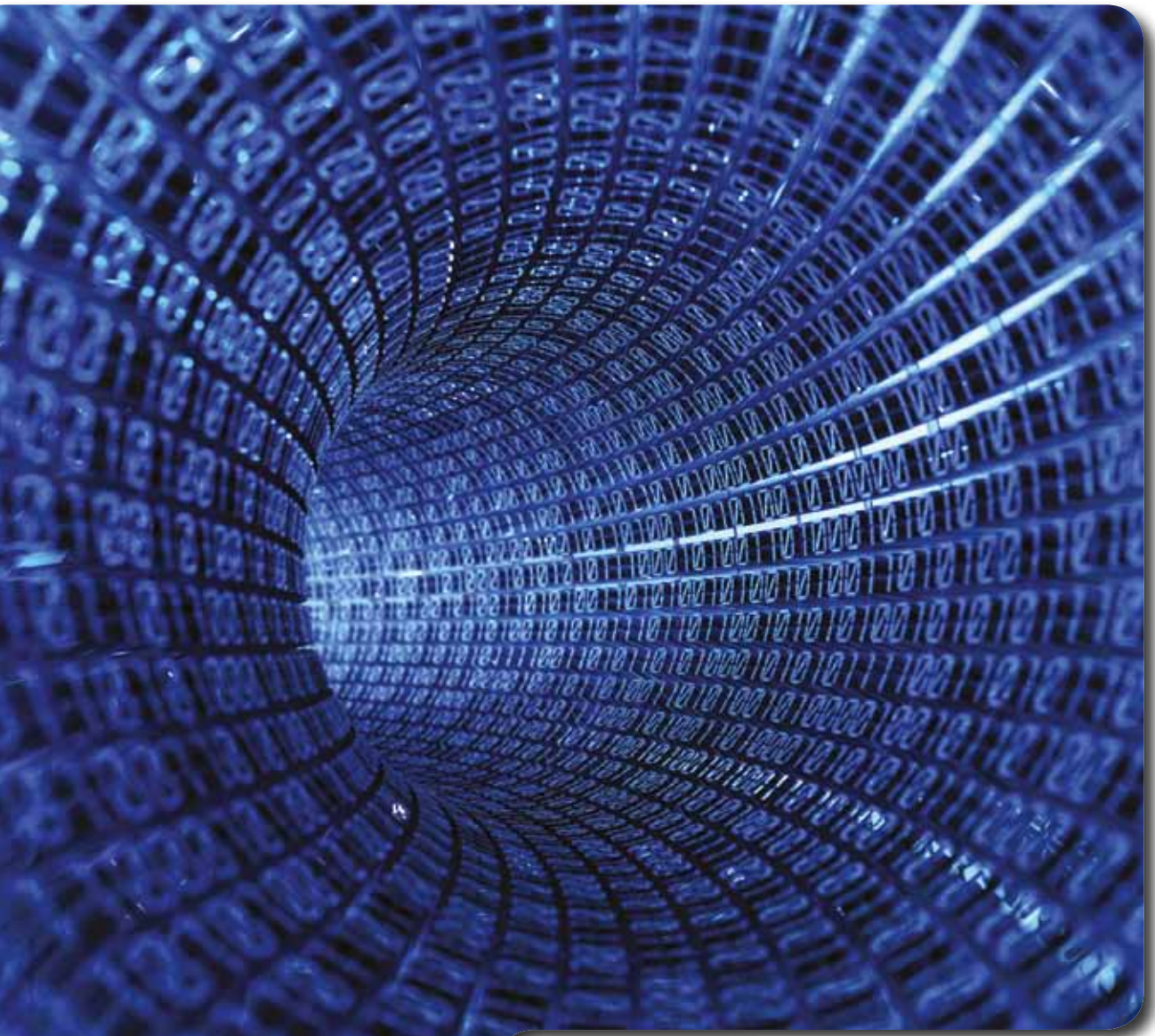




**Australian Government**

**Department of Defence**  
Intelligence and Security



**Australasian Information Security  
Evaluation Program (AISEP)**

# **AISEP Policy Manual**

**Release: 30 August 2011**  
**Version 4.0**



Commonwealth of Australia 2011  
Reproduction is not authorised

All Australian Government information, whether security classified or not, is protected from unauthorised disclosure under the Crimes Act 1914. Australian Government information may only be released in accordance with the Australian Government Protective Security Manual.

