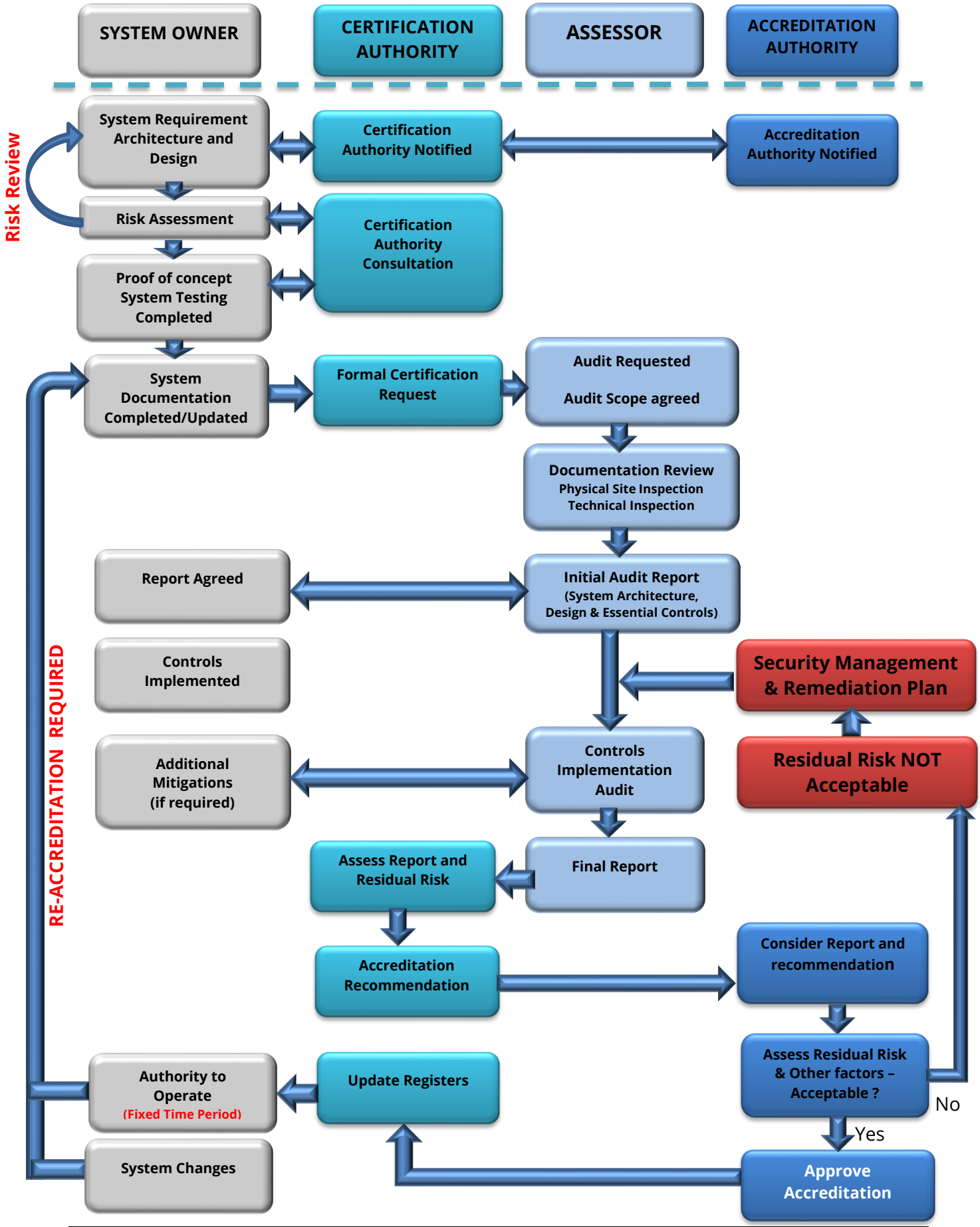
A Certification and Accreditation Plan for Information Systems Security Programs (Evaluating the Eff)	SANS Institute	https://www.sans.org/reading-room/whitepapers/accreditation/certification-accreditation-plan-information-systems-security-programs-evaluating-ef-597
Office of the Auditor-General - Managing conflicts of interest: Guidance for public entities	Office of the Auditor-General	http://www.oag.govt.nz/2007/conflicts-public-entities/docs/oag-conflicts-public-entities.pdf
Managing Conflict of Interest in the Public Service - OECD GUIDELINES AND COUNTRY EXPERIENCES	OECD	http://www.oecd.org/gov/ethics/48994419.pdf
Data Security Standard (DSS) Information Supplement, March 2008, PCI Security Standards Council,	PCI Security Standards	https://www.pcisecuritystandards.org/documents/information_supplement_11.3.pdf
SANS Institute InfoSec Reading Room, Conducting a Penetration Test on an Organization,	SANS Institute	http://www.sans.org/reading-room/whitepapers/auditing/conducting-penetration-test-organization-67
Commercially Available Penetration Testing Best Practice Guide, 8 May 2006, CPNI,	CPNI	http://www.cpni.gov.uk/Documents/Publications/2006/2006030-GPG_Penetration_testing.pdf
Beyond Best Practices: Web Application Security in the Real World, OWASP, June 2004,	OWASP	https://www.google.co.nz/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=14&cad=rja&uact=8&ved=0CEgQFjADOAo&url=https%3A%2F%2Fwww.owasp.org%2Fimages%2F1%2F15%2FAppSec2004-Dave_Aitel-Beyond_Best_Practices.ppt&ei=3lJJVaHwJ8azmAWF7oHwAw&usg=AFQjCNGPLB0YpXYcqr2L13mZiuy1FBjOeQ&bvm=bv.92291466,d.dGY
International Standard on Assurance Engagements (ISAE) 3402 - Assurance Reports on Controls at a Service Organization	International Federation of Accountants (IFAC)	http://www.ifac.org/system/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf

PSR references

4.1.31. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV3, GOV4, GOV7, INFOSEC1, INFOSEC2, INFOSEC4, INFOSEC5, PHYSEC1, PHYSEC6 and PHYSEC7	http://www.protectivesecurity.govt.nz
PSR content protocols and requirements sections	Developing Agency Protective Security Policies, Plans and Procedures Business Impact Levels Reporting Incidents and Conducting Security Investigations Compliance Reporting Physical Security of ICT Equipment, Systems and Facilities Agency Cyber Security Responsibilities for Publicly Accessible Information Systems.	http://www.protectivesecurity.govt.nz

System Certification and Accreditation Block Diagram



4.2. Conducting Certifications

Objective

4.2.1. The security posture of the organisation has been incorporated into its system security design, controls are correctly implemented, are performing as intended and that changes and modifications are reviewed for any security impact or implications.

Context

Scope

4.2.2. This section covers information on the process of undertaking a certification as part of the accreditation process for a system.

Certification

4.2.3. Certification is the assertion that a given ICT system complies with minimum standards and the agreed design. It is based on a comprehensive evaluation and may involve:

- development and review of security documentation;
- assurance over externally provided services such as Telecommunications and Cloud;
- a physical inspection;
- a technical review of the system and environment; and/or
- technical testing.

4.2.4. Certification is a **prerequisite** for accreditation. The Accreditation Authority for a specific system MUST NOT accredit that system until all relevant certifications have been provided.

Certification outcome

4.2.5. The outcome of certification is a certificate to the system owner acknowledging that the system has been appropriately audited and that the findings have been found to be of an acceptable standard.

Certification authorities

4.2.6. For all agency information systems the certification authority is the CISO unless otherwise delegated by the Agency Head.

4.2.7. For external organisations or service providers supporting agencies, the certification authority is the CISO of the agency.

4.2.8. For multi-national, multi-agency, and AoG systems the certification authority is determined by a formal agreement between the parties involved. Within NZ this is usually the lead agency.

References

4.2.9. Additional information relating to system auditing is contained in:

Reference	Title	Source
ISO/IEC_27006:2011	Information Technology – Security Techniques - Requirements for bodies providing audit and certification of information security management systems.	http://www.iso27001security.com/html/27006.html http://www.standards.co.nz
ISO/IEC_27007:2011	Information Technology – Security Techniques - Guidelines for information security management systems auditing.	http://www.iso27001security.com/html/27007.html http://www.standards.co.nz
ISO 19011:2011	Guidelines for Auditing Management Systems	https://www.iso.org/standard/50675.html

Rationale & Controls

4.2.10. Certification Audit

4.2.10.R.01. hnRationale

The purpose of a Certification Audit is to assess the actual implementation and effectiveness of controls for a system against the agency's risk profile, security posture, design specifications, agency policies and compliance with the PSR and in particular the relevant NZISM components.

4.2.10.R.02. Rationale

The extent and scope of the Certification Audit should consider the feasibility and cost-effectiveness of the audit against the risks and benefits of the system under review. Major or high-risk systems will require more detailed and extensive review than low-risk or minor systems. See also Section 4.3 Conducting Audits.

4.2.10.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

All systems MUST undergo an audit as part of the certification process.

4.2.11. Certification decision

4.2.11.R.01. Rationale

To award certification for a system the certification authority will need to be satisfied that the selected controls are appropriate, are consistent with the PSR and in particular the relevant NZISM components, have been properly implemented and are operating effectively.

4.2.11.R.02. Rationale

To cater for the different responsibilities for physical and technical Certification & Accreditation, separate reports and recommendations may be required.

4.2.11.R.03. Rationale

Certification acknowledges only that controls were appropriate, properly implemented and are operating effectively. Certification does NOT imply that the residual security risk is acceptable or an approval to operate has been granted.

4.2.11.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

The certification authority MUST accept that the controls are appropriate, effective and comply with the PSR and in particular the relevant NZISM components, in order to award certification.

4.2.12. Residual security risk assessment

4.2.12.R.01. Rationale

The purpose of the residual security risk assessment is to assess the risks, controls and residual security risk relating to the operation of a system. In situations where the system is non-conformant, the system owner may have taken corrective actions. The residual risk may not be great enough to preclude a certification authority recommending to the Accreditation Authority that accreditation be awarded but the risk MUST be acknowledged and appropriate qualifications or limitations documented.

4.2.12.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Following the audit, the certification authority SHOULD produce an assessment for the Accreditation Authority outlining the residual security risks relating to the operation of the system and a recommendation on whether to award accreditation or not.

4.3. Conducting Audits

Objective

4.3.1. The effectiveness of information security measures for systems is periodically reviewed and validated.

Context

Scope

4.3.2. This section covers information on the process of undertaking a certification and accreditation audit.

Audit objectives, scope and criteria

4.3.3. The aim of an audit is to review and assess:

- the risk identifications and assessment;
- design and complexity (including the system and security architectures);
- any available assurance reports on support or outsourced services;
- controls selection;
- actual implementation and effectiveness of controls for a system; and
- supporting information security documentation.

4.3.4. Only information that is verifiable should be accepted as audit evidence. Audit evidence should be recorded.

Audit outcome

4.3.5. The outcome of an audit is a report of compliance and control effectiveness for the certification authority outlining areas of non-compliance for a system and any suggested remediation actions.

4.3.6. Part of this audit is an assessment of whether the control systems adequately identify and address risk and information security requirements.

Who can assist with an audit

4.3.7. A number of other agencies and personnel within agencies are often consulted during an audit. Agencies or personnel that can be consulted on physical security aspects of information security may include:

- The NZSIS for Physical Security;
- GCSB for TOP SECRET sites and Sensitive Compartmented Information Facilities (SCIFs);
- MFAT for systems located at overseas posts and missions;
- The Chief Security Officer (CSO) may be consulted on personnel and physical security aspects of information security;

- The CISO, ITSM or communications security officer may be consulted on COMSEC aspects of information security; and
- The ITSM and System Owner on aspects of secure system design configuration and operation.

Independent audits

4.3.8. An audit may be conducted by agency auditors or an independent security organisation.

Audit Evidence

4.3.9. Audit evidence can be obtained from documentation described in Chapter 5 – Information Security Documentation. Other sources may include:

Source	
Agency Strategies and Statements of Intent.	Any additional process documentation referenced in the documentation described in the NZISM Chapter 5.
Third party service provider agreements.	Independent risk assessments or security evaluations, such as penetration tests by an internal team or an external organization.
The agency risk identification and assessment process.	Any internal audit reports, assessments and reviews.
Any statements of applicability.	Any relevant incident reports.

Audit evidence reliability

4.3.10. The reliability of audit evidence is influenced by its source, nature and the circumstances under which the evidence is gathered. In general terms documentary evidence is more reliable than oral evidence, self-generated evidence less reliable than evidence gathered elsewhere and externally generated evidence is more reliable than internally generated evidence as internally generated evidence may be more susceptible to selective presentation.

4.3.11. Confirmation should be obtained that:

- Risk owners have been identified; and
- Each risk owner has sufficient accountability and authority to manage their identified risks.

4.3.12. Audit evidence can be gathered through the following methods in order of preference:

Method	Description
Inspection	Physical inspections can provide an independent confirmation of the physical condition of the site or systems, its implementation and its management.
Analytical review	Reviews of records and documents will provide evidence of varying degrees of reliability depending on their nature and source. A review of the risk identification and selection of risk treatments is invaluable.
Enquiry	Here audit evidence is gathered by interview. Enquiries can be formal or informal and oral or written. It is essential that the auditor creates a written record of any enquiries conducted.
Observation	Observation of operations or procedures being performed by others with the aim of determining the manner of its performance only at that particular time. This may include checks on system configurations, change management processes or other key elements.
Computations	Rarely used for non-financial records but may include, for example, asset registers and validation of holdings of accountable equipment and software.

Audit evidence sufficiency

4.3.13. The Sufficiency is the measure of the quality (not the quantity) of audit evidence. It is important, however, that a balance is struck between the extent of the audit, the nature of the system under review, agency risk and the cost, effort and benefit of the audit. Sufficient evidence should be obtained to allow the auditor to be able to draw reasonable conclusions on which to base the audit opinion. For evidence to be deemed sufficient, the following aspects should be considered:

- Materiality. Materiality is the threshold where any distorted, missing and incorrect information is likely to have an impact on the risk and security of a system. Where it becomes clear that there are material deficiencies in the evidence presented more substantive tests may be required or the audit suspended until corrective action has been taken by the agency.
- Risk assessment: It is almost impossible to validate every risk identification and selection of risk treatments. For larger systems a more practical approach may be to validate the identification and treatment of major risks and use sampling techniques for the balance.
- Economy: Before gathering or requesting additional audit evidence, it is important to consider whether or not it is feasible or cost-effective to generate this evidence against the benefits, assessed value and time required.

References

Title	Publisher	Source
ISO 19011:2011 - Guidelines for auditing management systems	ISO	https://www.iso.org
ISO/IEC 27000:2014 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary	ISO	http://www.standards.co.nz http://www.iso.org
ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements	ISO	http://www.iso27001security.com/html/27006.html http://www.standards.co.nz http://www.iso.org
ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls	ISO	http://www.standards.co.nz http://www.iso.org
ISO/IEC_27006:2011 Information Technology – Security Techniques- Requirements for bodies providing audit and certification of information security management systems	ISO	http://www.standards.co.nz http://www.iso.org
ISO/IEC_27007:2011 Information Technology – Security Techniques - Guidelines for information security management systems auditing	ISO	http://www.standards.co.nz http://www.iso.org
International Standard On Auditing (New Zealand) 500 - Audit Evidence	External Reporting Board, NZ Audit and Assurance Standards Board	https://www.xrb.govt.nz/standards-for-assurance-practitioners/auditing-standards/isa-nz-500/

PSR references

Reference	Title	Source
PSR Mandatory Requirements	GOV5, INFOSEC2 and INFOSEC4	http://www.protectivesecurity.govt.nz
PSR content protocols and requirements sections	Compliance Reporting	http://www.protectivesecurity.govt.nz

Rationale & Controls

4.3.14. Independence of auditors

4.3.14.R.01. Rationale

As there can be a perceived conflict of interest in the system owner assessing the security of their own system it is important that the auditor is demonstrably independent. This does not preclude an appropriately qualified system owner from assessing the security of a system that they are not responsible for.

4.3.14.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that auditors conducting audits are able to demonstrate independence and are not also the system owner or certification authority.

4.3.15. Audit preparation

4.3.15.R.01. Rationale

Ensuring that the system owner has approved the system architecture and associated information security documentation will assist auditors in determining the scope of work for the first stage of the audit.

4.3.15.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Prior to undertaking the audit the system owner MUST approve the system architecture and associated information security documentation.

4.3.16. Audit (first stage)

4.3.16.R.01. Rationale

Auditing against the risk assessment and subsequent controls selection is preferable to a 'checklist' approach where all controls in the NZISM are checked for selection and implementation irrespective of applicability.

4.3.16.R.02. Rationale

The purpose of the first stage of the audit is to determine that the system and security architecture (including information security documentation) is based on sound information security principles and has addressed all **applicable** controls from this manual. During this stage the statement of applicability for the system will also be assessed along with any justification for non-compliance with applicable controls from this manual.

4.3.16.R.03. Rationale

Without implementing the controls for a system their effectiveness cannot be assessed during the second stage of the audit.

4.3.16.C.01. **Control:** System Classification(s): All Classifications; Compliance: MUST

The SecPol, SRMP, SecPlan, SOPs and IRP documentation MUST be reviewed by the auditor to ensure that it is comprehensive and appropriate for the environment the system is to operate within.

4.3.16.C.02. **Control:** System Classification(s): All Classifications; Compliance: MUST

The Information Security Policy (SecPol) MUST be reviewed by the auditor to ensure that all relevant controls specified in this manual are addressed.

4.3.16.C.03. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

The system and security architecture (including information security documentation) SHOULD be reviewed by the auditor to ensure that it is based on sound information security principles and meets information security requirements, including the NZISM.

4.3.16.C.04. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

The Information Security Policy (SecPol) SHOULD be reviewed by the auditor to ensure that policies have been developed or identified by the agency to protect classified information that is processed, stored or communicated by its systems.

4.3.16.C.05. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

The system owner SHOULD provide a statement of applicability for the system which includes the following topics:

- the baseline of this manual used for determining controls;
- controls that are, and are not, applicable to the system;
- controls that are applicable but are not being complied with; and
- any additional controls implemented as a result of the SRMP.

4.3.17. Implementing controls

4.3.17.R.01. **Rationale**

System testing is most effective on working systems. Desk checks have limited effectiveness in these situations.

4.3.17.C.01. **Control:** System Classification(s): All Classifications; Compliance: MUST

Prior to undertaking any system testing in support of the certification process, the system owner MUST implement the controls for the system.

4.3.18. Audit (second stage)

4.3.18.R.01. Rationale

The purpose of the second stage of the audit is to determine whether the controls, as approved by the system owner and reviewed during the first stage of the audit, have been implemented correctly and are operating effectively.

4.3.18.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

The implementation of controls MUST be assessed to determine whether they have been implemented correctly and are operating effectively.

4.3.18.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

The auditor MUST ensure that, where applicable, a physical security certification has been awarded by an appropriate physical security certification authority.

4.3.18.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

The physical security certification SHOULD be less than three (3) years old at the time of the audit.

4.3.19. Report of compliance

4.3.19.R.01. Rationale

The report of compliance assists the certification authority in conducting a residual security risk assessment to assess the residual security risk relating to the operation of a system following the audit and any remediation activities the system owner may have undertaken.

4.3.19.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

The auditor MUST produce a report of compliance for the certification authority outlining areas of non-compliance for a system and any suggested remediation actions.

4.4. Accreditation Framework

Objective

4.4.1. Accreditation is the formal authority for a system to operate, and an important element in fundamental information system governance. Accreditation requires risk identification and assessment, selection and implementation of baseline and other appropriate controls and the recognition and acceptance of residual risks relating to the operation of a system including any outsourced services such as Telecommunications or Cloud. Accreditation relies on the completion of system certification procedures.

Context

Scope

4.4.2. This section covers information on the accreditation framework for systems.

4.4.3. All types of government held information are covered, including Official Information and information subject to privacy requirements.

Rationale & Controls

4.4.4. Accreditation framework

4.4.4.R.01. Rationale

The development of an accreditation framework within the agency will ensure that accreditation activities are conducted in a repeatable and consistent manner across the agency and that consistency across government systems is maintained. This requirement is a fundamental part of a robust governance model and provides a sound process to demonstrate good governance of information systems.

4.4.4.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST develop an accreditation framework for their agency.

4.4.5. Accreditation

4.4.5.R.01. Rationale

Accreditation ensures that either sufficient security measures have been put in place to protect information that is processed, stored or communicated by the system or that deficiencies in such measures have been identified, assessed and acknowledged by an appropriate authority. As such, when systems are awarded accreditation the Accreditation Authority accepts that the residual security risks relating to the system are appropriate for the information that it processes, stores or communicates.

4.4.5.R.02. Rationale

Once systems have been accredited, conducting on-going monitoring activities will assist in assessing changes to its environment and operation and to determine the implications for the security risk profile and accreditation status of the system.

4.4.5.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that each of their systems is awarded accreditation.

4.4.5.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that that all systems are awarded accreditation before they are used operationally.

4.4.5.C.03. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that that all systems are awarded accreditation prior to connecting them to any other internal or external system.

4.4.5.C.04. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure information security monitoring, logging and auditing is conducted on all accredited systems.

4.4.6. Determining authorities

4.4.6.R.01. Rationale

Determining the certification and accreditation authorities for multi-national and multi-agency systems via a formal agreement between the parties will ensure that the system owner has identified appropriate points of contact and that risk is appropriately managed. See Section 4.5 – Conducting Accreditations.

4.4.6.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

For multi-national and multi-agency systems, the Certification and Accreditation Authorities SHOULD be determined by a formal agreement between the parties involved.

4.4.7. Notifying authorities

4.4.7.R.01. Rationale

In advising the certification and accreditation authorities of their intent to seek certification and accreditation for a system, the system owner can request information on the latest processes and requirements for their system.

4.4.7.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Prior to beginning the accreditation process the system owner SHOULD advise the certification and accreditation authorities of their intent to seek certification and accreditation for their system.

4.4.7.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD confirm governance arrangements with the certification authorities, and with the accreditation authorities.

4.4.8. Due diligence

4.4.8.R.01. Rationale

When an agency is connecting a system to another party they need to be aware of the security measures the other party has implemented to protect their information. More importantly, the agency needs to know where the other party may have varied from controls in this manual. This is vital where different classification systems are applied, such as in the use of multiple national classification systems.

4.4.8.R.02. Rationale

Methods that an agency may use to ensure that other agencies and third parties comply with the agency's information security expectations include:

- assurance and confirmation that the certification and accreditation process described in the NZISM is adhered to;
- conducting or utilising any third party reviewed assurance reports;
- conducting an accreditation of the system being connected to; and/or

- seeking a copy of existing accreditation deliverables in order to make their own accreditation determination.

4.4.8.R.03. Rationale

Ultimately, the agency MUST accept any security risks associated with connecting their system to the other party's system. This includes the risks of other party's system potentially being used as a platform to attack their system or "spilling" information requiring subsequent clean up processes.

4.4.8.R.04. Rationale

Special care MUST be taken for multi- national, multi-agency and All-of-Government systems.

4.4.8.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Where an agency's system exchanges information with a third-party system, the agency MUST ensure that the receiving party has appropriate measures in place to provide a level of protection commensurate with the classification or privacy requirements of their information and that the third party is authorised to receive that information.

4.4.8.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

An agency MUST ensure that a third party is aware of the agency's information security expectations and national security requirements by defining expectations in documentation that includes, but is not limited to:

- contract provisions;
- a memorandum of understanding;
- non-disclosure agreements.

4.4.8.C.03. Control: System Classification(s): All Classifications; Compliance: MUST

An agency MUST ensure that a third party complies with the agency's information security expectations through a formal process providing assurance to agency management that the operation of information security within the third party meets, and continues to meet, these expectations.

4.4.8.C.04. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD review accreditation deliverables when determining whether the receiving party has appropriate measures in place to provide a level of protection commensurate with the classification of their information.

4.4.9. Processing restrictions

4.4.9.R.01. Rationale

When security is applied to systems, protective measures are put in place based on the highest classification that will be processed, stored or communicated by the system. As such, any classified information placed on the system above the

level for which it has been accredited will receive an inappropriate level of protection and could be exposed to a greater risk of compromise.

4.4.9.C.01. Control: System Classification(s): All Classifications; Compliance: MUST NOT

Agencies MUST NOT allow a system to process, store or communicate classified information above the classification for which the system has received accreditation.

4.4.10. Accrediting systems bearing an endorsement or compartment marking

4.4.10.R.01. Rationale

When processing endorsed or compartmented information on a system, agencies need to ensure that the system has received accreditation for the information. Furthermore, when agencies are dealing with New Zealand Eyes Only (NZEO) information they need to be aware of the requirement for a New Zealand national to remain in control of the system and information at all times.

4.4.10.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

A system that processes, stores or communicates endorsed or compartmented information MUST be accredited for such endorsed or compartmented information by the GCSB.

4.4.11. Requirement for New Zealand control

4.4.11.R.01. Rationale

NZEO systems process, store and communicate information that is particularly sensitive to the government of New Zealand. It is, therefore, essential that control of such systems is maintained by New Zealand citizens working for the government of New Zealand.

4.4.11.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that systems processing, storing or communicating NZEO information remain under the control of a New Zealand national working for the New Zealand government, at all times.

4.4.12. Reaccreditation

4.4.12.R.01. Rationale

Agencies should reaccredit their systems at least every two years; however, they can exercise an additional one year's grace if they follow the procedures in this manual for non-compliance with a 'SHOULD' requirement, namely conducting a comprehensive security risk assessment, obtaining sign-off by senior management and formal acceptance of residual risk.

4.4.12.R.02. Rationale

Accreditations should be commenced at least six months before due date to allow sufficient time for the certification and accreditations processes to be completed. Once three years has elapsed between accreditations, the authority to operate the system (the accreditation) will lapse and the agency will need to either reaccredit the system or request a dispensation to operate without accreditation. It should be noted that operating a system without accreditation is considered extremely risky. This will be exacerbated when multiple agency or All-of-Government systems are involved.

4.4.12.R.03. Rationale

Additional reasons for conducting reaccreditation activities could include:

- changes in the agency's information security policies or security posture;
- detection of new or emerging threats to agency systems;
- the discovery that controls are not operating as effectively as planned;
- a major information security incident; and
- a significant change to systems, configuration or concept of operation for the accredited system.

4.4.12.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that the period between accreditations of each of their systems does not exceed three years.

4.4.12.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST notify associated agencies where multiple agencies are connected to agency systems operating with expired accreditations.

4.4.12.C.03. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST notify the Government CIO where All-of-Government systems are connected to agency systems operating with expired accreditations.

4.4.12.C.04. Control: System Classification(s): All Classifications; Compliance: MUST NOT

Agencies MUST NOT operate a system without accreditation or with a lapsed accreditation unless the accreditation authority has granted a dispensation.

4.4.12.C.05. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that the period between accreditations of each of their systems does not exceed two years.

4.5. Conducting Accreditations

Objective

4.5.1. As a governance good practice, systems are accredited before they are used operationally.

Context

Scope

4.5.2. This section covers information accreditation processes.

Accreditation aim

4.5.3. The aim of accreditation is to give formal recognition and acceptance of the residual security risk to a system and the information it processes, stores or communicates as part of the agency's governance arrangements.

Accreditation outcome

4.5.4. The outcome of accreditation is an approval to operate issued by the Accreditation Authority to the system owner.

Accreditation Authorities

4.5.5. For agencies the Accreditation Authority is the agency head or their formally authorised delegate.

4.5.6. For organisations supporting agencies the Accreditation Authority is the head of the supported agency or their authorised delegate.

4.5.7. For multi-national and multi-agency systems the Accreditation Authority is determined by a formal agreement between the parties involved.

4.5.8. For agencies with systems that process, store or communicate endorsed or compartmented information, or the use of High Grade Cryptographic Equipment (HGCE), the Director-General of the GCSB is the Accreditation Authority.

4.5.9. In all cases the Accreditation Authority will be at least a senior executive who has an appropriate level of understanding of the security risks they are accepting on behalf of the agency.

4.5.10. Depending on the circumstances and practices of an agency, the agency head could choose to delegate their authority to multiple senior executives who have the authority to accept security risks for the specific business functions within the agency, for example the CISO and the system owner.

4.5.11. More information on the delegation of the agency head's authority can be found in Section 3.1 - Agency Head.

Accreditation outcomes

4.5.12. Accreditation is awarded when the systems comply with the NZISM, the Accreditation Authority understands and accepts the residual security risk relating to the operation of the system and the Accreditation Authority gives formal approval for the system to operate.

4.5.13. In some cases the Accreditation Authority may not accept the residual security risk relating to the operation of the system. This outcome is predominately caused by security risks being insufficiently considered and documented within the SRMP resulting in an inaccurate scoping of security measures within the SecPlan. In such cases the Accreditation Authority may request that the SRMP and SecPlan be amended and security measures reassessed before accreditation is awarded.

4.5.14. In awarding accreditation for a system the Accreditation Authority may choose to define a reduced timeframe before reaccreditation, less than that specified in this manual, or place restrictions on the use of the system which are enforced until reaccreditation or until changes are made to the system within a specified timeframe.

Exception for undertaking certification

4.5.15. In exceptional circumstances the Accreditation Authority may elect not to have a certification conducted on a system before making an accreditation decision. The test to be satisfied in such circumstances is that if the system is not operated immediately it would have a devastating and potentially long lasting effect on the operations of the agency. This exception MUST be formally recorded and accepted.

4.5.16. Certification MUST occur as soon as possible as this is an essential part of the governance and assurance mechanism.

Rationale & Controls

4.5.17. Certification

4.5.17.R.01. Rationale

Certification is an essential component of the governance and assurance process and assists and supports risk management.

4.5.17.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

All systems MUST be certified as part of the accreditation process.

4.5.18. Accreditation decision

4.5.18.R.01. Rationale

In order to determine the agency's security posture, a system accreditation:

- examines the risks to systems identified in the certification process;
- reviews the controls applied to manage those risks; and then
- determines the acceptability of any residual risk.

4.5.18.R.02. Rationale

The accreditation process should also examine compliance with national policy, relevant international standards and good practice so that residual risk is managed prudently and pragmatically.

4.5.18.R.03. Rationale

It is especially important that All-of-Government systems and effects on systems of other agencies are also considered in the examination of risk and determination of residual risk.

4.5.18.R.04. Rationale

To assist in making an accreditation decision the Accreditation Authority may choose to review:

- Information Security Documentation as described in Chapter 5;
- any interaction with systems of other agencies or All-of-Government systems;
- compliance audit reports;
- the accreditation recommendation from the certification authority;
- supporting documentation for any decisions to be non-compliant with any controls specified in this manual;
- any additional security risk reduction strategies that have been implemented; and
- any third party reviews or assurance reports available.

4.5.18.R.05. Rationale

The Accreditation Authority may also choose to seek the assistance of one or more technical experts in understanding the technical components of information presented to them during the accreditation process to assist in making an informed accreditation decision.

4.5.18.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

The Accreditation Authority MUST accept the residual security risk relating to the operation of a system in order to award accreditation.

4.5.18.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

The Accreditation Authority MUST advise other agencies where the accreditation decision may affect those agencies.

4.5.18.C.03. Control: System Classification(s): All Classifications; Compliance: MUST

The Accreditation Authority MUST advise the GCIO where the accreditation decision may affect any All-of-Government systems.

5. Information security documentation

5.1. Documentation Fundamentals

Objective

5.1.1. Information security documentation is produced for systems, to support and demonstrate good governance.

Context

Scope

5.1.2. This section is an overview of the information security documentation that each agency will need to develop. More specific information on each document can be found in subsequent sections of this chapter.

5.1.3. While this section describes a number of different but essential documents, it may be more advantageous and efficient to provide agency wide documentation for some elements (for example Physical Security) which can then be re-used for all agency systems.

5.1.4. Similarly some consolidation may be appropriate, for example, SOPs IRPs and EPs can be easily combined into a single document.

Note: For smaller agencies and smaller systems it is acceptable that all documentation elements are combined into a single document provided each documentation element is clearly identifiable.

Note: Agencies may choose to name the documentation in different terms. This is acceptable provided the required level of detail is captured. Naming conventions presented in the NZISM are not mandatory.

Information Security Documentation

5.1.5. Information Security Documentation requirements are summarised in the table below.

Title	Abbreviation	Reference
Information Security Policy	SecPol	5.1.6
Systems Architecture	-	5.1.7
Security Risk Management Plan	SRMP	5.1.8
System Security Plan	SecPlan	5.1.9
Site Security Plan	SitePlan	8.2.7
Standard Operating Procedures	SOPs	5.1.10
Incident Response Plan	IRP	5.1.11
Emergency Procedures	EP	5.1.12
Independent Assurance reports for externally provided services	-	5.8

PSR references

Reference	Title	Source
PSR Mandatory Requirements	GOV3, GOV4, GOV7, INFOSEC1, INFOSEC2, INFOSEC4, INFOSEC5, PHYSEC1, PHYSEC6 and PHYSEC7	http://www.protectivesecurity.govt.nz
PSR content protocols and requirements sections	Developing Agency Protective Security Policies, Plans and Procedures Business Impact Levels Reporting Incidents and Conducting Security Investigations Compliance Reporting Physical Security of ICT Equipment, Systems and Facilities Agency Cyber Security Responsibilities for Publicly Accessible Information Systems.	http://www.protectivesecurity.govt.nz

Rationale & Controls

5.1.6. Information Security Policy (SecPol)

5.1.6.R.01. Rationale

The SecPol is an essential part of information security documentation as it outlines the high-level policy objectives. The SecPol can form part of the overall agency security policy.

5.1.6.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST have a SecPol for their agency. The SecPol is usually sponsored by the Chief Executive and managed by the CISO or Chief Information Officer (CIO). The ITSM should be the custodian of the SecPol. The SecPol should include an acceptable use policy for any agency technology equipment, systems, resources and data.

5.1.7. Systems Architecture

5.1.7.R.01. Rationale

The systems architecture illustrates the design of the system (including any outsourced services), consistency with the SecPol and provides the basis for the Security Risk Management Plan (SRMP).

5.1.7.R.02. Rationale

In this context Systems Architecture includes Security Architecture.

5.1.7.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

All systems MUST have a documented Systems Architecture.

5.1.8. Security Risk Management Plan (SRMP)

5.1.8.R.01. Rationale

The SRMP is considered to be a good practice approach to identifying and reducing identified security risks. Depending on the documentation framework chosen, multiple systems can refer to, or build upon, a single SRMP.

5.1.8.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that every system is covered by a Security Risk Management Plan, which includes identification of **risk owners**.

5.1.9. System Security Plan (SecPlan)

5.1.9.R.01. Rationale

The SecPlan describes the implementation and operation of controls within the system derived from the NZISM and the SRMP. Depending on the documentation framework chosen, some details common to multiple systems can be consolidated in a higher level SecPlan.

5.1.9.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that every system is covered by a SecPlan.

5.1.10. Standard Operating Procedures (SOPs)

5.1.10.R.01. Rationale

SOPs provide step-by-step guides to undertaking information security related tasks and processes. They provide assurance that tasks can be undertaken in a secure and repeatable manner, even by system users without strong technical knowledge of the system's mechanics. Depending on the documentation framework chosen, some procedures common to multiple systems could be consolidated into a higher level SOP.

5.1.10.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that Standard Operating Procedures (SOPs) are developed for systems.

5.1.11. Incident Response Plan (IRP)

5.1.11.R.01. Rationale

The purpose of developing an IRP is to ensure that information security incidents are appropriately managed. In most situations the aim of the response will be to contain the incident and prevent the information security incident from escalating. The preservation of any evidence relating to the information security incident for criminal, forensic and process improvement purposes is also an important consideration.

5.1.11.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST develop an Incident Response Plan and supporting procedures.

5.1.11.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Agency personnel MUST be trained in and periodically exercise the Incident Response Plan.

5.1.12. Emergency Procedures (EP)

5.1.12.R.01. Rationale

Classified information and systems are secured if a building emergency or evacuation is required.

5.1.12.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD document procedures relating to securing classified information and systems when required to evacuate a facility in the event of an emergency.

5.1.13. Developing content

5.1.13.R.01. Rationale

Ensuring personnel developing information security documentation are sufficiently knowledgeable of information security issues and business requirements will assist in achieving the most useful and accurate set of documentation.

5.1.13.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that information security documentation is developed by personnel with a good understanding of policy requirements, the subject matter, essential processes and the agency's business and operations.

5.1.14. Documentation content

5.1.14.R.01. Rationale

As the SRMP, Systems Architecture, SecPlan, SOPs and IRP are developed as a documentation suite for a system it is essential that they are logically connected and consistent within themselves and with other agency systems. Furthermore, each documentation suite developed for a system will need to be consistent with the agency's overarching SecPol.

5.1.14.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that their SRMP, Systems Architecture, SecPlan, SOPs and IRP are logically connected and consistent for each system, other agency systems and with the agency's SecPol.

5.1.15. Documentation framework

5.1.15.R.01. Rationale

The implementation of an overarching information security document framework ensures that all documentation is accounted for, complete and maintained appropriately. Furthermore, it can be used to describe linkages between documents, especially when higher level documents are used to avoid repetition of information in lower level documents.

5.1.15.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD create and maintain an overarching document describing the agency's documentation framework, including a complete listing of all information security documentation that shows a document hierarchy and defines how each document is related to the other.

5.1.15.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Where an agency lacks an existing, well-defined documentation framework, they SHOULD use the document names defined in this manual.

5.1.16. Documentation Consistency

5.1.16.R.01. Rationale

Consistency in approach, terminology and documentation simplifies the use and interpretation of documentation for different systems and agencies.

5.1.16.R.02. Rationale

Factors which should be taken into account when determining the classification of systems documentation include:

- Highest classification of information stored, processed or communicated over that system;
- Sensitivity including existence of the facility;
- Inclusion of vulnerability information, security mechanisms or special processing capability in the systems documentation;
- Potential data aggregation;
- Risk and threat levels; and
- Scope and use of the system.

5.1.16.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Where an agency uses alternative documentation names to those defined within this manual for their information security documentation they SHOULD convert the documentation names to those used in this manual.

5.1.17. Documentation Classification

5.1.17.R.01. Rationale

Systems documentation will usually reflect the importance or sensitivity of particular systems.

5.1.17.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that their SecPol, SRMP, SecPlan, SOPs and IRP are appropriately classified.

5.1.18. Outsourcing development of content

5.1.18.R.01. Rationale

Agencies outsourcing the development of information security documentation need to be aware of the contents of the documentation produced. As such, they will still need to review and control the documentation contents to make sure it is appropriate and meets their requirements.

5.1.18.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

When information security documentation development is outsourced, agencies SHOULD:

- review the documents for suitability;
- retain control over the content; and
- ensure that all policy requirements are met.

5.1.19. Obtaining formal sign-off

5.1.19.R.01. Rationale

Without appropriate sign-off of information security documentation within an agency, the security personnel will have a reduced ability to ensure appropriate security procedures are selected and implemented. Having sign-off at an appropriate level assists in reducing this security risk as well as ensuring that senior management is aware of information security issues and security risks to the agency's business.

5.1.19.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

All information security documentation SHOULD be formally approved and signed off by a person with an appropriate level of seniority and authority.

5.1.19.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that:

- all high-level information security documentation is approved by the CISO and the agency head or their delegate; and
- all system-specific documents are reviewed by the ITSM and approved by the system owner.

5.1.20. Documentation Maintenance

5.1.20.R.01. Rationale

The threat environment and agencies' businesses are dynamic. If an agency fails to keep their information security documentation up to date to reflect the changing environment, they do not have a means of ascertaining that their security measures and processes continue to be effective.

5.1.20.R.02. Rationale

Changes to risk and technology may dictate a reprioritisation of resources in order to maximise the effectiveness of security measures and processes.

5.1.20.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD develop a regular schedule for reviewing all information security documentation.

5.1.20.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that information security documentation is reviewed:

- at least annually; or
- in response to significant changes in the environment, business or system; and
- with the date of the most recent review being recorded on each document.

5.2. Information Security Policies

Objective

5.2.1. Information security policies (SecPol) set the strategic direction for information security.

Context

Scope

5.2.2. This section relates to the development of Information Security Policies and any supporting plans. Information relating to other mandatory documentation can be found in Section 5.1 - Documentation Fundamentals.

Rationale & Controls

5.2.3. The Information Security Policy (SecPol)

5.2.3.R.01. Rationale

To provide consistency in approach and documentation, agencies should consider the following when developing their SecPol:

- policy objectives;
- how the policy objectives will be achieved;
- the guidelines and legal framework under which the policy will operate;
- stakeholders;
- education and training;
- what resourcing will be available to support the implementation of the policy;
- what performance measures will be established to ensure that the policy is being implemented effectively; and
- a review cycle.

5.2.3.R.02. Rationale

In developing the contents of the SecPol, agencies may also consult any agency-specific directives that are applicable to information security within their agency.

5.2.3.R.03. Rationale

Agencies should also avoid outlining controls for systems within their SecPol. The controls for a system will be determined by this manual and based on the scope of the system, along with any additional controls as determined by the SRMP, and documented within the SecPlan.

5.2.3.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

The Information Security Policy (SecPol) SHOULD document the information security, guidelines, standards and responsibilities of an agency.

5.2.3.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

The Information Security Policy (SecPol) SHOULD include topics such as:

- accreditation processes;
- personnel responsibilities;
- configuration control;
- access control;
- networking and connections with other systems;
- physical security and media control;
- emergency procedures and information security incident management;
- change management; and
- information security awareness and training.

5.3. Security Risk Management Plans

Objective

5.3.1. Security Risk Management Plans (SRMP) identify security risks and appropriate treatment measures for systems.

Context

Scope

5.3.2. This section relates to the development of SRMPs, focusing on risks associated with the security of systems. Information relating to other mandatory documentation can be found in Section 5.1 - Documentation Fundamentals.

5.3.3. SRMPs may be developed on a functional basis, systems basis or project basis. For example, where physical elements will apply to all systems is use within that agency, a single SRMP covering all physical elements is acceptable. Generally each system will require a separate SRMP.

5.3.4. The agency's risk identification and assessment process should include:

- How risks are found, recognised and described; and
- How sources of possible risks are to be considered.

References

5.3.5. Information on the development of SRMPs can be found in:

Title	Publisher	Source
ISO 27005:2011, Information Security Risk Management	Standards New Zealand	http://www.standards.co.nz
HB 436:2013, Risk Management Guidelines	Standards New Zealand	http://www.standards.co.nz
ISO 22301:2012, Business Continuity	Standards New Zealand	http://www.standards.co.nz
ISO 31000:2009, Risk Management Principles and Guidelines	ISO / Standards New Zealand	http://www.standards.co.nz http://www.iso.org
ISO 31010:2009, Risk Management – Risk Assessment Techniques	ISO / Standards New Zealand	http://www.standards.co.nz http://www.iso.org
ISO Guide 73:2009, Risk Management - Vocabulary	ISO / Standards New Zealand	http://www.standards.co.nz http://www.iso.org
ISO 19011:2011 - Guidelines for auditing management systems	ISO	https://www.iso.org
ISO/IEC 27000:2014 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary	ISO	http://www.standards.co.nz http://www.iso.org
ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements	ISO	http://www.iso27001security.com/html/27006.html http://www.standards.co.nz http://www.iso.org
ISO/IEC_27006:2011 Information Technology – Security Techniques- Requirements for bodies providing audit and certification of information security management systems	ISO	http://www.standards.co.nz http://www.iso.org
ISO/IEC_27007:2011 Information Technology – Security Techniques - Guidelines for information security management systems auditing	ISO	http://www.standards.co.nz http://www.iso.org
ISO/IEC TR 27008, Guidelines for auditors on information security controls	ISO	http://www.iso.org/
ISO/IEC 27017, Code of practice for information security controls based on ISO/IEC 27002 for cloud services	ISO	http://www.iso.org/
ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	ISO	http://www.iso.org/

Rationale & Controls

5.3.6. Agency and system specific security risks

5.3.6.R.01. Rationale

While a baseline of security risks with associated levels of security risk and corresponding risk treatments are provided in this manual, agencies will almost certainly have variations to those considered during the security risk assessment. Such variations could be in the form of differing risk sources and threats, assets and vulnerabilities, or exposure and severity. In such cases an agency will need to follow its own risk management procedures to determine its risk appetite and associated risk acceptance, risk avoidance and risk tolerance thresholds. Risk owners **must** be identified.

5.3.6.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD determine agency and system specific security risks that could warrant additional controls to those specified in this manual.

5.3.7. Contents of SRMPs

5.3.7.R.01. Rationale

Risks within an agency cannot be managed if they are not known, and if they are known, failing to treat or accept them is also a failure of risk management. For this reason SRMPs consist of two components, a security risk assessment and a corresponding treatment strategy.

5.3.7.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

The Security Risk Management Plan SHOULD contain a security risk assessment and a corresponding treatment strategy.

5.3.8. Agency risk management

5.3.8.R.01. Rationale

If an agency fails to incorporate SRMPs for systems into their wider agency risk management plan then the agency will be unable to manage risks in a coordinated and consistent manner across the agency.

5.3.8.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD incorporate their SRMP into their wider agency risk management plan.

5.3.9. Risk Management standards

5.3.9.R.01. Rationale

For security risk management to be of true value to an agency there must be direct relevance to the specific circumstances of an agency and its systems, as well as being based on an industry recognised approach or risk management guidelines. For example, guidelines and standards produced by Standards New Zealand and the International Organization for Standardization.

The PSR requires that agencies adopt risk management approaches in accordance with ISO 31000:2009. Refer to PSR governance requirement GOV3.

5.3.9.R.02. Rationale

The International Organization for Standardization has developed an international risk management standard, including principles and guidelines on implementation, outlined in ISO 31000:2009, Risk Management – Principles and Guidance. The terms and definitions for this standard can be found in ISO/IEC Guide 73, Risk Management – Vocabulary – Guidelines. The ISO/IEC 2700x series of standards also provides guidance.

5.3.9.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD develop their SRMP in accordance with international standards for risk management.

5.4. System Security Plans

Objective

5.4.1. System Security Plans (SecPlan) specify the information security measures for systems.

Context

Scope

5.4.2. This section relates to the development of SecPlans. Information relating to other mandatory documentation can be found in Section 5.1 - Documentation Fundamentals.

5.4.3. Further information to be included in SecPlans relating to specific functionality or technologies that could be implemented for a system can be found in the applicable areas of this manual.

Stakeholders

5.4.4. There can be many stakeholders involved in defining a SecPlan, including representatives from the:

- project, who MUST deliver the capability (including contractors);
- owners of the information to be handled;
- system users for whom the capability is being developed;
- management audit authority;
- CISO, ITSM and system owners;
- system certifiers and accreditors;
- information management planning areas; and
- infrastructure management.

Rationale & Controls

5.4.5. Contents of SecPlans

5.4.5.R.01. Rationale

The NZISM provides a list of controls that are potentially applicable to a system based on its classification, its functionality and the technology it is implementing. Agencies will need to determine which controls are in scope of the system and translate those controls to the SecPlan. These controls will then be assessed on their implementation and effectiveness during an information security assessment as part of the accreditation process.

5.4.5.R.02. Rationale

In performing accreditations against the latest baseline of this manual, agencies are ensuring that they are taking the most recent threat environment into consideration. GCSB continually monitors the threat environment and conducts research into the security impact of emerging trends. With each release of this manual, controls can be added, rescinded or modified depending on changes in the threat environment.

5.4.5.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST select controls from this manual to be included in the SecPlan based on the scope of the system with additional system specific controls being included as a result of the associated SRMP. Encryption Key Management requires specific consideration; refer to Chapter 17 – Cryptography.

5.4.5.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use the latest baseline of this manual when developing, and updating, their SecPlans as part of the certification, accreditation and reaccreditation of their systems.

5.4.5.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD include a Key Management Plan in the SecPlan.

5.5. Standard Operating Procedures

Objective

5.5.1. Standard Operating Procedures (SOPs) ensure security procedures are followed in an appropriate and repeatable manner.

Context

Scope

5.5.2. This section relates to the development of security related SOPs. Information relating to other mandatory documentation can be found in Section 5.1 - Documentation Fundamentals.

