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 Assurance Cryptographic Equipment (HACE), the Director-General 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 SSP. In such cases the Accreditation Authority may request that the SRMP and SSP 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

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 Classifications(s): All Classifications; Compliance: Must** [CID:666]

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

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 Classifications(s): All Classifications; Compliance: Must** [CID:673]

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 Classifications(s): All Classifications; Compliance: Must** [CID:674]

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

4.5.18.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:675]

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