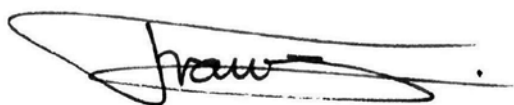
---

## Foreword

The Australian and New Zealand Governments employ Information Technology (IT) security solutions to deliver on-line services and protect official information. The Australasian Information Security Evaluation Program (AISEP) was established to ensure the ready availability of independently evaluated IT security products that meet these needs.

The AISEP is the Program that manages evaluation and certification of IT security products against the internationally recognised Common Criteria (CC) standard. The Defence Signals Directorate (DSD), as the Australian national authority on information security certifies the results of all evaluation tasks performed under the Program. These certification services are provided from DSD to government without cost. Successful completion of certification is published on the Evaluated Products List (EPL) on the DSD website.

This document is the policy for the management and operations of the AISEP.



Joe Franz  
Assistant Secretary  
Information Security Operations  
Defence Signals Directorate

All correspondence in connection with this document should be addressed to:

Director, Evaluations and Industry Coordination  
Information Security Operations  
Defence Signals Directorate  
Locked Bag 5076  
Kingston ACT 2604  
Australia

## Disclaimer

This AISEP Policy Manual has been prepared so as to provide a policy framework for the management and operations of the AISEP. Nothing in the AISEP Policy Manual should be construed as a representation as to the future conduct of the Commonwealth in any particular AISEP activity. The AISEP Policy Manual should not be relied upon as a substitute for independent legal advice.

In the event of any inconsistency, a descending order of precedence shall be accorded to:

- a. Any applicable legislation or law;
- b. The licensing agreement between DSD and AISEF; and
- c. The AISEP Policy Manual.

So that the higher ranked document prevails to the extent of any inconsistency.

## Amendment record

Version	Date	Description
1.0		Initial Release.
2.0	February 2001	Revised and updated.
3.0	21 February 2006	Expansion and clarification of program policy and incorporation of feedback from various sources. Consolidation of previous policy and licence framework documents.
3.1	29 September 2006	Reflection of EPL enhancements to be launched on 29 Sept 2006. Minor policy enhancements/clarifications.
3.2	25 January 2010	Removal of AISEP fees and reference to ITSEC, update of DSD IS organisational structure, policy updates and general editorial amendments.
4.0	30 August 2011	Major revision and update.

# Contents

Foreword.....	iii
Disclaimer.....	iv
Amendment record.....	v
Contents.....	vi
History.....	ix
<b>Chapter 1—Introduction.....</b>	<b>1</b>
1.1 AISEP overview.....	1
1.2 AISEP authority.....	2
1.3 Overview of AISEP policies.....	2
1.4 Mutual recognition agreements.....	2
1.5 Compliance language.....	3
<b>Chapter 2—Organisation of the AISEP.....</b>	<b>5</b>
2.1 AISEP management.....	5
2.1.1 AISEP governance and managerial roles.....	5
2.1.2 GCSB support to the AISEP.....	5
2.2 ACA roles and responsibilities.....	7
2.2.1 ACA management.....	7
2.2.2 ACA certifiers.....	8
2.2.3 ACA quality assurance and compliance.....	9
2.2.3.1 Assessment and compliance.....	9
2.2.3.2 Documentation control.....	9
2.2.3.3 ACA dispute resolution.....	9
2.2.3.4 Common Criteria certificate withdrawal.....	10
2.3 AISEF roles and responsibilities.....	10
2.3.1 AISEF management.....	11
2.3.2 AISEF evaluator.....	11
2.3.2.1 Principal evaluator.....	11
2.3.3 AISEF licensing requirements.....	12
2.3.5 NATA accreditation requirements for the AISEF.....	14
2.3.6 Associated costs for the AISEF.....	15
2.3.6 AISEF impartiality.....	15
2.3.7 AISEF security.....	15
2.3.8 AISEF archiving and disposal.....	17
<b>Chapter 3—AISEP Evaluation and Operational Policy.....</b>	<b>19</b>
3.1 IT security evaluation and certification.....	19
3.1.1 Plan phase.....	19
3.1.2 Conduct phase.....	22
3.1.3 Conclude phase.....	24
3.1.4 AISEF evaluation progress rules.....	24