Rationale & Controls

5.5.3. Development of SOPs

5.5.3.R.01. Rationale

In order to ensure that personnel undertake their duties in an appropriate manner, with a minimum of confusion, it is important that the roles of ITSMs, system administrators and system users are covered by SOPs. Furthermore, taking steps to ensure that SOPs are consistent with SecPlans will reduce the potential for confusion resulting from conflicts in policy and procedures.

5.5.3.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD develop SOPs for each of the following roles:

- ITSM;
- system administrator; and
- system user.

5.5.4. ITSM SOPs

5.5.4.R.01. Rationale

The ITSM SOPs are intended to cover the management and leadership of information security functions within the agency.

5.5.4.C.01. **Control:** System Classification(s): All Classifications; Compliance: SHOULD
The following procedures SHOULD be documented in the ITSMs SOPs.

Topic	Procedures to be included
Access control	Authorising access rights to applications and data.
Asset Musters	Labelling, registering and mustering assets, including media.
Audit logs	Reviewing system audit trails and manual logs, particularly for privileged users.
Configuration control	Approving and releasing changes to the system software or configurations.
Information security incidents	Detecting, reporting and managing potential information security incidents.
	Establishing the cause of any information security incident, whether accidental or deliberate.
	Actions to be taken to recover and minimise the exposure from an information security incident.
	Additional actions to prevent reoccurrence.
Data transfers	Managing the review of media containing classified information that is to be transferred off-site.
	Managing the review of incoming media for malware or unapproved software.
IT equipment	Managing the disposal & destruction of unserviceable IT equipment and media.
System Patching	Advising and recommending system patches, updates and version changes based on security notices and related advisories.
System integrity audit	Reviewing system user accounts, system parameters and access controls to ensure that the system is secure.
	Checking the integrity of system software.
	Testing access controls.
System maintenance	Managing the ongoing security and functionality of system software, including: maintaining awareness of current software vulnerabilities, testing and applying software patches/updates/signatures, and applying appropriate hardening techniques.
User account management	Authorising new system users.

5.5.5. System Administrator SOPs

5.5.5.R.01. Rationale

The system administrator SOPs focus on the administrative activities related to system operations.

5.5.5.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

The following procedures SHOULD be documented in the system administrator's SOPs.

Topic	Procedures to be included
Access control	Implementing access rights to applications and data.
Configuration control	Implementing changes to the system software or configurations.
System backup and recovery	Backing up data, including audit logs.
	Securing backup tapes.
	Recovering from system failures.
User account management	Adding and removing system users.
	Setting system user privileges.
	Cleaning up directories and files when a system user departs or changes roles.
Incident response	Detecting, reporting and managing potential information security incidents.
	Establishing the cause of any information security incident, whether accidental or deliberate.
	Actions to be taken to recover and minimise the exposure from information security incident.
	Additional actions to prevent reoccurrence.

5.5.6. System User SOPs

5.5.6.R.01. Rationale

The system user SOPs focus on day to day activities that system users need to be made aware of, and comply with, when using systems.

5.5.6.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

The following procedures SHOULD be documented in the system user's SOPs.

Topic	Procedures to be included
Acceptable Use	Acceptable uses of the system(s).
End of day	How to secure systems at the end of the day.
Information security incidents	What to do in the case of a suspected or actual information security incident.
Media control	Procedures for handling and using media.
Passwords	Choosing and protecting passwords.
Temporary absence	How to secure systems when temporarily absent.

5.5.7. Agreement to abide by SOPs

5.5.7.R.01. Rationale

When SOPs are produced the intended audience should be made aware of their existence and acknowledge that they have read, understood and agree to abide by their contents.

5.5.7.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

ITSMs, system administrators and system users SHOULD sign a statement that they have read and agree to abide by their respective SOPs.

5.6. Incident Response Plans

Objective

5.6.1. Incident Response Plans (IRP) outline actions to take in response to an information security incident.

Context

Scope

5.6.2. This section relates to the development of IRPs to address information security, and not physical incidents within agencies. Information relating to other mandatory documentation can be found in Section 5.1 - Documentation Fundamentals.

Rationale & Controls

5.6.3. Contents of IRPs

5.6.3.R.01. Rationale

The guidance provided on the content of IRPs will ensure that agencies have a baseline to develop an IRP with sufficient flexibility, scope and level of detail to address the majority of information security incidents that could arise.

5.6.3.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST include, as a minimum, the following content within their IRP:

- broad guidelines on what constitutes an information security incident;
- the minimum level of information security incident response and investigation training for system users and system administrators;
- the authority responsible for initiating investigations of an information security incident;
- the steps necessary to ensure the integrity of evidence supporting an information security incident;
- the steps necessary to ensure that critical systems remain operational;
- when and how to formally report information security incidents; and
- national policy requirements for incident reporting (see Chapter 7 – Information Security Incidents).

5.6.3.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD include the following content within their IRP:

- clear definitions of the types of information security incidents that are likely to be encountered;
- the expected response to each information security incident type;
- the authority within the agency that is responsible for responding to information security incidents;
- the criteria by which the responsible authority would initiate or request formal, police investigations of an information security incident;
- which other agencies or authorities need to be informed in the event of an investigation being undertaken; and
- the details of the system contingency measures or a reference to these details if they are located in a separate document.

5.7. Emergency Procedures

Objective

5.7.1. Classified information and systems are secured before personnel evacuate a facility in the event of an emergency.

Context

Scope

5.7.2. This section covers information relating to the securing of classified information and systems as part of the procedures for evacuating a facility in the event of an emergency.

5.7.3. The safety of personnel is of paramount importance.

Rationale & Controls

5.7.4. Evacuating facilities

5.7.4.R.01. Rationale

When evacuating a facility, it is important that personnel secure classified information and systems as they would at the end of operational hours. This includes, but is not limited to, securing media, logging off of workstations and securing safes and cabinets. This is important as an attacker could use such an opportunity to gain access to documents, applications or databases that a system user had already authenticated to or use another system user's credentials for a malicious purpose.

5.7.4.R.02. Rationale

During an evacuation, the safety of staff is of primary importance. Where it is immediately obvious to wardens and/or staff that the securing of classified information and systems prior to the evacuation of a facility would lead to, or exacerbate, serious injury or loss of life to personnel, the facility may evacuated without personnel following the necessary procedures to secure classified information and systems.

5.7.4.R.03. Rationale

Where facilities are evacuated and classified information and systems have NOT been secured, the Chief Warden or Floor Warden MUST be notified as soon as possible. Steps should be taken to secure the site as soon as it is safe to do so.

5.7.4.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST include in procedures for personnel evacuating a facility the requirement to secure classified information and systems prior to the evacuation.

5.8. Independent Assurance Reports

Objective

5.8.1. To provide assurance to System Owners, Certifiers, Practitioners and Accreditors and to assist system designers, enterprise and security architects where assurance reviews cannot be directly undertaken on service providers.

Context

Scope

5.8.2. Independent assurance reports are also variously referred to as third party assurance reporting, third party reviews, attestation reports and SAS 70 reports. It is important to note that SAS 70 has been superseded by the ISAE 3402 and SSAE 16 standards encompassing Type I and 2 and SOC 1, 2 and 3 reports. For reviews conducted in New Zealand the ISAE (NZ) 3402 or ISAE (NZ) 3000 standards are used. These various standards and report types are discussed later in this section. Agencies are likely to encounter a variety of report types, depending on the country of residence or country of jurisdiction of the service provider, or the geographic location of the data centre.

Purpose

5.8.3. Many organisations are outsourcing key components of their business such as telecommunications, data storage and cloud based services. Managing third-party relationships is particularly challenging with services provided from outside New Zealand. The global nature of these services and the global nature of associated risks must be recognised by organisations. As outsourced services are becoming more integrated with organisation's operations, they will have a larger impact on organisation's governance, assurance and control frameworks. It is important to note that risk ownership and accountability remains with agencies and respective risk owners, even when responsibility for specific functions have been outsourced.

5.8.4. Independent assurance reports provide customers and other interested parties with information on policies, procedures and controls related to the service provider's internal frameworks, control objectives and controls in cases where physical inspections and reviews by customers are impractical or not feasible. Service providers may also use the findings of such reports for their own purposes. These reports are used to understand the adequacy and effectiveness of the service provider's frameworks, control objectives, controls and implementation of controls. They allow:

- Business owners to identify and understand the risks associated with the service delivery;
- System owners to more fully assess system risks;
- System designers and security architects to make informed judgements on system structures, controls, defensive measures, and enterprise integration; and
- Regulators, certifiers and accreditors to obtain assurance over the service providers internal control structures and assess the suitability of system structures, controls and defensive measures.

5.8.5. An independent assurance review or third-party audit is invariably undertaken by independent auditors who are not employees of the service provider or their customers. There are two common types of independent third-party reviews: attestation reviews and direct non-attestation reviews.

5.8.6. Attestation reviews, such as an ISAE 3402 review (see below), are generally conducted by accounting or consulting organisations and are based upon recognised attestation standards issued by professional bodies such as the American Institute of Certified Public Accounts (AICPA) or the New Zealand External Reporting Board (XRB).

5.8.7. Direct or non-attestation reviews include those performed by IT consultants or others and may not follow standards referred to previously. They may be based upon other external standards or industry developed criteria such as ISO 2700x, ISACA's COBIT, the IIA, NIST, or the Cloud Security Alliance (CSA).

Assurance

5.8.8. Assurance is derived from an assessment of:

- A description of the service provider's business and control environment;
- Terms and conditions of the service contract or other legally binding agreement;
- Assertions supplied by the service provider (self-assessments);
- An independent validation of service provider assertions;
- Independent testing of controls implementation and effectiveness;
- Assurance in the service design and security architecture; and
- Assurance in the service components.

5.8.9. In general terms, the more ICT services that are outsourced in an agency, the less direct control and visibility the CE and management have over enterprise operations. Therefore, there is an increased reliance on assurance reporting from suppliers. Unless this is recognised in service contracts or legal agreements, agencies may find they are unable to obtain sufficient levels of assurance over the business services and enterprise operations.

Assurance Standards and schemes

ISAE (NZ) 3000

5.8.10. ISAE (NZ) 3000 (Revised) is issued by the External Reporting Board (XRB) of the New Zealand Audit and Assurance Standards Board and is the umbrella standard for other (non-financial) assurance engagements conducted in New Zealand. The standard covers a wide variety of engagements, ranging from assurance on statements about the effectiveness of internal control, for example, to assurance on sustainability reports and possible future engagements addressing integrated reporting. It is a principle-based standard that underpins current and future subject-specific ISAEs (NZ).

ISAE (NZ) 3402

5.8.11. In New Zealand the XRB issued the ISAE (NZ) 3402 in 2014, revised in 2016. This standard has essentially the same requirements as the international standard ISAE 3402 (see below), with some New Zealand specific adaptations. Australia, Singapore and many other jurisdictions have adopted this approach in the issue of this standard with some jurisdiction specific adaptations.

ISAE 3402

5.8.12. The most commonly used international standard for independent assurance reports is the International Standard on Assurance Engagements (ISAE) No. 3402, Assurance Reports on Controls at a Service Organization, issued in December 2009 by the International Auditing and Assurance Standards Board (IAASB), part of the International Federation of Accountants (IFAC).

5.8.13. Based on its predecessor standard SAS 70 (1992), ISAE 3402 was developed to provide an international assurance standard for allowing public accountants to issue a report for use by user organisations and their auditors (user auditors) on the controls at a service organisation that are likely to impact or be a part of the user organisation's system of internal control over financial reporting.

5.8.14. Auditing and associated consulting firms were required to use ISAE 3402 for all related work after June 2011.

ISAE 3402 Report Types

5.8.15. The ISAE 3402 provides for a report on controls at a point in time (Type 1 Report) or covering a specified period of time, usually between six and twelve months (Type 2 Report).

5.8.16. A Type 1 report is of limited use as it cannot cover the operating effectiveness of controls and is generally used for new operations where there is no evidence or documented history.

5.8.17. A Type 2 report not only includes the service organisation's description of controls, but also includes detailed testing of the service organisation's controls over a minimum six month period.

5.8.18. It is important to note that the descriptions Type 1 and Type 2 represent an audit approach and should not be confused with SOC 1, 2 and 3 reports under SSAE 16 (see below).

ISAE 3402 Report Uses and Limitations

5.8.19. This standard is used to obtain reasonable assurance about whether:

- The service organisation's description of its system fairly presents the system as designed and implemented throughout a specified period or a specific date;
- The controls related to the control objectives stated in the service organisation's description of its system were suitably designed throughout the specified period or at the specified date;
- Where included in the scope of the engagement, the controls were implemented and operated effectively to provide reasonable assurance that the control objectives stated in the service organisation's description of its system were achieved throughout the specified period.

5.8.20. This ISAE applies only when the service organisation is responsible for, or otherwise able to make an assertion about, the suitable design of controls. It does not cover situations where:

- reporting only whether controls at a service organisation operated as described; or
- reporting on controls at a service organisation other than those related to a service relevant to user entities.

ISAE 3402 Report Content

5.8.21. The ISAE 3402 report usually comprises:

- The service auditor's report;
- Assertions by the service provider;
- A description of control objectives and controls provided by the service organisation;
- Results of any tests and other information provided by the independent auditor; and
- Any other information provided by the service provider.

US Standard SSAE 16

5.8.22. The Statement on Standards for Attestation Engagements No. 16 (SSAE 16) is issued by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). It includes additional requirements to the superseded SAS 70 standard by requiring management to provide a written assertion (see below) regarding the design and operating effectiveness of the controls being reviewed. It is possible that agencies may encounter an SSAE16 based report for a US-based entity.

5.8.23. SSAE 16 is the US equivalent of the international ISAE 3402 and came into effect on 15 June 2011. While the SSAE 16 and ISAE 3402 standards have a common purpose and intent, , there are nine very specific requirements in SSAE 16, not covered in ISAE 3402:

- Intentional acts by the service providers staff;
- Anomalies;
- Direct assistance;
- Subsequent events;
- Statement restricting use of the service auditor's report;
- Disclaimer of Opinion;
- Documentation completion;
- Engagement acceptance and continuance; and
- Elements of the SSAE 16 report that are not required in the ISAE 3402 report.

5.8.24. These differences are summarised in the table below:

	SSAE 16	ISAE 3402
Use of report	Report specifically states it is restricted to intended users.	Report intended for user entities and their auditors but may include other restrictive use conditions.
Intentional Acts	Consideration of the impact of intention acts.	No requirement stated.
Subsequent Events	Auditors must consider Type 2 events after the report date.	Events after the report date are not considered.
Reporting	Sample deviations may not be discarded even when considered non-representative.	Sample deviations are assessed and may be discarded as not representative of the sample population.

5.8.25. The SSAE 16 standard specifies Type 1 and 2 audits (as does ISAE 3402).

5.8.26. A Type 1 is a report on a description of a service organisation's system and the suitability of the design of controls. A Type 1 report will test the design effectiveness of defined controls by examining a sample of one item per control. This provides a basic level of assurance that the organisation has some controls in place. It does not measure the completeness or effectiveness of these controls and represents a point in time.

5.8.27. A Type2 report is a report on policies and procedures placed in operation and tests of operating effectiveness for a specified period of time. A Type 2 report undertakes the tests in a Type 1 report together with an evaluation of the operating effectiveness of the controls for a period of at least six consecutive calendar months.

AICPA Service Organisation Control Reporting (SOC Reports)

5.8.28. Service Organisation Control (SOC) Reports, often known as SOC 1, SOC 2, and SOC 3 Reports, are derived from a framework published by the American Institute of Certified Public Accountants (AICPA) for reporting on controls at service organisations.

5.8.29. In New Zealand, SOC 1 reports follow the ISAE (NZ) 3402 standard and SOC 2 reports are follow the ISAE (NZ) 3000 standard, in conjunction with the NZ Standard for Assurance Engagements SAE 3150, for assurance engagements on controls.

5.8.30. Each of the three SOC reports are designed to meet specific needs and reporting requirements for service organisations themselves, rather than being designed to provide assurance to third parties (customers). It is important to note that these reports follow the US (SSAE 16) and Canadian accounting standards, rather than the international ISAE 3402.

SOC 1 Report – Report on Controls at a Service Organisation Relevant to User Entities' Internal Control over Financial Reporting. Reporting on controls relevant to internal control over financial reporting and usually conducted in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 16 and AT 801 – Reporting on Controls at a Service Organization. A SOC 1 report can be based on a Type 1 or a Type 2 audit.

SOC 2 Report— Report on Controls at a Service Organisation Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy. SOC 2 Reporting follows the AICPA AT Section 101 (not SSAE 16) and encompasses controls at service organisations on security, availability, processing Integrity, confidentiality and privacy. SOC 2 reports assist in comparing two or more data centres or service providers.

SOC 3 Report— Trust Services Report for Service Organisations. As well as reporting on controls relevant to security, availability, processing integrity, confidentiality and privacy a SOC 3 report provides the same level of assurance about controls over security, availability, processing integrity, confidentiality and/or privacy as a SOC 2 report. The key difference is that a SOC 3 report is intended for general release and does not include the detailed description of the testing performed by the auditor. In place of the detailed description a summary opinion regarding the effectiveness of the controls in place at the data centre or service organisation is provided.

SOC Reports Summary

Report	Standards	Content	Audience
SOC1 – Type 1	ISAE (NZ) 3402/ SAE 3150 or SSAE 16/AT 801	Internal controls over financial reporting at a point in time.	User auditors, organisation finance team, management.
SOC1 – Type 2	ISAE (NZ) 3402/ SAE 3150 or SSAE 16/AT 801	Internal controls over financial reporting over a specified time period, minimum 6 months.	User auditors, organisation finance team, management.
SOC2 – Type 1	ISAE (NZ) 3000/ SAE 3150 or AT 101	Security, availability, processing integrity, confidentiality and privacy controls at a point in time.	Management, regulators, third parties under Non-Disclosure Agreement.
SOC2 – Type 2	ISAE (NZ) 3000/ SAE 3150 or AT 101	Security, availability, processing integrity, confidentiality, privacy controls and operating effectiveness over a specified time period, minimum 6 months.	Management, regulators, third parties under Non-Disclosure Agreement.
SOC3	ISAE (NZ) 3000/ SAE 3150 or AT 101	Security, availability, processing integrity, confidentiality, privacy controls and operating effectiveness.	Public/general use version of SOC 2, excludes details of testing. Is less detailed and has less technical content than a SOC 2 report.

Management Assertions

5.8.31. See Assertions in Certification and Accreditation (NZISM 3.4.3 to 3.4.7) for a short discussion on the nature and purpose of assertions.

5.8.32. The SSAE 16 requires a written assertion by management. Also known as a management's assertion or service organisation assertion it is essentially an assertion made by the service organisation representing and asserting to a number of elements, including:

- The description fairly presents the service organisation's system;
- That the control objectives were suitably designed (SSAE 16 Type 1) and operating effectively (SSAE 16 Type 2) during the dates and/or periods covered by the report; and
- The criteria used for making these assertions, (which are additional statements with supporting matter regarding risk factors relating to control objectives and underlying controls) were in place (Type 1) and were consistently applied (Type 2).

ISO/IEC 27001 Certification

5.8.33. ISO/IEC 27001 is an international standard that provides a framework for Information Security Management Systems. The standard is designed to help organisations of all sizes and types to select suitable and proportionate security controls for information. It provides a structured approach to assist in managing risk by identifying information security vulnerabilities and selecting appropriate controls.

5.8.34. This standard enables independent, external certification bodies to audit the ISMS and certify that the requirements of the standard have been met. Such certification is another means of deriving assurance over the operations of service providers. The requirements for certification are described in the ISO/IEC 27006:2015 standard. Certification is based on two reviews:

- Stage 1 audit (also called Documentation review) checking the systems documentation is compliant with ISO 27001;
- Stage 2 audit (also called Main audit) checking that all the organisation's activities are compliant with both ISO 27001 and the systems documentation.

Other Guidance

Cloud Security Alliance's Security, Trust and Assurance Registry (STAR) Attestation

5.8.35. STAR Certification is a rigorous third party independent assessment of the security of a cloud service provider. It is based on the ISAE 3402 and SSAE 16 standards, supplemented by the criteria in the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM).

5.8.36. STAR is a free, publicly accessible registry that documents the security controls provided by various cloud computing service providers. The registry lists three levels of assurance:

1. Self-assessment;
2. Third party assessment based attestation or certification; and
3. Continuous monitoring based certification.

Note: Agencies should note that a self-assessment does not necessarily provide substantive assurance.

5.8.37. As at March 2017, the STAR scheme is still to be fully implemented although there are a number of cloud service providers listed in the registry.

5.8.38. Agencies can use this registry to further inform their judgement on the robustness of assurance over cloud service provider's internal operations and implementation of security controls.

Cloud Security Alliance's Cloud Controls Matric (CCM)

5.8.39. The CCM covers 16 control domains and provides fundamental security principles to guide cloud service providers and to assist prospective cloud customers in assessing the overall security risk of a cloud service provider.

5.8.40. The CCM references and maps its controls to internationally accepted industry standards, regulations, and control frameworks, such as ISO 27001/2/17/18, PCI: DSS v3, and AICPA 2014 Trust Service Principles and Criteria, Germany's BIS, Canada's PIPEDA, ISACA's COBIT, the US FedRAMP, HIPAA, Jericho Forum, NIST and the NZISM.

Cloud Security Alliance's Consensus Assessments Initiative Questionnaire (CAIQ)

5.8.41. The CAIQ is an extension to the CCM that provides exemplar control assertion questions that can be asked of service providers in the context of each CCM control, and can be tailored to suit each unique cloud customer's evidentiary requirements. GCIO maintain a mapping of the CAIQ questions to the *GCIO Cloud Security and Privacy Considerations* question set to further aid agencies in use of the CAIQ as an alternative to equivalent GCIO questions.

ISACA IT Audit and Assurance Program for Cloud Computing

5.8.42. Based on ISACA's IT Assurance Framework (ITAF), the Cloud Computing Assurance Program was developed as a comprehensive and good-practice model, aligned with the ISACA COBIT 5 framework. Building on the generic assurance program, the cloud computing guidance identifies a number of cloud specific risk areas encompassing:

- Greater dependency on third parties;
- Increased complexity of compliance with national and international laws and regulations;
- Reliance on the Internet as the primary conduit to the enterprise's data; and
- Risk due to the dynamic nature of cloud computing.

5.8.43. The ITAF assurance focus is on:

- The governance affecting cloud computing;
- The contractual compliance between the service provider and customer;
- Privacy and regulation issues concerning cloud computing; and
- Cloud computing specific attention points.

5.8.44. It is important to note that this cloud computing assurance review is not designed to provide assurance on the design and operational effectiveness of the cloud computing service provider's internal controls, as this assurance is often provided through ISAE 3604 or similar reviews.

5.8.45. The cloud computing assurance review focusses on the agency's or organisation's systems design and operational effectiveness in relation to cloud services. It is also important to note that this is dependent on the effectiveness of the underlying system design and controls and how well these are implemented and managed.

ASD Certified Cloud Services

5.8.46. The Australian Signals Directorate (ASD) conducts certification of cloud services based in Australia for Australian government use. ASD Certifications are based on the Australian Government Information Security Manual (ISM). It is important to note that there are detail differences between the Australian ISM and the NZISM and these documents have a different legislative and regulatory basis.

5.8.47. The ASD Cloud Computing Security documents describe security risk mitigations associated with cloud computing. Australian Government agencies are also required to perform due diligence reviews of the legal, financial and privacy risks associated with procuring cloud services, aspects which are **not** covered by the ASD certification.

NIST 800-53

5.8.48. The NIST Special Publication 800-53 Revision 4 - Security and Privacy Controls for Federal Information Systems and Organizations is the US unified information security framework for US federal government agencies. The New Zealand equivalent is the NZISM.

5.8.49. The underlying mandates are in FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems and FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems. US federal government agencies are required to categorise and analyse their system in terms of FIPS 199 and 200 then apply appropriate controls from NIST 800-53.

FedRAMP

5.8.50. The US Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program intended to provide a standardised approach to security assessment, authorisation, and continuous monitoring for cloud products and services. This approach is designed to provide reusable cloud security assessments in order to reduce cost, resource and time.

5.8.51. FedRAMP is a collaboration of cybersecurity and cloud experts from the General Services Administration (GSA), National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Department of Defense (DOD), National Security Agency (NSA), Office of Management and Budget (OMB), the Federal Chief Information Officer (CIO) Council and its working groups, as well as private industry.

5.8.52. FedRAMP authorises cloud systems in a three step process:

1. **Security Assessment:** The security assessment process uses a standardised set of requirements in accordance with FISMA using a baseline set of NIST 800-53 controls to grant security authorisations.

2. **Leveraging and Authorisation:** Federal agencies view security authorisation packages in the FedRAMP repository and leverage the security authorisation packages to grant a security authorisation at their own agency.

3. **Ongoing Assessment & Authorisation:** Once an authorisation is granted, ongoing assessment and authorisation activities are required to maintain the security authorisation.

5.8.53. Again it is important to note that the FedRAMP assessments are conducted on a different legislative and regulatory basis to assessments conducted in New Zealand.

PCI DSS

5.8.54. The Payment Card Industry Security Standards Council was formed by major credit card organisations and is a global open body formed to develop and promote understanding of essential security standards for payment account security. It develops, maintains and promotes the Payment Card Industry Data Security Standards (PCI DSS). It also provides tools to assist the implementation of the standards such as assessment and scanning qualifications, self-assessment questionnaires, training and education, and product certification programs.

5.8.55. This standard is designed to protect cardholder data (credit and debit cards) held by merchants, banks and other financial organisations. It applies to all organisations that accept, store, process and transmit credit cardholder data.

5.8.56. This standard is narrowly focussed and has specific applicability to New Zealand Government agencies that operate financial transaction services (e.g. AoG Banking services and citizen fee-paying services; such as vehicle registration, passport renewal, etc.). The PCI has published an information supplement on Third-Party Security Assurance (updated March 2016).

COSO

5.8.57. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) initially developed the COSO Internal Control-Integrated Framework in 1992. A revised framework was published in 2013 which included guidance on “outsourced service providers” and how they impact risk assessment, controls, monitoring, information flows and assurance. The 2013 Framework incorporates how organisations should manage IT innovation in light of globalisation, complex business processes, regulatory demands and security risk assessments. It is frequently used as the basis for SSAE16 assignments and the production of SOC reports.

References – Assurance Standards

Title	Publisher	Source
International Standard on Assurance Engagements (ISAE) 3402 - Assurance Reports on Controls at a Service Organization	International Federation of Accountants (IFAC)	http://www.ifac.org/system/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf
Reporting on Controls at a Service Organization - SSAE No. 16	AICPA	http://www.aicpastore.com/AST/Main/CPA2BIZ_Primary/InformationManagementTechnologyAssurance/PRDOVR~PC-023035/PC-023035.jsp
Service Organization Controls (SOC) Reports for Service Organizations	AICPA	http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/serviceorganization'smanagement.aspx
AT Section 101 Attest Engagements	AICPA	http://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AT-00101.pdf
AT Section 801 Reporting on Controls at a Service Organization	AICPA	http://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AT-00801.pdf
COBIT 5 Framework	ISACA	http://www.isaca.org/cobit/Pages/CobitFramework.aspx
ISA (NZ) 500 Audit Evidence	XRB	https://www.xrb.govt.nz/standards-for-assurance-practitioners/auditing-standards/isa-nz-500/
ISAE (NZ) 3000 (Revised) - Assurance Engagements Other than Audits or Reviews of Historical Financial Information	XRB	https://xrb.govt.nz/Site/Auditing_Assurance_Standards/Current_Standards/Other_Assurance_Engagements_Standards.aspx
ISAE (NZ) 3402 - Assurance Reports on Controls at a Service Organisation	XRB	https://xrb.govt.nz/Site/Auditing_Assurance_Standards/Current_Standards/Other_Assurance_Engagements_Standards.aspx
SAE 3150 - Standard on Assurance Engagements 3150	XRB	https://xrb.govt.nz/Site/Auditing_Assurance_Standards/Current_Standards/Other_Assurance_Engagements_Standards.aspx
NIST Special Publication 800-53 Revision 4 **Security and Privacy Controls for Federal Information Systems and Organizations**	NIST	http://csrc.nist.gov/publications/nistpubs
NIST Special Publication 500-299 (Draft) NIST Cloud Computing Security Reference Architecture	NIST	http://csrc.nist.gov/publications/nistpubs
Information Supplement: Third-Party Security Assurance	PCI Security Standards Council	https://www.pcisecuritystandards.org/documents/ThirdPartySecurityAssurance_March2016_FINAL.pdf

Title	Publisher	Source
ISO 19011:2011, Guidelines for Auditing Management Systems	ISO	https://www.iso.org/standard/50675.html
ISO/IEC 27000, Information security management systems — Overview and vocabulary	ISO	http://www.iso.org/
ISO/IEC 27001: 2013, Information security management systems — Requirements	ISO	http://www.iso.org/
ISO/IEC 27006, Requirements for bodies providing audit and certification of information security management systems	ISO	http://www.iso.org/
ISO/IEC 27007, Guidelines for information security management systems auditing	ISO	http://www.iso.org/
ISO/IEC TR 27008, Guidelines for auditors on information security controls	ISO	http://www.iso.org/
ISO/IEC 27014, Governance of information security	ISO	http://www.iso.org/
ISO/IEC 27017, Code of practice for information security controls based on ISO/IEC 27002 for cloud services	ISO	http://www.iso.org/
ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	ISO	http://www.iso.org/

References – Assurance Guidance

Title	Publisher	Source
FAQs — New Service Organization Standards and Implementation Guidance	American Institute of Certified Public Accountants (AICPA)	http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/faqs_service_orgs.pdf
The Federal Risk and Authorization Management Program (FedRAMP)	General Services Administration, US Federal Government	https://www.fedramp.gov
Controls and Assurance in the Cloud Using COBIT 5	ISACA	http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Controls-and-Assurance-in-the-Cloud-Using-COBIT-5.aspx
Special Publication 800-115 Technical Guide to Information Security Testing and Assessment	NIST	http://csrc.nist.gov/publications/nistpubs
Cloud Security Guidance	CESG	https://www.cesg.gov.uk/cloud-security-collection
Cloud Security Guidance: Summary of Cloud Security Principles	CESG	https://www.cesg.gov.uk/guidance/cloud-security-guidance-summary-cloud-security-principles
Cloud Security Guidance: Implementing Cloud Security Principles	CESG	https://www.cesg.gov.uk/guidance/cloud-security-guidance-implementing-cloud-security-principles
ASD Certified Cloud Services	ASD	http://www.asd.gov.au/infosec/irap/certified_clouds.htm
Security Framework for Governmental Clouds	ENISA	https://www.enisa.europa.eu/publications/security-framework-for-governmental-clouds
Good Practice Guide for securely deploying Governmental Clouds	ENISA	https://www.enisa.europa.eu/publications/good-practice-guide-for-securely-deploying-governmental-clouds
Security & Resilience in Governmental Clouds	ENISA	https://www.enisa.europa.eu/publications/security-and-resilience-in-governmental-clouds
Assurance on non-financial information Existing practices and issues, July 2008, ISBN 978-1-84152-604-1	Institute of Chartered Accountants in England and Wales (ICAEW).	https://www.icaew.com/~/media/corporate/files/technical/audit%20and%20assurance/assurance/assurance%20on%20non%20financial%20information.ashx
IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control, January 2013	The Institute of Internal Auditors (IIA)	https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf
Cloud Security Alliance Reference Architecture	Cloud Security Alliance	https://downloads.cloudsecurityalliance.org/initiatives/tci/TCI_Reference_Architecture_v2.0.pdf

Cloud Controls Matrix v3.0.1 (6-6-16 Update)	Cloud Security Alliance	https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/
Consensus Assessments Initiative Questionnaire (CAIQ) v3.0.1	Cloud Security Alliance	https://cloudsecurityalliance.org/media/news/ccm-caiq-v3-0-1-soft-launch/
Security Guidance for Critical Areas of Focus in Cloud Computing V3.0	Cloud Security Alliance	https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf
About CSA STAR Attestation	Cloud Security Alliance	https://cloudsecurityalliance.org/star/attestation/
Guidelines for CPAs Providing CSA STAR Attestation	Cloud Security Alliance	https://cloudsecurityalliance.org/download/guidelines-for-cpas-providing-csa-star-attestation/
CSA Security, Trust & Assurance Registry (STAR)	Cloud Security Alliance	https://cloudsecurityalliance.org/star
Payment Card Industry (PCI) Data Security Standard - Requirements and Security Assessment Procedures Version 3. **02 April 2016**	PCI Security Standards Council	https://www.pcisecuritystandards.org/
Enterprise Risk Management — Integrated Framework	COSO	http://www.coso.org/documents/coso_erm_executivesummary.pdf
Internal Control – Integrated Framework	COSO	http://www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf

Rationale & Controls

5.8.58. **Risk Assessment**

5.8.58.R.01. Rationale

The Security Risk Management Plan (SRMP – Section 5.3) encompasses all risks associated with the security of agency systems. The growth in outsourced services, particularly cloud services, has created situations where risk, controls and assurance cannot be directly examined and assessed. In such cases independent assurance reports are an effective means, possibly the only means, of obtaining some assurance on the service provider's operations.

5.8.58.R.02. Rationale

No single independent assurance scheme/standard covers the full range of considerations and control requirements of the NZISM. Agencies may find duplication of aspects analysed if multiple schemes are applied. . It is also important to note that none of the common mature assurance schemes cover specific government requirements and handling of Official Information; such as the personnel aspects (PERSEC) of user and administration vetting and security clearances, or sovereignty aspects of the information/data. Careful selection and consideration is required when placing reliance on reports available for a particular outsourced or cloud service.

5.8.58.R.03. Rationale

Reports from different assurance scheme have varying levels of detail as well as risk area coverage. Selection and usage of reports should be considered in the context of the intended service/system business and information value.

Understanding the business and technical risk context will drive the size and depth of a risk assessment, and the associated assurance process. Though even a lighter-weight risk assurance process will follow the C&A process model, such that the CE or authorised delegate is still formally accountable and responsible.

Re-use of assessments completed by other agencies is encouraged, noting the business or information value context may differ. To assist agencies and promote efficiency, the GCIO facilitates the sharing and re-use of existing cloud assessment materials among agencies.

5.8.58.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST conduct a risk assessment in order to determine the type and level of independent assurance required to satisfy certification and accreditation requirements.

5.8.58.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

In all cases where assurance on service provider operations cannot be obtained directly, agencies SHOULD obtain independent assurance reports.

5.8.58.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

In order to address identified risk areas, agencies SHOULD obtain relevant assurance reports and service provider certifications to inform a risk assessment and Certification activities as well as other aspects of the certification processes such as evidence of controls effectiveness and remediation plans.

5.8.59. Independent Assurance

5.8.59.R.01. Rationale

Independent assurance can be obtained directly from the service provider through Service Organisation Control (SOC) reports, as well as other internationally recognised assurance frameworks. It will be important to corroborate individual reports by comparison with other reporting mechanisms and independent certifications.

5.8.59.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST incorporate the results of any independent assurance reports into the agency Certification process, to understand the residual risk position and controls required to manage risk appropriately.

6. Information security monitoring

6.1. Information Security Reviews

Objective

6.1.1. Information security reviews maintain the security of agency systems and detect gaps and deficiencies.

Context

Scope

6.1.2. This section covers information on conducting reviews of any agency's information security posture and security implementation.

Information security reviews

6.1.3. An information security review:

- identifies any changes to the business requirements or concept of operation for the subject of the review;
- identifies any changes to the security risks faced by the subject of the review;
- assesses the effectiveness of the existing counter-measures;
- validates the implementation of controls and counter-measures; and
- reports on any changes necessary to maintain an effective security posture.

6.1.4. An information security review can be scoped to cover anything from a single system to an entire agency's systems.

References

6.1.5. Additional information relating to system auditing is contained in:

Reference	Title	Source
ISO/IEC_27006:2011	Information Technology – Security Techniques - Requirements for bodies providing audit and certification of information security management systems.	http://www.iso27001security.com/html/27006.html http://www.standards.co.nz
ISO/IEC_27007:2011	Information Technology – Security Techniques - Guidelines for information security management systems auditing.	http://www.iso27001security.com/html/27007.html http://www.standards.co.nz
ISO/IEC_27008:2011	Information Technology – Security Techniques - Guidelines for Auditors on information security controls.	http://www.iso27001security.com/html/27008.html http://www.standards.co.nz

PSR references

Reference	Title	Source
PSR Mandatory Requirements	GOV5, INFOSEC2 and INFOSEC4	http://www.protectivesecurity.govt.nz
PSR content protocols and requirements sections	Compliance Reporting	http://www.protectivesecurity.govt.nz

Rationale & Controls

6.1.6. Conducting information security reviews

6.1.6.R.01. Rationale

Annual reviews of an agency's information security posture can assist with ensuring that agencies are responding to the latest threats, environmental changes and that systems are properly configured in accordance with any changes to information security documentation and guidance.

6.1.6.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD undertake and document information security reviews of their systems at least annually.

6.1.7. Managing Conflicts of Interest

6.1.7.R.01. Rationale

Reviews may be undertaken by personnel independent of the target of evaluation or by an independent third party to ensure that there is no (perceived or actual) conflict of interest and that an information security review is undertaken in an objective manner.

6.1.7.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD have information security reviews conducted by personnel independent to the target of the review or by an independent third party.

6.1.8. Focus of information security reviews

6.1.8.R.01. Rationale

Incidents, significant changes or an aggregation of minor changes may require a security review to determine and support any necessary changes and to demonstrate good systems governance. An agency may choose to undertake an information security review:

- as a result of a specific information security incident;
- because a change to a system or its environment that significantly impacts on the agreed and implemented system architecture and information security policy; or
- as part of a regular scheduled review.

6.1.8.R.02. Rationale

In order to review risk, an information security review should analyse the threat environment and the highest classification of information that is stored, processed or communicated by that system.

6.1.8.R.03. Rationale

Depending on the scope and subject of the information security review, agencies may gather information on areas including:

- agency priorities, business requirements and/or concept of operations;
- threat data;
- risk likelihood and consequence estimates;
- effectiveness of existing counter-measures;
- other possible counter-measures;
- changes to standards, policies and guidelines;
- recommended good practices; and
- significant system incidents and changes.

6.1.8.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD review the components detailed in the table below.

Component	Review
Information security documentation	The SecPol, Systems Architecture, SRMPs, SecPlans, SitePlan, SOPs the IRP, and any third party assurance reports.
Dispensations	Prior to the identified expiry date.
Operating environment	When an identified threat emerges or changes, an agency gains or loses a function or the operation of functions are moved to a new physical environment.
Procedures	After an information security incident or test exercise.
System security	Items that could affect the security of the system on a regular basis.
Threats	Changes in threat environment and risk profile.
NZISM	Changes to baseline or other controls, any new controls and guidance.

6.2. Vulnerability Analysis

Objective

6.2.1. Exploitable information system weaknesses can be identified by vulnerability analyses and inform assessments and controls selection.

Context

Scope

6.2.2. This section covers information on conducting vulnerability assessments on systems as part of the suite of good IT governance activities.

Changes as a result of a vulnerability analysis

6.2.3. It is important that normal change management processes are followed where changes are necessary in order to address security risks identified in a vulnerability analysis.

Rationale & Controls

6.2.4. Vulnerability analysis strategy

6.2.4.R.01. Rationale

Vulnerabilities may be unintentionally introduced and new vulnerabilities are constantly identified, presenting ongoing risks to information systems security.

6.2.4.R.02. Rationale

While agencies are encouraged to monitor the public domain for information related to vulnerabilities that could affect their systems, they should not remain complacent if no specific vulnerabilities relating to deployed products are disclosed.

6.2.4.R.03. Rationale

In some cases, vulnerabilities can be introduced as a result of poor information security practices or as an unintended consequence of activities within an agency. As such, even if no new public domain vulnerabilities in deployed products have been disclosed, there is still value to be gained from regular vulnerability analysis activities.

6.2.4.R.04. Rationale

Furthermore, monitoring vulnerabilities, conducting analysis and being aware of industry and product changes and advances, including NZISM requirements, provides an awareness of other changes which may adversely impact the security risk profile of the agency's systems.

6.2.4.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD implement a vulnerability analysis strategy by:

- monitoring public domain information about new vulnerabilities in operating systems and application software;
- considering the use of automated tools to perform vulnerability assessments on systems in a controlled manner;
- running manual checks against system configurations to ensure that only allowed services are active and that disallowed services are prevented;
- using security checklists for operating systems and common applications; and
- examining any significant incidents on the agency's systems.

6.2.5. Conducting vulnerability assessments

6.2.5.R.01. Rationale

A baseline or known point of origin is the basis of any comparison and allows measurement of changes and improvements when further information security monitoring activities are conducted.

6.2.5.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD conduct vulnerability assessments in order to establish a baseline:

- before a system is first used;
- after any significant incident;
- after a significant change to the system;
- after changes to standards, policies and guidelines; and/or
- as specified by an ITSM or the system owner.

6.2.6. Resolving vulnerabilities

6.2.6.R.01. Rationale

Vulnerabilities may occur as a result of poorly designed or implemented information security practices, accidental activities or malicious activities, and not just as the result of a technical issue.

6.2.6.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD analyse and treat all vulnerabilities and subsequent security risks to their systems identified during a vulnerability assessment.

6.3. Change Management

Objective

6.3.1. To ensure information security is an integral part of the change management process, it should be incorporated into the agency's IT maintenance governance and management activities.

Context

Scope

6.3.2. This section covers information on identifying and managing routine and urgent changes to systems.

Identifying the need for change

6.3.3. The need for change can be identified in various ways, including:

- system users identifying problems or enhancements;
- vendors notifying of upgrades to software or IT equipment;
- vendors notifying of the end of life to software or IT equipment;
- advances in technology in general;
- implementing new systems that necessitate changes to existing systems;
- identifying new tasks or functionality requiring updates or new systems;
- organisational change;
- business process or concept of operation change;
- standards evolution;
- government policy or Cabinet directives;
- threat or vulnerability identification and notification; and
- other incidents or continuous improvement activities.

Types of system change

6.3.4. A proposed change to a system could involve:

- an upgrade to, or introduction of IT equipment;
- an upgrade to, or introduction of software;
- environment or infrastructure change; or
- major changes to access controls.

PSR references

Reference	Title	Source
PSR Mandatory Requirements	INFOSEC5	http://www.protectivesecurity.govt.nz
PSR content protocols and requirements sections	Information Security Management Protocol	http://www.protectivesecurity.govt.nz

Rationale & Controls

6.3.5. Change management

6.3.5.R.01. Rationale

A considered and accountable process requires consultation with all stakeholders before any changes are implemented. In the case of changes that will affect the security or accreditation status of a system, the Accreditation Authority is a key stakeholder and will need to be consulted and grant approval for the proposed changes.

6.3.5.R.02. Rationale

Change management processes are most likely to be bypassed or ignored when an urgent change needs to be made to a system. In these cases it is essential that the agency's change management process strongly enforces appropriate actions to be taken before and after an urgent change is implemented.

6.3.5.C.01. Control: System Classification(s): TS; Compliance: MUST

Agencies MUST ensure that for routine and urgent changes:

- the change management process, as defined in the relevant information security documentation, is followed;
- the proposed change is approved by the relevant authority;
- any proposed change that could impact the security or accreditation status of a system is submitted to the Accreditation Authority for approval; and
- all associated information security documentation is updated to reflect the change.

6.3.5.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that for routine and urgent changes:

- the change management process, as defined in the relevant information security documentation, is followed;
- the proposed change is approved by the relevant authority;
- any proposed change that could impact the security of a system or accreditation status is submitted to the Accreditation Authority for approval; and
- all associated information security documentation is updated to reflect the change.

6.3.6. Change management process

6.3.6.R.01. Rationale

Uncontrolled changes pose risks to information systems as well as the potential to cause operational disruptions. A change management process is fundamental to ensure a considered and accountable approach with appropriate approvals. Furthermore, the change management process provides an opportunity for the security impact of the change to be considered and if necessary, reaccreditation processes initiated.

6.3.6.C.01. Control: System Classification(s): TS; Compliance: MUST

An agency's change management process MUST define appropriate actions to be followed before and after urgent changes are implemented.

6.3.6.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

An agency's change management process SHOULD define appropriate actions to be followed before and after urgent changes are implemented.

6.3.6.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD follow this change management process outline:

- produce a written change request;
- submit the change request to all stakeholders for approval;
- document the changes to be implemented;
- test the approved changes;
- notification to user of the change schedule and likely effect or outage;
- implement the approved changes after successful testing;
- update the relevant information security documentation including the SRMP, SecPlan and SOPs
- notify and educate system users of the changes that have been implemented as close as possible to the time the change is applied; and
- continually educate system users in regards to changes.

6.3.7. Changes impacting the security of a system

6.3.7.R.01. Rationale

The accreditation of a system accepts residual security risk relating to the operation of that system. Changes may impact the overall security risk for the system. It is essential that the Accreditation Authority is consulted and accepts the changes and any changes to risk.

6.3.7.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

When a configuration change impacts the security of a system and is subsequently assessed as having changed the overall security risk for the system, the agency MUST reaccredit the system.

6.4. Business Continuity and Disaster Recovery

Objective

6.4.1. To ensure business continuity and disaster recovery processes are established to assist in meeting the agency's business requirements, minimise any disruption to the availability of information and systems, and assist recoverability.

Context

Scope

6.4.2. This section covers information on business continuity and disaster recovery relating specifically to systems.

References

6.4.3. Additional information relating to business continuity is contained in:

Reference	Title	Source
ISO/IEC_22301:2012	Societal Security – Business Continuity Management Systems - Requirements.	http://www.iso.org http://www.standards.co.nz
ISO/IEC 27001:2013	Information Technology – Security Techniques - Information Security Management Systems - Requirements	http://www.iso27001security.com/html/27001.html http://www.standards.co.nz
SAA/SNZ HB 221:2004	Business Continuity Management.	http://www.standards.co.nz
ISO/IEC_27002:2013	Information Technology – Security Techniques – Code of Practice for Information Security Controls	http://www.iso27001security.com/html/27002.html http://www.standards.co.nz
ISO/IEC_27005:2011	Information Technology – Security Techniques - Information Security Risk Management	http://www.iso27001security.com/html/27005.html http://www.standards.co.nz
ISO/IEC_27031:2011	Information Technology – Security Techniques - Guidelines for Information and Communication Technology readiness for Business Continuity	http://www.iso27001security.com/html/27031.html http://www.standards.co.nz

PSR references

Reference	Title	Source
PSR Mandatory Requirements	GOV10	http://www.protectivesecurity.govt.nz

Rationale & Controls

6.4.4. Availability requirements

6.4.4.R.01. Rationale

Availability and recovery requirements will vary based on each agency's business needs and are likely to be widely variable across government. Agencies will determine their own availability and recovery requirements and implement appropriate measures to achieve them as part of their risk management and governance processes.

6.4.4.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST determine availability and recovery requirements for their systems and implement appropriate measures to support them.

6.4.5. Backup strategy

6.4.5.R.01. Rationale

Having a backup strategy in place is a fundamental part of business continuity planning. The backup strategy ensures that critical business information is recoverable if lost. Vital records are defined as any information, systems data, configurations or equipment requirements necessary to restore normal operations.

6.4.5.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD:

- Identify vital records;
- backup all vital records;
- store copies of critical information, with associated documented recovery procedures, offsite and secured in accordance with the requirements for the highest classification of the information; and
- test backup and restoration processes regularly to confirm their effectiveness.

6.4.6. Business Continuity plan

6.4.6.R.01. Rationale

It is important to develop a business continuity plan to assist in ensuring that critical systems and data functions can be maintained when the system is operating under constraint, for example, when bandwidth is unexpectedly limited below established thresholds.

6.4.6.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD develop and document a business continuity plan.

6.4.7. Disaster recovery plan

6.4.7.R.01. Rationale

Developing and documenting a disaster recovery plan, will reduce the time between a disaster occurring, and critical functions of systems being restored.

6.4.7.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD develop and document a disaster recovery plan.

7. Information Security Incidents

7.1. Detecting Information Security Incidents

Objective

7.1.1. To ensure that appropriate tools, processes and procedures are implemented to detect information security incidents, to minimise impact and as part of the suite of good IT governance activities.

