4.1. The Certification and Accreditation Process

Objective

4.1.1. Executives and Security Practitioners understand and enforce the use of 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 Assurance Cryptographic Equipment (HACE) is required or caveated or compartmented information is processed, stored or communicated. In this case the Director-General, 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 formally authorised 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.

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 in a system or network, and testing existing security measures and 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.

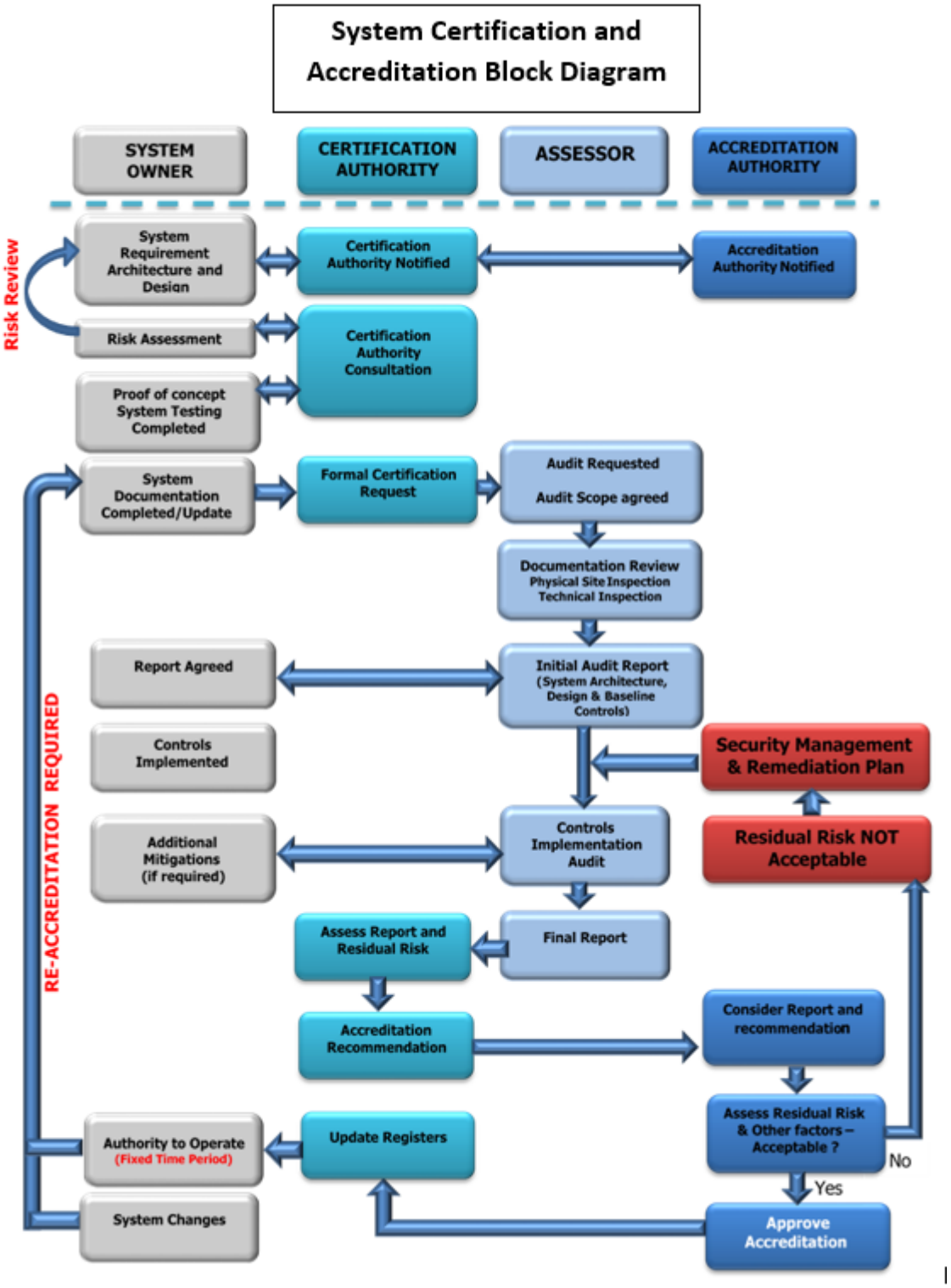
4.1.28. Organisations may conduct their own tests and regular simple tests are effective in maintaining the organisation’s security posture. Because of the level of expertise required to effectively conduct more complex testing, comprehensive penetration tests are often outsourced to specialist organisations.

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.

System Certification and Accreditation Diagram

4.1.30.



References

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

Reference	Title	Publisher	Source
	Office of the Auditor-General - Managing conflicts of interest: A Guide for the public sector	Office of the Auditor-General	https://oag.parliament.nz/2020/conflicts/docs/conflicts-of-interest.pdf [PDF, 445 KB]
ISO/IEC 27000:2018	**Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary**	ISO	ISO - ISO/IEC 27000:2018 - Information technology — Security techniques — Information security management systems — Overview and vocabulary
ISO/IEC 27001:2013	**Information technology -- Security techniques -- Information security management systems -- Requirements**	ISO	ISO - ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements
ISO/IEC 27002:2022	**Information security, cybersecurity, and privacy protection — Information security controls**	ISO	ISO - ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls
ISO/IEC 27006:2015	**Information Technology – Security Techniques - Requirements for bodies providing audit and certification of information security management systems**	ISO	ISO - ISO/IEC 27006:2015 - Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27007:2020	**Information Technology – Security Techniques - Guidelines for information security management systems auditing**	ISO	ISO - ISO/IEC 27007:2020 - Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing
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 [PDF, 1.51 MB]
NIST SP 800-171, Feb 2020	**Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations**	NIST	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf [PDF, 880 KB]
	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/
	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 [PDF, 662 KB]
	An Introduction to Certification and Accreditation	SANS Institute	https://www.sans.org/white-papers/1259/
	A Certification and Accreditation Plan for Information Systems Security Programs (Evaluating the Eff)	SANS Institute	https://www.sans.org/white-papers/597/
	SANS Institute InfoSec Reading Room, Conducting a Penetration Test on an Organization,	SANS Institute	https://www.sans.org/white-papers/67/
	Managing Conflict of Interest in the Public Service - OECD GUIDELINES AND COUNTRY EXPERIENCES	OECD	http://www.oecd.org/gov/ethics/48994419.pdf [PDF, 2.59 MB]
	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 [PDF, 1.44 MB]
	OWASP Top Ten for 2021	OWASP	OWASP Top Ten | OWASP Foundation
	OWASP Web security testing guide	OWASP	OWASP Web Security Testing Guide | OWASP Foundation
International Standard on Assurance Engagements (ISAE) 3402	**Assurance Reports on Controls at a Service Organization**	International Federation of Accountants (IFAC)	https://www.ifac.org/system/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf [PDF, 212 KB]

PSR references

4.1.32. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV2, GOV6, GOV7, GOV8, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2	Home | Protective Security Requirements Security governance (GOV) | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements Physical security (PHYSEC) | Protective Security Requirements
PSR requirements sections	Self assessment and reporting Protective security measures	Self-assessment and reporting | Protective Security Requirements Complying with the Protective Security Requirements | Protective Security Requirements