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	Publisher	Source
ISO/IEC 27006:2015	**Information Technology – Security Techniques - Requirements for bodies providing audit and certification of information security management systems**	ISO	https://www.iso.org/standard/62313.html
ISO/IEC 27007:2020	**Information Technology – Security Techniques - Guidelines for information security management systems auditing**	ISO	https://www.iso.org/standard/77802.html
ISO 19011:2018	**Guidelines for auditing management systems**	ISO	https://www.iso.org/standard/70017.html
AS/NZ ISO 19011:2019	**Guidelines for auditing management systems**	Standards NZ	https://standards.govt.nz/

Rationale & Controls

Certification Audit

4.2.10.R.01. **Rationale**

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 Protective Security Requirements (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 Classifications(s): All Classifications; Compliance: Must** [CID:535]

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

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 Protective Security Requirements (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 Classifications(s): All Classifications; Compliance: Must** [CID:540]

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

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 Classifications(s): All Classifications; Compliance: Should** [CID:543]

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.