Context

Scope

7.1.2. This section covers information relating to detecting information security incidents. Detecting physical and personnel security incidents is out of scope of this section, refer to Chapter 8 Physical Security and Chapter 9 Personnel Security.

7.1.3. Additional information relating to detecting information security incidents, and topics covered in this section, can be found in the following sections of this manual:

- Section 6.1 - Information Security Reviews;
- Section 6.2 - Vulnerability Analysis;
- Section 9.1 - Information Security Awareness and Training;
- Section 16.5 - Event Logging and Auditing; and
- Section 18.4 - Intrusion Detection and Prevention.

PSR references

Reference	Title	Source
PSR Mandatory Requirements	GOV7	http://www.protectivesecurity.govt.nz
PSR content protocols and requirements sections	Reporting Incidents and Conducting Security Investigations	http://www.protectivesecurity.govt.nz

Rationale & Controls

7.1.4. Preventing and detecting information security incidents

7.1.4.R.01. Rationale

Processes for the detection of information security incidents will assist in mitigating the most common vectors used to attack and exploit systems.

7.1.4.R.02. Rationale

Many potential information security incidents are noticed by personnel rather than automated or other software tools. Personnel should be well trained and aware of information security issues and indicators of possible information security incidents.

7.1.4.R.03. Rationale

Agencies may consider some of the tools described in the table below for detecting potential information security incidents.

Tool	Description
Network and host Intrusion Detection Systems (IDSs)	Monitor and analyse network and host activity, usually relying on a list of known attack signatures to recognise/detect malicious activity and potential information security incidents.
Anomaly detection systems	Monitor network and host activities that do not conform to normal system activity.
Intrusion Prevention Systems (IPS) and Host Based Intrusion Prevention Systems (HIPS)	Some IDSs are combined with functionality to counter detected attacks or anomalous activity (IDS/IPS).
System integrity verification and integrity checking	Used to detect changes to critical system components such as files, directories or services. These changes may alert a system administrator to unauthorised changes that could signify an attack on the system and inadvertent system changes that render the system open to attack.
Log analysis	Involves collecting and analysing event logs using pattern recognition to detect anomalous activities.
White Listing	Lists the authorised activities and applications and permits their usage.
Black Listing	Lists the non-authorised activities and applications and prevents their usage.
Data Loss Prevention (DLP)	Data Egress monitoring and control.

7.1.4.R.04. Rationale

Automated tools are only as good as the level of analysis they perform. If tools are not configured to assess all areas of potential security risk then some vulnerabilities will not be detected. In addition, if tools are not regularly updated, including updates for new vulnerabilities and attack methods, their effectiveness will be reduced.

7.1.4.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST develop, implement and maintain tools and procedures covering the detection of potential information security incidents, incorporating:

- counter-measures against malicious code;
- intrusion detection strategies;
- data egress monitoring & control;
- access control anomalies;
- audit analysis;
- system integrity checking; and
- vulnerability assessments.

7.1.4.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD develop, implement and maintain tools and procedures covering the detection of potential information security incidents, incorporating:

- counter-measures against malicious code;
- intrusion detection strategies;
- data egress monitoring & control;
- access control anomalies;
- audit analysis;
- system integrity checking; and
- vulnerability assessments.

7.1.4.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use the results of the security risk assessment to determine the appropriate balance of resources allocated to prevention versus detection of information security incidents.

7.2. Reporting Information Security Incidents

Objective

7.2.1. Reporting information security incidents, assists in maintaining an accurate threat environment picture for government systems, particularly All-of-Government or multi-agency systems.

Context

Scope

7.2.2. This section covers information relating specifically to the reporting of information security incidents. It does not cover the reporting of physical or personnel security incidents.

Information security incidents and outsourcing

7.2.3. The requirement to lodge an information security incident report still applies when an agency has outsourced some or all of its information technology functions and services.

Categories of information security incidents

7.2.4. The security threat and intelligence landscape continues to evolve driven by more advanced, capable, well -resourced and motivated adversaries. To assist in managing this threat a standardized form of threat information exchange is essential.

7.2.5. Incident categories, incident types and resolution types were previously defined in the Incident Object Description Exchange Format (IODEF) standard. IODEF was an e-GIF standard.

7.2.6. IODEF has been superseded by a group of protocols designed to automate and structure operational cybersecurity information sharing techniques on a global basis. International in scope and free for public use, TAXII, STIX and CybOX are community-driven technical specifications designed to enable automated information sharing for cybersecurity situational awareness, real-time network defense and sophisticated threat analysis. These protocols are:

- TAXII™, the Trusted Automated eXchange of Indicator Information;
- STIX™, the Structured Threat Information eXpression; and
- CybOX™, the Cyber Observable eXpression.

7.2.7. TAXII defines a set of services and message exchanges that enable sharing of actionable cyber threat information. It is not an information sharing programme itself and does not define trust agreements, governance, or other non-technical aspects of collaboration. It does allow organisations to share the information they choose with the partners they choose.

7.2.8. STIX is a standardised, structured language to represent cyber threat information, covering the full range of potential cyber threat data elements. It is designed to be flexible, extensible, automatable, and human-readable.

7.2.9. CybOX is a standardised schema for the specification, capture, characterisation, and communication of events in system and network operations providing a common structure and content types to improve consistency and interoperability. A wide variety of cybersecurity use cases rely on such information including event management/logging, malware characterisation, intrusion detection/prevention, incident response, and digital forensics.

7.2.10. New Zealand's National Cyber Security Centre has adopted this suite of protocols as the basis for incident reports to the NCSC and for reports issued by the NCSC.

References

7.2.11. Additional information relating to information security incidents can be found at:

Title	Publisher	Source
The Incident Object Description Exchange Format, RFC 5070, December 2007	The Internet Engineering Taskforce (IETF)	http://www.ietf.org/rfc/rfc5070.txt
Expert Review for Incident Object Description Exchange Format (IODEF) Extensions in IANA XML Registry, ISSN: 2070-1721, RFC 6685, July 2012	IETF	http://tools.ietf.org/html/rfc6685
Detect, SHARE, Protect **Solutions for Improving Threat Data Exchange among CERTs, October 2013**	ENISA	http://www.enisa.europa.eu/activities/cert/support/data-sharing/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs
Computer Security Incident Handling Guide, Special Publication 800-61: Revision 2, August 2012	NIST	http://dx.doi.org/10.6028/NIST.SP.800-61r2
NIST Special Publication 800-60 Volume I Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories	NIST	http://www.csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf
NIST Special Publication 800-60 Volume II Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories, Volume II: Appendices	NIST	http://www.csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf
The National Cyber Security Centre Voluntary Cyber Security Standards for Industrial Control Systems v1.0	GCSB NCSC	http://www.gcsb.govt.nz/assets/GCSB-Documents/NCSC-voluntary-cyber-security-standards-for-ICD-v.1.0.pdf http://www.ncsc.govt.nz/resources/
The New Zealand Security Incident Management Guide for Computer Security Incident Response Teams (CIRSTs)	NCSC	http://www.ncsc.govt.nz/resources/
Information Sharing Specifications for Cybersecurity	DHS	https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity

Rationale & Controls

7.2.12. Reporting information security incidents

7.2.12.R.01. Rationale

Reporting information security incidents provides management with a means to assess and minimise damage to a system and to take remedial actions. Incidents should be reported to an ITSM, as soon as possible. The ITSM may seek advice from GCSB as required.

7.2.12.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST direct personnel to report information security incidents to an ITSM as soon as possible after the information security incident is discovered in accordance with agency procedures.

7.2.12.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD:

- encourage personnel to note and report any observed or suspected security weaknesses in, or threats to, systems or services;
- establish and follow procedures for reporting software malfunctions;
- put mechanisms in place to enable the types, volumes and costs of information security incidents and malfunctions to be quantified and monitored; and
- deal with the violation of agency information security policies and procedures by personnel through a formal disciplinary process.

7.2.13. Responsibilities when reporting an information security incident

7.2.13.R.01. Rationale

The CISO is required to keep the CSO and/or Agency Head informed of information security incidents within their agency. The ITSM actively manages information security incidents and MUST ensure the CISO has sufficient awareness of and information on any information security incidents within an agency.

7.2.13.R.02. Rationale

Reporting on low-level incidents can be adequately managed through periodic (at least monthly) reports. Serious incidents will require more immediate attention.

7.2.13.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

The ITSM MUST keep the CISO fully informed of information security incidents within an agency.

7.2.14. Reporting significant information security incidents to National Cyber Security Centre (NCSC)

7.2.14.R.01. Rationale

The NCSC uses significant information security incident reports as the basis for identifying and responding to information security events across government. Reports are also used to develop new policy, procedures, techniques and training measures to prevent the recurrence of similar information security incidents across government.

7.2.14.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

The Agency ITSM, MUST report significant information security incidents, or incidents related to multi-agency or government systems, to the NCSC (see below).

7.2.15. Reporting non-significant information security incidents to National Cyber Security Centre (NCSC)

7.2.15.R.01. Rationale

The NCSC uses non-significant information security incident reports as the basis for identifying trends in information security incident occurrences and for developing new policy, procedures, techniques and training measures to prevent the recurrence of similar information security incidents across government.

7.2.15.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD, through an ITSM, report non-significant information security incidents to the NCSC.

7.2.16. How to report information security incidents to National Cyber Security Centre (NCSC)

7.2.16.R.01. Rationale

Reporting of information security incidents to the NCSC through the appropriate channels ensures that appropriate and timely assistance can be provided to the agency. In addition, it allows the NCSC to maintain an accurate threat environment picture for government systems.

7.2.16.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD formally report information security incidents using the NCSC adoption of the TAXII, STIX and CyBox protocols.

7.2.17. Outsourcing and information security incidents

7.2.17.R.01. Rationale

In the case of outsourcing of information technology services and functions, the agency is still responsible for the reporting of all information security incidents. As such, the agency MUST ensure that the service provider informs them of all information security incidents to allow them to formally report these to the NCSC.

7.2.17.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies that outsource their information technology services and functions MUST ensure that the service provider consults with the agency when an information security incident occurs.

7.2.18. Cryptographic keying material

7.2.18.R.01. Rationale

Reporting any information security incident involving the loss or misuse of cryptographic keying material is particularly important. Systems users in this situation are those that rely on the use of cryptographic keying material for the confidentiality and integrity of their secure communications.

7.2.18.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST notify all system users of any suspected loss or compromise of keying material.

7.2.19. High Grade Cryptographic Equipment (HGCE) keying material

7.2.19.R.01. Rationale

For information security incidents involving the suspected loss or compromise of HGCE keying material, GCSB will investigate the possibility of compromise, and where possible, initiate action to reduce the impact of the compromise.

7.2.19.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST notify GCSB of any suspected loss or compromise of keying material associated with HGCE.

7.3. Managing Information Security Incidents

Objective

7.3.1. To identify and implement processes for incident analysis and selection of appropriate remedies which will assist in preventing future information security incidents.

Context

Scope

7.3.2. This section covers information relating primarily to managing information security incidents. The management of physical and personnel security incidents is considered to be out of scope unless it directly impacts on the protection of systems (e.g. the breaching of physical protection for a server room).

References

7.3.3. Additional information relating to the management of ICT evidence is contained in:

Reference	Title	Source
ISO/IEC_27037	Information Technology – Security Techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence.	http://www.iso27001security.com/html/27037.html http://www.standards.co.nz
HB 171:2003	Guidelines for the Management of Information Technology Evidence	http://www.standards.co.nz
	The New Zealand Security Incident Management Guide for Computer Security Incident Response Teams (CIRSTs)	http://www.ncsc.govt.nz/resources/

Rationale & Controls

7.3.4. Information security incident management documentation

7.3.4.R.01. Rationale

Ensuring responsibilities and procedures for information security incidents are documented in relevant Information Security Documentation will ensure that when a information security incident does occur, agency personnel can respond in an appropriate manner. In addition, ensuring that system users are aware of reporting procedures will assist in identifying any information security incidents that an ITSM, or system owner fail to notice.

7.3.4.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST detail information security incident responsibilities and procedures for each system in the relevant Information Security Documents.

7.3.5. Recording information security incidents

7.3.5.R.01. Rationale

The purpose of recording information security incidents is to highlight the nature and frequency of information security incidents so that corrective action can be taken. This information can subsequently be used as an input to security risk assessments of systems.

7.3.5.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST follow the NZ implementation of the STIXX / TAXII and CyBox protocols and SHOULD include the following information in their register:

- the date the information security incident was discovered;
- the date the information security incident occurred;
- a description of the information security incident, including the personnel, systems and locations involved;
- the action taken;
- to whom the information security incident was reported; and
- the file reference.

7.3.5.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that all information security incidents are recorded in a register.

7.3.5.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use their incidents register as a reference for future security risk assessments.

7.3.6. Handling data spills

7.3.6.R.01. Rationale

A data spill is defined as the unauthorised or unintentional release, transmission or transfer of data. If there is a possibility that classified information may be compromised as a result of an information security incident, agencies MUST be able to respond in a timely fashion to limit damage and contain the incident.

7.3.6.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST implement procedures and processes to detect data spills.

7.3.6.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

When a data spill occurs agencies MUST assume that data at the highest classification held on or processed by the system, has been compromised.

7.3.6.C.03. Control: System Classification(s): All Classifications; Compliance: MUST

Agency SOPs MUST include procedure for:

- all personnel with access to systems;
- notification to the ITSM of any data spillage; and
- notification to the ITSM of access to any data which they are not authorised to access.

7.3.6.C.04. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST document procedures for dealing with data spills in their IRP.

7.3.6.C.05. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST treat any data spill as an information security incident and follow the IRP to deal with it.

7.3.6.C.06. Control: System Classification(s): All Classifications; Compliance: MUST

When a data spill occurs agencies MUST report the details of the data spill to the information owner.

7.3.7. Containing data spills

7.3.7.R.01. Rationale

The spillage of classified information onto a system not accredited to handle the information is considered a significant information security incident.

7.3.7.R.02. Rationale

Isolation may include disconnection from other systems and any external connections. In some cases system isolation may not be possible for architectural or operational reasons.

7.3.7.R.03. Rationale

Segregation may be achieved by isolation, enforcing separation of key elements of a virtual system, removing network connectivity to the relevant device or applying access controls to prevent or limit access.

7.3.7.R.04. Rationale

It is important to note that powering off a system can destroy information that may be useful in forensics analysis or other investigative work.

7.3.7.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

When classified information is introduced onto a system not accredited to handle the information, the following actions MUST be followed:

1. Immediately seek the advice of an ITSM;
2. Segregate or isolate the affected system and/or data spill;
3. Personnel MUST NOT delete the higher classified information unless specifically authorised by an ITSM.

7.3.7.C.02. Control: System Classification(s): All Classifications; Compliance: MUST NOT

When classified information is introduced onto a system not accredited to handle the information, personnel MUST NOT copy, view, print or email the information.

7.3.7.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

When a data spill occurs and systems cannot be *segregated* or *isolated* agencies SHOULD *immediately* contact the GCSB for further advice.

7.3.8. Handling malicious code infection

7.3.8.R.01. Rationale

The guidance for handling malicious code infections is provided to assist in preventing the spread of the infection and to prevent reinfection. Important details include:

- the infection date of the machine;
- the possibility that system records and logs could be compromised; and
- the period of infection.

7.3.8.R.02. Rationale

A complete operating system reinstallation, or an extensive comparison of checksums or other characterisation information, is the only reliable way to ensure that malicious code is eradicated.

7.3.8.R.03. Rationale

Agencies SHOULD be aware that some malicious code infections may be categorised as Advanced Persistent Threats (APTs) which may have been present for some time before detection. Specialist assistance may be required to deal with APTs.

7.3.8.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD follow the steps described below when malicious code is detected:

- isolate the infected system;
- decide whether to request assistance from GCSB;
- if such assistance is requested and agreed to, delay any further action until advised by GCSB;
- scan all previously connected systems and any media used within a set period leading up to the information security incident, for malicious code;
- isolate all infected systems and media to prevent reinfection;
- change all passwords and key material stored or potentially accessed from compromised systems, including any websites with password controlled access;
- advise system users of any relevant aspects of the compromise, including a recommendation to change all passwords on compromised systems;
- use up-to-date anti-malware software to remove the malware from the systems or media;
- monitor network traffic for malicious activity;
- report the information security incident and perform any other activities specified in the IRP; and
- in the worst case scenario, rebuild and reinitialise the system.

7.3.9. Allowing continued attacks

7.3.9.R.01. Rationale

Agencies allowing an attacker to continue an attack against a system in order to seek further information or evidence will need to establish with their legal advisor(s) whether the actions are breaching the Telecommunications (Interception Capability and Security) Act 2013.

7.3.9.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies considering allowing an attacker to continue some actions under controlled conditions for the purpose of seeking further information or evidence SHOULD seek legal advice.

7.3.10. Integrity of evidence

7.3.10.R.01. Rationale

While gathering evidence it is important to maintain the integrity of the information and the chain of evidence. Even though in most cases an investigation does not directly lead to a police prosecution, it is important that the integrity of evidence such as manual logs, automatic audit trails and intrusion detection tool outputs be protected.

7.3.10.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD:

- transfer a copy of raw audit trails and other relevant data onto media for secure archiving, as well as securing manual log records for retention; and
- ensure that all personnel involved in the investigation maintain a record of actions undertaken to support the investigation.

7.3.11. Seeking assistance

7.3.11.R.01. Rationale

If the integrity of evidence relating to an information security incident is compromised, it reduces GCSB's ability to assist agencies. As such, GCSB requests that no actions which could affect the integrity of the evidence are carried out prior to GCSB's involvement.

7.3.11.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that any requests for GCSB assistance are made as soon as possible after the information security incident is detected and that no actions which could affect the integrity of the evidence are carried out prior to GCSB's involvement.

8. Physical Security

8.1. Facilities

Objective

8.1.1. Physical security measures are applied to facilities protect systems and their infrastructure.

Context

Scope

8.1.2. This section covers information on the physical security of facilities. Information on physical security controls for servers and network devices, network infrastructure and IT equipment can be found in the following sections of this chapter.

Physical security requirements for storing classified information

8.1.3. Many of the physical controls in this manual are derived from the physical security protocol requirements within the PSR. In particular from the minimum standard for security containers, secure rooms or lockable commercial cabinets needed for storing classified information.

Secure and unsecure areas

8.1.4. In the context of this manual a secure area may be a single room or a facility that has security measures in place for the processing of classified information, or may encompass an entire building.

Physical security certification authorities

8.1.5. The certification of an agency's physical security measures is an essential part of the certification and accreditation process. The authority and responsibility are listed in the table below:

Classification	Authority	Responsibility
SECRET	CSO	Physical
TOP SECRET	NZSIS	Physical
TOP SECRET SCIF	GCSB	Network Infrastructure Technical Security Surveillance Counter Measures

8.1.6. Top Secret (TS) physical certification should be completed before any Technical inspections and certifications occur.

Facilities located outside of New Zealand

8.1.7. Agencies operating sites located outside of New Zealand can contact GCSB to determine any additional requirements which may exist such as technical surveillance and oversight counter-measures and testing.

References

8.1.8. High-level information relating to physical security is also contained in:

Title	Publisher	Source
ISO/IEC 27002:2013, **Section 11 - Physical and Environmental Security**	ISO /IEC Standards NZ	http://www.iso27001security.com/html/27002.html http://www.standards.co.nz

PSR references

Reference	Title	Source
PSR Mandatory Requirements	GOV3, GOV4, GOV7, INFOSEC1, INFOSEC2, INFOSEC4, INFOSEC5, PHYSEC1, PHYSEC6 and PHYSEC7	http://www.protectivesecurity.govt.nz
PSR content protocols and requirements sections	Physical Security of ICT Equipment Systems and Facilities and Mobile Electronic Device Risks and Mitigations	http://www.protectivesecurity.govt.nz

Rationale & Controls

8.1.9. Facility physical security

8.1.9.R.01. Rationale

The application of defence-in-depth to the protection of systems and infrastructure is enhanced through the use of successive layers of physical security.

Typically the layers of security are:

- site;
- building;
- room;
- racks;
- approved containers;
- operational hours; and
- manning levels.

8.1.9.R.02. Rationale

All layers are designed to control and limit access to those with the appropriate authorisation for the site, infrastructure and system. Deployable platforms need to meet physical security certification requirements as with any other system. Physical security certification authorities dealing with deployable platforms may have specific requirements that supersede the requirements of this manual and as such security personnel should contact their appropriate physical security certification authority to seek guidance.

8.1.9.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that any facility containing a system or its associated infrastructure, including deployable systems, are certified and accredited in accordance with the PSR.

8.1.10. Preventing observation by unauthorised people

8.1.10.R.01. Rationale

Agency facilities without sufficient perimeter security are often exposed to the potential for observation through windows or open doors. This is sometimes described as the risk of oversight. Ensuring classified information on desks and computer screens is not visible will assist in reducing this security risk.

8.1.10.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD prevent unauthorised people from observing systems, in particular desks, screens and keyboards.

8.1.10.C.02. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD position desks, screens and keyboards so that they cannot be seen by unauthorised people, or fix blinds or drapes to the inside of windows and away from doorways.

8.1.11. Bringing non-agency owned devices into secure areas

8.1.11.R.01. **Rationale**

No non-agency owned devices are to be brought into TOP SECRET areas without their prior approval of the Accreditation Authority.

8.1.11.C.01. **Control:** System Classification(s): TS; Compliance: MUST NOT

Agencies MUST NOT permit non-agency owned devices to be brought into TOP SECRET areas without prior approval from the Accreditation Authority.

8.1.12. Technical Inspection and surveillance counter-measure testing

8.1.12.R.01. **Rationale**

Technical surveillance counter-measure testing is conducted as part of the physical security certification to ensure that facilities do not have any unauthorised listening devices or other surveillance devices installed and that physical security measures are compatible with technical controls. This testing and inspection will normally occur AFTER the physical site accreditation has been completed (in accordance with the PSR). Further testing may also be necessary after uncleared access to the secure facility, such as contractors or visitors.

8.1.12.C.01. **Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST ensure that technical surveillance counter-measure tests are conducted as a part of the physical security certification.

8.1.12.C.02. **Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST determine if further technical surveillance counter-measure testing is required, particularly if visitors or contractors have entered secure areas.

8.2. Servers And Network Devices

Objective

8.2.1. Secured server and communications rooms provide appropriate physical security for servers and network devices.

Context

Scope

8.2.2. This section covers the physical security of servers and network devices. Information relating to network infrastructure and IT equipment can be found in other sections of this chapter.

Secured server and communications rooms

8.2.3. In order to reduce storage physical security requirements for information systems infrastructure, other network devices and servers, agencies may choose to certify and accredit the physical security of the site or IT equipment room to the standard specified in the PSR. This has the effect of providing an additional layer of physical security.

8.2.4. Agencies choosing NOT to certify and accredit the physical security of the site or IT equipment room, must continue to meet the full storage requirements specified in the PSR.

Rationale & Controls

8.2.5. Securing servers and network devices

8.2.5.R.01. Rationale

Security containers for IT infrastructure, network devices or servers situated in an unsecure area must be compliant with the requirements of the PSR. Installing IT infrastructure, network devices or servers in a secure facility can lower the storage requirements, provided multiple layers of physical security have been implemented, certified and accredited.

8.2.5.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that servers and network devices are secured within cabinets as outlined in PSR Physical Security Management Requirements – Physical Security of ICT Equipment, Systems and Facilities – ANNEX 1 Storage requirements for electronic information in ICT facilities.

8.2.5.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use a secured server or communications room within a secured facility.

8.2.6. Securing server rooms, communications rooms and security containers

8.2.6.R.01. Rationale

If personnel decide to leave server rooms, communications rooms or security containers with keys in locks, unlocked or with security functions disabled it negates the purpose of providing security in the first place. Such activities will compromise the security efforts of the agencies and should not be permitted by the agency.

8.2.6.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that keys or equivalent access mechanisms to server rooms, communications rooms and security containers are appropriately controlled.

8.2.6.C.02. Control: System Classification(s): All Classifications; Compliance: MUST NOT

Agencies MUST NOT leave server rooms, communications rooms or security containers in an unsecured state unless the server room is occupied by authorised personnel.

8.2.7. Server Physical Security – Site Security Plan

8.2.7.R.01. Rationale

Site security plans (SitePlan), the physical security equivalent of the SecPlan and SOPs for systems, are used to document all aspects of physical security for systems. Formally documenting this information ensures that standards, controls and procedures can easily be reviewed by security personnel.

8.2.7.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST develop a Site Security Plan (SitePlan) for each server and communications room. Information to be covered includes, but is not limited to:

- a summary of the security risk review for the facility the server or communications room is located in;
- roles and responsibilities of facility and security personnel;
- the administration, operation and maintenance of the electronic access control system or security alarm system;
- key management, the enrolment and removal of system users and issuing of personal identification number codes and passwords;
- personnel security clearances, security awareness training and regular briefings;
- regular inspection of the generated audit trails and logs;
- end of day checks and lockup;
- reporting of information security incidents; and
- what activities to undertake in response to security alarms.

8.2.8. No-lone-zones

8.2.8.R.01. Rationale

Areas containing particularly sensitive materials or IT equipment can be provided with additional security through the use of a designated no-lone-zone. The aim of this designation is to enforce two-person integrity, where all actions are witnessed by at least one other person.

8.2.8.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies operating no-lone-zones MUST suitably signpost the area and have all entry and exit points appropriately secured.

8.3. Network Infrastructure

Objective

8.3.1. Network infrastructure is protected by secure facilities and the use of encryption technologies.

Context

Scope

8.3.2. This section covers information relating to the physical security of network infrastructure. Information relating to servers, network devices and IT equipment can be found in other sections of this chapter. Additionally, information on using encryption for infrastructure in unsecure areas can be found in Section 17.1 - Cryptographic Fundamentals.

Rationale & Controls

8.3.3. Network infrastructure in secure areas

8.3.3.R.01. Rationale

Network infrastructure is considered to process information being communicated across it and as such needs to meet the minimum physical security requirements for processing classified information as specified in the PSR Physical Security Management Requirements – Physical Security of ICT Equipment, Systems and Facilities – ANNEX 1 Storage requirements for electronic information in ICT facilities.

8.3.3.R.02. Rationale

The physical security requirements for network infrastructure can be lowered if encryption is being applied to classified information communicated over the infrastructure (i.e. data in transit encryption). Note this does NOT change the classification of the data itself, only the physical protection requirements.

8.3.3.R.03. Rationale

It is important to note that physical controls do not provide any protection against malicious software or other malicious entities that may be residing on or have access to the system.

8.3.3.R.04. Rationale

If classified information being communicated over the infrastructure is not encrypted the malicious entry can capture, corrupt or modify the traffic to assist in furthering any attempts to exploit the network and the information being communicated across it.

8.3.3.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST certify the physical security of facilities containing network infrastructure to the highest classification of information being communicated over the network infrastructure.

8.3.3.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies communicating classified information over infrastructure in secure areas SHOULD encrypt their information with at least an Approved Cryptographic Protocol. See Section 17.3 – Approved Cryptographic Protocols.

8.3.4. Protecting network infrastructure

8.3.4.R.01. Rationale

In order to prevent tampering with patch panels, fibre distribution panels and structured wiring, any such enclosures need to be placed within at least lockable commercial cabinets. Furthermore, keys for such cabinets should not be remain in locks as this defeats the purpose of using lockable commercial cabinets in the first place.

8.3.4.C.01. Control: System Classification(s): TS; Compliance: MUST

Agencies MUST locate patch panels, fibre distribution panels and structured wiring enclosures within at least lockable commercial cabinets.

8.3.4.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD locate patch panels, fibre distribution panels and structured wiring enclosures within at least lockable commercial cabinets.

8.3.5. Network infrastructure in unsecure areas

8.3.5.R.01. Rationale

As agencies lose control over classified information when it is communicated over unsecure public network infrastructure or over infrastructure in unsecure areas they MUST ensure that it is encrypted to a sufficient level that if it was captured that it would be sufficiently difficult to determine the original information from the encrypted information.

8.3.5.R.02. Rationale

Encryption does not change the class level of the information itself but allows reduced handling requirements to be applied.

8.3.5.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies communicating classified information over public network infrastructure or over infrastructure in unsecure areas MUST use encryption to lower the handling instructions to be equivalent to those for unclassified networks.

8.4. IT Equipment

Objective

8.4.1. IT equipment is secured outside of normal working hours, is non-operational or when work areas are unoccupied.

Context

Scope

8.4.2. This section covers information relating to the physical security of IT equipment containing media. This includes but is not limited to workstations, printers, photocopiers, scanners and multi-function devices (MFDs).

8.4.3. Additional information relating to IT equipment and media can be found in the following chapters and sections of this manual:

- Section 11.2 - Fax Machines, Multifunction Devices and Network Printers;
- Chapter 12 - Product Security; and
- Chapter 13 – Decommissioning and Disposal.

Handling IT equipment containing media

8.4.4. During non-operational hours agencies need to store media containing classified information that resides within IT equipment in accordance with the requirements of the PSR. Agencies can comply with this requirement by undertaking one of the following processes:

- ensuring IT equipment always reside in an appropriate class of secure room;
- storing IT equipment during non-operational hours in an appropriate class of security container or lockable commercial cabinet;
- using IT equipment with removable non-volatile media which is stored during non-operational hours in an appropriate class of security container or lockable commercial cabinet as well as securing its volatile media;
- using IT equipment without non-volatile media as well as securing its volatile media;
- using an encryption product to reduce the physical storage requirements of the non-volatile media as well as securing its volatile media; or
- configuring IT equipment to prevent the storage of classified information on the non-volatile media when in use and enforcing scrubbing of temporary data at logoff or shutdown as well as securing its volatile media.

8.4.5. The intent of using cryptography or preventing the storage of classified information on non-volatile media is to enable agencies to treat the media within IT equipment in accordance with the storage requirements of a lower classification, as specified in the PSR, during non-operational hours. Temporary data should be deleted at log off or shut down and volatile media secured.

8.4.6. As the process of using cryptography and preventing the storage of classified information on non-volatile media does not constitute the sanitisation and reclassification of the media, the media retains its classification for the purposes of reuse, reclassification, declassification, sanitisation, destruction and disposal requirements as specified in this manual.

IT equipment using hybrid hard drives or solid state drives

8.4.7. The process of preventing the storage of classified information on non-volatile media, and enforcing deletion of temporary data at logoff or shutdown, is NOT approved as a method of lowering the storage requirements, when hybrid hard drives or solid state drives are used.

Rationale & Controls

8.4.8. Accounting for IT equipment

8.4.8.R.01. Rationale

Ensuring that IT equipment containing media is accounted for by using asset registers, equipment registers, operational & configuration records and regular audits will assist in preventing loss or theft, or in the cases of loss or theft, alerting appropriate authorities to its loss or theft.

8.4.8.R.02. Rationale

Asset registers may not provide a complete record as financial limits may result in smaller value items not being recorded. In such cases other registers and operational information can be utilised to assist in building a more complete record.

8.4.8.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST account for all IT equipment containing media.

8.4.9. Processing requirements

8.4.9.R.01. Rationale

As the media within IT equipment takes on the classification of the information it is processing, the area that it is used within needs to be certified to a level that is appropriate for the classification of that information.

8.4.9.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST certify the physical security of facilities containing IT equipment to the highest classification of information being processed, stored or communicated by the equipment within the facilities.

8.4.10. Storage requirements

8.4.10.R.01. Rationale

The PSR states that either Class C, B or A secure rooms or Class C, B or A security containers or lockable commercial cabinets can be used to meet physical security requirements for the storage of IT equipment containing media. The class of secure room or security container will depend on the physical security certification of the surrounding area and the classification of the information.

8.4.10.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that when secure areas are non-operational or when work areas are unoccupied IT equipment with media is secured in accordance with the minimum physical security requirements for storing classified information as specified in the PSR Physical Security Management Requirements – Physical Security of ICT Equipment, Systems and Facilities – ANNEX 1 Storage requirements for electronic information in ICT facilities.

8.4.11. Securing non-volatile media for storage

8.4.11.R.01. Rationale

The use of techniques to prevent the storage of classified information on non-volatile media and processes to delete temporary data at logoff or shutdown may sound secure but there is no guarantee that they will always work effectively or will not be bypassed in unexpected circumstances such as a loss of power. As such, agencies need to consider these risks when implementing such a solution.

8.4.11.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies choosing to prevent the storage of classified information on non-volatile media and enforcing scrubbing of temporary data at logoff or shutdown SHOULD:

- assess the security risks associated with such a decision; and
- specify the processes and conditions for their application within the system's SecPlan.

8.4.12. Securing volatile media for storage

8.4.12.R.01. Rationale

If agencies need to conduct a security risk assessment as part of the procedure for storing IT equipment containing media during non-operation hours, they should consider security risks such as:

- an attacker gaining access to the IT equipment immediately after power is removed and accessing the contents of volatile media to recover encryption keys or parts thereof. This is sometimes described as a data remanence attack;
- extreme environmental conditions causing data to remain in volatile media for extended periods after the removal of power; and
- the physical security of the locations in which the IT equipment will reside.

8.4.12.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies securing volatile media for IT equipment during non-operational hours SHOULD:

- disconnect power from the equipment the media resides within;
- assess the security risks if not sanitising the media; and
- specify any additional processes and controls that will be applied within the system's SecPlan.

8.4.13. Encrypting media within IT equipment

8.4.13.R.01. Rationale

Current industry good practice is to encrypt all media within IT equipment. Newer operating systems provide this functionality and older operating systems can be supported with the use of open source or proprietary applications.

8.4.13.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD encrypt media within IT equipment with an Approved Cryptographic Algorithm. See Section 17.2 - Approved Cryptographic Algorithms.

8.5. Tamper Evident Seals

Objective

8.5.1. Tamper evident seals and associated auditing processes identify attempts to bypass the physical security of systems and their infrastructure.

Context

Scope

8.5.2. This section covers information on tamper evident seals that can be applied to assets.

Rationale & Controls

8.5.3. Recording seal usage

8.5.3.R.01. Rationale

Recording information about seals in a register and on which asset they are used assists in reducing the security risk that seals could be substituted without security personnel being aware of the change.

8.5.3.C.01. Control: System Classification(s): TS; Compliance: MUST

Agencies MUST record the usage of seals in a register that is appropriately secured.

8.5.3.C.02. Control: System Classification(s): TS; Compliance: MUST

Agencies MUST record in a register, information on:

- issue and usage details of seals and associated tools;
- serial numbers of all seals purchased; and
- the location or asset on which each seal is used.

8.5.3.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD record the usage of seals in a register that is appropriately secured.

8.5.3.C.04. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD record in a register information on:

- issue and usage details of seals and associated tools;
- serial numbers of all seals purchased; and
- the location or asset on which each seal is used.

8.5.4. Purchasing seals

8.5.4.R.01. Rationale

Using uniquely numbered seals ensures that a seal can be uniquely mapped to an asset. This assists security personnel in reducing the security risk that seals could be replaced without anyone being aware of the change.

8.5.4.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD consult with the seal manufacturer to ensure that, if available, any purchased seals and sealing tools display a unique identifier or image appropriate to the agency.

8.5.4.C.02. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

Seals and any seal application tools SHOULD be secured when not in use.

8.5.4.C.03. **Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT allow contractors to independently purchase seals and associated tools on behalf of the government.

8.5.5. Reviewing seal usage

8.5.5.R.01. **Rationale**

Users of assets with seals should be encouraged to randomly check the integrity of the seals and to report any concerns to security personnel. In addition, conducting at least annual reviews will allow for detection of any tampering to an asset and ensure that the correct seal is located on the correct asset.

8.5.5.C.01. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD review seals for differences with a register at least annually. At the same time seals SHOULD be examined for any evidence of tampering.

9. Personnel Security

9.1. Information Security Awareness and Training

Objective

9.1.1. A security culture is fostered through induction training and ongoing security education tailored to roles, responsibilities, changing threat environment and sensitivity of information, systems and operations.

Context

Scope

9.1.2. This section covers information relating specifically to information security awareness and training.

PSR references

Reference	Title	Source
PSR Mandatory Requirements	GOV6, GOV9, INFOSEC1 and PERSEC6	http://www.protectivesecurity.govt.nz
PSR content protocols and requirements sections	Security Awareness Training	http://www.protectivesecurity.govt.nz

Rationale & Controls

9.1.3. Information security awareness and training responsibility

9.1.3.R.01. Rationale

Agency management is responsible for ensuring that an appropriate information security awareness and training program is provided to personnel. Without management support, security personnel might not have sufficient resources to facilitate awareness and training for other personnel.

9.1.3.R.02. Rationale

Awareness and knowledge degrades over time without ongoing refresher training and updates.. Providing ongoing information security awareness and training will assist in keeping personnel aware of issues and their responsibilities.

9.1.3.R.03. Rationale

Methods that can be used to continually promote awareness include logon banners, system access forms and departmental bulletins and memoranda.

9.1.3.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agency management MUST ensure that all personnel who have access to a system have sufficient information security awareness and training.

9.1.4. Information security awareness and training

9.1.4.R.01. Rationale

Information security awareness and training programs are designed to help system users:

- become familiar with their roles and responsibilities;
- understand any legislative or regulatory mandates and requirements;
- understand any national or agency policy mandates and requirements;
- understand and support security requirements;
- assist in maintaining security; and
- learn how to fulfil their security responsibilities.

9.1.4.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST provide ongoing information security awareness and training for personnel on topics such as responsibilities, legislation and regulation, consequences of non-compliance with information security policies and procedures, and potential security risks and counter-measures.

9.1.4.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST provide information security awareness training as part of their employee induction programmes.

9.1.5. Degree and content of information security awareness and training

9.1.5.R.01. Rationale

The detail, content and coverage of information security awareness and training will depend on the objectives of the organisation. Personnel with responsibilities beyond that of a general user should have tailored training to meet their needs.

9.1.5.R.02. Rationale

As part of the guidance provided to system users, there should be sufficient emphasis placed on the activities that are NOT allowed on systems. The minimum list of content will also ensure that personnel are sufficiently exposed to issues that could cause an information security incident through lack of awareness or through lack of knowledge.

9.1.5.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD align the detail, content and coverage of information security awareness and training to system user responsibilities.

9.1.5.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that information security awareness and training includes information on:

- the purpose of the training or awareness program;
- any legislative or regulatory mandates and requirements;
- any national or agency policy mandates and requirements;
- agency security appointments and contacts;
- the legitimate use of system accounts, software and classified information;
- the security of accounts, including shared passwords;
- authorisation requirements for applications, databases and data;
- the security risks associated with non-agency systems, particularly the Internet;
- reporting any suspected compromises or anomalies;
- reporting requirements for information security incidents, suspected compromises or anomalies;
- classifying, marking, controlling, storing and sanitising media;
- protecting workstations from unauthorised access;
- informing the support section when access to a system is no longer needed;
- observing rules and regulations governing the secure operation and authorised use of systems; and
- supporting documentation such as SOPs and user guides.

9.1.5.C.03. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that information security awareness and training includes advice to system users not to attempt to:

- tamper with the system;
- bypass, strain or test information security mechanisms;
- introduce or use unauthorised IT equipment or software on a system;
- replace items such as keyboards, pointing devices and other peripherals with personal equipment;
- assume the roles and privileges of others;
- attempt to gain access to classified information for which they have no authorisation; or
- relocate equipment without proper authorisation.

9.1.6. System familiarisation training

9.1.6.R.01. **Rationale**

A TOP SECRET system needs increased awareness by personnel. Ensuring familiarisation with information security policies and procedures, the secure operation of the system and basic information security training, will provide them with specific knowledge relating to these types of systems.

9.1.6.C.01. **Control:** System Classification(s): TS; Compliance: MUST

Agencies MUST provide all system users with familiarisation training on the information security policies and procedures and the secure operation of the system before being granted unsupervised access to the system.

9.1.7. Disclosure of information while on courses

9.1.7.R.01. **Rationale**

Government personnel attending courses with non-government personnel may not be aware of the consequences of disclosing information relating to the security of their agency's systems. Raising awareness of such consequences in personnel will assist in preventing disclosures that could lead to a targeted attack being launched against an agency's systems.

9.1.7.C.01. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD advise personnel attending courses along with non-government personnel not to disclose any details that could be used to compromise agency security.

9.2. Authorisations, Security Clearances And Briefings

Objective

9.2.1. Only appropriately authorised, cleared and briefed personnel are allowed access to systems.

Context

Scope

9.2.2. This section covers information relating to the authorisations, security clearances and briefings required by personnel to access systems. Information on the technical implementation of access controls for systems can be found in Section 16.2 - System Access.

Security clearances – New Zealand and foreign

9.2.3. Where this manual refers to security clearances, the reference applies to a national security clearance granted by a New Zealand government agency. Foreign nationals may be granted a national security clearance if risks can be mitigated. Refer to PSR Agency Personnel Security for more information.

PSR References

9.2.4. Additional policy and information on granting and maintaining security clearances can be found in:

Reference	Title	Source
PSR Mandatory Requirements	PERSEC1, PERSEC2, PERSEC3, PERSEC4, PERSEC5, PERSEC6, PERSEC7 and INFOSEC5	http://www.protectivesecurity.govt.nz

Rationale & Controls

9.2.5. Documenting authorisations, security clearance and briefing requirements

9.2.5.R.01. Rationale

Ensuring that the requirements for access to a system are documented and agreed upon will assist in determining if system users have appropriate authorisations, security clearances and need-to-know to access the system.

9.2.5.R.02. Rationale

Types of system users for which access requirements will need to be documented include general users, privileged users, system administrators, contractors and visitors.

9.2.5.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST specify in the System Security Plan (SecPlan) any authorisations, security clearances and briefings necessary for system access.

9.2.6. Authorisation and system access

9.2.6.R.01. Rationale

Personnel seeking access to a system will need to have a genuine business requirement to access the system as verified by their supervisor or manager. Once a requirement to access a system is established, the system user should be given only the privileges that they need to undertake their duties. Providing all system users with privileged access when there is no such requirement can cause significant security vulnerabilities in a system.

9.2.6.C.01. Control: System Classification(s): TS; Compliance: MUST

Agencies MUST:

- limit system access on a need-to-know/need-to-access basis;
- provide system users with the least amount of privileges needed to undertake their duties; and
- have any requests for access to a system authorised by the supervisor or manager of the system user.

9.2.6.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD:

- limit system access on a need-to-know/need to access basis;
- provide system users with the least amount of privileges needed to undertake their duties; and
- have any requests for access to a system authorised by the supervisor or manager of the system user.

9.2.7. Recording authorisation for personnel to access systems

9.2.7.R.01. Rationale

In many cases, the requirement to maintain a secure record of all personnel authorised to access a system, their user identification, who provided the authorisation and when the authorisation was granted, can be met by retaining a completed system account request form signed by the supervisor or manager of the system user.

9.2.7.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD:

- maintain a secure record of:
  - all authorised system users;
  - their user identification;
  - why access is required;
  - role and privilege level,
  - who provided the authorisation to access the system;
  - when the authorisation was granted; and
- maintain the record, for the life of the system or the length of employment whichever is the longer, to which access is granted.

9.2.8. Security clearance for system access

9.2.8.R.01. Rationale

Information classified as CONFIDENTIAL and above requires personnel to have been granted a formal security clearance before access is granted. Refer to the New Zealand Government Personnel Security Management Requirements – Agency Personnel Security.

9.2.8.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST NOT

System users MUST NOT be granted access to systems or information classified CONFIDENTIAL or above unless vetting procedures have been completed and formal security clearance granted.

9.2.8.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

All system users MUST:

- hold a security clearance at least equal to the system classification; or
- have been granted access in accordance with the requirements in the PSR for emergency access.

9.2.9. System access briefings

9.2.9.R.01. Rationale

Some systems process endorsed or compartmented information. As such, unique briefings may exist that system users need to receive before being granted access to the system. All system users will require a briefing on their responsibilities on access to and use of the system to which they have been granted access to avoid inadvertent errors and security breaches. Specialised system training may also be required.

9.2.9.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

All system users MUST have received any necessary briefings before being granted access to compartmented or endorsed information or systems.

9.2.10. Access by foreign nationals to NZEO systems

9.2.10.R.01. Rationale

NZEO information is restricted to New Zealand nationals.

9.2.10.C.01. Control: System Classification(s): All Classifications; Compliance: MUST NOT

Where systems process, store or communicate unprotected NZEO information, agencies MUST NOT allow foreign nationals, including seconded foreign nationals, to have access to the system.

9.2.10.C.02. Control: System Classification(s): All Classifications; Compliance: MUST NOT

Where agencies protect NZEO information on a system by implementing controls to ensure that NZEO information is not passed to, or made accessible to, foreign nationals, agencies MUST NOT allow foreign nationals, including seconded foreign nationals, to have access to the system.

9.2.11. Access by foreign nationals to New Zealand systems

9.2.11.R.01. Rationale

When information from foreign nations is entrusted to the New Zealand Government, care needs to be taken to ensure that foreign nationals do not have access to such information unless it has also been released to their country.

9.2.11.C.01. Control: System Classification(s): All Classifications; Compliance: MUST NOT

Where systems process, store or communicate classified information with nationality releasability markings, agencies MUST NOT allow foreign nationals, including seconded foreign nationals, to have access to such information that is not marked as releasable to their nation.

9.2.12. Granting limited higher access

9.2.12.R.01. Rationale

Under exceptional circumstances, temporary access to systems classified RESTRICTED and below may be granted.

9.2.12.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST NOT

Agencies MUST NOT permit limited higher access for systems and information classified CONFIDENTIAL or above.

9.2.12.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies granting limited higher access to information or systems MUST ensure that:

- the requirement to grant limited higher access is temporary in nature and is an exception rather than the norm;
- an ITSM has recommended the limited higher access;
- a cessation date for limited higher access has been set;
- the access period does not exceed two months;
- the limited higher access is granted on an occasional NOT non-ongoing basis;
- the system user is not granted privileged access to the system;
- the system user's access is formally documented; and
- the system user's access is approved by the CISO.

9.2.13. Controlling limited higher access

9.2.13.R.01. Rationale

When personnel are granted access to a system under the provisions of limited higher access they need to be closely supervised or have their access controlled such that they have access only to that information they require to undertake their duties.

9.2.13.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies granting limited higher access to a system MUST ensure that:

- effective controls are in place to restrict access to only classified information that is necessary to undertake the system user's duties; or
- the system user is continually supervised by another system user who has the appropriate security clearances to access the system.

9.2.14. Granting emergency access

9.2.14.R.01. Rationale

Emergency access to a system may be granted where there is an immediate and critical need to access information for which personnel do not have the appropriate security clearances. Such access will need to be granted by the agency head or their delegate and be formally documented.

9.2.14.R.02. Rationale

It is important that appropriate debriefs take place at the conclusion of any emergency in order to manage the ongoing security of information and systems and to identify "lessons learned".

9.2.14.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST NOT

Emergency access MUST NOT be granted unless personnel have a security clearance to at least CONFIDENTIAL level.

9.2.14.C.02. Control: System Classification(s): C, S, TS; Compliance: MUST NOT

Emergency access MUST NOT be used on reassignment of duties while awaiting completion of full security clearance procedures.

9.2.14.C.03. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies granting emergency access to a system MUST ensure that:

- the requirements to grant emergency access is due to an immediate and critical need to access classified information and there is insufficient time to complete clearance procedures;
- the agency head or their delegate has approved the emergency access;
- the system user's access is formally documented;
- the system user's access is reported to the CISO;
- appropriate briefs and debriefs for the information and system are conducted;
- access is limited to information and systems necessary to deal with the particular emergency and is governed by strict application of the "need to know" principle;
- emergency access is limited to ONE security clearance level higher than the clearance currently held; and
- the security clearance process is completed as soon as possible.

9.2.14.C.04. Control: System Classification(s): C, S, TS; Compliance: MUST

Personnel granted emergency access MUST be debriefed at the conclusion of the emergency.

9.2.15. Accessing endorsed or compartmented information

9.2.15.R.01. Rationale

Limited higher access to systems processing, storing or communicating endorsed or compartmented information is not permitted.

9.2.15.C.01. Control: System Classification(s): All Classifications; Compliance: MUST NOT

Agencies MUST NOT grant limited higher access to systems that process, store or communicate endorsed or compartmented information.

9.3. Using The Internet

Objective

9.3.1. Personnel use Internet services in a responsible and security conscious manner, consistent with agency policies.

Context

Scope

9.3.2. This section covers information relating to personnel using Internet services such as the Web, Web-based email, news feeds, subscriptions and other services. Whilst this section does not address Internet services such as IM, IRC, IPT and video conferencing, agencies need to remain aware that unless applications using these communications methods are evaluated and approved by GCSB they are NOT approved for communicating classified information over the Internet.

9.3.3. Additional information on using applications that can be used with the Internet can be found in the Section 14.3 - Web Applications and Section 15.1 - Email Applications.

Rationale & Controls

9.3.4. Using the Internet

9.3.4.R.01. Rationale

Agencies will need to determine what constitutes suspicious activity, questioning or contact in relation to their own work environment. Suspicious activity, questioning or contact may relate to the work duties of personnel or the specifics of projects being undertaken by personnel within the agency.

9.3.4.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure personnel are instructed to report any suspicious activity, questioning or contact when using the Internet, to an ITSM.

9.3.5. Awareness of Web usage policies

9.3.5.R.01. Rationale

Users MUST be familiar with and formally acknowledge agency Web usage policies for system users in order to follow the policy and guidance.

9.3.5.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST make their system users aware of the agency's Web usage policies.

9.3.5.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Personnel MUST formally acknowledge and accept agency Web usage policies.

9.3.6. Monitoring Web usage

9.3.6.R.01. Rationale

Agencies may choose to monitor compliance with aspects of Web usage policies, such as access attempts to blocked websites, pornographic and gambling websites, as well as compiling a list of system users that excessively download and/or upload data without an obvious or known legitimate business requirement.

9.3.6.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD implement measures to monitor their personnel, visitor and contractor compliance with their Web usage policies.

9.3.7. Posting information on the Web

9.3.7.R.01. Rationale

Personnel need to take special care not to accidentally post information on the Web, especially in forums and blogs. Even Official Information or UNCLASSIFIED information that appears to be benign in isolation could, in aggregate, have a considerable security impact on the agency, government sector or wider government.

9.3.7.R.02. Rationale

To ensure that personal opinions of agency personnel are not interpreted as official policy or associated with an agency, personnel will need to maintain separate professional and personal accounts when using websites, especially when using online social networks.

9.3.7.R.03. Rationale

Accessing personal accounts from an agency's systems is discouraged.

9.3.7.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure personnel are instructed to take special care when posting information on the Web.

9.3.7.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure personnel posting information on the Web maintain separate professional accounts from any personal accounts they have for websites.

9.3.7.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD monitor websites where personnel post information and if necessary remove or request the removal of any inappropriate information.

9.3.7.C.04. Control: System Classification(s): All Classifications; Compliance: SHOULD

Accessing personal accounts from agency systems SHOULD be discouraged.

9.3.8. Posting personal information on the Web

9.3.8.R.01. Rationale

Personnel need to be aware that any personal interest or other information they post on websites can be used to develop a detailed profile of their families, lifestyle, interest and hobbies in order to attempt to build a trust relationship with them or others. This relationship could then be used to attempt to elicit information from them or implant malicious software on systems by inducing them to, for instance, open emails or visit websites with malicious content.

9.3.8.R.02. Rationale

Profiling is a common marketing and targeting technique facilitated by the internet.

9.3.8.R.03. Rationale

Individuals who work for high-interest agencies, who hold security clearances or who are involved in high-profile projects are of particular interest to profilers, cyber criminals and other users of this information.

9.3.8.R.04. Rationale

The following is of particular interest to profilers:

- photographs;
- past and present employment details;
- personal details, including DOB, family members, birthdays, address and contact details;
- schools and institutions;
- clubs, hobbies and interests;
- educational qualifications;
- current work duties;
- details of work colleagues and associates; and
- work contact details.

9.3.8.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that personnel are informed of the security risks associated with posting personal information on websites, especially for those personnel holding higher level security clearances.

9.3.8.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Personnel SHOULD be encouraged to use privacy settings for websites to restrict access to personal information they post to only those they authorise to view it.

9.3.8.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Personnel SHOULD be encouraged to undertake a Web search of themselves to determine what personal information is available and contact an ITSM if they need assistance in determining if the information is appropriate to be viewed by the general public or potential adversaries.

9.3.9. Peer-to-peer applications

9.3.9.R.01. Rationale

Personnel using peer-to-peer file sharing applications are often unaware of the extent of files that are being shared from their workstation. In most cases peer-to-peer file sharing applications will scan workstations for common file types and share them automatically for sharing or public consumption. Examples of peer-to-peer file sharing applications include Shareaza, KaZaA, Ares, Limewire, eMule and uTorrent.

9.3.9.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT allow personnel to use peer-to-peer applications over the Internet.

9.3.10. Receiving files via the Internet

9.3.10.R.01. Rationale

When personnel receive files via peer-to-peer file sharing, IM or IRC applications they are often bypassing security mechanisms put in place by the agency to detect and quarantine malicious code. Personnel should be encouraged to send files via established methods such as email, to ensure they are appropriately scanned for malicious code.

9.3.10.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT allow personnel to receive files via peer-to-peer, IM or IRC applications.

9.4. Escorting Uncleared Personnel

Objective

9.4.1. Uncleared personnel are escorted within secure areas.

Context

Scope

9.4.2. This section covers information relating to the escorting of uncleared personnel without security clearances in secure areas.

PSR references

Reference	Title	Source
PSR Mandatory Requirements	PHYSEC6	http://www.protectivesecurity.govt.nz
PSR content protocols and requirements sections	Security Zones and Risk Mitigation Control Measures	http://www.protectivesecurity.govt.nz

Rationale & Controls

9.4.3. Unescorted access

9.4.3.R.01. Rationale

Ensuring that personnel have correct security clearances to access sensitive areas and that access by escorted personnel is recorded for auditing purposes is widely considered a standard security practice.

9.4.3.C.01. Control: System Classification(s): TS; Compliance: MUST

Agencies MUST ensure that all personnel with unescorted access to TOP SECRET areas have appropriate security clearances and briefings.

9.4.4. Maintaining an unescorted access list

9.4.4.R.01. Rationale

Maintaining an unescorted access list reduces the administrative overhead of determining if personnel can enter a TOP SECRET area without an escort. Personnel with approval for unescorted access must be able to verify their identity at all times while within the secure area.

9.4.4.C.01. Control: System Classification(s): TS; Compliance: MUST

Agencies MUST maintain an up to date list of personnel entitled to enter a TOP SECRET area without an escort.

9.4.4.C.02. Control: System Classification(s): TS; Compliance: MUST

Personnel MUST display identity cards at all times while within the secure area.

9.4.5. Displaying the unescorted access list

9.4.5.R.01. Rationale

Displaying an unescorted access list allows staff to quickly verify if personnel are entitled to be in a TOP SECRET area without an escort. Care should be taken not to reveal the contents of the access list to non-cleared personnel.

9.4.5.C.01. Control: System Classification(s): TS; Compliance: SHOULD

Agencies SHOULD display within a TOP SECRET area, an up to date list of personnel entitled to enter the area without an escort.

9.4.5.C.02. Control: System Classification(s): TS; Compliance: SHOULD NOT

The unescorted access list SHOULD NOT be visible from outside of the secure area.

9.4.6. Visitors

9.4.6.R.01. Rationale

Visitors to secure areas should be carefully supervised to ensure the need-to-know principle is strictly adhered to.

9.4.6.C.01. Control: System Classification(s): TS; Compliance: SHOULD

Visitors SHOULD be carefully supervised to ensure they do not gain access to or have oversight of information above the level of their clearance or outside of their need-to-know.

9.4.7. Recording visits in a visitor log

9.4.7.R.01. Rationale

Recording visitors to a TOP SECRET area ensures that the agency has a record of visitors should an investigation into an incident need to take place in the future.

9.4.7.C.01. Control: System Classification(s): TS; Compliance: MUST NOT

Agencies MUST NOT permit personnel not on the unescorted access list to enter a TOP SECRET area unless their visit is recorded in a visitor log and they are escorted by a person on the unescorted access list.

9.4.8. Content of the visitor log

9.4.8.R.01. Rationale

The contents of the visitor log ensure that security personnel have sufficient details to conduct an investigation into an incident if required.

9.4.8.C.01. Control: System Classification(s): TS; Compliance: MUST

Agencies MUST, at minimum, record the following information in a visitor log for each entry:

- name;
- organisation;
- person visiting;
- contact details for person visiting; and
- date and time in and out.

9.4.9. Separate visitor logs

9.4.9.R.01. Rationale

Maintaining a separate visitor log for TOP SECRET areas assists in enforcing the need-to-know principle. General visitors do not need-to-know of personnel that have visited TOP SECRET areas.

9.4.9.C.01. Control: System Classification(s): TS; Compliance: MUST

Agencies with a TOP SECRET area within a larger facility MUST maintain a separate log from any general visitor log.

10. Infrastructure

10.1. Cable Management Fundamentals

Objective

10.1.1. Cable management systems are implemented to allow easy integration of systems across government and minimise the opportunity for tampering or unauthorised change.

Context

Scope

10.1.2. This section covers information relating to cable distribution systems used in facilities within New Zealand. When designing cable management systems, Section 10.5 - Cable Labelling and Registration and Section 10.6 - Cable Patching of this chapter also apply.

Applicability of controls within this section

10.1.3. The controls within this section are applicable only to communications infrastructure located within facilities in New Zealand. For deployable platforms or facilities outside of New Zealand Emanation Security Threat Assessments (Section 10.7) of this chapter of this manual MUST be consulted.

Common implementation scenarios

10.1.4. This section provides common requirements for non-shared facilities. Specific requirements for facilities shared between agencies and facilities shared with non-government entities can be found in subsequent sections of this chapter.

Red/Black Concept and Cable Separation

10.1.5. Black is the designation applied to information systems and networks where information IS NOT encrypted using HGCE. Conversely Red is the designation applied to information systems and networks where information IS encrypted using HGCE. In general terms systems accredited for classifications RESTRICTED and below are BLACK and CONFIDENTIAL and above are RED.

10.1.6. All cables with metal conductors (the signal carrier, the strengthening member or an armoured outer covering) can act as fortuitous signal conductors allowing signals to escape or to cross-contaminate other cables and signals. This provides a path for the exploitation of signals, data and information.

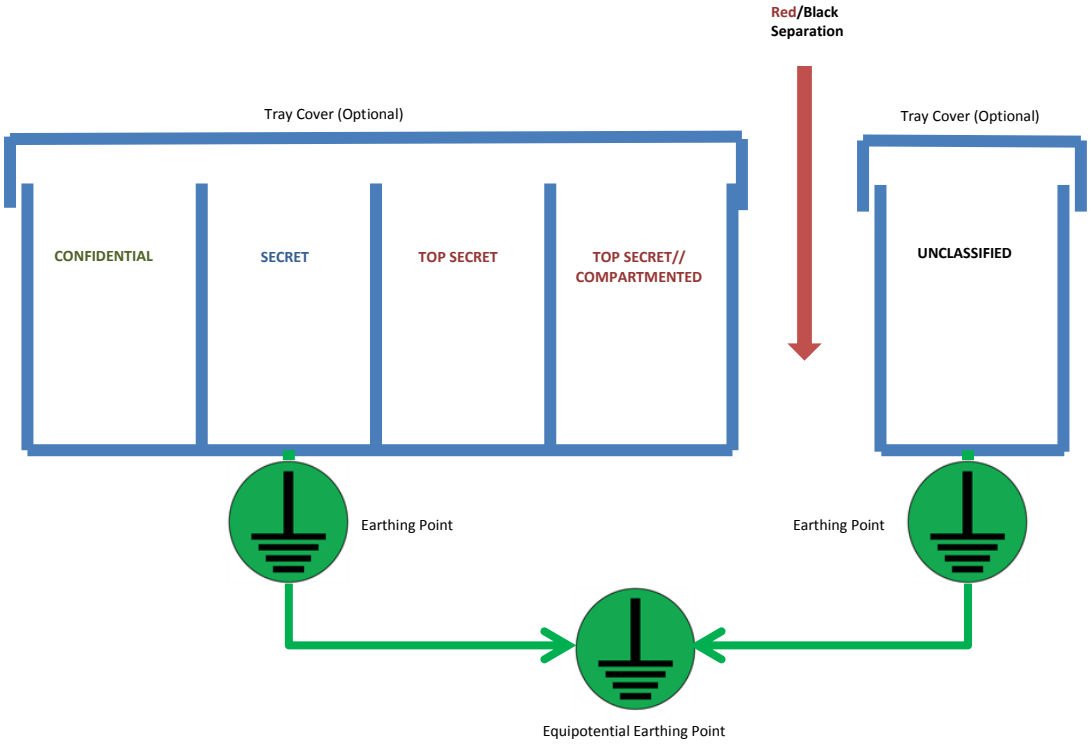
10.1.7. The Red/Black concept is the separation of electrical and electronic circuits, devices, equipment cables, connectors and systems that transmit store or process national security information (Red) from non-national security information (Black).

10.1.8. An important control is the separation of cables and related equipment with sufficient distance between them to prevent cross-contamination.

Cable trays

10.1.9. Where copper or a combination of copper and fibre cables are used, cable trays will provide separation, assist cable management and enhance cable protection. While preferable to separate **red** cables of different classification for cable management purposes, the most important element is to maintain **RED/BLACK** separation.

10.1.10. It is preferable that cable trays contain dividers. Some cable trays provide only a single receptacle for cables (no dividers). If dividers are not available, multi-core fibre cables should be used. Cables of similar classifications should be bundled. A typical cable tray layout with dividers is depicted below.



Catenary

10.1.11. The use of catenary (wire, rope, nylon cord or similar cable support mechanisms) is becoming more widespread in place of cable trays. Care MUST be taken to maintain **RED/BLACK** separation is this method of cable support is used.

Earthing

10.1.12. It is important that any metal trays or metal catenary are earthed for both safety and to avoid creating any fortuitous conductors. All earthing points MUST be equipotentially bonded.

Fibre optic cabling

10.1.13. Fibre optic cabling does not produce, and is not influenced by, electromagnetic emanations; as such it offers the highest degree of protection from electromagnetic emanation effects.

10.1.14. Many more fibres can be run per cable diameter than wired cables thereby reducing cable infrastructure costs. Fibre Optic cable is usually constructed with a glass core, cladding on the core and a further, colour coded coating. Multiple cores can be bundled into a single cable and multiple cables can be bundled into a high capacity cable. This is illustrated in Figures 1 below. Cables also have a central strength member of mylar or some similar high strength, non-conductive material

10.1.15. Fibre cable is considered the best method to future proof against unforeseen threats.

10.1.16. Cable trays for **fibre only cable** may be of any suitable material. If metal trays are used they MUST be earthed.

Armoured Fibre optic cabling

10.1.17. Some fibre optic cable also includes conductive metal cable strengtheners and conductive metal armoured sheaths which may be wire-wound or stainless steel mesh for external cable protection and steel wire cores as core strength members. This strengthening and armouring is conductive and specialist advice may be needed to avoid earth loops, cross-coupling, inductive coupling or the introduction of other compromising signals and currents. Fibre optic cable with metal cable strengtheners or conductive armoured sheaths is considered *unsuitable* for secure installations.

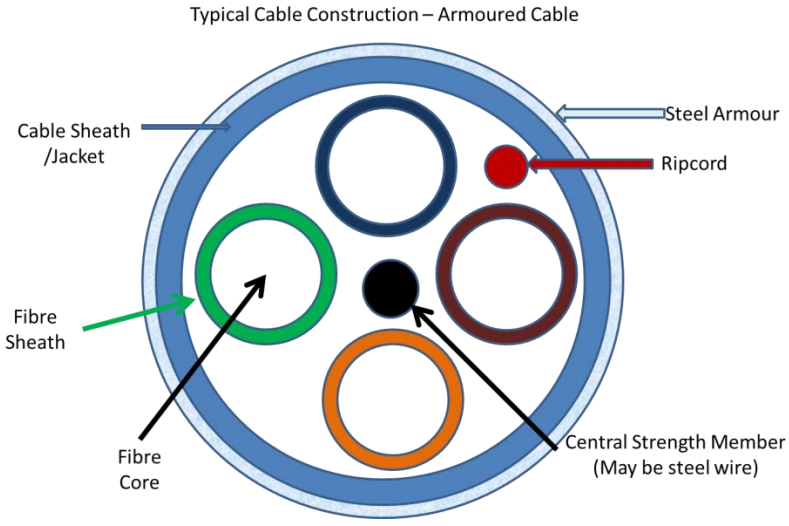


Figure 1

Backbone

10.1.18. A backbone or core is the central cabling that connects the infrastructure (servers, databases, gateways, equipment and telecommunication rooms etc.) to local areas networks, workstations and other devices, such as MFD's. Smaller networks may also be connected to the backbone.

10.1.19. A backbone can span a geographic area of any size including an office, a single building, multi-story buildings, campus, national and international infrastructure. In the context of the NZISM the term backbone generally refers to the central cabling within a building or a campus.

10.1.20. Backbones can be defined in terms of six criteria:

- transmission media;
- topology;
- security required;
- access control;
- transmission technique;
- transmission speed and capability.

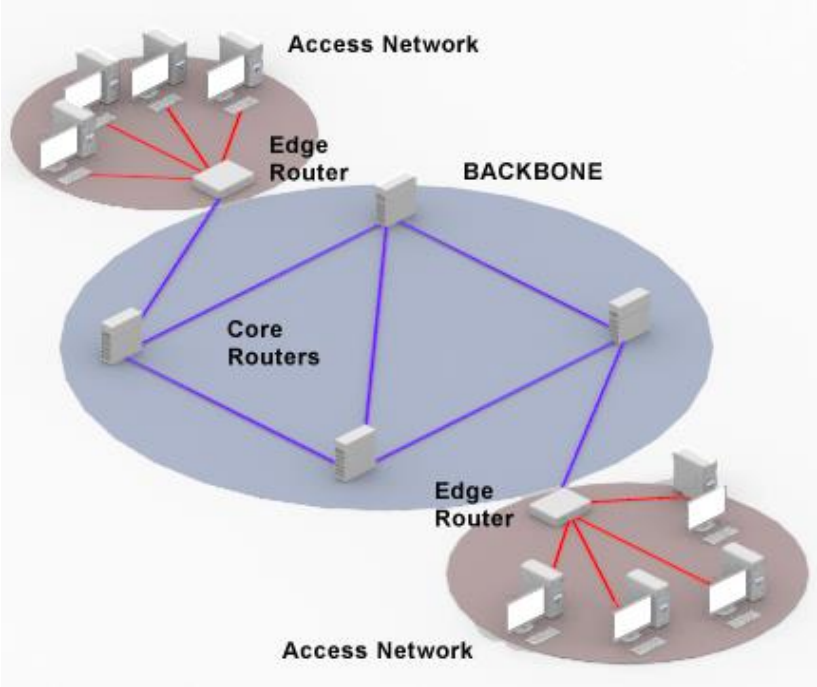


Figure 2

TOP SECRET cabling

10.1.21. For TOP SECRET cabling the cable's non-conductive protective sheath IS NOT considered to be a conduit. For TOP SECRET fibre optic cables with sub-units, the cable's outer protective sheath IS considered to be a conduit.

References

Title	Publisher	Source
NZCSS 400: New Zealand Communications Security Standard No 400 (Document classified CONFIDENTIAL)	GCSB	GCSB CONFIDENTIAL document available on application to authorised personnel
AS/NZS 3000:2007/Amdt 2:2012 - Electrical Installations (Known as the Australia/New Zealand Wiring Rules,	Standards NZ	Standards New Zealand http://www.standards.co.nz/
ANSI/TIA-568-C.3 – Optical Fiber Cabling Components	American National Standards Institute (ANSI)	http://www.ansi.org/
IEEE 802 – Local and Metropolitan Area Networks: Overview and Architecture	Institute of Electrical and Electronics Engineers (IEEE)	http://standards.ieee.org/getieee802/download/802-2014.pdf

PSR references

Reference	Title	Source
PSR Mandatory Requirements	INFOSEC5, PHYSEC3 and PHYSEC6	http://www.protectivesecurity.govt.nz
PSR content protocols and requirements sections	Security Zones and Risk Mitigation Control Measures Physical Security of ICT Equipment, Systems and Facilities	http://www.protectivesecurity.govt.nz

Rationale & Controls

10.1.22. Backbone

10.1.22.R.01. Rationale

The design of a backbone requires consideration of a number of criteria including the capacity of the cable to carry the predicted volume of data at acceptable speeds. An element of "future proofing" is also required as re-cabling to manage capacity issues can be costly. Fibre optic cable provides a convenient means of securing and "future proofing" backbones.

10.1.22.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST use fibre optic cable for backbone infrastructures and installations.

10.1.22.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use fibre optic cable for backbone infrastructures and installations.

10.1.23. Use of Fibre Optic Cable

10.1.23.R.01. Rationale

Fibre optic cable is considered more secure than copper cables and provides electrical isolation of signals. Fibre will also provide higher bandwidth and speed to allow a degree of future-proofing in network design.

10.1.23.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use fibre optic cabling.

10.1.23.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD consult with the GCSB where fibre optic cable incorporating conductive metal strengtheners or sheaths is specified.

10.1.23.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD consult with the GCSB where copper cables are specified.

10.1.23.C.04. Control: System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT use fibre optic cable incorporating conductive metal strengtheners or sheaths except where essential for cable integrity.

10.1.24. Cabling Standards

10.1.24.R.01. Rationale

Unauthorised personnel could inadvertently or deliberately access system cabling. This could result in loss or compromise of classified information. Non-detection of covert tampering or access to system cabling may result in long term unauthorised access to classified information by a hostile entity.

10.1.24.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST install all cabling in accordance with the relevant New Zealand standards as directed by AS/NZS 3000:2007 and NZCSS400.

10.1.25. Cable colours

10.1.25.R.01. Rationale

To facilitate cable management, maintenance and security cables and conduit should be colour-coded to indicate the classification of the data carried and/or classification of the compartmented data.

10.1.25.R.02. Rationale

Cables and conduit may be the distinguishing colour for their entire length or display a distinguishing label marking and colour at each end and at a maximum of two metre intervals along the cable.

10.1.25.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST comply with the cable and conduit colours specified in the following table.

Classification	Cable colour
Compartmented Information (SCI)	**Orange/Yellow/Teal or other colour**
TOP SECRET	**Red**
SECRET	**Blue**
CONFIDENTIAL	**Green**
RESTRICTED and all lower classifications	**Black**

10.1.25.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Additional colours may be used to delineate special networks and compartmented information of the same classification. These networks MUST be labelled and covered in the agency's SOPs.

10.1.26. Cable colours for foreign systems in New Zealand facilities

10.1.26.R.01. Rationale

Foreign systems should be segregated and separated from other agency systems for security purposes. Colour-coding will facilitate installation, maintenance, certification and accreditation.

10.1.26.C.01. Control: System Classification(s): TS; Compliance: MUST

The cable colour to be used for foreign systems MUST be agreed between the host agency, the foreign system owner and the Accreditation Authority.

10.1.26.C.02. Control: System Classification(s): TS; Compliance: MUST NOT

Agencies MUST NOT allow cable colours for foreign systems installed in New Zealand facilities to be the same colour as cables used for New Zealand systems.

10.1.26.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

The cable colour to be used for foreign systems SHOULD be agreed between the host agency, the foreign system owner and the Accreditation Authority.

10.1.26.C.04. Control: System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT allow cable colours for foreign systems installed in New Zealand facilities to be the same colour as cables used for New Zealand systems.

10.1.27. Cable groupings

10.1.27.R.01. Rationale

Grouping cables provides a method of sharing conduits and cable reticulation systems in the most efficient manner. These conduits and reticulation system must be inspectable and cable separations must be obvious.

10.1.27.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST contact GCSB for advice when combining the cabling of special networks.

10.1.27.C.02. Control: System Classification(s): All Classifications; Compliance: MUST NOT

Agencies MUST NOT deviate from the approved fibre cable combinations for shared conduits and reticulation systems as indicated below.

Group	Approved combination
1	UNCLASSIFIED
	RESTRICTED
2	CONFIDENTIAL
	SECRET
3	TOP SECRET
	Other Special Networks

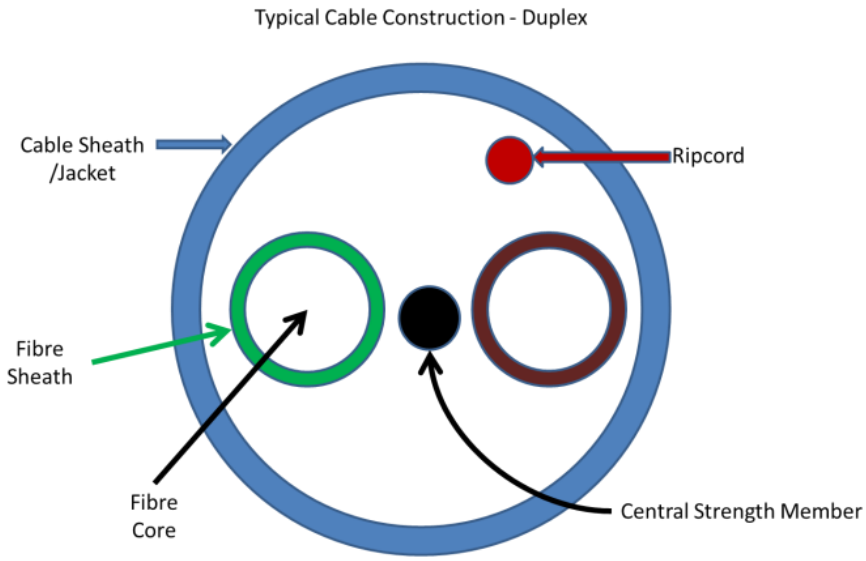
10.1.28. Fibre optic cables sharing a common conduit

10.1.28.R.01. Rationale

The use of multi-core fibre optic cables can reduce installation costs. The principles of separation and containment of cross-talk and leakage must be adhered to.

10.1.28.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

With fibre optic cables the arrangements of fibres within the cable sheath, as illustrated in Figure 3, MUST carry a single classification only.



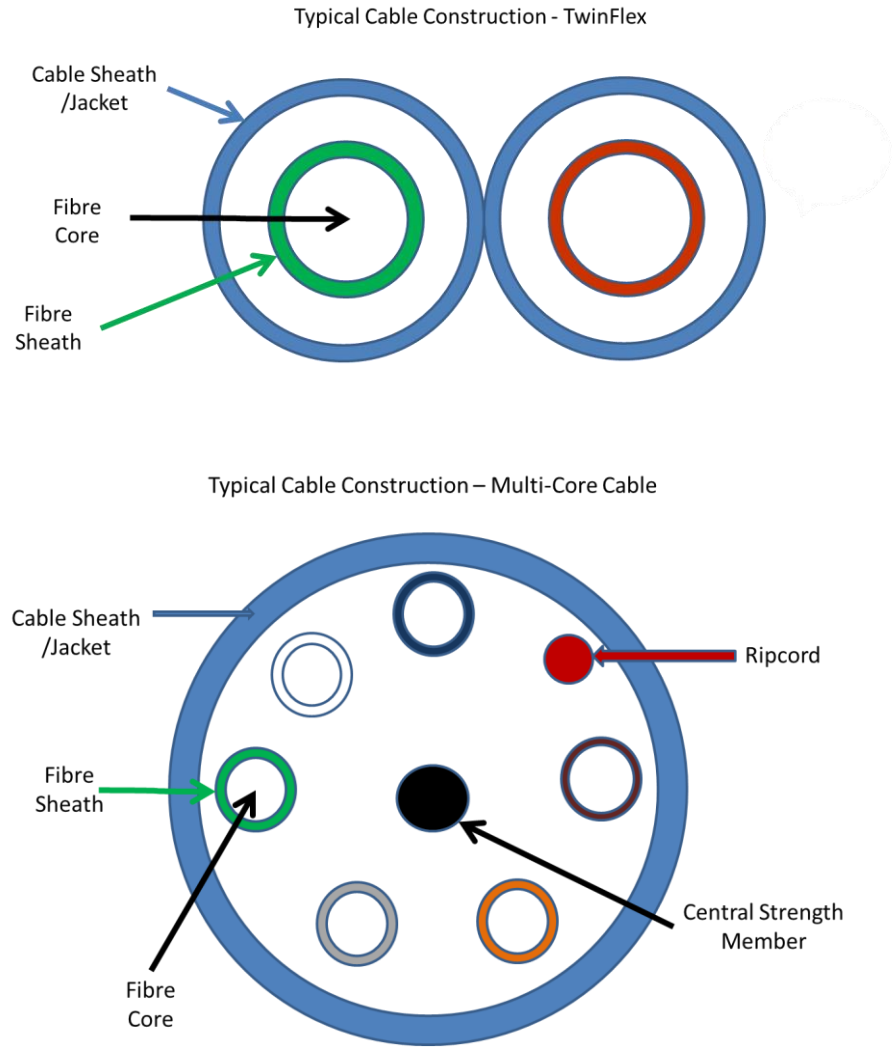


Figure 3

10.1.28.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

If a fibre optic cable contains subunits, as shown in Figure 4, each subunit MUST carry only a single classification.

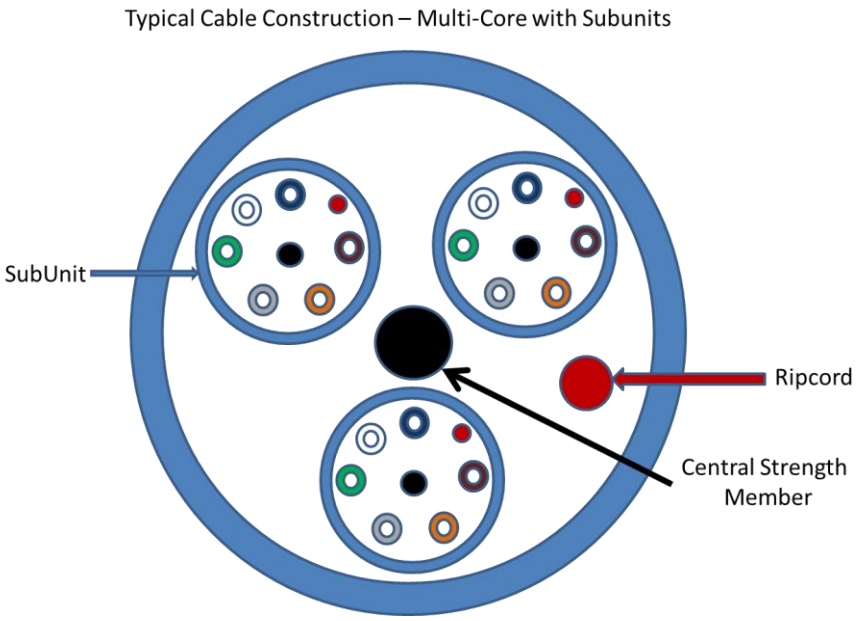


Figure 4

10.1.28.C.03. Control: System Classification(s): All Classifications; Compliance: MUST NOT

Agencies MUST NOT mix classifications up to RESTRICTED with classifications of CONFIDENTIAL and above in a single cable.

10.1.29. Audio secure areas

10.1.29.R.01. Rationale

Audio secure areas are designed to prevent audio conversation from being heard outside the walls. Penetrating an audio secure area in an unapproved manner can degrade this. Consultation with GCSB needs to be undertaken before any modifications are made to audio secure areas.

10.1.29.C.01. Control: System Classification(s): TS; Compliance: MUST

When penetrating an audio secure area, agencies MUST comply with all directions provided by GCSB.

10.1.30. Wall outlet terminations

10.1.30.R.01. Rationale

Wall outlet boxes are the preferred method of connecting cable infrastructure to workstations and other equipment. They allow the management of cabling and can utilise a variety of connector types for allocation to different classifications.

10.1.30.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Cable groups sharing a wall outlet MUST use different connectors for systems of different classifications.

10.1.30.C.02. Control: System Classification(s): TS; Compliance: MUST

In areas containing outlets for both TOP SECRET systems and systems of other classifications, agencies MUST ensure that the connectors for the TOP SECRET systems are different to those of the other systems.

10.1.30.C.03. Control: System Classification(s): C, S, TS; Compliance: MUST

Cable outlets MUST be labelled with the system classification and connector type.

10.1.30.C.04. Control: System Classification(s): All Classifications; Compliance: SHOULD

Cable outlets SHOULD be labelled with the system classification and connector type.

10.2. Cable Management for Non-Shared Government Facilities

Objective

10.2.1. Cable management systems in non-shared government facilities are implemented in a secure and easily inspectable and maintainable way.

Context

Scope

10.2.2. This section provides specific requirements for cabling installed in facilities solely occupied by a single agency. This section is to be applied in addition to common requirements for cabling as outlined in the Section 10.1 - Cable Management Fundamentals.

Applicability of controls within this section

10.2.3. The controls within this section are only applicable to communications infrastructure located within facilities in New Zealand. For deployable platforms or facilities outside of New Zealand, Emanation Security Threat Assessments (Section 10.7) of this chapter of this manual will need to be consulted.

References

Title	Publisher	Source
NZCSS 400: New Zealand Communications Security Standard No 400 (Document classified CONFIDENTIAL)	GCSB	GCSB CONFIDENTIAL document available on application to authorised personnel
AS/NZS 3000:2007/Amdt 2:2012 - Electrical Installations (Known as the Australia/New Zealand Wiring Rules,	Standards NZ	http://www.standards.co.nz

Rationale & Controls

10.2.4. Cabling Inspection

10.2.4.R.01. Rationale

Regular inspections of cable installations are necessary to detect any unauthorised or malicious tampering or cable degradation.

10.2.4.C.01. Control: System Classification(s): TS; Compliance: MUST

In TOP SECRET areas or zones, all cabling MUST be inspectable at a minimum of five-metre intervals.

10.2.4.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Cabling SHOULD be inspectable at a minimum of five-metre intervals.

10.2.5. Cables sharing a common reticulation system

10.2.5.R.01. Rationale

Laying cabling in a neat and controlled manner, observing separation requirements, allows for inspections and reduces the need for individual cable trays for each classification.

10.2.5.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Approved cable groups may share a common reticulation system but SHOULD have either a dividing partition or a visible gap between the differing cable groups or bundles.

10.2.6. Cabling in walls

10.2.6.R.01. Rationale

Cabling run correctly in walls allows for neater installations while maintaining separation and inspectability requirements.

10.2.6.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Flexible or plastic conduit SHOULD be used in walls to run cabling from cable trays to wall outlets.

10.2.7. Cabinet separation

10.2.7.R.01. Rationale

Having a definite gap between cabinets allows for ease of inspections for any unauthorised or malicious cabling or cross patching.

10.2.7.C.01. Control: System Classification(s): TS; Compliance: SHOULD

TOP SECRET cabinets SHOULD have a visible gap of at least 400mm between themselves and lower classified cabinets.

10.3. Cable Management for Shared Government Facilities

Objective

10.3.1. Cable management systems in shared government facilities are implemented in a secure and easily inspectable and maintainable way.

Context

Scope

10.3.2. This section provides specific requirements for cabling installed in facilities shared exclusively by agencies. This section is to be applied in addition to common requirements for cabling as outlined in the Section 10.1 - Cable Management Fundamentals.

Applicability of controls within this section

10.3.3. The controls within this section are applicable only to communications infrastructure located within facilities in New Zealand. For deployable platforms or facilities outside of New Zealand, Emanation Security Threat Assessments (Section 10.7) of this chapter of this manual will need to be consulted.

Rationale & Controls

10.3.4. Use of fibre optic cabling

10.3.4.R.01. Rationale

Fibre optic cabling does not produce and is not influenced by electromagnetic emanations; as such it offers the highest degree of protection from electromagnetic emanation effects especially in a shared facility where you do not have total control over other areas of the facility.

10.3.4.R.02. Rationale

It is more difficult to tap than copper cabling.

10.3.4.R.03. Rationale

Many more fibres can be run per cable diameter than wired cables thereby reducing cable infrastructure costs.

10.3.4.R.04. Rationale

Fibre cable is the best method to future proof against unforseen threats.

10.3.4.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use fibre optic cabling.

10.3.5. Cabling inspection

10.3.5.R.01. Rationale

In a shared facility it is important that cabling systems are inspected for illicit tampering and damage on a regular basis and have stricter controls than a non-shared facility.

10.3.5.C.01. Control: System Classification(s): TS; Compliance: MUST

In TOP SECRET areas, cables MUST be fully inspectable for their entire length.

10.3.5.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Cabling SHOULD be inspectable at a minimum of five-metre intervals.

10.3.6. Cables sharing a common reticulation system

10.3.6.R.01. Rationale

In a shared facility with another government agency, tighter controls may be required for sharing reticulation systems. Note also the red/black separation requirements in paragraph 10.1.5.

10.3.6.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Approved cable groups SHOULD have either a dividing partition or a visible gap between the individual cable groups. If the partition or gap exists, cable groups may share a common reticulation system.

10.3.7. Enclosed cable reticulation systems

10.3.7.R.01. Rationale

In a shared facility with another government agency, TOP SECRET cabling is enclosed in a sealed reticulation system to restrict access and control cable management.

10.3.7.C.01. Control: System Classification(s): TS; Compliance: SHOULD

The front covers of conduits, ducts and cable trays in floors, ceilings and of associated fittings that contain TOP SECRET cabling, SHOULD be clear plastic.

10.3.8. Cabling in walls

10.3.8.R.01. Rationale

In a shared facility with another government agency, cabling run correctly in walls allows for neater installations while maintaining separation and inspectability requirements. Controls are slightly more stringent than in a non-shared facility.

10.3.8.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Cabling from cable trays to wall outlets SHOULD run in flexible or plastic conduit.

10.3.9. Wall penetrations

10.3.9.R.01. Rationale

Wall penetrations by cabling, requires the integrity of the classified area to be maintained. All cabling is encased in conduit with no gaps in the wall around the conduit. This prevents any visual access to the secure area.

10.3.9.C.01. Control: System Classification(s): TS; Compliance: SHOULD

For wall penetrations that exit into a lower classified area, cabling SHOULD be encased in conduit with all gaps between the conduit and the wall filled with an appropriate sealing compound.

10.3.10. Power reticulation

10.3.10.R.01. Rationale

In a shared facility with lesser-classified systems, it is important that TOP SECRET systems have control over the power system to prevent denial of service by deliberate or accidental means.

10.3.10.C.01. Control: System Classification(s): TS; Compliance: SHOULD

TOP SECRET facilities SHOULD have a power distribution board, separately reticulated, located within the TOP SECRET area and supply UPS power to all equipment.

10.3.11. Power Filters

10.3.11.R.01. Rationale

Power filters are used to provide a filtered (clean) power supply and reduce opportunity for technical attacks.

10.3.11.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Power filters SHOULD be used to provide a filtered power supply and reduce opportunity for technical attacks.

10.3.12. Cabinet separation

10.3.12.R.01. Rationale

Having a visible gap between cabinets facilitates inspection for any unauthorised, malicious or cross patch cabling.

10.3.12.C.01. Control: System Classification(s): TS; Compliance: SHOULD

TOP SECRET cabinets SHOULD have a visible gap to separate them from lower classified cabinets.

10.4. Cable Management for Shared Non-Government Facilities

Objective

10.4.1. Cable management systems are implemented in shared non-government facilities to minimise risks to data and information.

Context

Scope

10.4.2. This section provides specific requirements for cabling installed in facilities shared by agencies and non-government organisations. This section is to be applied in addition to common requirements for cabling as outlined in Section 10.1 - Cable Management Fundamentals section.

Applicability of controls within this section

10.4.3. The controls within this section are applicable only to communications infrastructure located within facilities in New Zealand. For deployable platforms or facilities outside New Zealand, Emanation Security Threat Assessments (Section 10.7) of this chapter of this manual MUST be consulted.

Rationale & Controls

10.4.4. Use of fibre optic cabling

10.4.4.R.01. Rationale

Fibre optic cabling is essential in a shared non-government facility. Fibre optic cabling does not produce and is not influenced by electromagnetic emanations; as such it offers the highest degree of protection from electromagnetic emanation effects especially in a shared non-government facility where an agency's controls may have a limited effect outside the agency controlled area.

10.4.4.R.02. Rationale

Fibre optic cable is more difficult to tap than copper cabling and anti-tampering monitoring can be employed to detect tampering.

10.4.4.R.03. Rationale

Many more fibres can be run per cable diameter than wired cables, reducting cable infrastructure costs.

10.4.4.C.01. Control: System Classification(s): TS; Compliance: MUST

In TOP SECRET areas, agencies MUST use fibre optic cabling.

10.4.4.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use fibre optic cabling.

10.4.5. Cabling inspection

10.4.5.R.01. Rationale

In a shared non-government facility, it is imperative that cabling systems be inspectable for tampering and damage on a regular basis particularly where higher threat levels exist or where threats are unknown.

10.4.5.C.01. Control: System Classification(s): TS; Compliance: MUST

In TOP SECRET areas, cables MUST be fully inspectable for their entire length.

10.4.5.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Cabling SHOULD be inspectable at a minimum of five-metre intervals.

10.4.6. Cables sharing a common reticulation system

10.4.6.R.01. Rationale

In a shared non-government facility, tighter controls are placed on sharing reticulation systems as the threats attributable to tampering and damage are increased.

10.4.6.C.01. **Control:** System Classification(s): TS; Compliance: MUST

In TOP SECRET areas, approved cable groups can share a common reticulation system but MUST have either a dividing partition or a visible gap between the differing cable groups.

10.4.6.C.02. **Control:** System Classification(s): TS; Compliance: MUST

TOP SECRET cabling MUST run in a non-shared, enclosed reticulation system.

10.4.6.C.03. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

Approved cable groups can share a common reticulation system but SHOULD have either a dividing partition or a visible gap between the differing cable groups.

10.4.7. Enclosed cable reticulation systems

10.4.7.R.01. **Rationale**

In a shared non-government facility, TOP SECRET cabling is enclosed in a sealed reticulation system to prevent access and control cable management.

10.4.7.C.01. **Control:** System Classification(s): TS; Compliance: MUST

In TOP SECRET areas, the front covers for conduits and cable trays in floors, ceilings and of associated fittings MUST be clear plastic or be inspectable and have tamper proof seals fitted.

10.4.7.C.02. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

The front covers of conduits, ducts and cable trays in floors, ceilings and of associated fittings SHOULD be clear plastic or be inspectable and have tamper proof seals fitted.

10.4.8. Cabling in walls or party walls

10.4.8.R.01. **Rationale**

In a shared non-government facility, cabling run correctly in walls allows for neater installations facilitating separation and inspectability. Controls are more stringent than in a non-shared facility or a shared government facility.

10.4.8.R.02. **Rationale**

A party wall is a wall shared with an unclassified area where there is no control over access. In a shared non-government facility, cabling is not allowed in a party wall. An inner wall can be used to run cabling where the area is sufficient for inspection of the cabling.

10.4.8.C.01. **Control:** System Classification(s): C, S, TS; Compliance: MUST NOT

Cabling MUST NOT run in a party wall.

10.4.9. Sealing reticulation systems

10.4.9.R.01. Rationale

In a shared non-government facility, where the threats of access to cable reticulation systems is increased, GCSB endorsed anti-tamper seals are required to provide evidence of any tampering or illicit access.

10.4.9.R.02. Rationale

In a shared non-government facility, all conduit joints and wall penetrations are sealed with a visible smear of glue or sealant to prevent access to cabling.

10.4.9.C.01. Control: System Classification(s): TS; Compliance: MUST

Agencies MUST use GCSB endorsed tamper evident seals to seal all removable covers on reticulation systems, including:

- conduit inspection boxes;
- outlet and junction boxes; and
- T-pieces.

10.4.9.C.02. Control: System Classification(s): TS; Compliance: MUST

Tamper evident seals MUST be uniquely identifiable and a register kept of their unique number and location.

10.4.9.C.03. Control: System Classification(s): TS; Compliance: MUST

Conduit joints MUST be sealed with glue or sealant.

10.4.9.C.04. Control: System Classification(s): All Classifications; Compliance: SHOULD

Conduit joints SHOULD be sealed with glue or sealant.

10.4.10. Wall penetrations

10.4.10.R.01. Rationale

A cable wall penetration into a lesser-classified area requires the integrity of the classified area be maintained. All cabling is encased in conduit with no gaps in the wall around the conduit. This prevents any visual access to the secure area.

10.4.10.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Wall penetrations that exit into a lower classified area, cabling MUST be encased in conduit with all gaps between the conduit and the wall filled with an appropriate sealing compound.

10.4.11. Power reticulation

10.4.11.R.01. Rationale

In a shared non-government facility, it is important that TOP SECRET systems have control over the power system to prevent denial of service by deliberate or accidental means. The addition of a UPS is required to maintain availability of the TOP SECRET systems.

10.4.11.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Secure facilities MUST have a power distribution board located within the secure area and supply UPS power all equipment.

10.4.12. Power Filters

10.4.12.R.01. Rationale

Power filters should be used to provide filtered (clean) power and reduce opportunity for technical attacks. Consult the GCSB for technical advice.

10.4.12.C.01. Control: System Classification(s): C, S ,TS; Compliance: MUST

Power filters MUST be used to provide filtered (clean) power and reduce opportunity for technical attacks.

10.4.13. Equipment Cabinet separation

10.4.13.R.01. Rationale

A visible gap between equipment cabinets will make any cross-cabling obvious and will simplify inspections for unauthorised or compromising changes.

10.4.13.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Equipment cabinets MUST have a visible gap or non-conductive isolator between cabinets of different classifications.

10.4.13.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

There SHOULD be a visible gap or non-conductive isolator between equipment cabinets of different classifications.

10.5. Cable Labelling and Registration

Objective

10.5.1. To facilitate cable management, and identify unauthorised additions or tampering.

Context

Scope

10.5.2. This section covers information relating to the labelling of cabling infrastructure installed in secure areas.

Applicability of controls within this section

10.5.3. The controls within this section are applicable only to communications infrastructure located within facilities in New Zealand. For deployable platforms or facilities outside New Zealand, Emanation Security Threat Assessments (Section 10.7) of this chapter of this manual MUST be consulted.

Rationale & Controls

10.5.4. Conduit label specifications

10.5.4.R.01. Rationale

Conduit labelling of a specific size and colour will facilitate identifying secure conduits.

10.5.4.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST comply with the conduit label colours specified in the following table.

Classification	Cable colour
Compartmented Information (SCI)	**Orange/Yellow/Teal or other colour**
TOP SECRET	**Red**
SECRET	**Blue**
CONFIDENTIAL	**Green**
RESTRICTED and all lower classifications	**Black**

10.5.5. Installing conduit labelling

10.5.5.R.01. Rationale

Conduit labelling in public or reception areas should not draw undue attention to the level of classified processing or any other agency capability.

10.5.5.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD NOT

Conduit labels installed in public or visitor areas SHOULD NOT be labelled in such a way as to draw attention to or reveal classification of data processed or other agency capability.

10.5.6. Labelling wall outlet boxes

10.5.6.R.01. Rationale

Clear labelling of wall outlet boxes reduces the possibility of incorrectly attaching IT equipment of a lesser classification to the wrong outlet.

10.5.6.C.01. Control: System Classification(s): C, S,TS; Compliance: MUST

Wall outlet boxes MUST denote the classification, cable and outlet numbers.

10.5.6.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Wall outlet boxes SHOULD denote the classification, cable and outlet numbers.

10.5.7. Standard operating procedures

10.5.7.R.01. Rationale

Recording labelling conventions in SOPs facilitates maintenance and fault finding.

10.5.7.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

The SOPs SHOULD record the site conventions for labelling and registration.

10.5.8. Labelling cables

10.5.8.R.01. Rationale

Labelling cables with the correct socket number, equipment type, source or destination minimises the likelihood of improperly cross connecting equipment and can assist in fault finding and configuration management.

10.5.8.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST label cables at each end, with sufficient information to enable the physical identification and inspection of the cable.

10.5.8.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD label cables at each end, with sufficient information to enable the physical identification and inspection of the cable.

10.5.9. Cable register

10.5.9.R.01. Rationale

Cable registers provide a source of information that assessors can view to verify compliance.

10.5.9.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST maintain a register of cables.

10.5.9.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD maintain a register of cables.

10.5.10. Cable register contents

10.5.10.R.01. Rationale

Cable registers allow installers and assessors to trace cabling for inspection, tampering or accidental damage. It tracks all cable management changes through the life of the system.

10.5.10.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

The cable register MUST record at least the following information:

- cable identification number;
- classification;
- socket number, equipment type, source or destination site/floor plan diagram; and
- seal numbers if applicable.

10.5.10.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

The cable register SHOULD record at least the following information:

- cable identification number;
- classification;
- socket number, equipment type, source or destination site/floor plan diagram; and
- seal numbers if applicable.

10.5.11. Cable inspections

10.5.11.R.01. Rationale

Regular cable inspections, are a method of checking the cable management system against the cable register as well as detecting tampering, damage, breakages or other anomalies.

10.5.11.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD inspect cables for inconsistencies with the cable register in accordance with the frequency defined in the SecPlan.

10.6. Cable Patching

Objective

10.6.1. Communications systems are designed to prevent cross-connecting or cross-patching systems of differing classifications.

Context

Scope

10.6.2. This section covers information relating to the configuration and installation of patch panels, patch cables and fly leads associated with communications systems.

Applicability of controls within this section

10.6.3. The controls within this section are applicable only to communications infrastructure located within facilities in New Zealand. For deployable platforms or facilities outside New Zealand the Emanation Security Threat Assessments (Section 10.7) of this chapter of this manual MUST be consulted.

Exception for patch cable and fly lead connectors

10.6.4. For patch cables, the same connectors can be used for different classifications if the length of the higher classified patch cables is less than the distance between the higher classified patch panel and any patch panel of a lower classification.

Rationale & Controls

10.6.5. Terminations to patch panels

10.6.5.R.01. Rationale

Cross-connecting a system to another system of a lesser classification through a patch panel may result in a data spill. A data spill could result in the following issues:

- inadvertent or deliberate access to information and systems by non-cleared personnel; and/or
- information spilling to a system of another classification.

10.6.5.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that only approved cable groups terminate on a patch panel.

10.6.6. Patch cable and fly lead connectors

10.6.6.R.01. Rationale

Cables equipped with connectors specific to a classification will prevent inadvertent cross-connection.

10.6.6.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

In areas containing cabling for multiple classifications, agencies MUST ensure that the connectors for each classification are distinct and different to those of the other classifications.

10.6.6.C.02. Control: System Classification(s): C, S, TS; Compliance: MUST

In areas containing cabling for multiple classifications, agencies MUST document the selection of connector types for each classification.

10.6.6.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

In areas containing cabling for systems of different classifications, agencies SHOULD ensure that the connectors for each system are different to those of the other systems.

10.6.6.C.04. Control: System Classification(s): All Classifications; Compliance: SHOULD

In areas containing cabling for systems of different classifications, agencies SHOULD document the selection of connector types.

10.6.7. Physical separation of patch panels

10.6.7.R.01. Rationale

Appropriate physical separation between a TOP SECRET system and a system of a lesser classification will:

- reduce or eliminate the chances of cross patching between the systems; and
- reduce or eliminate the possibility of unauthorised personnel or personnel gaining access to TOP SECRET system elements.

10.6.7.C.01. Control: System Classification(s): C, S, TS; Compliance: SHOULD

Agencies SHOULD physically separate patch panels of different classifications by installing them in separate cabinets.

10.6.7.C.02. Control: System Classification(s): C, S, TS; Compliance: MUST

Where spatial constraints demand patch panels of different classification are located in the same cabinet, agencies MUST:

- provide a physical barrier within the cabinet to separate patch panels;
- ensure that only personnel cleared to the highest classification of the circuits in the panel have access to the cabinet; and
- obtain approval from the relevant Accreditation Authority prior to installation.

10.6.8. Fly lead installation

10.6.8.R.01. Rationale

Keeping the lengths of fly leads to a minimum prevents clutter around desks, prevents damage to fibre optic cabling and reduces the chance of cross patching and tampering. If lengths become excessive then agencies will need to treat the cabling as infrastructure and run it in conduit or fixed infrastructure such as desk partitioning.

10.6.8.C.01. Control: System Classification(s): C, S, TS; Compliance: SHOULD

Agencies SHOULD ensure that the fibre optic fly leads used to connect wall outlets to IT equipment either:

- do not exceed 5m in length; or
- if they exceed 5m in length:
  - are run in the facility's fixed infrastructure in a protective and easily inspected pathway;
  - are clearly labelled at the equipment end with the wall outlet designator; and
  - are approved by the Accreditation Authority.

10.7. Emanation Security Threat Assessments

Objective

10.7.1. In order to minimise compromising emanations or the opportunity for a technical attack, a threat assessment is used to determine appropriate countermeasures.

Context

Scope

10.7.2. This section relates to emanation security threat assessment advice and identification of appropriate countermeasures to minimise the loss of classified information through compromising emanations or a technical attack.

10.7.3. This section is applicable to:

- agencies located outside New Zealand;
- secure facilities within New Zealand; and
- mobile platforms and deployable assets that process classified information.

References

10.7.4. Information on conducting an emanation security threat assessment and additional information on cabling and separation standards, as well as the potential dangers of operating RF transmitters in proximity to classified systems, is documented in:

Title	Publisher	Source
NZCSS400 Installation Engineering	GCSB	CONFIDENTIAL document available on application to authorised personnel
NZCSI 403B TEMPEST Threat and Countermeasures Assessment	GCSB	CONFIDENTIAL document available on application to authorised personnel
NZCSI 420 **Laboratory Tempest Test Standard for Equipment in Controlled Environments**	GCSB	CONFIDENTIAL document available on application to authorised personnel

PSR references

Reference	Title	Source
PSR content protocols and requirements sections	Physical Security of ICT Equipment, Systems and Facilities	http://www.protectivesecurity.govt.nz

Rationale & Controls

10.7.5. Emanation security threat assessments within New Zealand

10.7.5.R.01. Rationale

Obtaining the current threat advice from GCSB on potential adversaries and threats and applying the appropriate countermeasures is vital in maintaining the confidentiality of classified systems from an emanation security attack.

10.7.5.R.02. Rationale

Failing to implement recommended countermeasures against an emanation security attack can lead to compromise. Having a good cable infrastructure and installation methodology will provide a strong backbone that will not need updating if the threat increases. Infrastructure is very expensive and time consuming to retro-fit.

10.7.5.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Agencies designing and installing systems with RF transmitters within or co-located with their facility MUST:

- contact GCSB for guidance on conducting an emanation security threat assessment; and
- install cabling and equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment.

10.7.5.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies designing and installing systems with RF transmitters that co-locate with systems of a classification CONFIDENTIAL and above MUST:

- contact GCSB for guidance on conducting an emanation security threat assessment; and
- install cabling and equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment.

10.7.6. Emanation security threat assessment outside New Zealand

10.7.6.R.01. Rationale

Fixed sites and deployed military platforms are more vulnerable to emanation security attack and require a current threat assessment and countermeasure implementation. Failing to implement recommended countermeasures and standard operating procedures to reduce threats could result in the platform emanating compromising signals which, if intercepted and analysed, could lead to platform compromise with serious consequences.

10.7.6.C.01. **Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies deploying systems overseas in temporary, mobile or fixed locations MUST:

- contact GCSB for assistance with conducting an emanation security threat assessment; and
- install cabling and equipment in accordance with this manual plus any specific installation criteria derived from the emanation security threat assessment.

10.7.6.C.02. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies deploying systems overseas SHOULD:

- contact GCSB for assistance with conducting an emanation security threat advice; and
- install cabling and equipment in accordance with this document plus any specific installation criteria derived from the emanation security threat assessment.

10.7.7. Early identification of emanation security issues

10.7.7.R.01. **Rationale**

The identification of emanation security controls that need to be implemented for a system at an early stage in the project lifecycle. This can significantly affect project costs. Costs are invariably greater where changes are necessary once the system had been designed or has been implemented.

10.7.7.C.01. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD conduct an emanation security threat assessment as early as possible in project lifecycles.

10.7.8. IT equipment in SECURE areas

10.7.8.R.01. **Rationale**

All equipment must conform to applicable industry and government standards, including NZCSI 420; Laboratory Tempest Test Standard for Equipment in Controlled Environments. Not all equipment within a secure facility in New Zealand requires testing against TEMPEST standards.

10.7.8.C.01. **Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST ensure that IT equipment within secure areas meet industry and government standards relating to electromagnetic interference/electromagnetic compatibility.

11. Communications Systems and Devices

11.1. Radio Frequency and Infrared Devices

Objective

11.1.1. To maintain the integrity of secure areas, only approved radio frequency (RF) and infrared devices (IR) are brought into secure areas.

Context

Scope

11.1.2. This section covers information relating to the use of RF and infrared devices in secure areas. Information on the use of RF devices outside secure areas can be found in Chapter 21 - Working Off-Site.

11.1.3. RF devices include any transmitter on any frequency, including mobile phones, cordless phones, Bluetooth, Wi-Fi, RFID and other similar devices.

Exemptions for the use of infrared and laser devices

11.1.4. An infrared device and laser device can be used in a secure area provided it does not have the potential to communicate classified information.

Exemptions for the use of RF devices

11.1.5. The following devices, *at the discretion of the Accreditation Authority*, can be exempted from the controls associated with RF transmitters:

- pagers that can only receive messages;
- garage door openers;
- car lock/alarm keypads;
- medical and exercise equipment that uses RF to communicate between sub-components;
- access control sensors; and
- laser pointers.

References

Title	Publisher	Source
NIST 800-121 Guide to Bluetooth Security	NIST	http://csrc.nist.gov/publications/nistpubs/800-121-rev1/sp800-121_rev1.pdf

PSR references

Reference	Title	Source
PSR content protocols and requirements sections	Security Zones and Risk Mitigation Control Measures Physical Security of ICT Equipment, Systems and Facilities Communications Security Mobile Electronic Device Risks and Mitigation	http://www.protectivesecurity.govt.nz

Rationale & Controls

11.1.6. Pointing devices

11.1.6.R.01. Rationale

Wireless RF pointing devices can pose an emanation security risk. They are not to be used in secure areas unless within a RF screened building.

11.1.6.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST NOT

Wireless RF pointing devices MUST NOT be used in secure areas unless used within a RF screened building or RF mitigations are implemented.

11.1.7. Infrared keyboards

11.1.7.R.01. Rationale

When using infrared keyboards with CONFIDENTIAL or SECRET systems, drawn opaque curtains are an acceptable method of protecting windows and managing line of sight and reflected transmissions.

11.1.7.R.02. Rationale

When using infrared keyboards with a TOP SECRET system, windows with curtains that can be opened are NOT acceptable as a method of permanently blocking infrared transmissions. While infrared transmissions are generally designed for short range (5 to 10 metres) manufacturing and design variations and some environmental conditions can amplify and reflect infrared over much greater distances.

11.1.7.C.01. Control: System Classification(s): C, S; Compliance: MUST NOT

Agencies using infrared keyboards MUST NOT allow:

- line of sight and reflected communications travelling into an unsecure area;
- multiple infrared keyboards at different classifications in the same area;
- other infrared devices to be brought into line of sight of the keyboard or its receiving device/port; and
- infrared keyboards to be operated in areas with unprotected windows.

11.1.7.C.02. Control: System Classification(s): TS; Compliance: MUST NOT

Agencies using infrared keyboards MUST NOT allow:

- line of sight and reflected communications travelling into an unsecure area;
- multiple infrared keyboards at different classifications in the same area;
- other infrared devices within the same area; and
- infrared keyboards in areas with windows that have not had a permanent method of blocking infrared transmissions applied to them.

11.1.7.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies using infrared keyboards SHOULD ensure that infrared ports are positioned to prevent line of sight and reflected communications travelling into an unsecure area.

11.1.8. Bluetooth and wireless keyboards

11.1.8.R.01. Rationale

As the Bluetooth protocol provides little security and wireless keyboards often provide no security, they cannot be relied upon for the protection of classified information. As with infrared transmissions Bluetooth transmissions can reach considerable distances.

11.1.8.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST complete a technical evaluation of the secure area before the use of Bluetooth keyboards or other Bluetooth devices are permitted.

11.1.8.C.02. Control: System Classification(s): C, S, TS; Compliance: MUST NOT

Agencies using Bluetooth keyboards or other Bluetooth devices MUST NOT allow:

- line of sight and reflected communications travelling into an unsecure area;
- multiple keyboards or other devices at different classifications in the same area;
- other Bluetooth infrared devices to be brought into range of the keyboard or its receiving device/port; and
- Bluetooth keyboards or other devices to be operated in areas with unprotected windows.

11.1.8.C.03. Control: System Classification(s): C, S, TS; Compliance: MUST NOT

Agencies MUST NOT use Bluetooth or wireless keyboards unless within a RF screened building.

11.1.9. RF devices in secure areas

11.1.9.R.01. Rationale

RF devices pose security threat as they are capable of picking up and transmitting classified background conversations. Furthermore, many RF devices can connect to IT equipment and act as unauthorised data storage devices or bridge "air gaps".

11.1.9.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST prevent RF devices from being brought into secure areas unless authorised by the Accreditation Authority.

11.1.9.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD prevent RF devices from being brought into secure areas unless authorised by the Accreditation Authority.

11.1.10. Detecting RF devices in secure areas

11.1.10.R.01. Rationale

As RF devices are prohibited in secure areas, agencies should deploy technical measures to detect and respond to the unauthorised use of such devices.

11.1.10.C.01. Control: System Classification(s): C, S, TS; Compliance: SHOULD

Agencies SHOULD deploy measures to detect and respond to active RF devices within secure areas.

11.1.11. RF controls

11.1.11.R.01. Rationale

Minimising the output power of wireless devices and using RF shielding on facilities will assist in limiting the wireless communications to areas under the control of the agency.

11.1.11.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD limit the effective range of communications outside the agency's area of control by:

- minimising the output power level of wireless devices;
- RF shielding; and
- Physical layout and separation.

11.2. Fax Machines, Multifunction Devices and Network Printers

Objective

11.2.1. Fax machines, multifunction devices (MFD's) and network printers are used in a secure manner.

Context

Scope

11.2.2. This section covers information relating to fax machines, MFDs and network printers connected to either the ISDN, PSTN, HGCE or other networks. Further information on MFDs communicating via network gateways can be found in Section 20.2 - Data Import and Export.

Rationale & Controls

11.2.3. Fax machine, MFD and network printer usage policy

11.2.3.R.01. Rationale

Fax machines, MFDs and network printers are capable of communicating classified information, and are a potential source of information security incidents. It is therefore essential that agencies develop a policy governing their use.

11.2.3.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST develop a policy governing the use of fax machines, MFDs, and network printers.

11.2.4. Sending fax messages

11.2.4.R.01. Rationale

Once a fax machine or MFD has been connected to cryptographic equipment and used to send a classified fax message it can pose risks if subsequently connected directly to unsecured telecommunications infrastructure or the public switched telephone network (PSTN). For example, if a fax machine fails to send a classified fax message the device will continue attempting to send the fax message even if it has been disconnected from the cryptographic device and connected directly to the public switched telephone network. In such cases the fax machine could then send the classified fax message in the clear causing an information security incident.

11.2.4.R.02. Rationale

Non-encrypted communications may be exposed in transmission and, if incorrectly addressed or an incorrect recipient number is entered, may cause a data breach.

11.2.4.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Agencies sending classified fax messages MUST ensure that the fax message is encrypted to an appropriate level when communicated over unsecured telecommunications infrastructure or the public switched telephone network.

11.2.4.C.02. Control: System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST have separate fax machines or MFDs for sending classified fax messages and messages classified RESTRICTED and below.

11.2.5. Sending fax messages using HGCE

11.2.5.R.01. Rationale

The establishment and use of appropriate procedures for sending a classified fax message will ensure that it is sent securely to the correct recipient.

11.2.5.R.02. Rationale

Using the correct memory erase procedure will prevent a classified fax message being communicated in the clear.

11.2.5.R.03. Rationale

Implementing the correct procedure for establishing a secure call will prevent sending a classified fax message in the clear.

11.2.5.R.04. Rationale

Overseeing the receipt and transmission of fax messages, clearing equipment memory after use and then powering off the equipment will prevent unauthorised access to this information.

11.2.5.R.05. Rationale

Ensuring fax machines and MFDs are not connected to unsecured phone lines will prevent accidentally sending classified messages stored in memory

11.2.5.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Agencies intending to use fax machines or MFDs to send classified information MUST comply with additional requirements. Contact the GCSB for further details.

11.2.6. Receiving fax messages

11.2.6.R.01. Rationale

Whilst the communications path between fax machines and MFDs may be appropriately protected, personnel need to remain cognisant of the need-to-know of the information that is being communicated. As such it is important that fax messages are collected from the receiving fax machine or MFD as soon as possible. Furthermore, if an expected fax message is not received it may indicate that there was a problem with the original transmission or the fax message has been taken by an unauthorised person.

11.2.6.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

The sender of a fax message SHOULD make arrangements for the receiver to:

- collect the fax message as soon as possible after it is received; and
- notify the sender immediately if the fax message does not arrive when expected.

11.2.7. Connecting MFDs to telephone networks

11.2.7.R.01. Rationale

When a MFD is connected to a computer network and a telephone network the device can act as a bridge between the networks. As such the telephone network needs to be accredited to the same classification as the computer network the MFD is connected to.

11.2.7.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST NOT

Agencies MUST NOT enable a direct connection from a MFD to a telephone network unless the telephone network is accredited to at least the same classification as the computer network to which the device is connected.

11.2.7.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT enable a direct connection from a MFD to a telephone network unless the telephone network is accredited to at least the same classification as the computer network to which the device is connected.

11.2.8. Connecting MFDs to computer networks

11.2.8.R.01. Rationale

As network connected MFDs are considered to be devices that reside on a computer network they need to be able to process the same classification of information that the network is capable of processing.

11.2.8.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Where MFDs connected to computer networks have the ability to communicate via a gateway to another network, agencies MUST ensure that:

- each MFD applies user identification, authentication and audit functions for all classified information communicated by that device;
- these mechanisms are of similar strength to those specified for workstations on that network; and
- each gateway can identify and filter the classified information in accordance with the requirements for the export of data through a gateway.

11.2.9. Copying documents on MFDs

10.2.9.R.01. Rationale

As networked MFDs are capable of sending scanned or copied documents across a connected network, personnel need to be aware that if they scan or copy documents at a classification higher than that of the network the device is connected to they could be causing a data spill onto the connected network.

11.2.9.C.01. Control: System Classification(s): All Classifications; Compliance: MUST NOT

Agencies MUST NOT permit MFDs connected to computer networks to be used to copy classified documents above the classification of the connected network.

11.2.10. Observing fax machine and MFD use

11.2.10.R.01. Rationale

Placing fax machines and MFDs in public areas can assist in reducing the likelihood that any suspicious use of fax machines and MFDs by personnel will go unnoticed.

11.2.10.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that fax machines and MFDs are located in an area where their use can be observed.

11.2.11. Servicing and Maintenance

11.2.11.R.01. Rationale

Network and MFD printers invariably use hard disk drives, flash drives or other reusable storage which can contain copies of classified information. Any maintenance or servicing should be conducted under supervision or by cleared personnel.

11.2.11.R.02. Rationale

Copiers and laser printers may use electrostatic drums as part of the reproduction and printing process. These drums can retain a “memory” of recent documents which can be recovered. Any storage devices or drums replaced during maintenance should follow the prescribed media disposal and destruction processes (See Chapter 13 – Decommissioning and Disposal).

11.2.11.R.03. Rationale

Toner cartridges and other components may incorporate a memory chip, often used to track pages numbers and estimate print capacity. These chips have read/write capability and may pose a risk to classified systems. Once chips have been removed, the toner cartridges themselves may be disposed of through supplier recycling or other approved disposal channels.

11.2.11.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Any maintenance or servicing MUST be conducted under supervision or by cleared personnel.

11.2.11.C.02. Control: System Classification(s): C, S, TS; Compliance: MUST

Any storage devices, drums or cartridges with memory chips removed during maintenance or servicing MUST be disposed of following the processes prescribed in Chapter 13 - Decommissioning and Disposal.

11.2.11.C.03. Control: System Classification(s): C, S, TS; Compliance: MUST

Toner cartridges MUST have the memory chip removed *before* the cartridge is recycled or otherwise disposed of. The memory chip MUST be disposed of following the processes prescribed in Chapter 13 - Decommissioning and Disposal.

11.2.11.C.04. Control: System Classification(s): All Classifications; Compliance: SHOULD

Any maintenance or servicing SHOULD be conducted under supervision or by cleared personnel.

11.2.11.C.05. Control: System Classification(s): All Classifications; Compliance: SHOULD

Any storage devices, drums or cartridges with memory chips removed during maintenance or servicing SHOULD be disposed of following the processes prescribed in Chapter 13 - Decommissioning and Disposal.

11.2.12. USB Devices

11.2.12.R.01. Rationale

MFDs may also be equipped with USB ports for maintenance and software updates. It is possible to copy data from installed storage devices to USB devices. Any use of USB capabilities must be carefully managed.

11.2.12.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

The use of any USB capability MUST be conducted under supervision or by cleared personnel.

11.2.12.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

The use of any USB capability SHOULD be conducted under supervision or by cleared personnel.

11.2.13. Decommissioning and Disposal

11.2.13.R.01. Rationale

The use of storage media and the characteristics of electrostatic drums allow the recovery of information from such devices and components. To protect the information, prescribed disposal procedures should be followed.

11.2.13.R.02. Rationale

The use of storage media and the characteristics of electrostatic drums allow the recovery of information from such devices and components. To protect the information, prescribed disposal procedures should be followed.

11.2.13.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Any storage devices, drums, cartridge memory chips or other components that may contain data or copies of documents MUST be disposed of following the processes prescribed in Chapter 13 - Decommissioning and Disposal.

11.2.13.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Any storage devices, drums, cartridge memory chips or other components that may contain data or copies of documents SHOULD be disposed of following the processes prescribed in Chapter 13 - Decommissioning and Disposal.

11.3. Telephones and Telephone Systems

Objective

11.3.1. Telephone systems are prevented from communicating unauthorised classified information.

Context

Scope

11.3.2. This section covers information relating to the secure use of fixed, including cordless, telephones, as well as the systems they use to communicate information.

11.3.3. Information regarding Voice over Internet Protocol (VoIP) and encryption of data in transit is covered in Section 18.3 – Video & Telephony Conferencing and Internet Protocol Telephony and Section 17.1 - Cryptographic Fundamentals.

11.3.4. It MUST be noted that VOIP and cellular phones have some of the same vulnerabilities as wired and cordless phones.

Rationale & Controls

11.3.5. Telephones and telephone systems usage policy

11.3.5.R.01. Rationale

All unsecure telephone networks are subject to interception. The level of expertise needed to do this varies greatly. Accidentally or maliciously revealing classified information over a public telephone networks can lead to interception.

11.3.5.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST develop a policy governing the use of telephones and telephone systems.

11.3.6. Personnel awareness

11.3.6.R.01. Rationale

There is a high risk of unintended disclosure of classified information when using telephones. It is important that personnel are made aware of what levels of classified information they discuss on particular telephone systems as well as the audio security risk associated with the use of telephones.

11.3.6.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST advise personnel of the maximum permitted classification for conversations using both internal and external telephone connections.

11.3.6.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD advise personnel of the audio security risk posed by using telephones in areas where classified conversations can occur.

11.3.7. Visual indication

11.3.7.R.01. Rationale

When single telephone systems are approved to hold conversations at different classifications, alerting the user to the classification level they can speak at when using their phone will assist in the reducing the risk of unintended disclosure of classified information.

11.3.7.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Agencies permitting different levels of conversation for different types of connections MUST use telephones that give a visual indication of the classification of the connection made.

11.3.8. Use of telephone systems

11.3.8.R.01. Rationale

When classified conversations are to be held using telephone systems, the conversation needs to be appropriately protected through the use of encryption measures.

11.3.8.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Agencies intending to use telephone systems for the transmission of classified information MUST ensure that:

- the system has been accredited for the purpose; and
- all classified traffic that passes over external systems is appropriately encrypted.

11.3.9. Cordless telephones

11.3.9.R.01. Rationale

Cordless telephones have little or no effective transmission security, therefore should not be used for classified or sensitive communications. They also operate in an unlicensed part of the radio spectrum used for a wide range of other devices.

11.3.9.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST NOT

Agencies MUST NOT use cordless telephones for classified conversations.

11.3.9.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT use cordless telephones for classified or sensitive conversations.

11.3.10. Cordless telephones with secure telephony devices

11.3.10.R.01. Rationale

As the data between cordless handsets and base stations is not secure, cordless telephones MUST NOT be used for classified communications even if the device is connected to a secure telephony device.

11.3.10.C.01. Control: System Classification(s): All Classifications; Compliance: MUST NOT

Agencies MUST NOT use cordless telephones in conjunction with secure telephony devices.

11.3.11. Speakerphones

11.3.11.R.01. Rationale

Speakerphones are designed to pick up and transmit conversations in the vicinity of the device they should not be used in secure areas as the audio security risk is extremely high.

11.3.11.R.02. Rationale

If the agency is able to reduce the audio security risk through the use of appropriate countermeasures then an exception may be approved by the Accreditation Authority.

11.3.11.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

If a speakerphone is to be used on a secure telephone system within a secure area, agencies MUST apply the following controls:

- it is located in a room rated as audio secure;
- the room is audio secure during any conversations;
- only cleared personnel involved in discussions are present in the room; and
- ensure approval for this exception is granted by the Accreditation Authority.

11.3.12. Off-hook audio protection

11.3.12.R.01. Rationale

Providing off-hook security minimises the chance of accidental classified conversation being coupled into handsets and speakerphones. Limiting the time an active microphone is open limits this threat.

11.3.12.R.02. Rationale

Simply providing an off-hook audio protection feature is not, in itself, sufficient. To ensure that the protection feature is used appropriately personnel will need to be made aware of the protection feature and trained in its proper use.

11.3.12.R.03. Rationale

Many new digital desk phones control these functions through software, rather than a mechanical switch.

11.3.12.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST ensure that off-hook audio protection features are used on all telephones that are not accredited for the transmission of classified information in areas where such information could be discussed.

11.3.12.C.02. Control: System Classification(s): C, S, TS; Compliance: SHOULD

Agencies SHOULD use push-to-talk handsets to meet the requirement for off-hook audio protection.

11.3.12.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that off-hook audio protection features are used on all telephones that are not accredited for the transmission of classified information in areas where such information could be discussed.

11.3.13. Electronic Records Retention and Voicemail

11.3.13.R.01. Rationale

Voicemail and other messages and communications may fall within the legal definition of electronic records. If so retention and archive requirements are prescribed.

11.3.13.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST remove unused voice mailboxes.

11.3.13.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST expire and archive or delete voicemail messages after the retention period determined by the agency's electronic records retention policy.

11.3.13.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD develop and implement a policy to manage the retention and disposal of such electronic records, including voicemail, email and other electronic records.

11.4. Mobile Telephony

Objective

11.4.1. Mobile telephone systems and devices are prevented from communicating unauthorised classified information.

Context

Scope

11.4.2. This section covers information relating to the secure use of mobile telephones, tablets and other mobile, voice communication capable devices, as well as the systems they use to communicate information.

11.4.3. Mobile devices use RF in various parts of the spectrum to communicate including Wi-Fi, cellular, satellite, RFID, and NFC frequencies. All such mobile devices are considered to be transmitters.

11.4.4. Mobile devices with cellular capability will regularly "poll" for the strongest signal and base or relay station. Monitoring such activity can be used for later interception of transmissions.

11.4.5. Information regarding Voice over Internet Protocol (VoIP) and encryption of data in transit is covered in Section 18.3 – Video & Telephony Conferencing and Internet Protocol Telephony and Section 17.1 - Cryptographic Fundamentals.

11.4.6. It is important to note that VoIP phones have some of the same vulnerabilities as the mobile devices discussed in this section.

11.4.7. Mobile devices can be equipped with a variety of capabilities including internet connectivity, cameras, speakerphones, recording and remote control. Such devices are also susceptible to Internet malware and exploits. All risks related to the use of the Internet will apply to mobile devices with 3G/4G capability.

PSR references

Reference	Title	Source
PSR Mandatory Requirements	INFOSEC1	http://www.protectivesecurity.govt.nz

Rationale & Controls

11.4.8. Mobile device usage policy

11.4.8.R.01. Rationale

All mobile devices are subject to interception. The required level of expertise needed varies greatly. Accidentally or maliciously revealing classified information over mobile devices can be intercepted leading to a security breach.

11.4.8.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST develop a policy governing the use of mobile devices.

11.4.9. Personnel awareness

11.4.9.R.01. Rationale

There is a high risk of unintended disclosure of classified information when using mobile devices. It is important that personnel are aware of what levels of classified information they discuss as well as the wide range of security risks associated with the use of mobile devices.

11.4.9.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST advise personnel of the maximum permitted classification for conversations using both internal and external mobile devices.

11.4.9.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD advise personnel of all known security risks posed by using mobile devices in areas where classified conversations can occur.

11.4.10. Use of mobile devices

11.4.10.R.01. Rationale

When classified conversations are to be held using mobile devices the conversation needs to be appropriately protected through the use of encryption measures and a secure network.

11.4.10.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Agencies intending to use mobile devices for the transmission of classified information MUST ensure that:

- the network has been certified and accredited for the purpose;
- all classified traffic that passes over mobile devices is appropriately encrypted; and
- users are aware of the area, surroundings, potential for overhearing and potential for oversight when using the device.

11.4.11. Mobile Device Physical Security

11.4.11.R.01. Rationale

Mobile devices are invariably software controlled and are subject to malware or other means of compromise. No “off-hook” or “power off” security can be effectively provided, creating vulnerabilities for secure areas. Secure areas are defined in Chapter 1 at 1.1.33.

11.4.11.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Mobile devices MUST be prevented from entering secure areas.

11.4.11.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD provide a storage area or lockers where mobile devices can be stored before personnel enter secure or protected areas.

11.5. Personal Wearable Devices

Objective

11.5.1. Wearable devices are prevented from unauthorised communication or from compromising secure areas.

Context

Scope

11.5.2. This section covers information relating to the use of personal wearable devices, fitness devices, smart watches, devices embedding in clothing and similar wearable devices.

11.5.3. These devices can use RF in various parts of the spectrum to communicate including Wi-Fi, cellular, satellite, RFID, NFC and Bluetooth frequencies as well as providing data storage capability, audio and video recording and USB connectivity. All such wearable or mobile devices are considered to be transmitters.

11.5.4. Personal wearable devices can be equipped with a variety of capabilities including smart phone pairing, internet connectivity, cameras, speakerphones, audio and video recording and remote control. Some devices (for example Narrative and Autographer) will automatically take snapshots at intervals during the day. In some cases the snapshots are geotagged.

11.5.5. Such devices are also susceptible to Internet malware and exploits. All risks related to the use of the Internet will apply to these devices.

11.5.6. Merely disabling the capabilities described above is not a sufficient mitigation and is not acceptable, posing a high risk of compromise, whether intentional or accidental. The device MUST NOT have such capabilities installed if the device is to enter a secure area.

11.5.7. There is a wide variety of devices now available with upgrades and new models appearing frequently. There are many hundreds of models with a variety of custom operating systems and programmes and other applications. Some industry surveys and predications are forecasting explosive growth in the use of wearable devices, reaching over 100 million devices by 2020. Checking the capabilities and vulnerabilities of each device and subsequent security testing or validation will be an onerous task for agencies and may be infeasible.

Key Risk Areas

11.5.8. Personal wearable devices are not only about the technological aspects, the human factor is equally important. Users often forget about personal information security and their own safety, which enables social engineering attacks on the devices. The main protective measure for users is awareness, but even the *trust-but-verify* rule is not completely reliable in this situation. Accordingly, the information gathered by wearable devices should be appropriately secured to maintain privacy and personal security.

11.5.9. There are four important risk groups to be considered when managing personal wearable devices:

1. Data leaks and breaches;
2. Network security compromises;
3. Personally Identifiable Information (PII) leaks; and
4. Privacy violations.

Personally Identifiable Information (PII)

11.5.10. In most cases, the protection of PII will be the responsibility of the individual. In cases where the use of devices is permitted under a medical exemption, agencies MAY be required to ensure that devices that collect and store data comply with relevant regulation and guidance, such as the Privacy Act and the HIPAA.

PSR references

Reference	Title	Source
PSR Mandatory Requirements	INFOSEC1	http://www.protectivesecurity.govt.nz

References

References	Publisher	Source
ITL bulletin for April 2010 - Guide to protecting personally identifiable information	NIST	http://csrc.nist.gov/publications/nistbul/april-2010_guide-protecting-pii.pdf
NIST Special Publication 800-122 **Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) - Recommendations of the National Institute of Standards and Technology**	NIST	http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf
Privacy Act 1993 (the Privacy Act)		Office of The Privacy Commissioner http://www.privacy.org.nz http://www.legislation.govt.nz/
The Health Insurance Portability and Accountability Act of 1996 (USA)	US Congress	https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm http://www.hhs.gov/hipaa
Health Information Technology for Economic and Clinical Health Act (HITECH Act) (USA)	US Congress	https://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf http://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html
Technology, Media and Telecommunications Predictions, 2014	Deloitte	http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/gx-tmt-predictions-2014-interactive.pdf
Technology, Media and Telecommunications Predictions, 2015	Deloitte	http://www2.deloitte.com/au/en/pages/technology-media-and-telecommunications/articles/tmt-predictions.html
Study: Wearable Technology & Preventative Healthcare	Technology Advice Research	http://technologyadvice.com
Security Analysis of Wearable Fitness Devices (Fitbit)	Massachusetts Institute of Technology	https://courses.csail.mit.edu/6.857/2014/files/17-cyrbritt-webbhorn-specter-dmiao-hacking-fitbit.pdf
Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device	School of Computing and Information Sciences, Florida International University	https://arxiv.org/pdf/1304.5672.pdf
Survey of Security and Privacy Issues of Internet of Things		http://arxiv.org/ftp/arxiv/papers/1501/1501.02211.pdf

Rationale & Controls

11.5.11. Personal Wearable Device usage policy

11.5.11.R.01. Rationale

Any device that uses part of the RF spectrum to communicate is subject to interception. The required level of expertise to conduct intercepts needed varies greatly. Other capabilities of Personal Wearable Devices can be used for malicious purposes, including the theft of classified information and revealing the identities of personnel. Accidentally or maliciously revealing classified information through Personal Wearable Devices can lead to a security breach.

11.5.11.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST develop a policy governing the use of personal wearable devices, including fitness devices.

11.5.12. Personnel awareness

11.5.12.R.01. Rationale

There is a high risk of unintended disclosure of classified information when using personal wearable devices. It is important that personnel are aware of the level of classified information they discuss, the environment in which they are operating as well as the wide range of security risks associated with the use of mobile and personal wearable devices.

11.5.12.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST advise personnel of the maximum permitted classification for conversations where any personal wearable or mobile device may be present.

11.5.12.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD advise personnel of all known security risks posed by using personal wearable devices in secure areas or other areas where classified conversations can occur.

11.5.13. Mobile Device Physical Security

11.5.13.R.01. Rationale

Personal wearable devices are invariably software controlled and can be infected with malware or other means of compromise. No “off-hook” or “power off” security can be effectively provided, creating vulnerabilities for secure areas. Secure areas are defined in Chapter 1 at 1.1.33.

11.5.13.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST NOT

Personal wearable devices MUST NOT be allowed to enter secure areas.

11.5.13.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD provide a storage area or lockers where personal wearable devices can be stored before personnel enter secure or protected areas.

11.5.14. Medical Exemptions

11.5.14.R.01. Rationale

In some isolated cases personal wearable devices are necessary for the medical well-being of the individual. In such cases personal wearable devices MAY be permitted with the written authority of the Agency's Accreditation Authority. Such devices MUST NOT have any of the following capabilities:

- Camera;
- Microphone;
- Voice/video/still photograph recording;
- Cellular, Wi-Fi or other RF.

Merely disabling such capabilities is not acceptable. The device MUST NOT have such capabilities installed. Permitted device capabilities are:

- Accelerometer;
- Altimeter;
- Gyroscope;
- Heart Activity monitor;
- Vibration feature for the personal notification purposes.

11.5.14.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST NOT

Any personal wearable devices approved on medical grounds MUST NOT have any of the following capabilities:

- Camera;
- Microphone;
- Voice/video/still photograph recording;
- Cellular, Wi-Fi or other RF means of transmission.

11.5.14.C.02. Control: System Classification(s): C, S, TS; Compliance: MUST

Where personal wearable devices are exempted on medical grounds and used in secure areas agencies MUST ensure that:

- the agency networks in secure areas have been certified and accredited for the purpose; and
- users are aware of the area, surroundings, potential for overhearing and potential for oversight.

11.5.14.C.03. Control: System Classification(s): All Classifications; Compliance: MUST

Where the use of personal wearable devices is permitted on medical grounds and used within a corporate or agency environment, agencies MUST ensure any relevant legislation and regulation pertaining to the protection of Personally Identifiable Information (PII) is properly managed and protected.

11.6. Radio Frequency Identification Devices

Objective

11.6.1. To ensure Radio Frequency Identification (RFID) devices are used safely and securely in order to protect privacy, prevent unauthorised access and to prevent the compromise of secure spaces.

Context

Scope

11.6.2. This section provides information relating to the risks, security and secure use of RFID devices. Access Control Systems incorporating RFID or smart cards are discussed in more detail in Section 11.7.

Background

11.6.3. This section contains a short description of the history, formats, operating frequencies, risks, controls and countermeasures related to the use of RFID.

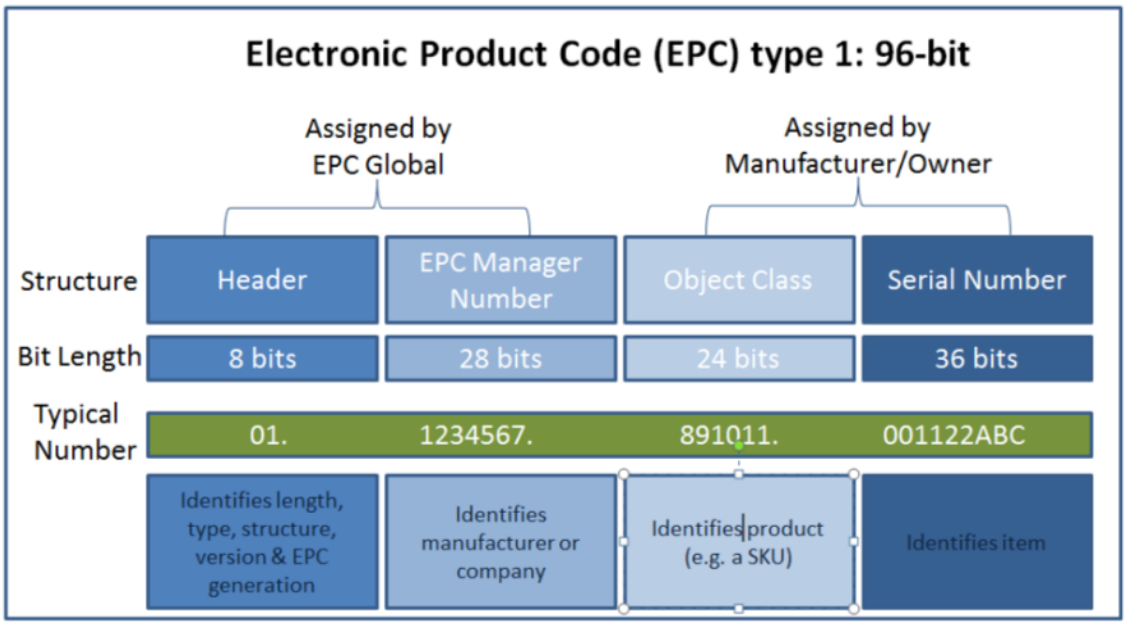
11.6.4. In practical use since the 1970's, RFID is now widely used for product identification, stock control, as anti-theft in manufacturing and retail organisations, payment cards (smart ATM and paywave cards) and access control systems. They are useful tools in improving logistics, profoundly changing cost structures for business, and improving levels of safety and authenticity in a wide range of applications such as access control, passports, payment cards, vehicle immobilisers, toll roads, pharmaceuticals tracking, management of high value items and weapons control. RFID tags are now produced in a wide variety of types and sizes, from the size of a grain of rice or printed on paper to much larger devices incorporating a battery or other power supply.

11.6.5. Unlike bar coding systems, RFID devices can communicate without requiring line of sight and over distances ranging from a few centimetres to kilometres. They can be equipped with sensors to collect data on temperature changes, sudden shocks, humidity or other factors affecting product safety and quality.

11.6.6. RFID devices typically use radio signals to transmit identifying information such as product or serial numbers, manufacture date, origin and batch number. This identifying information is invariably in the form of an Electronic Product Code (EPC) following the standards and conventions published by GS1. GS1 is a global group that also develops standards for other identifiers such as barcodes. The GS1 standards and conventions are now incorporated into ISO standards, see references table below at 11.6.55.

Basic Formats

11.6.7. The basic format of an Electronic Product Code (EPC) is illustrated below:



11.6.8. RFID devices are often referred to as "tags". Passive tags are unpowered and harvest power from the RFID reader. Active tags incorporate a power supply, usually a battery. Tags are produced in Classes 0 to 5 and are now generally produced to Generation 2 specifications. The EPCGen2 standard for Class 1 tags focuses on reliability and efficiency but supports only very basic security. Features of the Gen 2 specification include:

- **a 96 bit EPC number** with read/write capability and can be designated used for other data ;
- **a 32/64 bit tag identifier** (TID) – identifies the manufacturer of the tag, also with read/write capabilities;
- **32 bit kill password** to permanently disable the tag;
- **32 bit access password** to lock the read/write characteristics of the tag and also set the tag for disabling ;
- **User memory** – dependant on the manufacturer and can be as little as 0 bits to 2048 bits. Larger user memory is in development.

11.6.9. The distance from which a tag can be read is termed the read range. A read range will depend on a number of factors, including the radio frequency used for reader/tag/reader communication, the size and orientation of the antennae, the power output of the reader, and whether the tags have a battery or other power supply. Battery-powered tags typically have a read range of 100 meters (approximately 300 feet) although this can extend to kilometres under favourable conditions. It is possible that powered RFID tags, typically used on cargo containers, railway wagons, vehicles and other large assets, could be read from a satellite if there is little background "noise" and the broadcast signal is sufficiently powerful.

11.6.10. RFID tags are divided into classes 0 to 5:

Class	Description
0	Read only, passive tags
1	Write once passive tags. 128-bit memory.
2	Read/Write with up to 65Kb read/write memory and authenticated access control. Can monitor temperature, pressure, vibration.
3	Semi-Passive. Own power source but cannot initiate communication. Remains passive until activated by a reader. Up to 65 Kb read/write memory and integrated sensor circuitry.
4	Active tags (own power source) with integrated transmitter. Can communicate with readers and other tags operating in the same RF band. Rewritable memory and ad hoc networking capability. Read range >100 metres (approx. 300').
5	Reader tags, can power class 1 to 3 tags and communicate with all classes. Includes all the capabilities of class 4 tags.

Operating Frequencies

11.6.11. RFID operates in several parts of the Radio Spectrum. Not all frequencies are authorised for use in all countries and will depend on the radio spectrum allocation authority in each country. It is important to note, however, that some RFID tags designed to operate at frequencies not used in the importing country may be attached to imported goods. This can represent a risk from scanning at frequencies not authorised or normally monitored in the importing country.

11.6.12. Depending on the design and intended application, RFID tag can operate at different frequencies. It is important to note that longer range RFID tags operate at frequencies close to or within allocated Wi-Fi frequencies. Allocated frequencies are:

Band	Frequency	Typical Range
LF	125-134.2 kHz and 140-148.5 kHz	Up to 1/2 metre
HF	13.553 - 13.567 MHz and 26.957 - 27.283 MHz	Up to 1 metre
UHF	433 MHz, 858 - 930 MHz, 2.400 - 2.483 GHz, 2.446 - 2.454GHz	1 to 10 metres
SHF	5.725 - 5.875 GHz	> 100 metres

11.6.13. As RFID devices are deployed in more sophisticated applications such as matching hospital patients with laboratory test results or tracking systems for dangerous materials, concerns have been raised about protecting such systems against eavesdropping, unauthorised uses and privacy breaches.

Smart Cards

11.6.14. Smart cards typically comprise an embedded integrated circuit incorporating a microchip with internal memory, a read-only CSN (Card Serial Number) or a UID (User Identification). The card connects to a reader with direct physical contact or a contactless radio frequency (RFID) interface. With an embedded microchip, smart cards can store large amounts of data, carry out on-card functions (such as encryption and authentication) and interact intelligently with a smart card reader. Smart card technology can be found in a variety of form factors, including plastic cards, key fobs, watches, subscriber identification modules used in mobile phones, and USB-based tokens. Smart cards are widely used in payment card (debit and credit cards and electronic wallets) and access control systems.

11.6.15. The ISO/IEC 14443 standard for contactless smart card communications defines two types of contactless cards ("A" and "B") and allows for communications at distances up to 10 cm operating at 13.56 MHz. The alternative ISO/IEC 15693 standard allows communications at distances up to 50 cm. The ISO/IEC 7816 standard (in 15 parts) defines the physical, electrical interface and operating characteristics of these cards.

11.6.16. In common with other RFID devices, smart cards incorporate an antenna embedded in the body of the card (or key fob, watch or token). When the card is brought within range of the reader, the chip in the card is powered on. Once powered on, an RF communication protocol is initiated and communication established between the card and the reader for data transfer.

11.6.17. Smart cards typically incorporate protective mechanisms including authentication, secure data storage, encryption, tamper-resistance and secure communication. Support for biometric authentication may also be incorporated.

Threats and Vulnerabilities

11.6.18. Some important characteristics of RFID, inherent in the design and properties of the technology are:

- RFID tags are powered by the field emitted by an RFID reader, so whenever a tag is placed in a reader field it is activated and available. In general terms, class 0 and class 1 tags cannot be powered off, only permanently deactivated;
- RFID tags automatically respond to reader interactions without explicit control of the tag owner, so RFID tags can be operated without their owner's consent;
- It is trivial to establish a communication with an RFID tag and there is no visual confirmation of a tag/reader interaction (i.e., no physical connection or manual operation is required), so it is possible to interact with an RFID tag without being detected.

11.6.19. Specific threats and vulnerabilities in the use of RFID technologies include:

- **Legitimate data-mining**: This risk predates the use of RFID technology, but the volume of data provided by RFID tags, loyalty cards, Near Field Communication (NFC) for bank cards and for electronic wallets increases the risk. Some data collection methods keep to ethical use of data-mining techniques to discover the characteristics and habits of an individual or an organisation. This can pose a business intelligence risk. At times, however, this may challenge the bounds of privacy and data ownership. For example, customer loyalty card data used to discover medical information about an individual or RFID tags to track shipments or deliveries to an organisation by a competitor.
- **Eavesdropping and Data theft**: This risk is similar to the data-mining risk but employs unethical and possibly illegal methods of data collection or obtaining data for nefarious or malicious purposes. RFID tags are designed to broadcast information and data theft by easily concealable RFID scanners is technically trivial. Data theft can pose a risk to business processes.
- **Skimming:** Occurs when an unauthorised reader gains access to data stored on a token. This type of attack is particularly dangerous where contactless access or payment cards are used.
- **Relay Attacks**: Relay attacks use eavesdropping to intercept legitimate tag/reader transmissions and relay these to a device at some distance from the legitimate tag. The device can then behave as the genuine tag. Again this type of attack is particularly dangerous where contactless access or payment cards are used.
- **Insert Attacks**: Insert attacks insert system commands where normal data is expected and relies on a lack of data validation. It is possible that a tag can have legitimate data replaced by a malicious command.
- **Tag Cloning**: Clones replicate the functionality of legitimate tags and can be used to access controlled areas, abuse private data, or make an unauthorised electronic transaction. Tag authentication using a challenge-response protocol is a defence against cloning as the information that attackers can obtain through the air interface (such as by eavesdropping) is insufficient to provide a legitimate response. The design of the tag can also incorporate measures at the circuit manufacturing stage to protect tags from duplication by reverse engineering.
- **Data corruption**: Most RFID tags are rewritable by design. This feature may be locked (turning the tag into a write-once, read-many device) or left active, depending on application and security sensitivity. For example, in libraries, the RFID tags are frequently left unlocked for the convenience of librarians in reusing the tags on different books or to track check-ins and check-outs. If tags are not protected, it creates an opportunity for malicious users to overwrite data, typically in the theft of high-value goods by marking them as low-value items or in the case of weapons monitoring, changing the weapon identification.

- **Shipment or People tracking**: While RFID tags are designed to assist in stock control and supply chain management, unauthorised tracking of shipments or of people is undesirable and may even be dangerous. It is possible to follow individuals carrying tags using several techniques, including placing fake readers at building access points, deploying unauthorised readers near legitimate readers and creating relay points along expected routes.
- **Tag Blocking:** This is a form of denial of service by introducing a blocker tag which is designed to simulate all possible tags in an allocated range. This causes readers to continually perform multiple reads on non-existent and non-responsive tags. Blocker tags are sometimes used where privacy or confidentiality are required.
- **Denial of Service (DOS):** Also known as flooding attacks where a signal is flooded with more data than it is designed to handle. Similar in many respects to RF Jamming.

Attack Vectors

11.6.20. Attack vectors for RFID devices include:

- interception of legitimate transmissions (man-in-the-middle [MITM] attacks);
- interception of authorised reader data by an unauthorised device;
- unauthorised access to tags and readers;
- rogue/cloned tags;
- rogue and unauthorised RFID readers;
- side-channel attacks (timing measurements, electromagnetic radiations etc.);
- attacks on back-end systems;
- jamming of legitimate signals.

11.6.21. Because RFID devices incorporate antennas, there is a possibility of radiation hazards from high –powered devices, particularly active tags and readers. It is important to note however that these cases are rare, occur in high powered devices only and that the vast majority of RFID devices do not pose radiation hazards. Related hazards include electromagnetic radiation hazards to personnel (HERP), fuel (HERF) and ordnance (HERO).

11.6.22. Threats and Vulnerabilities of RFID systems are summarised in the table below:

Threat/Vulnerability	Tag	RF	Reader	Network	Back-End	People
Eavesdropping	●	●		●	●	
Relay Attack		●				
Unauthorised Tag Reading (skimming)	●	●	●			
People Tracking	●	●				●
Shipment Tracking	●	●				
Tag Cloning	●	●				
Replay Attack	●	●				
Insert Attack	●		●	●	●	
Tag Content Modification	●					
Malware	●		●	●	●	
RFID System Failure			●	●	●	●
Tag Destruction	●					
Tag Blocking	●	●				
Denial of Service (DoS)	●		●	●		
RF Jamming	●	●				●
Back-End Attacks				●	●	
Radiation Hazard	●	●	●			●

11.6.23. It is important to note that attacks are often used in combination creating blended attacks. Blended attacks may be a combination of attack types, use of multiple attack vectors, the targeting of individual sub-systems or combinations of all three elements.

Good Practices and Countermeasures

11.6.24. Good practice for ensuring the security and privacy of RFID systems includes:

- a risk assessment to determine the nature and extent of risk and threat in the proposed use of RFID;
- strong security architecture to protect RFID databases and communication systems;
- authentication of approved users of RFID systems;
- encryption of radio signals when feasible;
- temporarily or permanently disabling tags when not required;
- shielding RFID tags and tag reading areas to prevent unauthorised access or modification;
- incident management, audit procedures, logging and time stamping to help detect and manage security breaches; and
- tag disposal and recycling procedures that permanently disable or destroy sensitive data.

Authentication

11.6.25. By design and usage, RFID technologies are item, product or shipment identification but **not** authentication technologies. Authentication of a reader or tag requires a common secret (key) shared when establishing communication, and before data is exchanged. Currently, only RFID tags with microprocessors have sufficient computation resources to use authentication techniques. These can be found in such applications as e-passports, or payment or ticketing applications (public transport, for example).

11.6.26. With a challenge/response authentication mechanism the reader issues an enquiry to the tag which results in a response. The secret tag information is computed information from internal cryptographic algorithms by both the tag and reader and the results are sent. Correct responses are required for a successful information exchange. The system is essentially the same as encrypting data over a standard radio link.

11.6.27. The ISO/JTC1/SC31 committee is in the process of establishing new standards to support the use of simple RFID authentication and encryption protocols.

Keyed-Hash Message Authentication Code (HMAC)

11.6.28. HMAC is a protocol where both an RFID reader and RFID tag share a common secret key that can be used in combination with a hash algorithm to provide one-way or mutual authentication between tag and reader. When HMAC is applied to messages, it also assures the integrity of data in the messages.

11.6.29. HMAC is not specified in any RFID standard, but the capability is generally available in vendor products. HMAC is often used where the risk of eavesdropping is high and passwords alone are considered to offer an inadequate authentication mechanism. This will be determined by the risk assessment. HMAC is also used where applications require evidence of a tag's authenticity.

Digital Signatures

11.6.30. Digital signatures are compatible with existing RFID tag standards. In authenticated RFID systems, tags can receive, store, and transmit digital signatures with existing read and write commands because the complexity is managed by readers or back-end systems. However, the use of digital signatures to support authentication of readers to tags would require tags to support relatively complex cryptographic functions, beyond the capacity of common tag designs.

11.6.31. In addition, digital signatures that are not generated by the tag itself are subject to replay attacks. An adversary could query a tag to obtain its evidence of authenticity (i.e., the digital signature created by a previous reader) and then replicate that data on a cloned tag. Consequently, password or symmetric key authentication systems likely will support tag access control, as opposed to tag authenticity verification, for the immediate future.

Encryption

11.6.32. Data stored in the memory of an RFID tag is intended to be freely shared with the various tag users (manufacturers, stock controllers, shipping agents, etc.). Only an RFID reader is required to access the data which raises the question of data security. Memory and computational power of an RFID tag is limited, but data elements can be password-protected or reserved for nominated usage. Several levels of authorisation (read-only, read and write, delete, etc.) can be determined. It is also advisable to encrypt the data entered onto the tag, the encryption/decryption taking place at the RFID reader or back-end system.

Cover-Coding

11.6.33. Cover-coding is a method of hiding information from eavesdroppers. In the EPCglobal Class-1 Generation-2 standard, cover-coding is used to obscure passwords and information written to a tag using the write command. Some proprietary technologies also support similar features. Cover-coding is an example of minimalist cryptography because it operates within the challenging power and memory constraints of passive RFID tags.

11.6.34. Cover-coding is a useful mitigation where eavesdropping is a risk, but adversaries are expected to be at a greater distance from the tags than readers. Cover-coding helps prevent the execution of unauthorised commands that could disable a tag or modify the tag's data. Cover-coding mitigates business process, business intelligence, and privacy risks.

Rolling Code

11.6.35. A rolling code approach is a scheme where the identifier given by the RFID tag changes after each read action. It requires the RFID reader and RFID tag to use identical algorithms. If multiple readers are used, they must be linked so that tracking of code changes can be monitored. This scheme reduces the usefulness of any responses that may be observed unless the pattern of change can be detected or deduced.

Other Defensive Measures

11.6.36. Other defensive measures, sometimes described as palliative techniques, include shielding, blocker tags, tag "kill" commands, tamper resistance and temporary deactivation. It is important to note these techniques do not use encryption.

Shielding

11.6.37. RF shielding is designed to limit the propagation of RF signals outside of the shielded area. Shielding helps to prevent unauthorised reading, access to or modification of the RFID tag data or interfering with RFID readers. Shielding can be applied to small, individual items, such as passports and credit cards or to large elements such as shipping containers.

11.6.38. Shielding is also important where interference is present or detected. This may be caused by environmental conditions, such as operating in a port area, or by deliberate attempts to access readers or tags.

11.6.39. Engineering assessments will determine the requirement for shielding from adverse environmental conditions and the risk assessment will determine the likelihood and threat from unauthorised and deliberate attempts to access readers, tags and data.

11.6.40. RFID blocking wallets and **RFID card sleeves** are available to block RFID frequencies. These are typically used for credit and other payment, access and transit cards and e-passports, as a countermeasure for skimming attacks or unauthorised tracking.

Blocker Tags

11.6.41. A special tag, called a "blocker" tag, blocks an RFID reader by simultaneously answering with 0 and 1 to every reader's request during the identification protocol. The reader is then incapable of distinguishing individual tags. The blocker tag may block a reader universally or within ranges.

11.6.42. This furnishes privacy by shielding consumers from the unwanted scanning of RFID tags that they may carry or wear. It also protects against unauthorised readers and eavesdroppers. The blocker tag is an alternative to more simple solutions such as the kill command, shielding and active jamming. It is important to note that active jamming may be illegal (see 11.6.53).

11.6.43. Blocker tags can also implement one or more privacy policies and multiple blocker tags may cover multiple zones. The blocker tag has a very low-cost of implementation and standard tags need no modification and little support for password-protected bit flipping. A threat is that blocker tags can be used to mount DoS attacks in which a malicious blocker tag universally blocks readers.

Tag "Kill" Command

11.6.44. The "kill" command is a password-protected command specified in the EPC Gen-1 and EPC Gen-2 standards intended to make a tag non-operational. A typical application is anti-theft where the kill command is activated at a point-of-sale terminal, after goods have been paid for. Kill commands can be password protected.

11.6.45. Kill commands function by fusing a ROM component or antenna connection by applying a large amount of power to the tag at the point of sale reader/terminal. It is important to note that the antenna deactivation method does not completely kill the tag but rather disable its RF interface. Once in the disabled state, the tag still retains data and can still function.

11.6.46. The kill feature can represent a threat to an RFID system if the password is compromised. This risk is particularly apparent where the same password is used for multiple tags. If a weak (e.g., short or easily guessed) password is assigned to the kill command, tags can be disabled at will. Also important is the longer a tag uses the same password, the more likely it is that the password will be compromised.

11.6.47. Data stored on the tag is still present in the tag's memory after it is disabled (although it can no longer be accessed wirelessly), and, therefore, still may be accessible with physical access to the tag.

Tamper Resistance

11.6.48. Some RFID tags are designed with tamper resistant or tamper-evident features to help prevent unauthorised alteration of removal of tags from the objects to which they are attached. A simple type of tamper resistance is the use of a frangible, or easily broken, antenna. If this tag is removed, the connection with the antenna is severed, rendering the tag inoperable. Other, more complex types of RFID systems monitor the integrity of objects associated with the tags to ensure that the objects have not been compromised, altered, or subjected to extreme conditions.

11.6.49. Simple forms of tamper resistance may leave data intact and subject to the same threats described above. In addition it is possible to circumvent tamper resistance mechanisms by repairing a frangible antenna. It is important to note that tamper-resistance and tamper-evidence technologies do not prevent the theft or destruction of the tag or its associated items.

Temporary Deactivation

11.6.50. Some tags allow the RF interface to be temporarily deactivated. Methods vary amongst manufacturers with some methods requiring physical intervention. Typically tags would be activated inside a designated area and deactivated when shipped, preventing eavesdropping or other unauthorised transactions during shipment. When the tags arrive at their destination, they can be reactivated, for example for inventory management. Conversely, tags can be used for tracking during shipment and may be deactivated on delivery.

RFID Risks and Controls Summary

11.6.51. A summary of RFID Risks and Controls is presented in the Table below:

Risk Control	Business Process	Business Intelligence	Privacy	Electro-Magnetic Radiation	Back-End System Attack
Tag Access Controls	●	●	●		●
Password Authentication	●	●	●		●
HMAC	●	●	●		●
Digital Signature	●	●			●
Cover-Coding	●	●	●		
Encryption – Data in Transit		●	●		
Encryption – Data at Rest		●			●
Encryption – Data on Tag	●	●	●		
Shielding	●	●	●	●	
Blocker Tags		●	●		
Tag Kill Feature		●	●		
Tamper Resistance	●	●			
Temporary Deactivation	●	●	●		
RF Engineering and Frequency Selection	●	●	●	●	

Relevant Legislation

11.6.52. In New Zealand, operation of radio and other equipment in the RF spectrum is controlled Radiocommunications Act 1989, Reprint as at 5 December 2013 and administered by the Ministry of Business Innovation and Employment.

RF Jammers

11.6.53. It is illegal to import, manufacture, sell or use a radio jammer in New Zealand except with a licence issued by the Radio Spectrum Management unit of the Ministry of Business, Innovation and Employment. The use and management of RF jammers is governed by the Radiocommunications Regulations (Prohibited Equipment – Radio Jammer Equipment) Notice 2011 under the Regulation 32(1)(i) [a notice in the Gazette] of the Radiocommunications Regulations 2001.

Secure Spaces

11.6.54. The use of RFID technology in secure areas must be carefully considered, recognising that an RFID tag or system incorporates antennae and transmitting capabilities which may compromise the security of such areas. Passive tags (classes 0 and 1) pose little risk in themselves as they require a reader to activate and have little on-board capability. Read/write tags (class 2) pose a higher risk as they have the capability to store data. Other tags (classes 3 to 5) can pose a significant risk to secure spaces.

PSR references

11.6.55. The relevant PSR Mandatory Requirements are:

References	Title	Source
PSR Mandatory Requirements	INFOSEC1	http://www.protectivesecurity.govt.nz

References - Guidance

References	Publisher	Source
Special Publication 800-98 Guidelines for Securing Radio Frequency Identification (RFID) Systems	NIST	http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf
FIPS PUB 198-1 The Keyed-Hash Message Authentication Code (HMAC), July 2008	NIST	http://csrc.nist.gov/publications/PubsFIPS.html#198-1
FIPS PUB 180-4 Secure Hash Standard (SHS)	NIST	http://csrc.nist.gov/publications/PubsFIPS.html#180-4
Implementation Guide for the use of GS1 EPCglobal Standards in the Consumer Electronics Supply Chain	GS1/EPCglobal	http://www.gs1.org/epc-rfid
Smart Border Alliance RFID Feasibility Study Final Report Attachment D – RFID Technology Overview	US Department of Homeland Security	https://www.dhs.gov/xlibrary/assets/foia/US-VISIT_RFIDattachD.pdf
Smart Border Alliance RFID Feasibility Study Final Report Attachment E – RFID Security And Privacy White Paper	US Department of Homeland Security	https://www.dhs.gov/xlibrary/assets/foia/US-VISIT_RFIDattachE.pdf
Test Operations Procedure (TOP) 03-2-616A Electromagnetic Radiation Hazards Testing For Non-Ionizing Radio Frequency Transmitting Equipment	US Defense Technical Information Center (DTIC),	www.dtic.mil/dtic/tr/fulltext/u2/a577863.pdf
Electromagnetic Environmental Effects Requirements for Systems – MIL-STD-46C	US Department of Defense Interface Standard	http://everyspec.com/MIL-STD/MIL-STD-0300-0499/MIL-STD-464C_28312/
RFID Tags – Privacy Threats and Countermeasures	European Commission	https://ec.europa.eu/jrc/sites/default/files/jrc78156_report_rfid_en.pdf
OECD Policy Guidance – A Focus on Information Security and Privacy Applications, Impacts and Country Initiatives.	OECD Directorate for Science, Technology and Industry	http://www.oecd.org/sti/ieconomy/40892347.pdf
Technical Guideline TR-03126-5 Technical Guidelines for the Secure Use of RFID (TG RFID) Subdocument 5: Application area "Electronic Employee ID Card" Version 1.0	BSI – The German Federal Office for Information Security	https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03126/TG_03126_5_Application_area_Electronic_Employee_ID_Card.pdf?__blob=publicationFile
Establishing Security Best Practices in Access Control	Rohr *et al*	www.git-security.com/file/track/5743/1

References - Standards

References	Publisher	Source
EPC Tag Data Standard Version 1.9, Ratified, Nov-2014	GS1/EPCglobal	http://www.gs1.org/epcrfid-epcis-id-keys/epc-rfid-tds/1-9
EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID Specification for RFID Air Interface Protocol for Communications at 860 MHz – 960 MHz Version 2.0.1	GS1/EPCglobal	http://www.gs1.org/epcrfid/epc-rfid-uhf-air-interface-protocol/latest
ICAO Doc 9303, Machine Readable Travel Documents Parts 1-12	International Civil Aviation Organization (ICAO)	http://www.icao.int/Security/mrtd/pages/Document9303.aspx
ISO/IEC 7816-1:2011 - Identification cards -- Integrated circuit cards -- Part 1: Cards with contacts -- Physical characteristics	ISO	http://www.iso.org
ISO/IEC 7816-2:2007 - Identification cards -- Integrated circuit cards -- Part 2: Cards with contacts -- Dimensions and location of the contacts	ISO	http://www.iso.org
ISO/IEC 7816-3:2006 Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols	ISO	http://www.iso.org
ISO/IEC 7816-4:2013 - Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange	ISO	http://www.iso.org
ISO/IEC 7816-5:2004 - Identification cards -- Integrated circuit cards -- Part 5: Registration of application providers	ISO	http://www.iso.org
ISO/IEC 7816-6:2004 - Identification cards -- Integrated circuit cards -- Part 6: Interindustry data elements for interchange	ISO	http://www.iso.org
ISO/IEC 7816-7:1999 - Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured Card Query Language (SCQL)	ISO	http://www.iso.org
ISO/IEC 7816-8:2004 Identification cards -- Integrated circuit cards -- Part 8: Commands for security operations	ISO	http://www.iso.org
ISO/IEC 7816-9:2004 - Identification cards -- Integrated circuit cards -- Part 9: Commands for card management	ISO	http://www.iso.org
ISO/IEC 7816-10:1999 - Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards	ISO	http://www.iso.org

References	Publisher	Source
ISO/IEC 7816-11:2004 - Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods	ISO	http://www.iso.org
ISO/IEC 7816-12:2005 - Identification cards - Integrated circuit cards -- Part 12: Cards with contacts -- USB electrical interface and operating procedures	ISO	http://www.iso.org
ISO/IEC 7816-13:2007 - Identification cards -- Integrated circuit cards -- Part 13: Commands for application management in a multi-application environment	ISO	
ISO/IEC 7816-15:2004 - Identification cards -- Integrated circuit cards -- Part 15: Cryptographic information application	ISO	http://www.iso.org
ISO 14443-1:2008 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 1: Physical characteristics	ISO	http://www.iso.org
ISO/IEC 14443-2:2010 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 2: Radio frequency power and signal interface	ISO	http://www.iso.org
ISO/IEC 14443-3:2011 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 3: Initialization and anticollision	ISO	http://www.iso.org
ISO/IEC 14443-4:2008 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 4: Transmission protocol	ISO	http://www.iso.org
ISO/IEC 15961-1:2013 Information technology -- Radio frequency identification (RFID) for item management: Data protocol -- Part 1: Application interface	ISO	http://www.iso.org
ISO/IEC 15963:2009 Information technology – Radio frequency identification for item management – Unique identification for RF tags	ISO	http://www.iso.org
ISO/IEC 18000-1:2008 Information technology -- Radio frequency identification for item management -- Part 1: Reference architecture and definition of parameters to be standardized	ISO	http://www.iso.org
ISO/IEC 18000-2:2009 Information technology -- Radio frequency identification for item management -- Part 2: Parameters for air interface communications below 135 kHz	ISO	http://www.iso.org

References	Publisher	Source
ISO/IEC 18000-3:2010 Information technology -- Radio frequency identification for item management -- Part 3: Parameters for air interface communications at 13,56 MHz	ISO	http://www.iso.org
ISO/IEC 18000-4:2015 Information technology -- Radio frequency identification for item management -- Part 4: Parameters for air interface communications at 2,45 GHz	ISO	http://www.iso.org
ISO/IEC 18000-6:2013 Information technology -- Radio frequency identification for item management -- Part 6: Parameters for air interface communications at 860 MHz to 960 MHz General	ISO	http://www.iso.org
ISO/IEC 18000-7:2014 Information technology -- Radio frequency identification for item management -- Part 7: Parameters for active air interface communications at 433 MHz	ISO	http://www.iso.org
ISO/IEC 18000-61:2012 Information technology -- Radio frequency identification for item management -- Part 61: Parameters for air interface communications at 860 MHz to 960 MHz Type A	ISO	http://www.iso.org
ISO/IEC 18000-62:2012 Information technology -- Radio frequency identification for item management -- Part 62: Parameters for air interface communications at 860 MHz to 960 MHz Type B	ISO	http://www.iso.org
ISO/IEC 18000-63:2015 Information technology -- Radio frequency identification for item management -- Part 63: Parameters for air interface communications at 860 MHz to 960 MHz Type C	ISO	http://www.iso.org
ISO/IEC 18000-64:2012 Information technology -- Radio frequency identification for item management -- Part 64: Parameters for air interface communications at 860 MHz to 960 MHz Type D	ISO	http://www.iso.org
ISO/IEC TR 18047-4:2004 Information technology -- Radio frequency identification device conformance test methods -- Part 4: Test methods for air interface communications at 2,45 GHz	ISO	http://www.iso.org
ISO/IEC TR 18047-7:2010 Information technology -- Radio frequency identification device conformance test methods -- Part 7: Test methods for active air interface communications at 433 MHz	ISO	http://www.iso.org

References	Publisher	Source
ISO/IEC TR 24710:2005 Information technology -- Radio frequency identification for item management -- Elementary tag licence plate functionality for ISO/IEC 18000 air interface definitions	ISO	http://www.iso.org
ISO/IEC TR 24729-1:2008 Information technology -- Radio frequency identification for item management -- Implementation guidelines -- Part 1: RFID-enabled labels and packaging supporting ISO/IEC 18000-6C	ISO	http://www.iso.org
ISO/IEC 24753:2011 Information technology -- Radio frequency identification (RFID) for item management -- Application protocol: encoding and processing rules for sensors and batteries	ISO	http://www.iso.org
ISO/IEC 24791-2:2011 Information technology -- Radio frequency identification (RFID) for item management -- Software system infrastructure -- Part 2: Data management	ISO	http://www.iso.org
ISO/IEC TR 20017:2011 Information technology -- Radio frequency identification for item management -- Electromagnetic interference impact of ISO/IEC 18000 interrogator emitters on implantable pacemakers and implantable cardioverter defibrillators	ISO	http://www.iso.org
ISO/IEC TR 29123:2007 Identification Cards – Proximity Cards – Requirements for the enhancement of interoperability	ISO	http://www.iso.org

Legislation and Regulation

References	Publisher	Source
Radiocommunications Act 1989	Parliamentary Counsel Office	http://www.legislation.govt.nz
Radiocommunications Regulations 2001, Reprint as at 1 February 2015 (SR 2001/240)	Parliamentary Counsel Office	http://www.legislation.govt.nz
Radiocommunications Regulations (Prohibited Equipment - Radio Jammer Equipment) Notice 2011	New Zealand Gazette Office, Government Information Services, Department of Internal Affairs	https://gazette.govt.nz/notice/id/2011-go4051
Radio Spectrum Management	Ministry of Business, Innovation and Employment	http://www.rsm.govt.nz/

Rationale and Controls

11.6.56. Risk Assessment

11.6.56.R.01. Rationale

As with many technologies, adoption of RFID has the potential to introduce a wide range of risks in addition to the risks that already exist for agency systems. This may include privacy risks, depending on the use, information held and implementation of the RFID system. A risk assessment is an essential tool in determining and assessing the range and extent of risk and threat in the use of RFID devices.

11.6.56.R.02. Rationale

Risks to RFID system vary according to the technology used, system engineering, the systems architecture, application, context and deployment scenario. A holistic approach to risk at each stage of the system life cycle and each for system component is essential if a robust security strategy is to be developed.

11.6.56.R.03. Rationale

The identification of classes of tags is fundamental to managing the risks of RFID devices in secure spaces. Classes 0 and 1 pose little risk. Other classes of tag (2 to 5), however, have limited data storage capability and active tags include transmitter functionality which introduces higher levels of risk. RFID readers are, by definition, transmitters and are not permitted in secure spaces.

11.6.56.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST conduct and document a risk assessment *before* implementing or adopting an RFID solution.

11.6.56.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

This risk assessment MUST be the basis of a security architecture design.

11.6.57. Security Architecture

11.6.57.R.01. Rationale

The foundation of strong security architecture in RFID follows three important principles:

- **Controlled access to the data** – only authorised entities (people, systems, devices) can read and write information to and from the RFID tags (EPC number, tag identifier, kill password, access password and user memory) and RFID databases;
- **Control over access to the system –** only authorised entities can configure or add devices to the system, and all devices on the system are authentic and trustworthy;

- **Confidence and trust –** back-end systems are designed and implemented in accordance with the current version of the NZISM.

11.6.57.R.02. Rationale

Sensitive data should be held in a secure RFID Enterprise Subsystem and retrieved using the tag's unique identifier with only an identifier stored on the tag itself. The Enterprise RFID subsystem should be established as a separate domain where data can be more adequately protected. This structure makes it more difficult for adversaries to obtain information from the tag through scanning or eavesdropping. Data encryption and access control is often more cost-effectively performed in the enterprise subsystem than in the RF subsystem.

11.6.57.R.03. Rationale

Some RFID systems may cover several organisations, for example in supply chains. In such cases, multiple organisations may require access to databases that contain tag identifiers and passwords. The security architecture should incorporate strong security controls including the authentication of external entities, incident management, audit logging and other essential security controls.

11.6.57.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST develop a strong security architecture to protect RFID databases and RFID systems.

11.6.57.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST minimise the information stored on RFID tags and in the RFID subsystem.

11.6.57.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD disable any rewrite functions on RFID devices.

11.6.57.C.04. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD apply the access control requirements of the NZISM (Chapter 11) to RFID systems.

11.6.58. Policy

11.6.58.R.01. Rationale

An RFID Usage Policy is an essential component of an agency's privacy policy, addressing topics such as how personal information is stored and shared. The RFID usage policy should also address privacy issues associated with the tag identifier formats and the potential disclosure of information based solely on the tag identifier format selected. Agencies MAY be required to ensure that devices that collect and store data comply with relevant regulation and guidance, such as the Privacy Act and the HIPAA. Refer also to Chapter 20 – Data Management.

11.6.58.R.02. Rationale

Any RFID implementation should also be incorporated into the agency's security policies. Refer also to Chapter 5 – Information Security Documentation.

11.6.58.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD develop, implement and maintain an RFID Usage Policy.

11.6.58.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD incorporate RFID into the agency's security policies and information security documentation.

11.6.59. Inspections

11.6.59.R.01. Rationale

Many system component manufacturers use RFID tags to track shipments. RFID tags may be embedded in the packaging, printed on the reverse of labels, attached to or embedded in the device itself. The ability to identify and track devices may pose a security concern for secure areas or equipment deployed in high security applications.

11.6.59.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST conduct visual and technical inspections of packaging and devices to determine if RFID devices have been attached and either permanently disable or remove such devices.

11.6.59.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD conduct visual inspections of packaging and devices to determine if RFID devices have been attached and if these RFID devices pose a security concern.

11.6.59.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD conduct visual inspections of packaging and devices to determine if RFID devices or labelling have been tampered with and whether this is a security concern.

11.6.60. Shielding

11.6.60.R.01. Rationale

RF shielding is designed to limit the propagation of RF signals outside of the shielded area. Shielding helps to prevent unauthorised reading, access to or modification of the RFID tag data or interfering with RFID readers. Shielding can be applied to small, individual items, such as passports and credit cards or to large elements such as shipping containers. The requirement for shielding is determined by the risk assessment and an engineering assessment.

11.6.60.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD consider undertaking an RF engineering assessment where security concerns exist or where the RFID systems are to be used in areas with high levels of RF activity.

11.6.60.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Shielding SHOULD be considered where eavesdropping or RF radiation is a concern, as determined by the risk assessment.

11.6.61. Positioning of Tags and Readers

11.6.61.R.01. Rationale

In order to minimise unnecessary electromagnetic radiation tags and readers should be carefully positioned. Care should be taken in use of RFID readers in proximity to:

- Fuel, ordnance, and other hazardous materials,
- Humans and sensitive products (e.g., blood, medicine) that may be harmed by sustained exposure to RF radiation,
- Metal and reflective objects that can modify and amplify signals in unintended and potentially harmful ways, and
- Legitimate radio and Wi-Fi systems to avoid interference.

11.6.61.R.02. Rationale

Tag location cannot always be controlled, such as when tags are used to track mobile items or goods in transit. Other difficulties occur with persistent radio interference. In these situations, relocation of readers and tags may provide a solution. Consideration should be given to alternative but cost-effective RF protection measures, such as grounded wire fencing. The engineering assessment undertaken to determine the shielding requirements will assist in determining such measures.

11.6.61.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD consider placement of tags and location of readers to avoid unnecessary electromagnetic radiation.

11.6.62. Encoding and Encryption

11.6.62.R.01. Rationale

If an adversary reads an identifier that is encoded with a published format, such as in the EPC standard, an adversary may be able to obtain useful information such as the manufacturer or issuer of the item, as well as the type of item. Because RFID tags hold limited information and identifier formats are published in standards, it may be important to use identifier formats that do not reveal any information about tagged items or the agency using the RFID system. This will be determined in the risk assessment.

Encoding schemes to limit information revealed from unauthorised scanning may include serially or randomly assigning identifiers.

11.6.62.R.02. Rationale

Adversaries can often obtain valuable information from the identifier alone. For example, knowledge of the EPC manager ID and object class bits may reveal the make and model of tagged objects in a container. If individual items or boxes of items are tagged, the quantities may also be discernible. An adversary might target containers based on their contents.

11.6.62.R.03. Rationale

The smallest tags generally used for consumer items, such as clothing, do not have enough computing power to support data encryption. At best these tags can cater for PIN-style or password-based protection. Data can, however, be encrypted before it is stored on a tag. In these designs, encryption is undertaken by the RFID subsystem or the RFID reader. This is an effective means of protecting the data on a tag. Refer also to Chapter 17 – Cryptography.

11.6.62.R.04. Rationale

The current Gen 2 standard provides for an on-chip 16-bit Pseudo-Random Number Generator (RNG) and a 16-bit Cyclic Redundancy Code (CRC-16) to protect tag/reader channels. Neither of these encryption methods is strong because of the short bit length in the RNG and because CRCs are not suitable for protection against malicious alteration of data.

11.6.62.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST follow the requirements of the NZISM in the selection and implementation of cryptographic protocols and algorithms, and in key management, detailed in Chapter 17.

11.6.62.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD encrypt data before it is written to RFID tags.

11.6.62.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD assign RFID identifiers using formats that limit information about tagged items or about the agency operating the RFID system.

11.6.63. Authentication

11.6.63.R.01. Rationale

Both an RFID reader and RFID tag share a common secret key that can be used in combination with a hash algorithm to provide one-way or mutual authentication between tag and reader. This is known as a **Keyed-Hash Message Authentication Code (HMAC).** When HMAC is applied to messages, it also assures the integrity of data in the messages. HMAC is not specified in any RFID standard, but the capability is generally available in vendor products. HMAC is often used where the risk of eavesdropping is high

and passwords alone are considered to offer an inadequate authentication mechanism. This will be determined by the risk assessment. HMAC is also used where applications require evidence of a tag's authenticity.

11.6.63.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD consider the use of HMAC when tag authenticity is required.

11.6.64. Password Management

11.6.64.R.01. Rationale

RFID tags generally require passwords before execution of commands such as reading and writing of tag data, memory access control, and the tag kill feature. Passwords are an important control in maintaining the security and integrity of the RFID system. Refer also to Chapter 16 – Access Control.

11.6.64.R.02. Rationale

Tags should not share passwords, although this may not be practical in all cases. In applications such as supply chains, multiple organisations may require access to databases that contain tag identifiers and passwords. In such cases external entities must be authenticated and incident management, audit logging and other security controls are essential. While in traditional IT systems, passwords are often changed on a periodic basis, in RFID systems, such changes may be impractical, especially if the tags are not always accessible to the agency assigning the passwords.

11.6.64.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST assign passwords for critical RFID functions.

11.6.64.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD follow the guidance for passwords management in the NZISM (Chapter 16 – Access Control).

11.6.65. Temporary Deactivation of Tags

11.6.65.R.01. Rationale

The RF interface on some tags can be temporarily deactivated. In a supply chain application, for example, tags may be turned off to prevent unauthorised access to the tags during shipment. This feature is useful when communication between readers and a tag is infrequent allowing the tag to be activated when required but limiting vulnerability to rogue transactions if left operational for extended periods with no authorised activity. Temporary deactivation can also extend battery life in powered tags.

11.6.65.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD consider temporary deactivation of RFID tags where the tag is likely to be inactive for extended periods.

11.6.66. Incident Management

11.6.66.R.01. Rationale

Incident management and audit procedures, logging and time stamps help detect and manage security breaches. These are important tools in protecting systems and managing security breaches.

11.6.66.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST develop and implement incident identification and management processes in accordance with this manual (See Chapter 5 – Information Security Documentation, Chapter 6 – Information Security Monitoring, Chapter 7 – Information Security Incidents, Chapter 9 – Personnel Security and Chapter 16 – Access Control).

11.6.67. Disposal

11.6.67.R.01. Rationale

Tag disposal and recycling procedures that permanently disable or destroy sensitive data reduces the possibility that they could be used later for tracking or targeting, and prevents access to sensitive data stored on tags. In addition the continued operating presence of a tag after it has performed its intended function can pose a business intelligence or privacy risk, including tracking, targeting or access to sensitive data on the tag.

11.6.67.R.02. Rationale

Disposal may be undertaken electronically by using a tag's "kill" feature or using a strong electromagnetic field to permanently deactivate a tag's circuitry. Alternatively physical destruction can be achieved by tearing or shredding. Where a tag supports an electronic deactivation mechanism, tags should be electronically deactivated before physical destruction.

11.6.67.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD consider secure disposal procedures and incorporate these into the RFID Usage Policy. Refer also to Chapter 13 – Decommissioning and Disposal.

11.6.68. Operator Training and User Awareness

11.6.68.R.01. Rationale

Operator training can help ensure that personnel using the RFID system have the necessary skills and knowledge follow appropriate guidelines and policies. If HERF/HERO/HERP risks are present, appropriate security training covers mitigation techniques, such as safe handling distances.

11.6.68.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST develop and implement user awareness and training programmes to support and enable safe use of RFID services (See Section 9.1 – Information Security Awareness and Training).

11.6.69. Secure Spaces

11.6.69.R.01. Rationale

The identification of classes of tags is fundamental to managing the risks of RFID devices in secure spaces. Classes 0 and 1 pose little risk. Other classes of tag (2 to 5), however, have limited data storage capability and active tags include transmitter functionality which introduces higher levels of risk. RFID readers are, by definition, transmitters and are not permitted in secure spaces. Some exceptions may be permitted for testing, and inspection and monitoring purposes. Any such exceptions must be carefully controlled and monitored.

11.6.69.C.01. Control: System Classification(s): All Classifications; Compliance: MUST NOT

Any RFID tags of class 3, 4, or 5 MUST NOT be permitted in secure spaces.

11.6.69.C.02. Control: System Classification(s): All Classifications; Compliance: MUST NOT

RFID readers MUST NOT be permitted in secure spaces.

11.6.69.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD NOT

Class 2 RFID tags SHOULD NOT be permitted in secure spaces.

Abbreviations

Term	Meaning
EMV	Europay, MasterCard, and Visa technical standard
EPC	**Electronic Product Code**
HERF	Hazards of Electromagnetic Radiation to Fuel
HERO	Hazards of Electromagnetic Radiation to Ordnance
HERP	Hazards of Electromagnetic Radiation to Personnel
HMAC	Keyed-Hash Message Authentication Code
RFID	Radio Frequency Identification
SAM	Secure Access Module/ Secure Application Module

Terms

Term	Meaning
EMV	**E**uropay, **M**asterCard, and **V**isa technical standard for payment cards, payment terminals and automated teller machines (ATMs)
EPC	An Electronic Product Code (EPC) is a universal identifier that gives a unique identity to a specific physical object. In most instances, EPCs are encoded on RFID tags attached to the object and used for stock tracking and management purposes. Many types of assets can be tagged including fixed assets, documents, transport containers and clothing items.
Radio Frequency Identification (RFID)	RFID is technology utilising electromagnetic or electrostatic coupling in the radio frequency (RF) portion of the electromagnetic spectrum to uniquely identify an object, item, animal, or person. RFID is increasingly used as replacement for bar codes. An RFID system consists of three components: an antenna, transceiver (usually the RFID reader) and a transponder (also known as a tag).
Secure Access Module	A **Secure Access Module** (or Secure Application Module) is used to enhance the security and cryptographic performance of devices. SAMs are commonly found in devices needing to perform secure transactions, such as payment terminals. It can be used for cryptographic computation and secure authentication against smart cards or contactless EMV cards. Physically a SAM card can either be a separate component and plugged into a device when required or incorporated into an integrated circuit.
Tag	The transponder in an RFID system, frequently found attached to an item or object to provide electronic identification.

11.7. Access Control Systems

Objective

11.7.1. To ensure Access Control Systems incorporating contactless RFID or smart cards are used safely and securely in order to protect privacy, prevent unauthorised access and to prevent the compromise of secure spaces.

Context

Scope

11.7.2. This section provides information relating to the risks, security and secure use of RFID or smart cards in access control systems. This section does not discuss biometric access control systems.

11.7.3. The previous section (11.6. Radio Frequency Identification Devices) provides background information and technical detail of the RFID aspects and should be read in conjunction with this section.

Background

11.7.4. Contactless access control systems based on RFID (Radio Frequency Identification) has largely replaced earlier technologies such as magnetic swipe cards in almost all security-critical applications. Two generations of RFID access cards exist:

- an earlier generation of cards, which use only basic proprietary security mechanisms; and
- a more recent generation that incorporates advances in CMOS and smart card technology to implement cryptography and other protective measures.

11.7.5. Older access control systems often incorporated a magnetic strip and were easily cloned. More recent systems support the use of PINs in addition to RFID. Unfortunately PINs are also sometimes stored on the cards, often unencrypted and unprotected, and thus facilitating attacks on both the card and the PIN.

11.7.6. Access control systems typically comprise four components:

- A reader that programmes the access cards for particular employees and their permitted access to parts of the site, building to secure areas.
- A transceiver at each control point to communicate with cards.
- A controller to control the locks of access points (doors).
- The backend system that hosts all permissions and authorised data and interfaces with the reader, transceiver and controllers.

11.7.7. Traditionally access control systems were hosted by stand-alone equipment. Modern access control system may be hosted on standard computer equipment and hosted in the organisation's datacentre. It is possible that a system intrusion can target access control systems, making the switches, gates and locks remotely accessible.

11.7.8. Low frequency RFID badge systems use 125KHz, (ISO 11784/5 and ISO 14223). Newer high frequency RFID cards use 13.56MHz (ISO 15693, ISO 14443 and ISO 18000-3).

11.7.9. Some cards also operate at UHF frequencies of 850-960Mhz (ISO 18000-6). Some cards are designed to operate at low and high frequencies by embedding multiple antennae in the cards.

11.7.10. The ISO/IEC 14443 standard for contactless smart card communications defines two types of contactless cards ("A" and "B") and allows for communications at distances up to 10 cm operating at 13.56 MHz.

11.7.11. The alternative ISO/IEC 15693 standard allows communications at distances up to 50 cm. The ISO/IEC 7816 standard (in 15 parts) defines the physical, electrical interface and operating characteristics of these cards.

11.7.12. UHF cards follow the EPC Global Gen2 standard and the ISO 18000-6 standards and are designed to operate at distances of up to 10 metres.

Smart Cards

11.7.13. Smart cards typically incorporate an embedded integrated circuit typically incorporating a microchip with internal memory, a read-only CSN (Card Serial Number) or a UID (User Identification). The card connects to a reader with direct physical contact or a contactless radio frequency (RFID) interface. With an embedded microchip, smart cards can store large amounts of data, carry out on-card functions (such as encryption and authentication) and interact intelligently with a smart card reader. Smart card technology can be found in a variety of form factors, including plastic cards, key fobs, watches, subscriber identification modules used in mobile phones, and USB-based tokens. Smart cards are widely used in payment card (debit and credit cards and electronic wallets) and access control systems.

11.7.14. In common with other RFID devices, smart cards incorporate an antenna embedded in the body of the card (or key fob, watch or token). When the card is brought within range of the reader, the chip in the card is powered on. Once powered on, an RF communication protocol is initiated and communication established between the card and the reader for data transfer.

11.7.15. Smart cards typically incorporate protective mechanisms including authentication, secure data storage, encryption, tamper-resistance and secure communication. Support for biometric authentication may also be incorporated.

Near Field Communication (NFC)

11.7.16. NFC is an RFID technology that enables two electronic devices to establish communication by bringing them within 4 cm of each other. As with other "proximity" technologies, NFC employs electromagnetic induction between two loop antennae when NFC devices exchange information. NFC operates in the globally available unlicensed radio frequency band of 13.56 MHz conforming to the ISO/IEC 18000-3 standard. In access control applications these devices are sometimes known as “prox cards”.

Attacks

11.7.17. In addition to attacks on RFID components described in the previous section, access control cards can be susceptible to relay and chip hacking attacks.

11.7.18. Relay attacks rely on rogue readers to activate the tag even when not in proximity to a legitimate reader. The card holder will be unaware that such an attack is underway. An effective defence is to incorporate distance-to-reader verification although few RFID systems incorporate this mechanism.

11.7.19. Signals between cards and a legitimate reader can be intercepted at distances of up to a metre. Greater distances are possible with higher powered equipment, special antennae and in low interference environments. The signals and data, including card credentials, are captured off-line and used to clone access cards. Again the card holder will be unaware that such an attack is underway.

11.7.20. Chip hacking is facilitated by physical access to the card but can be mitigated by second factor authentication, encryption of data on the card and card tamper detection.

11.7.21. Threats, vulnerabilities and mitigations of RFID access control systems are summarised in the table below:

Threat/Vulnerability	Mitigation
Interception of the RFID signals	Encryption of RF links Harden RFID elements
Implants	Physical security CCTV Tamper resistant readers
Cryptographic attacks	Use of approved cryptographic algorithms and protocols Strong key management Incident detection and management Use of evaluated products
Replay Authentications	Robust Random Number Generation on readers
Key extraction reader attacks through side channel analysis or fault injection	Use of evaluated products with SAM chips Incident detection and management
Attack on authentication keys on the card	Key diversification Strong key management Incident detection and management
Chip Hacking	Use of approved cryptographic algorithms and protocols on the card Tamper protection Incident detection and management
Malware	Update and patching for all system components Incident detection and management
Backend systems	System hardening Update and patching for all system components Intrusion detection Incident detection and management

Product Selection

11.7.22. A number of protection profiles related to smartcards and related devices and systems are provided on the Common Criteria website. Refer also to Chapter 12 – Product Security.

Secure Access Module

11.7.23. A Secure Access Module (or Secure Application Module - SAM) is used to enhance the security and cryptographic performance of devices. SAMs are commonly found in devices needing to perform secure transactions, such as payment terminals. It can be used for cryptographic computation and secure authentication against smart cards or contactless payment cards.

11.7.24. Physically a SAM card can either be a separate component and plugged into a device when required or incorporated into an integrated circuit. A typically use is for the secure storage of cryptographic keys or other sensitive data. SAM hardware and software are designed to prevent information leakage and incorporates countermeasures against electromagnetic radiation, timing measurements, and other side channel attacks. These properties mean that SAMs offer a much higher level of protection than the terminals and readers, which often utilise general-purpose computers.

11.7.25. SAM's typically support 3DES and AES cryptographic algorithms and SHA hashing algorithms in their hardware cryptographic co-processor implementations. Refer to Chapter 17 for information on approved cryptographic algorithms and protocols. It is important to note that 3DES is approved for use on legacy systems only and SHA-1 is not an approved hashing algorithm.

Card Protection

11.7.26. RFID blocking wallets and RFID card sleeves are available to block RFID frequencies. These are typically used for the protection of credit and other payment, access, transit cards and e-passports as a countermeasure for skimming attacks.

References - Guidance

References	Publisher	Source
Establishing Security Best Practices in Access Control	Rohr, Nohl and Plotz	www.git-security.com/file/track/5743/1
Common Criteria Protection Profiles	Common Criteria	https://www.commoncriteriaportal.org/pps/
Defending Risky Electronic Access Points into a "Closed" Industrial Control System (ICS) Network Perimeter	NSA	https://www.nsa.gov/ia/_files/security_configuration/Defending_Risky_Electronic_Access_Points.pdf

References - Standards

References	Publisher	Source
ISO/IEC 7816-1:2011 - Identification cards -- Integrated circuit cards -- Part 1: Cards with contacts -- Physical characteristics	ISO	http://www.iso.org
ISO/IEC 7816-2:2007 - Identification cards -- Integrated circuit cards -- Part 2: Cards with contacts -- Dimensions and location of the contacts	ISO	http://www.iso.org
ISO/IEC 7816-3:2006 Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols	ISO	http://www.iso.org
ISO/IEC 7816-4:2013 - Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange	ISO	http://www.iso.org
ISO/IEC 7816-5:2004 - Identification cards -- Integrated circuit cards -- Part 5: Registration of application providers	ISO	http://www.iso.org
ISO/IEC 7816-6:2004 - Identification cards -- Integrated circuit cards -- Part 6: Interindustry data elements for interchange	ISO	http://www.iso.org
ISO/IEC 7816-7:1999 - Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured Card Query Language (SCQL)	ISO	http://www.iso.org
ISO/IEC 7816-8:2004 Identification cards -- Integrated circuit cards -- Part 8: Commands for security operations	ISO	http://www.iso.org
ISO/IEC 7816-9:2004 - Identification cards -- Integrated circuit cards -- Part 9: Commands for card management	ISO	http://www.iso.org

References	Publisher	Source
ISO/IEC 7816-10:1999 - Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards	ISO	http://www.iso.org
ISO/IEC 7816-11:2004 - Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods	ISO	http://www.iso.org
ISO/IEC 7816-12:2005 - Identification cards - Integrated circuit cards -- Part 12: Cards with contacts -- USB electrical interface and operating procedures	ISO	http://www.iso.org
ISO/IEC 7816-13:2007 - Identification cards -- Integrated circuit cards -- Part 13: Commands for application management in a multi-application environment	ISO	http://www.iso.org
ISO/IEC 7816-15:2004 - Identification cards -- Integrated circuit cards -- Part 15: Cryptographic information application	ISO	http://www.iso.org
ISO/IEC 10373-7:2008 - Identification cards -- Test methods -- Part 7: Vicinity cards	ISO	http://www.iso.org
ISO 11784:1996 Amd 2:2010- Radio frequency identification of animals -- Code structure	ISO	http://www.iso.org
ISO 14223-1:2011 - Radiofrequency identification of animals -- Advanced transponders -- Part 1: Air interface	ISO	http://www.iso.org
ISO 14223-2:2010 - Radiofrequency identification of animals -- Advanced transponders -- Part 2: Code and command structure	ISO	http://www.iso.org
ISO 14443-1:2008 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 1: Physical characteristics	ISO	http://www.iso.org
ISO/IEC 14443-2:2010 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 2: Radio frequency power and signal interface	ISO	http://www.iso.org
ISO/IEC 14443-3:2011 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 3: Initialization and anticollision	ISO	http://www.iso.org
ISO/IEC 14443-4:2008 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 4: Transmission protocol	ISO	http://www.iso.org

References	Publisher	Source
ISO/IEC 18000-3:2010 Information technology -- Radio frequency identification for item management -- Part 3: Parameters for air interface communications at 13,56 MHz	ISO	http://www.iso.org
ISO/IEC 18000-6:2013 Information technology -- Radio frequency identification for item management -- Part 6: Parameters for air interface communications at 860 MHz to 960 MHz General	ISO	http://www.iso.org
ISO/IEC TR 29123:2007 Identification Cards – Proximity Cards – Requirements for the enhancement of interoperability	ISO	http://www.iso.org
ISO/IEC 15693-1:2010 - Identification cards -- Contactless integrated circuit cards -- Vicinity cards -- Part 1: Physical characteristics	ISO	http://www.iso.org
ISO/IEC 15693-2:2006 - Identification cards -- Contactless integrated circuit cards -- Vicinity cards -- Part 2: Air interface and initialization	ISO	http://www.iso.org
ISO/IEC 15693-3:2009 Amd 3:2015- Identification cards -- Contactless integrated circuit cards -- Vicinity cards -- Part 3: Anticollision and transmission protocol	ISO	http://www.iso.org

Rationale and Controls

11.7.27. Risk Assessment

11.7.27.R.01. Rationale

As with many technologies, adoption of RFID access cards has the potential to introduce a wide range of risks in addition to the risks that already exist for agency systems. This may compromise the cards and enable unauthorised access, in addition to RFID risks discussed in the previous section. A risk assessment is an essential tool in determining and assessing the range and extent of risk and threat in the use of RFID access cards.

11.7.27.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST conduct and document a risk assessment *before* implementing or adopting an RFID access card system.

11.7.27.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

This risk assessment MUST be the basis of a security architecture design.

11.7.28. Security Architecture

11.7.28.R.01. Rationale

The foundation of strong security architecture in RFID follows these important principles:

1. **Physical Security** - over readers, secure areas, issued and unissued access cards;
2. **Controlled access to the data** – only authorised entities (people, systems, devices) can read and write information to the cards, card databases and backend systems;
3. **Control over access to the system –** only authorised entities can configure or add devices to the system, and all devices on the system are authentic and trustworthy;
4. **Confidence and trust –** back-end systems are designed and implemented in accordance with the current version of the NZISM. This includes intrusion detection and incident management mechanisms and procedures.

11.7.28.R.02. Rationale

Some access systems may cover several organisations or sites. In such cases, multiple organisations or sites may require access to databases that contain personnel identifiers, passwords and access permissions. The security architecture should incorporate strong security controls including the authentication of external entities, incident management, audit logging and other essential security controls.

11.7.28.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST develop a strong security architecture to protect access to databases and systems.

11.7.28.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD apply the NZISM access controls (Chapter 11) and cryptographic controls (Chapter 19) to access card systems.

11.7.28.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD consider the application of the following design elements:

- Implement a Demilitarized Zone (DMZ) to isolate card systems from other parts of the organisation's network and from high-risk Internet Protocol (IP) network connections;
- Secure or remove connections between the Internet and card system network segments;
- Secure or remove vulnerable dialup modem links;
- Secure or remove vulnerable wireless radio links and network access points; and
- Network activity monitoring for unusual or anomalous access activity and well as intrusion detection.

11.7.29. Policy

11.7.29.R.01. Rationale

An Access Card Usage Policy is an essential component addressing topics such as how personal information is stored and shared, card holder responsibilities and procedures to manage card loss or damage. Refer also to Chapter 20 – Data Management.

11.7.29.R.02. Rationale

Any access card implementation should also be incorporated into the agency's security policies. Refer also to Chapter 5 – Information Security Documentation.

11.7.29.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD develop, implement and maintain an Access Card Usage Policy.

11.7.29.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD incorporate access cards into the agency's security policies and information security documentation.

11.7.30. Physical Security

11.7.30.R.01. Rationale

Physical security over readers, door controls, cables and control systems, as well as the cards themselves is fundamental to the operation of a secure system.

11.7.30.R.02. Rationale

In order to minimise unnecessary electromagnetic radiation readers and control equipment should be carefully positioned. Care should be taken with the use of card readers in proximity to:

- Fuel, ordnance, and other hazardous materials,
- Metal and reflective objects that can modify and amplify signals in unintended and potentially harmful ways, and
- Legitimate radio systems to avoid interference.

11.7.30.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD select systems that provide resistance to physical or electronic tampering.

11.7.30.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD implement systems to minimise the risk of physical or electronic tampering.

11.7.30.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD consider placement of tags and location of readers to avoid unnecessary electromagnetic radiation.

11.7.30.C.04. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD consider and select other physical controls in accordance with the PSR.

11.7.31. Card Data Protection

11.7.31.R.01. Rationale

Cards are invariably retained by the card holder and subject to loss, theft or being misplaced. Cards are also not always within the control of the card holder outside of normal office hours. Measures to protect cards in these situations are fundamental to the maintenance of the integrity and security of the access control system.

11.7.31.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST follow the requirements of the NZISM in the selection and implementation of cryptographic protocols and algorithms, and in key management, detailed in Chapter 17.

11.7.31.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD encrypt data before it is written to cards.

11.7.31.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD consider the use of cards systems incorporating Secure Access Modules (SAMs).

11.7.32. Incident Management

11.7.32.R.01. Rationale

Incident management and audit procedures, logging and time stamps help detect and manage security breaches. These are important tools in protecting systems and managing security breaches.

11.7.32.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST develop and implement incident identification and management processes in accordance with this manual (See Chapter 5 – Information Security Documentation, Chapter 6 – Information Security Monitoring, Chapter 7 – Information Security Incidents, Chapter 9 – Personnel Security and Chapter 16 – Access Control).

11.7.32.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST develop and implement incident identification and management processes in accordance with this manual (See Chapter 5 – Information Security Documentation, Chapter 6 – Information Security Monitoring, Chapter 7 – Information Security Incidents, Chapter 9 – Personnel Security and Chapter 16 – Access Control).

11.7.33. Disposal

11.7.33.R.01. Rationale

Card disposal and recycling procedures that permanently disable or destroy sensitive data reduces the possibility that they could be used later for tracking or targeting, and prevents access to sensitive data stored on cards. In addition the continued operating presence of a card after it has performed its intended function can pose an unauthorised access, business intelligence or privacy risk, including tracking and targeting of personnel or access to sensitive data on the access card.

11.7.33.R.02. Rationale

Disposal may be undertaken by electronically by using a card's wipe feature or using a strong electromagnetic field to permanently deactivate a tag's circuitry. Alternatively physical destruction can be achieved by tearing or shredding. Where a tag supports an electronic deactivation mechanism, tags should be electronically deactivated before physical destruction.

11.7.33.C.01. Control: System Classification(s): All Classifications; Compliance SHOULD

Agencies SHOULD consider secure disposal procedures and incorporate these into the Access Card Usage Policy. Refer also to Chapter 13 – Decommissioning and Disposal.

12. Product Security

12.1. Product Selection and Acquisition

Objective

12.1.1. Products providing security functions for the protection of classified information are formally evaluated in order to provide a degree of assurance over the integrity and performance of the product.

Context

Scope

12.1.2. This section covers information on the selection and acquisition of any product that provide security functionality for the protection of information. It DOES NOT provide information on the selection or acquisition of products that do not provide security functionality or physical security products.

Selecting products without security functions

12.1.3. Agencies selecting products that do not provide a security function or selecting products that will not use their security functions are free to follow their own agency or departmental acquisition guidelines.

Product specific requirements

12.1.4. Where consumer guides exist for evaluated products, agencies should identify and assess any potential conflicts with this manual. Where further advice is required, consult the GCSB.

Convergence

12.1.5. Convergence is the integration of a number of discrete technologies into one product. Converged solutions can include the advantages and disadvantages of each discrete technology.

12.1.6. Most products will exhibit some element of convergence. When products have converged elements, agencies will need to comply with the relevant areas of this manual for the discrete technologies when deploying the converged product.

12.1.7. As an example, when agencies choose to use evaluated media, such as encrypted flash memory media, the requirements for evaluated products, media and cryptographic security apply.

Assurance

12.1.8. In Common Criteria (CC), assurance is the confidence that a Target of Evaluation (TOE) meets the Security Functional Requirements (SFR) of the product.

Determining Assurance

12.1.9. In order to determine the level of assurance (the EAL), the CC standard requires tests, checks and evaluations in several areas. Higher levels of assurance require more extensive design, documentation, testing and evaluation. Determining assurance requires assessment of the following elements:

- Development;
- Guidance documents;
- Life-cycle support;
- Security Target evaluation;
- Tests; and
- Vulnerability assessment.

Augmented Assurance

12.1.10. It is possible to "augment" an evaluation to provide additional assurance without changing the fundamental assurance level. This mechanism allows the addition of assurance components not specifically required for a specific level of evaluation or the substitution of assurance components from the specification of another hierarchically higher assurance component. Of the assurance constructs defined in the CC, only EALs may be augmented. An augmented EAL is often indicated by a "+"-sign (for example EAL4+). The concept of negative augmentation or an "EAL minus" is not recognised by the standard.

High Assurance

12.1.11. High Assurance is a generic term encompassing EAL levels 5, 6 and 7. ASD run an independent High Assurance Evaluation scheme which is not related to AISEP or an EAL rating.

Evaluated Products List

12.1.12. The Evaluated Products List (EPL) records products that have been, or are in the process of being, evaluated through one or more of the following schemes:

- Common Criteria;
- high assurance evaluation; or
- an Australasian Information Security Evaluation Program (AISEP) approved evaluation.

12.1.13. The AISEP Evaluated Products List (EPL) is maintained by the Australian Signals Directorate (ASD) (http://www.asd.gov.au/infosec/epl/index.php) and provides a listing of approved products for the protection of classified information. Other EPL's are available through the Common Criteria website.

Evaluation level mapping

12.1.14. The Information Technology Security Evaluation Criteria (ITSEC) and Common Criteria (CC) assurance levels used in the EPL are similar, but not identical, in their relationship. The table below shows the relationship between the two evaluation criteria.

12.1.15. This manual refers only to Common Criteria Evaluation Assurance Levels (EALs). The table below maps ITSEC evaluation assurance levels to Common Criteria EALs. EAL's are defined in the Common Criteria Standard – part 3.

Criteria	Assurance level							
Common Criteria	N/A	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
ITSEC	E0	N/A	E1	E2	E3	E4	E5	E6

Recognition arrangements

12.1.16. The AISEP programme has a number of recognition arrangements regarding evaluated products. Before choosing a product that has **not** been evaluated by the AISEP, agencies are encouraged to contact the GCSB to enquire whether the product will be recognised for New Zealand use once it has complete evaluation in a foreign scheme.

12.1.17. Two such recognition arrangements are for the Common Criteria Recognition Arrangement up to the assurance level of EAL2 with the lifecycle flaw remediation augmentation and for degausser products listed on the National Security Agency/Central Security Service's EPLD.

Australasian Information Security Evaluation Program (AISEP)

12.1.18. The AISEP exists to ensure that a range of evaluated products are available to meet the needs of Australian and New Zealand Government agencies.

12.1.19. The AISEP performs the following functions:

- evaluation and certification of products using the Common Criteria;
- continued maintenance of the assurance of evaluated products; and
- recognition of products evaluated by a foreign scheme with which the AISEP has a mutual recognition agreement (generally the Common Criteria Recognition Agreement – CCRA).

Protection Profiles

12.1.20. A Protection Profile (PP) describes the security functionality that must be included in a Common Criteria evaluation to meet a range of defined threats. PPs also define the activities to be taken to assess the security functions of a product. Agencies can have confidence that a product evaluated against an AISEP or GCSB approved PP addresses the defined threats. Approved PPs are published on the AISEP Evaluated Product List.

12.1.21. The introduction of PP's is to reduce the time required for evaluation, compared with the traditional approach to allow the AISEP to keep pace with the rapid evolution, production and release of security products and updates. Cryptographic security functionality is included in the scope of evaluation against an approved Protection Profile.

12.1.22. To facilitate the transition to AISEP approved Protection Profiles, a cap of Evaluation Assurance Level (EAL) 2 applies for all traditional AISEP (EAL based evaluations), including for technologies with no existing approved Protection Profile. EAL 2 is considered to represent a sensible trade-off between completion time and meaningful security assurance gains.

12.1.23. Evaluations conducted in other nations' Common Criteria schemes will continue to be recognised by the GCSB under the AISEP.

12.1.24. Some High Assurance evaluations continue to be conducted in European Approved Testing Facilities and use the EAL rating scheme. ASD run an independent High Assurance Evaluation scheme which is not related to AISEP or an EAL rating.

12.1.25. It is important that Agencies check the evaluation has examined the security enforcing functions by reviewing the target of evaluation/security target and other testing documentation.

12.1.26. The UK utilises several product evaluation schemes such as the CESG Assisted Products Service (CAPS), CESG Assured Service (CAS) and IT Security Evaluation Criteria (ITSEC). Agencies should consult the GCSB if further clarity on the utilisation of these evaluation schemes and products is required.

Product Selection

12.1.27. The diagram in Figure 5 below summarises the product selection process described in this chapter.

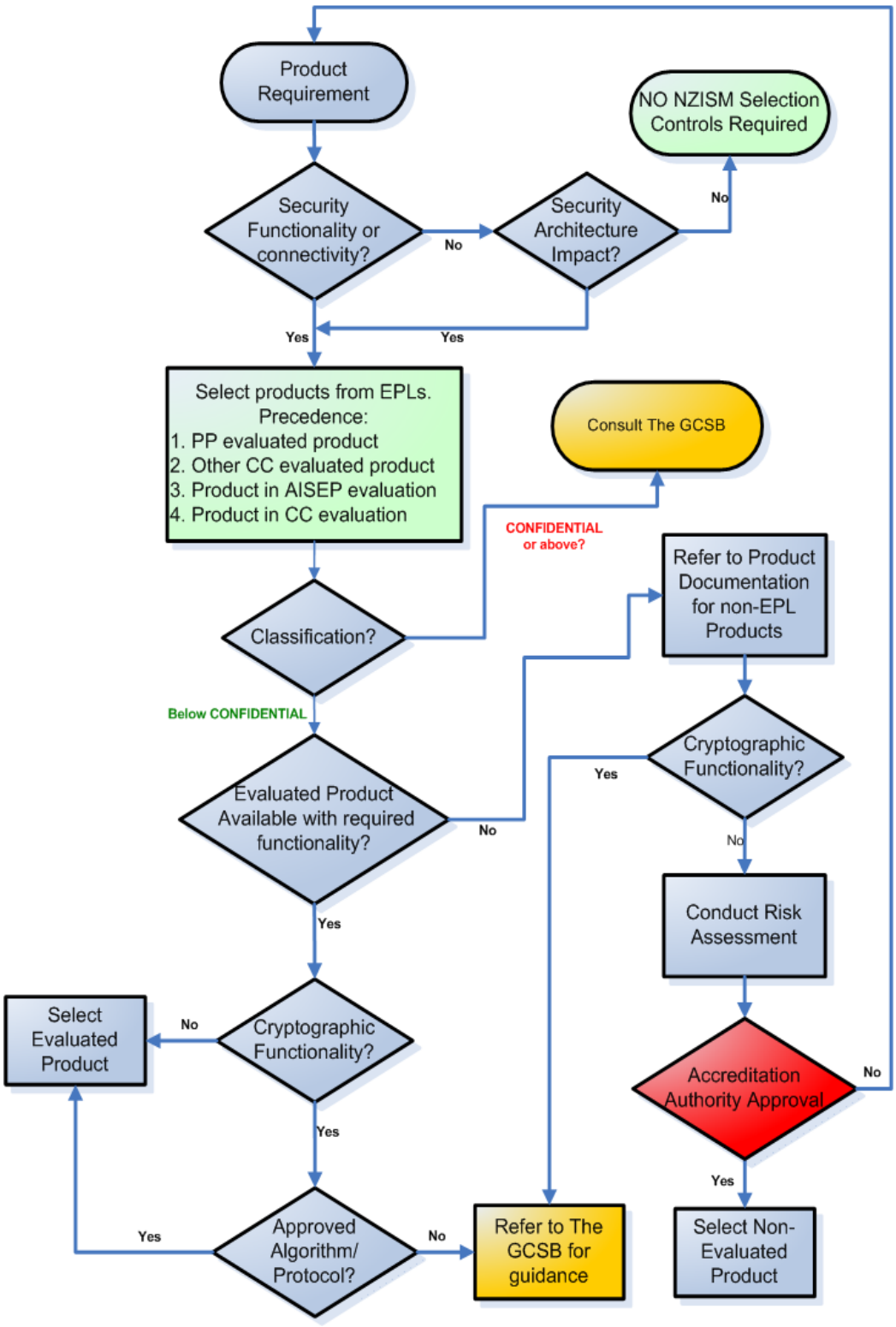


Figure 5 – Product Selection Guide

References

Topic	Publisher	Source
Evaluated Products List (EPL)	ASD	http://www.asd.gov.au/infosec/epl/index.php
Australian Information Security Evaluation Program (AISEP)	ASD	http://www.asd.gov.au/infosec/aisep/index.htm
Common Criteria	CC	http://www.commoncriteriaportal.org
CESG Service Catalogue	CESG	https://www.cesg.gov.uk/products-and-services
National Information Assurance Partnership (NIAP)	NIAP	https://ww.niap-ccevs.org
Government Rules of Sourcing	Ministry of Business Innovation & Employment (MBIE)	http://www.procurement.govt.nz/procurement/pdf-library/agencies/rules-of-sourcing/government-rules-of-sourcing-April-2013.pdf

PSR references

Reference	Title	Source
PSR Mandatory Requirements	GOV8, INFOSEC5 and PHYSEC6	http://www.protectivesecurity.govt.nz
PSR content protocols and requirements sections	Security Requirements of Outsourced Services and Functions New Zealand Government Information in Outsourced or Offshore ICT Arrangements	http://www.protectivesecurity.govt.nz

Rationale & Controls

12.1.28. Evaluated product selection preference order

12.1.28.R.01. Rationale

In selecting products for use, agencies should note that completed evaluations provide greater assurance than those products that are still undergoing evaluation or have not completed any formal evaluation activity. This assurance gradation is reflected in the preference order for selecting security products. If an agency selects a product that is ranked lower in the preference order, the justification for this decision MUST be recorded.

12.1.28.R.02. Rationale

For products that are currently in evaluation, agencies should select those that are undergoing evaluation through AISEP in preference to those being conducted in a recognised foreign scheme. If a major vulnerability is found during the course of an AISEP evaluation, the GCSB may advise agencies on appropriate risk reduction strategies.

12.1.28.R.03. Rationale

It is important to recognise that a product that is under evaluation has not, and might never, complete all relevant evaluation processes.

12.1.28.R.04. Rationale

Agencies should be aware that while this section provides a product selection preference order, policy stated elsewhere in this manual, or product specific advice from the GCSB, could override this standard by specifying more rigorous requirements for particular functions and device use.

12.1.28.R.05. Rationale

Additionally, where an EAL rating is mandated for a product to perform a cryptographic function for the protection of data at rest or in transit, as specified within Chapter 17 – Cryptography, products that have not completed an Approved Evaluation do not satisfy the requirement.

12.1.28.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST select products in the following order of preference:

- a protection profile (PP) evaluated product;
- products having completed an evaluation through the AISEP or recognised under the Common Criteria Recognition Arrangement (CCRA);
- products in evaluation in the AISEP;
- products in evaluation in a scheme where the outcome will be recognised by the GCSB when the evaluation is complete; or
- If products do not fall within any of these categories, contact the GCSB.

12.1.28.C.02. Control: System Classification(s): C, S, TS; Compliance: MUST

When choosing a product, agencies MUST document the justification for any decision to choose a product that is still in evaluation and accept any security risk introduced by the use of such a product.

12.1.28.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD select products in the following order of preference:

- a protection profile (PP) evaluated product;
- products having completed an evaluation through the AISEP or recognised under the Common Criteria Recognition Arrangement (CCRA);
- products in evaluation in the AISEP;
- products in evaluation in a scheme where the outcome will be recognised by the GCSB when the evaluation is complete; or
- If products do not fall within any of these categories, normal selection criteria (such as functionality and security) will apply.

12.1.29. Evaluated product selection

12.1.29.R.01. Rationale

A product listed on the EPL might not meet the security requirements of an agency. This could occur for a number of reasons, including that the scope of the evaluation is inappropriate for the intended use or the operational environment differs from that assumed in the evaluation. As such, an agency should ensure that a product is suitable by reviewing all available documentation. In the case of Common Criteria certified products, this documentation includes the protection profile, target of evaluation, security target, certification report, consumer guide and any qualifications and limitations contained in the entry on the EPL.

12.1.29.R.02. Rationale

Products that are in evaluation will not have a certification report and may not have a published security target. A protection profile will, as a rule, exist. A draft security target can be obtained from the GCSB for products that are in evaluation through AISEP. For products that are in evaluation through a foreign scheme, the vendor can be contacted directly for further information.

12.1.29.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD select products that have their desired security functionality within the scope of the product's evaluation and are applicable to the agency's intended environment.

12.1.30. Product specific requirements

12.1.30.R.01. Rationale

Whilst this manual may recommend a minimum level of assurance in the evaluation of a product's security functionality not all evaluated products may be found suitable for their intended purpose even if they pass their Common Criteria evaluation. Typically such products will have cryptographic functionality that is not covered in sufficient depth under the Common Criteria. Where products have specific usage requirements, in addition to this manual, or supersede requirements in this manual, they will be outlined in the product's consumer guide.

12.1.30.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST check consumer guides for products, where available, to determine any product specific requirements.

12.1.30.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Where product specific requirements exist in a consumer guide, agencies MUST comply with the requirements outlined in the consumer guide.

12.1.30.C.03. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies selecting high assurance products and HGCE MUST contact the GCSB and comply with any product specific requirements, before any purchase is made.

12.1.31. Sourcing non-evaluated software

12.1.31.R.01. Rationale

Software downloaded from websites on the Internet can contain malicious code or malicious content that is installed along with the legitimate software. Agencies need to confirm the integrity of the software they are installing before deploying it on a system to ensure that no unintended software is installed at the same time.

12.1.31.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD:

- obtain software from verifiable sources and verify its integrity using vendor supplied checksums; and
- validate the software's interaction with the operating systems and network within a test environment prior to use on operational systems.

12.1.32. Delivery of evaluated products

12.1.32.R.01. Rationale

It is important that agencies ensure that the selected product is the actual product received. If the product differs from the evaluated version, then NO assurance can be gained from an evaluation being previously performed.

12.1.32.R.02. Rationale

For products evaluated under the ITSEC or the Common Criteria scheme at EAL2 or higher, delivery information is available from the developer in the delivery procedures document.

12.1.32.R.03. Rationale

For products that do not have evaluated delivery procedures, it is recommended that agencies assess whether the vendor's delivery procedures are sufficient to maintain the integrity of the product.

12.1.32.R.04. Rationale

Other factors that the assessment of the delivery procedures for products might consider include:

- the intended environment of the product;
- likely attack vectors;
- the types of attackers that the product will defend against;
- the resources of any potential attackers;
- the likelihood of an attack;
- the level of importance of maintaining confidentiality of the product purchase; and
- the level of importance of ensuring adherence to delivery timeframes.

12.1.32.R.05. Rationale

Delivery procedures can vary greatly from product to product. For most products the standard commercial practice for packaging and delivery can be sufficient for agencies requirements. More secure delivery procedures can include measures to detect tampering or masquerading. Some examples of specific security measures include tamper evident seals, cryptographic checksums and signatures, and secure transportation.

12.1.32.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies procuring high assurance products and HGCE MUST contact the GCSB and comply with any product specific delivery procedures.

12.1.32.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that products are delivered in a manner consistent with any delivery procedures defined in associated documentation.

12.1.33. Delivery of non-evaluated products

12.1.33.R.01. Rationale

When a non-evaluated product is purchased agencies should determine if the product has arrived in a state that they were expecting it to and that there are no obvious signs of tampering.

12.1.33.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that products purchased without the delivery assurances provided through the use of formally evaluated procedures are delivered in a manner that provides confidence that they receive the product that they expect to receive in an unaltered state, including checking:

- any labelling changes;
- any damage; and
- any signs of tampering.

12.1.34. Leasing arrangements

12.1.34.R.01. Rationale

Agencies should consider security and policy requirements when entering into a leasing agreement for IT equipment in order to avoid potential information security incidents during maintenance, repairs or disposal processes.

12.1.34.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that leasing agreements for IT equipment takes into account the:

- difficulties that could be encountered when the equipment needs maintenance;
- control of remote maintenance, software updates and fault diagnosis;
- if the equipment can be easily sanitised prior to its return; and
- the possible requirement for destruction if sanitisation cannot be performed.

12.1.35. Ongoing maintenance of assurance

12.1.35.R.01. Rationale

Developers that have demonstrated a commitment to ongoing maintenance or evaluation are more likely to be responsive to ensuring that security patches are independently assessed.

12.1.35.R.02. Rationale

A vendor's commitment to assurance continuity can be gauged through the number of evaluations undertaken and whether assurance maintenance has been performed on previous evaluations.

12.1.35.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD choose products from developers that have made a commitment to the ongoing maintenance of the assurance of their product.

12.2. Product Installation and Configuration

Objective

12.2.1. Evaluated products use evaluated configurations.

Context

Scope

12.2.2. This section covers information on installing and configuring products providing security functionality. It does not provide information on the installation and configuration of general products or physical security products.

Evaluated configuration

12.2.3. A product is considered to be operating in its evaluated configuration if:

- functionality is used that was within the scope of the evaluation and implemented in the specified manner;
- only patches that have been assessed through a formal assurance continuity process have been applied; and
- the environment complies with assumptions or organisational security policies stated in the product's security target or similar document.

Unevaluated configuration

12.2.4. A product is considered to be operating in an unevaluated configuration when it does not meet the requirements of an evaluated configuration.

Rationale & Controls

12.2.5. Installation and configuration of evaluated products

12.2.5.R.01. Rationale

An evaluation of products provides assurance that the product will work as expected with a clearly defined set of constraints. These constraints, defined by the scope of the evaluation, generally consist of what security functionality can be used, and how the products are configured and operated.

12.2.5.R.02. Rationale

Using an evaluated product in manner which it was not intended could result in the introduction of new threats and vulnerabilities that were not considered by the initial evaluation.

12.2.5.R.03. Rationale

For products evaluated under the Common Criteria and ITSEC, information is available from the developer in the product's installation, generation and startup documentation. Further information is also available in the security target and certification report.

12.2.5.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that high assurance products and HGCE are installed, configured, operated and administered in accordance with all product specific policy.

12.2.5.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD install, configure, operate and administer evaluated products in accordance with available documentation resulting from the product's evaluation.

12.2.6. Use of evaluated products in unevaluated configurations

12.2.6.R.01. Rationale

To ensure that a product will still provide the assurance desired by the agency when used in a manner for which it was not intended, a security risk assessment MUST be conducted upon the altered configuration. The further that a product deviates from its evaluated configuration, the less assurance can be gained from the evaluation.

12.2.6.R.02. Rationale

Given the potential threat vectors and the value of the classified information being protected, high assurance products and HGCE MUST be configured in accordance with the GCSB's guidelines.

12.2.6.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies wishing to use a product in an unevaluated configuration MUST undertake a security risk assessment including:

- the necessity of the unevaluated configuration;
- testing of the unevaluated configuration; and
- the environment in which the unevaluated product is to be used.

12.2.6.C.02. Control: System Classification(s): All Classifications; Compliance: MUST NOT

High assurance products and HGCE MUST NOT be used in unevaluated configurations.

12.3. Product Classifying and Labelling

Objective

12.3.1. IT equipment is classified and appropriately labelled.

Context

Scope

12.3.2. This section covers information relating to the classification and labelling of both evaluated and non-evaluated IT equipment.

Non-essential labels

12.3.3. Non-essential labels are labels other than classification and asset labels.

Rationale & Controls

12.3.4. Classifying IT equipment

12.3.4.R.01. Rationale

Much of today's technology incorporates an internal data storage capability. When media is used in IT equipment there is no guarantee that the equipment has not automatically accessed classified information from the media and stored it locally to the device, without the knowledge of the system user. As such, the IT equipment needs to be afforded the same degree of protection as that of the associated media.

12.3.4.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST classify IT equipment based on the highest classification of information the equipment and any associated media within the equipment, are approved for processing, storing or communicating.

12.3.5. Labelling IT equipment

12.3.5.R.01. Rationale

The purpose of applying protective markings to all assets in a secure area is to reduce the likelihood that a system user will accidentally input classified information into another system residing in the same area that is of a lower classification than the information itself.

12.3.5.R.02. Rationale

Applying protective markings to assets also assists in determining the appropriate usage, sanitisation, disposal or destruction requirements of the asset based on its classification. This is of particular importance in data centres and computer rooms.

12.3.5.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST clearly label all IT equipment capable of storing or processing classified information, with the exception of HGCE, with the appropriate protective marking.

12.3.5.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST clearly label all IT equipment in data centres or computer rooms with an asset identification and the level of classification to which that equipment has been accredited.

12.3.6. Labelling high assurance products

12.3.6.R.01. Rationale

High assurance products often have tamper-evident seals placed on their external surfaces. To assist system users in noticing changes to the seals, and to prevent functionality being degraded, agencies MUST limit the use of non-essential labels.

12.3.6.C.01. Control: System Classification(s): All Classifications; Compliance: MUST NOT

Agencies MUST NOT have any non-essential labels applied to external surfaces of high assurance products.

12.3.7. Labelling HGCE

12.3.7.R.01. Rationale

HGCE often have tamper-evident seals placed on their external surfaces. To assist system users in noticing changes to the seals, and to prevent functionality being degraded, agencies MUST only place seals on equipment with GCSB approval.

12.3.7.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD seek GCSB authorisation before applying labels to external surfaces of HGCE.

12.4. Product Patching and Updating

Objective

12.4.1. To ensure security patches are applied in a timely fashion to manage software and firmware corrections, vulnerabilities and performance risks.

Context

Scope

12.4.2. This section covers information on patching both evaluated and non-evaluated software and IT equipment.

Rationale & Controls

12.4.3. Vulnerabilities and patch availability awareness

12.4.3.R.01. Rationale

It is important that agencies monitor relevant sources for information about new vulnerabilities and security patches. This way, agencies can take pro-active steps to address vulnerabilities in their systems.

12.4.3.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD monitor relevant sources for information about new vulnerabilities and security patches for software and IT equipment used by the agency.

12.4.4. Patching vulnerabilities in products

12.4.4.R.01. Rationale

The assurance provided by an evaluation is related to the date at which the results were issued. Over the course of a normal product lifecycle, patches are released to address known security vulnerabilities. Applying these patches should be considered as part of an agency's overall risk management strategy.

12.4.4.R.02. Rationale

Given the potential threat vectors and the value of the classified information being protected, high assurance products MUST NOT be patched by an agency without specific direction from the GCSB. If a patch is released for a high assurance product, the GCSB will conduct an assessment of the patch and might revise the product's usage guidance. Likewise, for patches released for HGCE, the GCSB will subsequently conduct an assessment of the cryptographic vulnerability and might revise usage guidance in the consumer guide for the product.

12.4.4.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST apply all critical security patches as soon as possible and within two (2) days of the release of the patch or update.

12.4.4.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST implement a patch management strategy, including an evaluation or testing process.

12.4.4.C.03. Control: System Classification(s): All Classifications; Compliance: MUST NOT

Agencies MUST NOT patch high assurance products or HGCE without the patch being approved by the GCSB.

12.4.4.C.04. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD apply all critical security patches as soon as possible and preferably within two (2) days of the release of the patch or update.

12.4.4.C.05. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD apply all non-critical security patches as soon as possible.

12.4.4.C.06. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that security patches are applied through a vendor recommended patch or upgrade process.

12.4.5. When security patches are not available

12.4.5.R.01. **Rationale**

When a security patch is not available for a known vulnerability, there are a number of approaches to reducing the risk to a system. This includes resolving the vulnerability through alternative means, preventing exploitation of the vulnerability, containing the exploit or implementing measures to detect attacks attempting to exploit the vulnerability.

12.4.5.C.01. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

Where known vulnerabilities cannot be patched, or security patches are not available, agencies SHOULD implement:

- controls to resolve the vulnerability such as:
    - disable the functionality associated with the vulnerability though product configuration;
    - ask the vendor for an alternative method of managing the vulnerability;
    - install a version of the product that does not have the identified vulnerability;
    - install a different product with a more responsive vendor; or
    - engage a software developer to correct the software.

- controls to prevent exploitation of the vulnerability including:
    - apply external input sanitisation (if an input triggers the exploit);
    - apply filtering or verification on the software output (if the exploit relates to an information disclosure);
    - apply additional access controls that prevent access to the vulnerability; or
    - configure firewall rules to limit access to the vulnerable software.

- controls to contain the exploit including:
    - apply firewall rules limiting outward traffic that is likely in the event of an exploitation;
    - apply mandatory access control preventing the execution of exploitation code; or
    - set file system permissions preventing exploitation code from being written to disk;
    - white and blacklisting to prevent code execution; and

- controls to detect attacks including:
    - deploy an IDS;
    - monitor logging alerts; or
    - use other mechanisms as appropriate for the detection of exploits using the known vulnerability.

- controls to prevent attacks including:
    - deploy an IPS or HIPS; or
    - use other mechanisms as appropriate for the diversion of exploits using the known vulnerability, such as honey pots and Null routers.

12.4.6. Firmware updates

12.4.6.R.01. Rationale

As firmware provides the underlying functionality for hardware it is essential that the integrity of any firmware images or updates are maintained.

12.4.6.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that any firmware updates are performed in a manner that verifies the integrity and authenticity of the source and of the updating process.

12.4.7. Unsupported products

12.4.7.R.01. Rationale

Once a cessation date for support is announced for software or IT equipment, agencies will increasingly find it difficult to protect against vulnerabilities found in the software or IT equipment as no security patches will be made available by the manufacturer. Once a cessation date for support is announced agencies should investigate new solutions that will be appropriately supported and establish a plan to implement the new solution.

12.4.7.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD assess the security risk of using software or IT equipment when a cessation date for support is announced or when the product is no longer supported by the developer.

12.5. Product Maintenance and Repairs

Objective

12.5.1. Products are repaired by cleared or appropriately escorted personnel.

Context

Scope

12.5.2. This section covers information on maintaining and repairing both evaluated and non-evaluated IT equipment.

Rationale & Controls

12.5.3. Maintenance and repairs

12.5.3.R.01. Rationale

Making unauthorised repairs to high assurance products or HGCE can impact the integrity of the product or equipment.

12.5.3.R.02. Rationale

Using cleared technicians on-site at an agency's facilities is considered the most desired approach to maintaining and repairing IT equipment. This ensures that if classified information is disclosed during the course of maintenance or repairs, the technicians are aware of the protection requirements for the information.

12.5.3.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST seek GCSB approval before undertaking any repairs to high assurance products or HGCE.

12.5.3.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Maintenance and repairs of IT equipment containing media SHOULD be carried out on-site by an appropriately cleared technician.

12.5.4. Maintenance and repairs by an uncleared technician

12.5.4.R.01. Rationale

Agencies choosing to use uncleared technicians to maintain or repair IT equipment on-site at an agency's facilities, or off-site at a company's facilities, should be aware of the requirement for cleared personnel to escort the uncleared technicians during maintenance or repair activities.

12.5.4.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

If an uncleared technician is used to undertake maintenance or repairs of IT equipment, the technician MUST be escorted by someone who:

- is appropriately cleared and briefed;
- takes due care to ensure that classified information is not disclosed;
- takes all responsible measures to ensure the integrity of the equipment; and
- has the authority to direct the technician.

12.5.4.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

If an uncleared technician is used to undertake maintenance or repairs of IT equipment, agencies SHOULD sanitise and reclassify or declassify the equipment and associated media before maintenance or repair work is undertaken.

12.5.4.C.03. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that the ratio of escorts to uncleared technicians allows for appropriate oversight of all activities.

12.5.4.C.04. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

If an uncleared technician is used to undertake maintenance or repairs of IT equipment, the technician SHOULD be escorted by someone who is sufficiently familiar with the product to understand the work being performed.

12.5.5. Off-site maintenance and repairs

12.5.5.R.01. **Rationale**

Agencies choosing to have IT equipment maintained or repaired off-site need to be aware of requirements for the company's off-site facilities to be approved to process and store the products at the appropriate classification.

12.5.5.R.02. **Rationale**

Agencies choosing to have IT equipment maintained or repaired off-site can sanitise, declassify or lower the classification of the product prior to transport and subsequent maintenance or repair activities, to lower the physical transfer, processing and storage requirements.

12.5.5.C.01. **Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies having IT equipment maintained or repaired off-site MUST ensure that the physical transfer, processing and storage requirements are appropriate for the classification of the product and are maintained at all times.

12.5.6. Maintenance and repair of IT equipment from secure areas

12.5.6.R.01. **Rationale**

Where equipment is maintained or repaired offsite, agencies should identify any co-located equipment of a higher classification. This higher classification equipment may be at risk of compromise from modifications or repairs to the lower classification equipment.

12.5.6.C.01. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

Offsite repairs and maintenance SHOULD treat all equipment in accordance with the requirements for the highest classification of information processed, stored or communicated in the area that the equipment will be returned to.

12.5.6.C.02. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD conduct or arrange to have technical inspections conducted on all equipment returned to the secure area after maintenance or repair.

12.6. Product Sanitisation and Disposal

Objective

12.6.1. IT equipment is sanitised and disposed of in an approved manner.

Context

Scope

12.6.2. This section covers information on sanitising and disposing of both evaluated and non-evaluated IT equipment. Additional information on the sanitisation, destruction and disposal of media can be found in Chapter 13 – Decommissioning and Disposal.

12.6.3. Media typically found within IT equipment are electrostatic memory devices such as laser printer cartridges and photocopier drums, non-volatile magnetic memory such as hard disks, non-volatile semi-conductor memory such as flash cards and volatile memory such as RAM cards.

Rationale & Controls

12.6.4. Sanitisation or destruction of IT equipment

12.6.4.R.01. Rationale

In order to prevent the disclosure of classified information into the public domain agencies will need to ensure that IT equipment is either sanitised or destroyed before being declassified and authorised for released into the public domain.

12.6.4.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST sanitise or destroy, then declassify, IT equipment containing media before disposal.

12.6.4.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

IT equipment and associated media that have processed or stored NZEO information, and cannot be sanitised, MUST be returned to New Zealand for sanitisation or destruction, declassification and disposal.

12.6.5. Disposal of IT equipment

12.6.5.R.01. Rationale

When disposing of IT equipment, agencies need to sanitise or destroy and subsequently declassify any media within the product that are capable of storing classified information. Once the media have been removed from the product it can be considered sanitised. Following subsequent approval for declassification from the owner of the information previously processed by the product, it can be disposed of by the agency.

12.6.5.R.02. Rationale

The GCSB provides specific advice on how to securely dispose of high assurance products, HGCE and TEMPEST rated equipment. There are a number of security risks that can occur due to improper disposal, including providing an attacker with an opportunity to gain insight into government capabilities.

12.6.5.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST have a documented process for the disposal of IT equipment.

12.6.5.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST contact the GCSB and comply with any requirements for the disposal of high assurance products.

12.6.5.C.03. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST contact the GCSB and comply with any requirements for the disposal of HGCE.

12.6.5.C.04. **Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST contact GCSB and comply with any requirements for the disposal of TEMPEST rated IT equipment or if the equipment is non-functional.

12.6.5.C.05. **Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST formally sanitise and then authorise the disposal of IT equipment, or waste, into the public domain.

12.6.6. Sanitising printer cartridges and copier drums

12.6.6.R.01. **Rationale**

Electrostatic drums can retain an image of recently printed documents providing opportunity for unauthorised access to information. Some printer cartridges may have integrated drums. Printing random text with no blank areas on each colour printer cartridge or drum ensures that no residual information will be kept on the drum or cartridge.

12.6.6.C.01. **Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST print at least three pages of random text with no blank areas on each colour printer cartridge with an integrated drum or separate copier drum.

12.6.6.C.02. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD print at least three pages of random text with no blank areas on each colour printer cartridge with an integrated drum or separate copier drum.

12.6.7. Destroying printer cartridges and copier drums

12.6.7.R.01. **Rationale**

When printer cartridges with integrated copier drums or discrete drums cannot be sanitised due to a hardware failure, or when they are empty, there is no other option available but to destroy them.

12.6.7.C.01. **Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies unable to sanitise printer cartridges with integrated copier drums or discrete copier drums, MUST destroy the cartridge or drum.

12.6.7.C.02. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies unable to sanitise printer cartridges with integrated copier drums or discrete copier drums, SHOULD destroy the cartridge or drum.

12.6.8. Disposal of televisions and monitors

12.6.8.R.01. Rationale

Turning up the brightness to the maximum level on video screens will allow agencies to easily determine if information has been burnt in or persists upon the screen.

12.6.8.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST visually inspect video screens by turning up the brightness to the maximum level to determine if any classified information has been burnt into or persists on the screen.

12.6.9. Sanitising televisions and monitors

12.6.9.R.01. Rationale

All types of video screens are capable of retaining classified information on the screen if appropriate mitigation measures are not taken during the lifetime of the screen. CRT monitors and plasma screens can be affected by burn-in whilst LCD screens can be affected by image persistence.

12.6.9.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST attempt to sanitise video screens with minor burn-in or image persistence by displaying a solid white image on the screen for an extended period of time.

12.7. Supply Chain

Objective

12.7.1. Technology supply chains are established and managed to ensure continuity of supply and protection of sensitive related information.

Context

12.7.2. A supply chain is the movement of materials as they move from their source (raw materials) through manufacture to the end customer. A supply chain can include materials acquisition, purchasing, design, manufacturing, warehousing, transportation, customer service, and supply chain management. It requires people, information and resources to move a product from manufacturer to supplier to customer. Every supply chain carries some risk which may include product protection; counterfeit products and goods and defective products. ICT supply chains are invariably global and complex.

12.7.3. Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (e.g. through supply contracts, interagency agreements, lines of business arrangements, service-level agreements), licensing agreements, and/or supply chain exchanges. The growing use of external service providers and new relationships being established with those providers present new and difficult challenges for organisations, especially in the area of information system security. These challenges include:

- Defining the types of external information system services provided to organisations;
- Describing how those external services are protected; and
- Obtaining the necessary assurances that the risks to organisational operations and assets, individuals, other organisations, and national security arising from the use of the external services are acceptable.

12.7.4. The degree of confidence that the risk from using external services is at an acceptable level depends on the assurance external organisations provide and trust that organisations place in external service providers. In some cases, the level of trust is based on the amount of direct control organisations are able to exert on external service providers in the use of security controls and assurance on the effectiveness of those controls.

12.7.5. The level of control is usually established by the terms and conditions of the contracts or service-level agreements with the external service providers and can range from extensive control (e.g., negotiating contracts or agreements that specify detailed security requirements for the providers) to very limited control (e.g., using contracts or service-level agreements to obtain commodity services such as commercial telecommunications services).

12.7.6. From an Information Assurance viewpoint, there are five key aspects to supply chain risk:

1. Protection of sensitive information and systems;
2. Continuity of supply;
3. Product assurance;
4. Security validation; and
5. National Procurement Policy

Protection of sensitive information and systems

12.7.7. This relates to the security of the supply chain, products and information relating to the intended use, purchaser, location and type of equipment.

Continuity of supply

12.7.8. This is the traditional set of risks associated with supply chain. As supply chains have globalised and components are sourced from a number of countries, a disruption to supply may have a global effect.

Product assurance

12.7.9. This relates to assurance that the product, technology or device performs as designed and specified and includes the provenance of the product, equipment, or device.

Security validation

12.7.10. Security validation checks the performance and security of the equipment. The security design elements and features of the equipment or product will need to be separately considered from any operational drivers.

National procurement policy

12.7.11. All agencies are required to follow the guidance of the Government Rules of Procurement. Some exemptions are permitted under Rule 13 including that of security, "essential security interests: Measures necessary for the protection of essential security interests, procurement indispensable for national security or for national defence…". Care must be taken to follow these rules wherever possible.

Scope

12.7.12. This manual provides additional guidance for managing supply chain security risks associated with the acquisition (lease or purchase) of ICT equipment or services for use in NZ Government systems.

References

12.7.13. While NOT an exhaustive list, further information on procurement and supply chain can be found at:

Title	Publisher	Source
Government Use of Offshore Information and Communication Technologies (ICT) Service Providers - Advice on Risk Management April 2009	State Services Commission	http://ict.govt.nz/assets/ICT-System-Assurance/offshore-ICT-service-providers-april-2009.pdf
The new Government Rules of Sourcing	Procurement.govt.NZ	http://www.business.govt.nz/procurement/for-agencies/key-guidance-for-agencies/the-new-government-rules-of-sourcing
Government Rules of Sourcing - Rules for planning your procurement, approaching the market and contracting	Ministry of Business Innovation and Employment	http://www.business.govt.nz/procurement/pdf-library/agencies/rules-of-sourcing/government-rules-of-sourcing-April-2013.pdf
Special Publication 800-161, Supply Chain Risk Management	Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology (NIST)	http://csrc.nist.gov/publications/drafts/800-161/sp800_161_draft.pdf
Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations	NIST	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
NISTIR 7622, Notional Supply Chain Risk Practices for Federal Information Systems	NIST	http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf
Commercial Procurement & Relationships	UK Cabinet Office	https://www.gov.uk/government/organisations/cabinet-office
CIO Council Government ICT Offshoring (International Sourcing) Guidance	UK Cabinet Office	https://www.gov.uk/government/publications/government-ict-offshoring-international-sourcing-guidance

Reference	Publisher	Source
Commonwealth Procurement Rules	Department of Finance and Deregulation (Financial Management Group)	http://www.finance.gov.au/procurement/docs/cpr_commonwealth_procurement_rules_july_2012.pdf
ISO 31000:2009, Risk management – Principles and guidelines	ISO / IEC Standards NZ	http://www.iso.org http://www.standards.co.nz
HB 231:2004, Information Security Risk Management Guidelines.	Standards NZ	http://www.standards.co.nz
ISO Guide 73:2009, Risk management - Vocabulary	ISO / IEC Standards NZ	http://www.iso.org http://www.standards.co.nz
ISO/IEC 31010:2009, Risk management – Risk assessment techniques	ISO / IEC Standards NZ	http://www.iso.org http://www.standards.co.nz
ISO/IEC_27002:2013, Information technology — Security techniques — Code of practice for information security controls	ISO / IEC Standards NZ	http://www.iso27001security.com/html/27002.html http://www.standards.co.nz
ISO/IEC_27005:2012 Information Technology – Security Techniques - Information Security Risk Management	ISO / IEC Standards NZ	http://www.iso27001security.com/html/27005.html http://www.standards.co.nz
ISO 28000 supply chain security management system standard	ISO / IEC Standards NZ	http://www.iso.org http://www.standards.co.nz

Rationale & Controls

12.7.14. Risk Management

12.7.14.R.01. Rationale

ICT supply chains can introduce particular risks to an agency. In order to manage these risks, in addition to other identified ICT risks, supply chain risks are incorporated into an agency's assessment of risk and the Security Risk Management Plan (SRMP). Identified risks are managed through the procurement process and through technical checks and controls (See Section 5.3 – Security Risk Management Plans and Chapter 4 – System Certification and Accreditation).

12.7.14.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD incorporate the consideration of supply chain risks into an organisation-wide risk assessment and management process.

12.7.14.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD monitor supply chain risks on an ongoing basis and adjust mitigations and controls appropriately.

12.7.14.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD follow the Government Rules of Procurement.

12.7.15. Contractor or Supplier Capability

12.7.15.R.01. Rationale

Agencies can assess the capability of a contractor and any subcontractors to meet their security of information, supply and product requirements.

12.7.15.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD require tenderers and contractors to provide information:

- identifying any restrictions on the disclosure, transfer or use of technology arising out of export controls or security arrangements; and
- demonstrating that their supply chains comply with the security of supply requirements set out in the contract documents.

12.7.15.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD request information from contractors and subcontractors to assess their ability to protect information.

12.7.16. Security of Information

12.7.16.R.01. Rationale

After conducting a risk assessment, agencies and suppliers have the means and capability to protect classified information throughout the tendering and contracting process.

12.7.16.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST include contractual obligations on all contractors and subcontractors to safeguard information throughout the tendering and contracting procedure.

12.7.16.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD include contractual obligations to safeguard information throughout the tendering and contracting procedure.

12.7.16.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD reject contractors and subcontractors where they do not possess the necessary reliability to exclude risks to national security; or have breached obligations relating to security of information during a previous contract in circumstances amounting to grave misconduct.

12.7.17. Continuity of Supply

12.7.17.R.01. Rationale

You can also require suppliers to provide commitments on the continuity of supply. These can include commitments from the supplier to ensure:

- delivery time;
- stock levels;
- visibility of the supply chain; and
- supply chain resilience.

12.7.17.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that changes in their supply chain during the performance of the contract will not adversely affect the continuity of supply requirements.

12.7.18. Product Assurance

12.7.18.R.01. Rationale

In addition to the product selection and acquisition guidance in this section, agencies are able to identify and mitigate risks through supply chain visibility, provenance, security validation and pre-installation tests and checks.

12.7.18.R.02. Rationale

Agencies, with the cooperation of their suppliers, should establish the provenance of any products and equipment. Provenance is defined as a record of the origin, history, specification changes and supply path of the products or equipment.

12.7.18.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST require suppliers and contractors to provide the provenance of any products or equipment.

12.7.18.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD require suppliers and contractors to provide the provenance of any products or equipment.

12.7.19. Security validation

12.7.19.R.01. Rationale

Validation of the performance and security of the equipment is a vital part of the ongoing integrity and security of agency systems. The security design elements and features of the equipment or product will need to be separately considered from any operational drivers. Where compromises in security performance, capability or functionality are apparent, additional risk mitigation, controls and countermeasures may be necessary.

12.7.19.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD validate the security of the equipment against security performance, capability and functionality requirements.

12.7.19.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Where deficiencies in security performance, capability and functionality are identified, agencies SHOULD implement additional risk mitigation measures.

12.7.20. Pre-Installation Tests and Checks

12.7.20.R.01. Rationale

An essential part of quality and security assurance is the delivery inspection, pre-installation and functional testing of any equipment. In particular, large systems that integrate equipment from different suppliers or that have specialised configuration and operational characteristics may require additional testing to provide assurance that large scale disruptions and security compromises are avoided.

12.7.20.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST consult with the GCSB on pre-installation, security verification and related tests before the equipment is used in an operational system.

12.7.20.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD inspect equipment on receipt for any obvious signs of tampering, relabelling or damage.

12.7.20.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD inspect equipment on receipt and test the operation before installation.

12.7.20.C.04. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD conduct installation verification and related tests before the equipment is used in an operational system.

12.7.20.C.05. Control: System Classification(s): All Classifications; Compliance: SHOULD

Where any software, firmware or other forms of programme code are required for the initialisation, operation, servicing or maintenance of the equipment, malware checks SHOULD be conducted before the equipment is installed in an operational system.

12.7.21. Equipment Servicing

12.7.21.R.01. Rationale

Some larger or complex systems can have dependencies on particular infrastructures, equipment, software or configurations. Although these types of systems can be less flexible in responding to the rapid changes in technologies, the risks are outweighed by the functionality of the system. In such cases, the continuing support and maintenance of essential components is vital.

12.7.21.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

For equipment that is expected to have an extended operational life in a critical system, agencies SHOULD provide for the acquisition of necessary licences and information to produce spare parts, components, assemblies, testing equipment and technical assistance agreements in the event that the supplier is no longer able to supply the equipment, products and essential spares.

13. Media Management, Decommissioning and Disposal

13.1. System Decommissioning

Objective

13.1.1. To ensure systems are safely decommissioned and that software, system logic and data are properly transitioned to new systems or archived in accordance with agency, legal and statutory requirements.

Context

Scope

13.1.2. This section discusses the retirement and safe decommissioning of systems. Specific requirements on media handling, usage, sanitisation, destruction and disposal are discussed later in this chapter. System decommissioning is the retirement or termination of a system and its operations. System decommissioning does NOT deal with the theft or loss of equipment.

Definitions

13.1.3. A system decommissioning will have the one or more of the following characteristics:

- Ending a capability completely i.e. no migration, redevelopment or new version of a capability occurs;
- Combining parts of existing capabilities services into a new, different system;
- As part of wider redesign, where a capability is no longer provided and is decommissioned or merged with other capabilities or systems.

13.1.4. ICT requirements evolve as business needs change and technology advances. In some cases this will lead to the retirement and decommissioning of obsolete systems or systems surplus to requirements.

13.1.5. Security requires a structured approach to decommissioning in order to cease information system operations in a planned, orderly and secure manner. It is also important that the approach for decommissioning systems is consistent and coordinated. Sanitisation is important to eliminate any remnant data that could be retrieved by unauthorised parties. These procedures include the following:

- A migration plan;
- A decommissioning plan;
- Archiving;
- Safe disposal of equipment and media;
- Robust procedures to manage any residual data and associated risk in cloud services; and
- Audit and final signoff.

13.1.6. As a final step, a review of the decommissioning should be undertaken to ensure no important elements, data or equipment have been overlooked.

References

Title	Publisher	Source
Risk Management And Accreditation Of Information Systems Also Released As HMG Infosec Standard No. 2, August 2005	UK Centre for the Protection of National Infrastructure (CPNI)	http://www.cpni.gov.uk/Documents/Publications/2005/2005003-Risk_management.pdf
NIST Special Publication 800-88 Guidelines for Media Sanitization, Rev.1, December, 2014	National Institute of Standards and Technology (NIST), U.S. Department of Commerce	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
Better Practice Checklist – Decommissioning Government Websites, March 2011	Australian Government Information Management Office (AGIMO)	http://agict.gov.au/policy-guides-procurement/better-practice-checklists-guidance/bpc-decommissioning

PSR references

Reference	Title	Source
PSR Mandatory Requirements	INFOSEC4 and PHYSEC6	http://www.protectivesecurity.govt.nz
PSR content protocols and requirements sections	Physical Security of ICT Equipment, Systems and Facilities Handling Requirements for Protectively Marked Information and Equipment	http://www.protectivesecurity.govt.nz

Rationale & Controls

13.1.7. Agency Policy

13.1.7.R.01. Rationale

Information systems are often supported by service and supply contracts and may also be subject to obligations to provide a service, capability or information. Decommissioning of a system will require the termination of these contracts and service obligations. Other aspects of system decommission may be subject to security, regulatory or legislative requirements. An Agency policy will provide a comprehensive approach to system decommissioning from the inception of a system, thus facilitating the termination of supply contracts and service obligations while managing any risks to the Agency.

13.1.7.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

When the Information System reaches the end of its service life in an organisation, policy and procedures SHOULD be in place to ensure secure decommissioning and transfer or disposal, in order to satisfy corporate, legal and statutory requirements.

13.1.8. Migration plan

13.1.8.R.01. Rationale

Once the decision to decommission a system has been taken, it is important to migrate processes, data, users and licences to replacement systems or to cease activities in an orderly fashion. It is also important to carefully plan the decommissioning process in order to avoid disruption to other systems, ensure business continuity, ensure security, protect privacy and meet any archive and other regulatory and legislative requirements. The basis of a decommissioning plan is a risk assessment.

13.1.8.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD undertake a risk assessment with consideration given to proportionality in respect of scale and impact of the processes, data, users and licences system and service to be migrated or decommissioned.

13.1.8.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

The risk assessment SHOULD include the following elements:

- Evaluation of the applications inventory and identification of any redundancies;
- Identification of data owners and key stakeholders;
- Identification of types of information (Active or Inactive) processed and stored;
- Identification of software and other (including non-transferable) licences;

- Identification of access rights to be transferred or cancelled;
- Identification of any emanation control equipment or security enhancements;
- Consideration of short and long term reporting requirements;
- Assessment of equipment and hardware for redeployment or disposal; n67
- Identification of any cloud-based data and services; and
- User re-training.

13.1.8.C.03. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD consider the need for a Privacy Impact Assessment.

13.1.8.C.04. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD identify relevant service and legal agreements and arrange for their termination.

13.1.9. Decommissioning plan

13.1.9.R.01. **Rationale**

The decommissioning of a system can be a complex process. A decommissioning plan is an important tool in properly managing the safe decommissioning of a system and in providing reasonable assurance that due process and agency policy has been followed.

13.1.9.C.01. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

The decommissioning plan will be based on the migration plan and SHOULD incorporate the following elements:

- An impact analysis;
- Issue of notification to service providers, users and customers;
- Issue of notification of decommissioning to all relevant interfaces and interconnections;
- Timeframe, plan and schedule;
- Data integrity and validation checks before archiving;
- Transfer or redeployment of equipment and other assets;
- Transfer or cancellation of licences;
- Removal of redundant equipment and software;
- Removal of redundant cables and termination equipment;
- Removal of any emanation control equipment or security enhancements;
- Return or safe disposal of any emanation control equipment or security enhancements;

- Updates to systems configurations (switches, firewalls etc.);
- Equipment and media sanitisation including any cloud-based data and services (discussed later in this chapter);
- Equipment and media disposal (discussed later in this chapter);
- Any legal considerations for supply or service contract terminations;
- Asset register updates; and
- Retraining for, or redeployment of, support staff.

13.1.10. Archiving

13.1.10.R.01. Rationale

Availability and integrity requirements in respect of information may persist for legal and other statutory or compliance reasons and require transfer to other ownership or custodianship for archive purposes. This will also require assurance that the data can continue to be accessed when required (availability) and assurance that it remains unchanged (integrity).

13.1.10.R.02. Rationale

Confidentiality requirements must also be considered. If an information system has been processing sensitive information or contains sensitive security components, which attract special handling requirements, it will require robust purging and overwrites or destruction. There are a number of methods and proprietary products available for such purposes.

13.1.10.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD identify data retention policies, regulation and legislation.

13.1.10.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure adequate system documentation is archived.

13.1.10.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD archive essential software, system logic, and other system data to allow information to be recovered from archive to ensure adequate system documentation is archived.

13.1.11. Audit and Final signoff

13.1.11.R.01. Rationale

Update the organisation's tracking and management systems to identify the specific information system components that are being removed from the inventory. To comply with governance, asset management and audit requirements, the Agency's Accreditation Authority will certify that appropriate

processes have been followed. This demonstrates good governance and avoids privacy breaches.

13.1.11.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

The Agency's Accreditation Authority SHOULD confirm IA compliance on decommissioning and disposal.

13.1.11.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

The Agency's Accreditation Authority SHOULD confirm secure equipment and media disposal.

13.1.11.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

The Agency's Accreditation Authority SHOULD confirm asset register updates.

13.1.11.C.04. Control: System Classification(s): All Classifications; Compliance: SHOULD

Once all security relevant activities associated with decommissioning and disposal have been completed and verified, a Security Decommissioning Compliance Certificate SHOULD be issued by the Agency's Accreditation Authority.

13.1.12. Final Review

13.1.12.R.01. Rationale

As a final step, a review of the decommissioning should be undertaken to ensure no important elements, data, equipment, contractual or legislative, obligations have been overlooked.

13.1.12.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD undertake a post-decommissioning review.

13.2. Media Handling

Objective

13.2.1. Media is properly classified, labelled and registered in order to clearly indicate the required handling instructions and degree of protection to be applied.

Context

Scope

13.2.2. This section covers information relating to classifying, labelling and registering media. Information relating to classifying and labelling IT equipment can be found in Section 12.3 - Product Classifying and Labelling.

Exceptions for labelling and registering media

13.2.3. Labels are not needed for internally mounted fixed media if the IT equipment containing the media is labelled. Likewise fixed media does not need to be registered if the IT equipment containing the media is registered.

References

13.2.4. Additional information relating to media handling is contained in:

Title	Publisher	Source
ISO/IEC 27001:2013 **10.7, Media Handling**	ISO / IEC Standards NZ	http://www.iso27001security.com/html/27001.html http://www.standards.co.nz

PSR references

Reference	Title	Source
PSR Mandatory Requirements	GOV10, INFOSEC3, INFOSEC4, and PHYSEC6	http://www.protectivesecurity.govt.nz
PSR content protocols and requirements sections	Handling Requirements for protectively marked information and equipment Physical Security of ICT Equipment, Systems and Facilities	http://www.protectivesecurity.govt.nz

Rationale & Controls

13.2.5. Reclassification and declassification procedures

13.2.5.R.01. Rationale

When reclassifying or declassifying media the process is based on an assessment of risk, including:

- the classification of the media and associated handling instructions;
- the effectiveness of any sanitisation or destruction procedure used;
- the planned redeployment; and
- the intended destination of the media.

13.2.5.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST document procedures for the reclassification and declassification of media.

13.2.6. Classifying media storing information

13.2.6.R.01. Rationale

Media that is not classified or not correctly classified may be stored, identified and handled inappropriately.

13.2.6.R.02. Rationale

Incorrect or no classification may result in access by a person or persons without the appropriate security clearance.

13.2.6.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST classify media to the highest classification of data stored on the media.

13.2.7. Classifying media connected to systems of higher classifications

13.2.7.R.01. Rationale

Unless connected through a data diode or similar infrastructure, there is no guarantee that classified information was not copied to the media while it was connected to a system of higher classification than the classification level of the media itself.

13.2.7.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST classify any media connected to a system of a higher classification at the higher system classification until confirmed not to be the case.

13.2.8. Classifying media below that of the system

13.2.8.R.01. Rationale

When sufficient assurance exists that information cannot be written to media that is used with a system, then the media can be treated in accordance with the handling instructions of the classification of the information it stores rather than the classification of the system it is connected to or used with.

13.2.8.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies intending to classify media below the classification of the system to which it is connected to MUST ensure that:

- the media is read-only;
- the media is inserted into a read-only device; or
- the system has a mechanism through which read-only access can be assured such as approved data diodes, write-blockers or similar infrastructure.

13.2.9. Reclassifying media to a lower classification

13.2.9.R.01. Rationale

Agencies must follow the reclassification process as illustrated in Section 13.6 – Media Disposal.

13.2.9.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies wishing to reclassify media to a lower classification MUST ensure that:

- a formal decision is made to reclassify, or redeploy the media; and
- the reclassification of all information on the media has been approved by the originator, or the media has been appropriately sanitised or destroyed.

13.2.10. Reclassifying media to a higher classification

13.2.10.R.01. Rationale

The media will always need to be protected in accordance with the classification of the information it stores. As such, if the classification of the information on the media changes, then so will the classification of the media.

13.2.10.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST reclassify media if:

- information copied onto the media is of a higher classification; or
- information contained on the media is subjected to a classification upgrade.

13.2.11. Labelling media

13.2.11.R.01. Rationale

Labelling helps all personnel to identify the classification of media and ensure that they afford the media the correct protection measures.

13.2.11.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST label media with a marking that indicates the maximum classification and any endorsements applicable to the information stored.

13.2.11.C.02. Control: System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST ensure that the classification of all media is easily visually identifiable.

13.2.11.C.03. Control: System Classification(s): All Classifications; Compliance: MUST

When using non-textual (colour, symbol) protective markings for operational security reasons, agencies MUST document the labelling scheme and train personnel appropriately.

13.2.11.C.04. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD label media with a marking that indicates the maximum classification and any endorsements applicable to the information stored.

13.2.12. Labelling sanitised media

13.2.12.R.01. Rationale

It is not possible to effectively sanitise and subsequently reclassify SECRET or TOP SECRET non-volatile media to a classification lower than SECRET. Media of other classifications may be reclassified (See Section 13.6 – Media Disposal).

13.2.12.C.01. Control: System Classification(s): S, TS; Compliance: MUST

Agencies MUST label non-volatile media that has been sanitised and reclassified for redeployment with a notice similar to:

Warning: media has been sanitised and reclassified from [classification] to [classification]. Further lowering of classification only via destruction.

13.2.13. Registering media

13.2.13.R.01. Rationale

If agencies fail to register media with an appropriate identifier they will not be able to effectively keep track of their classified media and there will be a greater likelihood of unauthorised disclosure of classified information.

13.2.13.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST register all media with a unique identifier in an appropriate register.

13.2.13.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD register all media with a unique identifier in an appropriate register.

13.3. Media Usage

Objective

13.3.1. Media is used with systems in a controlled and accountable manner.

Context

Scope

13.3.2. This section covers information on using media with systems. Further information on using media to transfer data between systems can be found in Section 20.1 - Data Transfers.

PSR references

Reference	Title	Source
PSR Mandatory Requirements	GOV10	http://www.protectivesecurity.govt.nz

Rationale & Controls

13.3.3. Using media with systems

13.3.3.R.01. Rationale

To prevent classified data spills agencies will need to prevent classified media from being connected to, or used with, systems of a lesser classification than the protective marking of the media.

13.3.3.R.02. Rationale

Where media is used for backup purposes, the media will be certified for use at the highest level of classification to be backed-up. Refer also to Section 6.4 – Business Continuity and Disaster Recovery.

13.3.3.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST NOT

Agencies MUST NOT use media containing classified information with a system that has a classification lower than the classification of the media.

13.3.4. Storage of media

13.3.4.R.01. Rationale

The security requirements for storage and physical transfer of classified information and IT equipment are specified in the Protective Security Requirements (PSR).

13.3.4.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that storage facilities for media containing classified information meets the minimum physical security storage requirements as specified in the Protective Security Requirements (PSR).

13.3.5. Connecting media to systems

13.3.5.R.01. Rationale

Some operating systems provide functionality to automatically execute or read certain types of programs that reside on optical media and flash memory media when connected. While this functionality was designed with a legitimate purpose in mind, such as automatically loading a graphical user interface for the system user to browse the contents of the media, or to install software residing on the media, it can also be used for malicious purposes.

13.3.5.R.02. Rationale

An attacker can create a file on optical media or a connectable device that the operating system will attempt to automatically execute. When the operating system executes the file, it can have the same effect as when a system user explicitly executes malicious code. The operating system executes the file without asking the system user for permission.

13.3.5.R.03. Rationale

Some operating systems will cache information on media to improve performance. As such, inserting media of a higher classification into a system of a lower classification could cause data to be read and saved from the device without user intervention.

13.3.5.R.04. Rationale

Using device access control software will prevent unauthorised media from being attached to a system. Using a whitelisting approach allows security personnel greater control over what can, and what cannot, be connected to the system.

13.3.5.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST disable any automatic execution features within operating systems for connectable devices and media.

13.3.5.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST prevent unauthorised media from connecting to a system via the use of:

- device access control software;
- seals;
- physical means; or
- other methods approved by the Accreditation Authority.

13.3.5.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

When writable media is connected to a writable communications port or device, agencies SHOULD implement controls to prevent the unintended writing of data to the media.

13.3.6. IEEE 1394 (FIREWIRE) interface connections

13.3.6.R.01. Rationale

Known vulnerabilities have been demonstrated where attackers can connect a FireWire capable device to a locked workstation and modify information in RAM to gain access to encryption keys. Furthermore, as FireWire provides direct access to the system memory, an attacker can read or write directly to memory.

13.3.6.R.02. Rationale

The best defence against this vulnerability is to disable access to FireWire ports using either software controls or physically disabling the FireWire ports so that devices cannot be connected. Alternatively select equipment without FireWire capability.

13.3.6.C.01. **Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST disable IEEE 1394 interfaces.

13.3.6.C.02. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD disable IEEE 1394 interfaces.

13.3.7. Transferring media

13.3.7.R.01. **Rationale**

As media is often transferred through areas not certified to process the level of classified information on the media, additional protection mechanisms need to be implemented.

13.3.7.R.02. **Rationale**

Applying encryption to media may reduce the requirements for storage and physical transfer as outlined in the PSR. The reduction of any requirements is based on the original classification of information residing on the media and the level of assurance in the cryptographic product being used to encrypt the media.

13.3.7.R.03. **Rationale**

Further information on reducing storage and physical transfer requirements can be found in Section 17.1 - Cryptographic Fundamentals.

13.3.7.C.01. **Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that processes for transferring media containing classified information meets the minimum physical transfer requirements as specified in the PSR.

13.3.7.C.02. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD encrypt data stored on media with at least an Approved Cryptographic Algorithm (See Section 17.2 – Approved Cryptographic Algorithms) if it is to be transferred to another area or location.

13.3.8. Using media for data transfers

13.3.8.R.01. **Rationale**

Agencies transferring data between systems of different security domains or classifications are strongly encouraged to use media such as write-once CDs and DVDs. This will limit opportunity for information from the higher classified systems to be accidently transferred to lower classified systems. This procedure will also make each transfer a single, auditable event.

13.3.8.C.01. **Control:** System Classification(s): All Classifications; Compliance: SHOULD

Data transfers between systems of different classification SHOULD be logged in an auditable log or register.

13.3.8.C.02. **Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies transferring data manually between two systems of different security domains or classifications SHOULD NOT use rewriteable media.

13.3.9. Media in secure areas

13.3.9.R.01. **Rationale**

Certain types of media including USB, FireWire and eSATA capable devices MUST be disabled or explicitly approved as an exception by the Accreditation Authority for a TOP SECRET environment (the GCSB). This provides an additional level of system user awareness and security.

13.3.9.R.02. **Rationale**

This practice should be used in addition to device access control software on workstations in case system users are unaware of, or choose to ignore, security requirements for media.

13.3.9.C.01. **Control:** System Classification(s): TS; Compliance: MUST NOT

Agencies MUST NOT permit any media that uses external interface connections within a TOP SECRET area without prior written approval from the Accreditation Authority.

13.4. Media Sanitisation

Objective

13.4.1. Media that is to be redeployed or is no longer required is sanitised.

Context

Scope

13.4.2. This section covers information relating to sanitising media. Information relating to sanitising IT equipment can be found in Section 12.6 - Product Sanitisation and Disposal.

Definition

13.4.3. Sanitisation is defined as the process of removal of data and information from the storage device such that data recovery using any known technique or analysis is prevented or made unfeasible. The process includes the removal of all useful data from the storage device, including metadata, as well as the removal of all labels, markings, classifications and activity logs. Methods vary depending upon the nature, technology used and construction of the storage device or equipment and may include degaussing, incineration, shredding, grinding, knurling or embossing and chemical immersion.

Sanitising media

13.4.4. The process of sanitisation does not automatically change the classification of the media, nor does sanitisation necessarily involve the destruction of media.

Product selection

13.4.5. Agencies are permitted to use non-evaluated products to sanitise media. However, the product will still need to meet the specifications and achieve the requirements for sanitising media as outlined in this section.

Hybrid hard drives, Solid State Drives and Flash Memory Devices

13.4.6. Hybrid hard drives, solid state drives and flash memory devices are difficult or impossible to sanitise effectively. In most cases safe disposal will require destruction. The sanitisation and post sanitisation treatment requirements for redeployment of such devices should be carefully observed.

New Zealand Eyes Only (NZEO) Materials

13.4.7. NZEO endorsed material requires additional protection at every level of classification. In general terms, media containing NZEO material should be sanitised and redeployed or sanitised and destroyed in accordance with the procedures in this section. Media that has contained NZEO material must not be disposed of to e-recyclers or sold to any third party.

References

Title	Publisher	Source
Data Remanence in Semiconductor Devices	Peter Gutmann IBM T.J.Watson Research Center	http://www.cypherpunks.to/~peter/usenix01.pdf
RAM testing tool memtest86+		http://www.memtest.org
MemtestG80 and MemtestCL: Memory Testers for CUDA- and OpenCL-enabled GPUs	Simbios project funded by the National Institutes of Health	https://simtk.org/home/memtest
HDDerase **Capable of calling the ATA secure erase command for non-volatile magnetic hard disks. It is also capable of resetting host protected area and device configuration overlay table information on the media.**	A freeware tool developed by the Center for Magnetic Recording Research at the University of California San Diego.	http://cmrr.ucsd.edu/people/hughes/Secure-Erase.html
AISEP Evaluated Products List (EPL)	Australasian Information Security Evaluation Program	http://www.asd.gov.au/infosec/epl/index.php
ATA Secure Erase	ATA ANSI specifications	http://www.ansi.org
Data Sanitisation - Flash Based Storage Version 0.3	CESG, UK	https://www.cesg.gov.uk/content/files/protected_files/document_files/CPA%20SC%20Flash%20Based%20Storage%20v0-3.pdf
Reliably Erasing Data From Flash-Based Solid State Drives	Wei, Grupp, Spada and Swanson Department of Computer Science and Engineering, University of California, San Diego	https://www.usenix.org/legacy/event/fast11/tech/full_papers/Wei.pdf

Title	Publisher	Source
The 2012 Analysis of Information Remaining on Computer Hard Disks Offered for Sale on the Second Hand Market in the UAE	Edith Cowan University Research Online. Australian Digital Forensics Conference	http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1110&context=adf
2010 Zombie Hard disks - Data from the Living Dead	Edith Cowan University Research Online. Australian Digital Forensics Conference	http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1085&context=adf
The 2009 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market	Edith Cowan University Research Online. Australian Digital Forensics Conference	http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1079&context=adf
NSA/CSS Storage Device Declassification Manual December 2007	NSA	http://www.nsa.gov/ia/_files/government/MDG/NSA_CSS_Storage_Device_Declassification_Manual.pdf

Rationale & Controls

13.4.8. Sanitisation procedures

13.4.8.R.01. Rationale

Sanitising media prior to reuse or redeployment in a different environment ensures that classified information is not inadvertently accessed by an unauthorised individual or inadequately protected.

13.4.8.R.02. Rationale

Using approved sanitisation methods provides a high level of assurance that no remnant data is on the media.

13.4.8.R.03. Rationale

The procedures used in this manual are designed not only to prevent common attacks that are currently feasible, but also to protect from threats that could emerge in the future.

13.4.8.R.04. Rationale

When sanitising media, it is necessary to read back the contents of the media to verify that the overwrite process completed successfully.

13.4.8.R.05. Rationale

If the sanitising process cannot be successfully completed, destruction will be necessary.

13.4.8.R.06. Rationale

It is important to note that "factory reset" or similar terms **do not** constitute sanitisation for the purposes of the NZISM.

13.4.8.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST document conditions and procedures for the sanitisation of media.

13.4.9. Media that cannot be sanitised

13.4.9.R.01. Rationale

Some types of media cannot be sanitised and therefore MUST be destroyed. It is not possible to use these types of media while maintaining a high level of assurance that no previous data can be recovered.

13.4.9.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST destroy the following media types prior to **disposal**, as they cannot be effectively sanitised:

- microfiche;
- microfilm;
- optical discs;
- printer ribbons and the impact surface facing the platen;
- programmable read-only memory (PROM, EPROM, EEPROM);
- flash memory and solid state or hybrid data storage devices;
- read-only memory; and
- faulty magnetic media that cannot be successfully sanitised.

13.4.10. Volatile media sanitisation

13.4.10.R.01. Rationale

The following guidance applies in cases where media is to be redeployed.

When sanitising volatile media, the specified time to wait following removal of power is based on applying a safety factor to research on recovering the contents of volatile media.

13.4.10.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST sanitise volatile media by:

- overwriting all locations of the media with an arbitrary pattern;
- followed by a read back for verification; and
- removing power from the media for at least 10 minutes.

13.4.11. Treatment of volatile media following sanitisation

13.4.11.R.01. Rationale

The following guidance applies in cases where media is to be redeployed.

There is published literature that supports the existence of short-term data remanence effects in volatile media. Data retention time is reported to range from minutes (at normal room temperatures) to hours (in extreme cold), depending on the temperature of the volatile media. Further, published literature has shown that some volatile media can suffer from long-term data remanence effects resulting from physical changes to the media due to continuous storage of static data for an extended period of time. It is for these reasons that TOP SECRET volatile media MUST always remain at this classification, even after sanitisation.

13.4.11.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Following sanitisation, volatile media MUST be treated as indicated in the table below.

Pre-sanitisation classification Endorsement	Post-sanitisation classification Endorsement
New Zealand Eyes Only (NZEO) Endorsement	NZEO
TOP SECRET	TOP SECRET
SECRET	SECRET
CONFIDENTIAL	UNCLASSIFIED
RESTRICTED and all lower classifications	UNCLASSIFIED

13.4.12. Non-volatile magnetic media sanitisation

13.4.12.R.01. Rationale

The following guidance applies in cases where media is to be redeployed.

Both the host protected area and device configuration overlay table of non-volatile magnetic hard disks are normally not visible to the operating system or the computer's BIOS. Hence any sanitisation of the readable sectors on the media will not overwrite these hidden sectors leaving any classified information contained in these locations untouched. Some sanitisation programs include the ability to reset devices to their default state removing any host protected areas or device configuration overlays. This allows the sanitisation program to see the entire contents of the media during the subsequent sanitisation process.

13.4.12.R.02. Rationale

Modern non-volatile magnetic hard disks automatically reallocate space for bad sectors at a hardware level. These bad sectors are maintained in what is known as the growth defects table or 'g-list'. If classified information was stored in a sector that is subsequently added to the g-list, sanitising the media will not overwrite these non-addressable bad sectors, and remnant data will exist in these locations. Whilst these sectors may be considered bad by the device quite often this is due to the sectors no longer meeting expected performance norms for the device and not due to an inability to read/write to the sector.

13.4.12.R.03. Rationale

The ATA secure erase command is built into the firmware of post-2001 devices and is able to access sectors that have been added to the g-list. Modern non-volatile magnetic hard disks also contain a primary defects table or 'p-list'. The p-list contains a list of bad sectors found during post-production processes. No information is ever stored in sectors on the p-list for a device as they are inaccessible before the media is used for the first time.

13.4.12.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST sanitise non-volatile magnetic media by:

- if pre-2001 or under 15GB: overwriting the media at least three times in its entirety with an arbitrary pattern followed by a read back for verification; or
- if post-2001 or over 15GB: overwriting the media at least once in its entirety with an arbitrary pattern followed by a read back for verification.

13.4.12.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST boot from separate media to the media being sanitised when undertaking sanitisation.

13.4.12.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD reset the host protected area and drive configuration overlay table of non-volatile magnetic hard disks prior to overwriting the media.

13.4.12.C.04. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD attempt to overwrite the growth defects table (g-list) on non-volatile magnetic hard disks.

13.4.12.C.05. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use the ATA security erase command for sanitising non-volatile magnetic hard disks instead of using block overwriting software.

13.4.13. Treatment of non-volatile magnetic media following sanitisation

13.4.13.R.01. Rationale

The following guidance applies in cases where media is to be redeployed.

Highly classified non-volatile magnetic media cannot be sanitised below its original classification because of concerns with the sanitisation of the host protected area, device configuration overlay table and growth defects table.

13.4.13.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Following sanitisation, non-volatile magnetic media MUST be treated as indicated in the table below.

Pre-sanitisation classification	Post-sanitisation classification
New Zealand Eyes Only (NZEO) Endorsement	NZEO
TOP SECRET	TOP SECRET
SECRET	SECRET
CONFIDENTIAL	UNCLASSIFIED
RESTRICTED	UNCLASSIFIED

13.4.14. Non-volatile EPROM media sanitisation

13.4.14.R.01. Rationale

The following guidance applies in cases where media is to be redeployed.

When erasing non-volatile EPROM, the manufacturer's specified ultraviolet erasure time is multiplied by a factor of three to provide an additional level of certainty in the process. Verification is provided by read-back.

13.4.14.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST sanitise non-volatile EPROM media by erasing as per the manufacturer's specification, increasing the specified ultraviolet erasure time by a factor of three, then overwriting the media at least once in its entirety with a pseudo random pattern, followed by a read back for verification.

13.4.15. Non-volatile EEPROM media sanitisation

13.4.15.R.01. Rationale

The following guidance applies in cases where media is to be redeployed.

A single overwrite with a pseudo random pattern is considered good practice for sanitising non-volatile EEPROM media.

13.4.15.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST sanitise non-volatile EEPROM media by overwriting the media at least once in its entirety with a pseudo random pattern, followed by a read back for verification.

13.4.16. Treatment of non-volatile EPROM and EEPROM media following sanitisation

13.4.16.R.01. Rationale

The following guidance applies in cases where media is to be redeployed.

As little research has been conducted on the ability to recover data on non-volatile EPROM or EEPROM media after sanitisation, highly classified media retains its original classification.

13.4.16.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Following sanitisation, non-volatile EPROM and EEPROM media MUST be treated as indicated in the table below.

Pre-sanitisation classification	Post-sanitisation classification
New Zealand Eyes Only (NZEO) Endorsement	NZEO
TOP SECRET	TOP SECRET
SECRET	SECRET
CONFIDENTIAL	UNCLASSIFIED
RESTRICTED	UNCLASSIFIED

13.4.17. Non-volatile flash memory media sanitisation

13.4.17.R.01. Rationale

The following guidance applies in cases where media is to be redeployed.

Wear levelling ensures that writes are distributed evenly across each memory block in flash memory. Flash memory SHOULD be overwritten with a pseudo random pattern twice, rather than once, as this helps to ensure that all memory blocks are overwritten during sanitisation. Verification is provided by read-back.

13.4.17.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST sanitise non-volatile flash memory media by overwriting the media at least twice in its entirety with a pseudo random pattern, followed by a read back for verification.

13.4.18. Treatment of non-volatile flash memory media following sanitisation

13.4.18.R.01. Rationale

The following guidance applies in cases where media is to be redeployed.

Owing to the use of wear levelling in flash memory, it is possible that not all physical memory locations are written to when attempting to overwrite the media. Classified information can therefore remain on the media. It is for these reasons that TOP SECRET, SECRET and CONFIDENTIAL flash memory media MUST always remain at their respective classification, even after sanitisation.

13.4.18.R.02. Rationale

Non-volatile flash memory may be redeployed within systems of the same classification only after all manufacturer's sanitisation procedures have been followed. Destruction and Disposal are covered in Sections 13.5 and 13.6 respectively.

13.4.18.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Following sanitisation, non-volatile flash memory media MUST be treated as indicated in the table below.

Pre-sanitisation classification	Post-sanitisation classification
New Zealand Eyes Only (NZEO) Endorsement	NZEO
TOP SECRET	TOP SECRET
SECRET	SECRET
CONFIDENTIAL	CONFIDENTIAL
RESTRICTED	UNCLASSIFIED

13.4.18.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Where manufacturer sanitisation procedures cannot be determined, items MUST be destroyed.

13.4.19. Sanitising solid state drives

13.4.19.R.01. Rationale

Solid state drives operate a Flash Translation Layer (FTL) to interface with the storage devices – usually NAND chips. Current sanitation techniques address the FTL, rather than destroying the underlying data. It is possible to bypass the FTL, thus accessing the underlying data. With current technology, there is no effective means of sanitising solid state drives.

13.4.19.R.02. Rationale

Solid state drives also use wear equalisation or levelling techniques which can leave data remnants.

13.4.19.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Solid state drives MUST be destroyed before disposal.

13.4.19.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Solid state drives MUST be sanitised using ATA Secure Erase sanitation software before redeployment.

13.4.19.C.03. Control: System Classification(s): C, S, TS; Compliance: MUST NOT

Solid state drives MUST NOT be redeployed in a lower classification environment.

13.4.20. Hybrid Drives

13.4.20.R.01. Rationale

Hybrid drives combine solid state memory devices with magnetic disk technologies. As such they are subject to the same difficulties in effective sanitisation as solid state devices.

13.4.20.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Hybrid drives MUST be treated as solid state drives for sanitisation purposes.

13.4.21. Sanitising media prior to reuse

13.4.21.R.01. Rationale

Sanitising media prior to reuse at the same or higher classification assists with enforcing the need-to-know principle within the agency. This includes any material with an NZEO endorsement.

13.4.21.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD sanitise all media prior to reuse at the same or higher classification.

13.4.22. Verifying sanitised media

13.4.22.R.01. Rationale

Verifying the sanitisation of media with a different product to the one conducting the sanitisation process provides an independent level of assurance that the sanitisation process was conducted correctly.

13.4.22.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD verify the sanitisation of media using a different product from the one used to perform the initial sanitisation.

13.5. Media Destruction

Objective

13.5.1. Media that cannot be sanitised is destroyed before disposal.

Context

Scope

13.5.2. This section covers information relating to the destruction of media. Information relating to the destruction of IT equipment can be found in Section 12.6 - Product Sanitisation and Disposal.

New Zealand Eyes Only (NZEO) Materials

13.5.3. NZEO endorsed material requires additional protection at every level of classification.

13.5.4. In general terms, media containing NZEO material should be sanitised and redeployed or sanitised and destroyed in accordance with the procedures in this section. Media that has contained NZEO material must not be disposed of, to e-recyclers or sold to any third party.

References

Topic	Publisher	Source
Secure Destruction of Sensitive Items	CPNI	http://www.cpni.gov.uk/documents/publications/2013/2013062-secure-destruction-sensitive-information.pdf

Rationale & Controls

13.5.5. Destruction procedures

13.5.5.R.01. Rationale

Documenting procedures for media destruction will ensure that media destruction is carried out in an appropriate and consistent manner within the agency.

13.5.5.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST document procedures for the destruction of media.

13.5.6. Media destruction

13.5.6.R.01. Rationale

The destruction methods given are designed to ensure that recovery of data is impossible or impractical. Health and safety training and the use of safety equipment may be required with these methods.

13.5.6.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

To destroy media agencies MUST use at least one of the methods shown in the following table.

Item	Destruction methods					
	Furnace/ Incinerator	Hammer mill	Disintegrator	Grinder/ Sander	Cutting	Degausser
Magnetic floppy disks	Yes	Yes	Yes	No	Yes	Yes
Magnetic hard disks	Yes	Yes	Yes	Yes	No	Yes
Magnetic tapes	Yes	Yes	Yes	No	Yes	Yes
Optical disks	Yes	Yes	Yes	Yes	Yes	No
Electrostatic memory devices	Yes	Yes	Yes	Yes	No	No
Semi-conductor memory	Yes	Yes	Yes	No	No	No

13.5.7. Media destruction equipment

13.5.7.R.01. Rationale

A variety of equipment for media destruction exists. Evaluated products will provide assurance that the product will be effective. Approved products are discussed in Chapter 12 – Product Security.

13.5.7.R.02. Rationale

Where a product is not an evaluated product or is NOT listed in the PSR. Consult the GCSB for advice.

13.5.7.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST employ approved equipment, for the purpose of media destruction.

13.5.7.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Where agency owned approved destruction equipment is not available agencies MUST use an approved destruction facility for media destruction.

13.5.8. Storage and handling of media waste particles

13.5.8.R.01. Rationale

Following destruction, normal accounting and auditing procedures do not apply for media items. As such, it is essential that when an item is recorded as being destroyed, destruction is assured.

13.5.8.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST, at minimum, store and handle the resulting media waste for all methods, as for the classification given in the table below.

Initial media classification	Screen aperture size particles can pass through	
	Less than or equal to 3mm	Less than or equal to 6mm
TOP SECRET	UNCLASSIFIED	RESTRICTED
SECRET	UNCLASSIFIED	RESTRICTED
CONFIDENTIAL	UNCLASSIFIED	RESTRICTED
RESTRICTED	UNCLASSIFIED	UNCLASSIFIED

13.5.9. Degaussers

13.5.9.R.01. Rationale

Coercivity varies between media types and between brands and models of the same type. Care is needed when determining the desired coercivity as a degausser of insufficient strength will not be effective. The National Security Agency/Central Security Service's EPLD contains a list of common types of media and their associated coercivity ratings.

13.5.9.R.02. Rationale

Since 2006 perpendicular magnetic media have become available. Some degaussers are only capable of sanitising longitudinal magnetic media. As such, care needs to be taken to ensure that a suitable degausser is used when sanitising perpendicular magnetic media.

13.5.9.R.03. Rationale

Some degaussers will have product specific requirements. Agencies will need to comply with any directions provided by the GCSB to ensure that degaussers are being used in the correct manner to achieve an effective destruction outcome. Refer also to Chapter 12 - Product Security.

13.5.9.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST use a degausser of sufficient field strength for the coercivity of the media.

13.5.9.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST use a degausser which has been evaluated as capable for the magnetic orientation (longitudinal or perpendicular) of the media.

13.5.9.C.03. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST comply with product specific directions provided by the manufacturers, along with any provided by the GCSB.

13.5.10. Supervision of destruction

13.5.10.R.01. Rationale

To ensure that classified media is appropriately destroyed it will need to be supervised to the point of destruction and have its destruction overseen by at least one person cleared to the highest classification of the media being destroyed. To provide accountability and traceability, a destruction register should be maintained.

13.5.10.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST perform the destruction of media under the supervision of at least one person cleared to the highest classification of the media being destroyed.

13.5.10.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Personnel supervising the destruction of media MUST:

- supervise the handling of the media to the point of destruction; and
- ensure that the destruction is completed successfully.

13.5.10.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

The Destruction Register SHOULD record:

- Date of destruction;
- Operator and witness;
- Media classification; and
- Media type, characteristics and serial number.

13.5.11. Supervision of accountable material destruction

13.5.11.R.01. Rationale

As accountable material is more sensitive than standard classified media, it needs to be supervised by at least two personnel and have a destruction certificate signed by the personnel supervising the process. This includes any NZEO material.

13.5.11.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST perform the destruction of accountable material under the supervision of at least two personnel cleared to the highest classification of the media being destroyed.

13.5.11.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Personnel supervising the destruction of accountable media MUST:

- supervise the handling of the material to the point of destruction;
- ensure that the destruction is completed successfully;
- sign a destruction certificate; and
- complete the relevant entries in the destruction register.

13.5.12. Outsourcing media destruction

13.5.12.R.01. Rationale

Agencies may wish to outsource media destruction for efficiency and cost reasons.

13.5.12.C.01. Control: System Classification(s): TS; Compliance: MUST NOT

Agencies MUST NOT outsource the supervision and oversight of the destruction of TOP SECRET or NZEO media or other accountable material to a non-government entity or organisation.

13.5.12.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies outsourcing the destruction of media to a commercial facility MUST use an approved facility and comply with the procedures and instructions in this Chapter.

13.5.13. Transporting media for offsite destruction

13.5.13.R.01. Rationale

Requirements on the safe handling and physical transfer of media between agencies or to commercial facilities can be found in the PSR.

13.5.13.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD sanitise media prior to transporting it to an offsite location for destruction.

13.6. Media Disposal

Objective

13.6.1. Media is declassified and approved by the CISO, or delegate, for release before disposal into the public domain.

Context

Scope

13.6.2. This section covers information relating to the disposal of media. Information relating to the disposal of IT equipment can be found in Section 12.6 - Product Sanitisation and Disposal.

13.6.3. NZEO endorsed material requires additional protection at every level of classification.

13.6.4. In general terms, media containing NZEO material should be sanitised and redeployed or sanitised and destroyed in accordance with the procedures in this section. Media that has contained NZEO material must not be disposed of, to e-recyclers or sold to any third party.

Rationale & Controls

13.6.5. Declassification prior to disposal

13.6.5.R.01. Rationale

Prior to its disposal, media needs to be declassified to ensure that classified information is not accidentally released into the public domain.

13.6.5.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST declassify all media prior to disposing of it into the public domain.

13.6.5.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

Media that cannot be effectively sanitised or declassified MUST be destroyed and not released into the public domain.

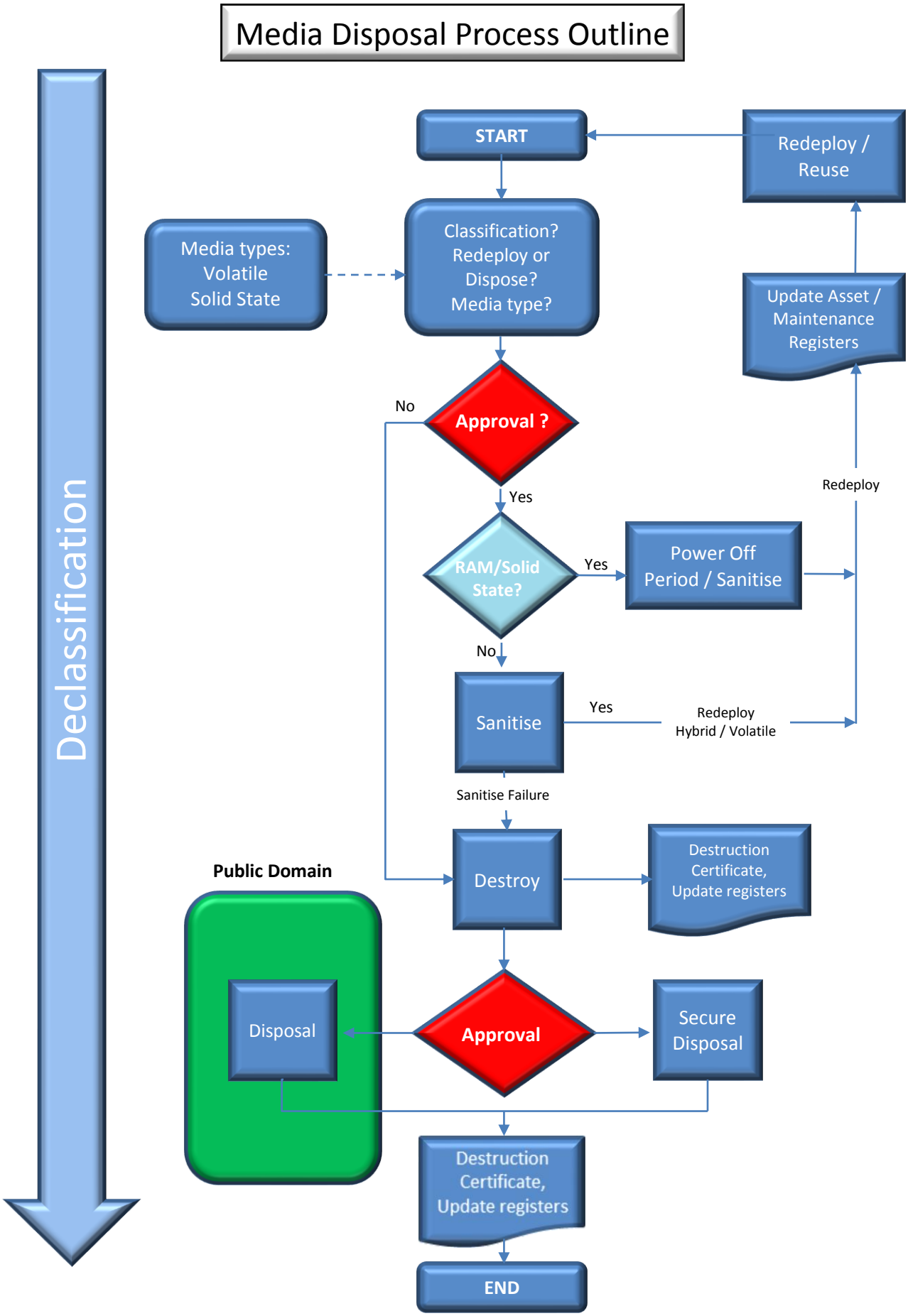
13.6.6. Disposal procedures

13.6.6.R.01. Rationale

The following diagram illustrates the mandated disposal process. Note declassification describes the entire process, including any reclassifications, approvals and documentation, before media and media waste can be released into the public domain.

13.6.6.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST document procedures for the disposal of media.


Media Disposal Process Outline
Declassification
START
Redeploy / Reuse
Media types: Volatile Solid State
Classification? Redeploy or Dispose? Media type?
Update Asset / Maintenance Registers
No
Approval ?
Yes
Redeploy
RAM/Solid State?
Yes
Power Off Period / Sanitise
No
Sanitise
Yes
Redeploy Hybrid / Volatile
Sanitise Failure
Public Domain
Destroy
Destruction Certificate, Update registers
Disposal
Approval
Secure Disposal
Destruction Certificate, Update registers
END

13.6.7. Declassifying media

13.6.7.R.01. Rationale

The process of reclassifying, sanitising or destroying media does not provide sufficient assurance for media to be declassified and released into the public domain. In order to declassify media, formal administrative approval is required before releasing the media or waste into the public domain.

13.6.7.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies declassifying media MUST ensure that:

- the reclassification of all classified information on the media has been approved by the originator, or the media has been appropriately sanitised or destroyed; and
- formal approval is granted before the media is released into the public domain.

13.6.8. Disposal of media

13.6.8.R.01. Rationale

Disposing of media in a manner that does not draw undue attention ensures that media that was previously classified is not subjected to additional scrutiny over that of regular waste. This can include the removal of labels, markings and serial numbers.

13.6.8.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST dispose of media in a manner that does not draw undue attention to its previous classification.

13.6.9. New Zealand Eyes Only (NZEO) Materials

13.6.9.R.01. Rationale

NZEO endorsed material requires additional protection at every level of classification and creates a special case in the destruction and disposal process.

13.6.9.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Media that has contained NZEO material MUST be sanitised and redeployed or sanitised and destroyed in accordance with the procedures in this chapter.

13.6.9.C.02. Control: System Classification(s): All Classifications; Compliance: MUST

For disposal of all NZEO endorsed materials, an approved destruction facility MUST be used.

13.6.9.C.03. Control: System Classification(s): All Classifications; Compliance: MUST NOT

Media that has contained NZEO material MUST NOT be disposed of via e-recyclers or sold to any third party.