3.2	AISEP assurance continuity.....	25
3.2.2	AAC acceptance.....	26
3.2.2	AISEP assurance continuity for maintenance.....	26
3.2.3	AISEP assurance continuity for re-evaluation.....	26
3.2.4	Non-compliance of AAC evaluations.....	27
3.3	Supporting functions of program management.....	27
3.3.1	AISEF progress reporting.....	27
3.3.2	Interpretations and technical alignment.....	28
<b>Chapter 4</b>	<b>—Documents and Standards.....</b>	<b>31</b>
4.1	Program standard.....	31
4.1.1	Common Criteria.....	31
4.1.2	Criteria interpretations.....	32
4.1.3	Common Criteria Recognition Arrangement.....	32
4.1.4	Conduct of mutual recognition.....	32
4.1.5	Accreditation standards.....	33
4.2	Program publications.....	33
4.2.1	Program policy and manual.....	33
4.2.2	Stakeholder guidance.....	33
4.2.3	AISEP publication updates.....	33
4.3	Program operational outputs.....	34
4.3.1	Evaluated Products List (EPL).....	34
4.3.2	Certification report.....	35
4.3.3	Certificate.....	35
4.3.4	Maintenance report.....	36
4.3.5	Evaluation technical report.....	36
<b>Chapter 5</b>	<b>—Reviewable Decisions.....</b>	<b>39</b>
5.1	Decisions.....	39
5.1.1	Reviewable decisions.....	39
5.1.2	Non-reviewable decisions.....	39
5.2	Review process.....	40
5.2.1	Requests for review.....	40
5.2.2	Review outcomes.....	40
<b>Chapter 6</b>	<b>—Product Vendor Responsibilities.....</b>	<b>42</b>
6.1	Common Criteria logo marketing.....	42
6.2	Product vendor notification requirements.....	42
<b>Annex A</b>	<b>—References and Abbreviations.....</b>	<b>43</b>
A.1	References.....	43
A.2	Abbreviations.....	44
<b>Annex B</b>	<b>—AISEF Applications.....</b>	<b>45</b>
B.1	Company information.....	45
B.2	Statement of claims.....	46
B.3	Resource capabilities.....	47

# List of Figures

Figure 1: AISEP Stakeholders..... 1

Figure 2: AISEP Management Framework..... 6

Figure 3: ACA Roles ..... 7

Figure 4: AISEF Roles ..... 10

Figure 5: AISEP Evaluation and Certification Workflow of Activities ..... 19

Figure 6: Common Criteria Certification Mark..... 42

---

# History

1. The Australian and New Zealand (Australasian) public and private sectors increasingly rely on information technology. The use of computer systems and networks offer many benefits, but there are also risks associated with their use. This is of particular concern to government agencies and organisations that provide critical services.
2. Users need confidence that products providing security functionality for their IT systems perform as claimed by the product vendor. This confidence is best achieved through an impartial assessment of the product by an independent entity against clearly identified security claims using internationally recognised criteria.
3. In the late 1980s and early 1990s, DSD performed evaluations internally to meet the need for the assessment of IT security products. This provided a level of confidence in the security functionality of key IT security products that were being used by Australian Government agencies. However, with the rapid proliferation of information technology and the reliance on security, the demand for evaluated products grew. In June 1994, DSD announced the establishment of the Australian Information Security Evaluation Program (AISEP).
4. Initially, evaluations in Australia were undertaken solely in accordance with the European Information Technology Security Evaluation Criteria (ITSEC) standard (Ref. [1]). The ITSEC standard is a harmonised version of national security evaluation criteria developed by the United Kingdom, France, the Netherlands and Germany in the early 1990s.
5. In the mid-1990s, the Common Criteria (CC) project began to consolidate the evaluation criteria of the European nations, the United States and Canada and to establish a foundation for widespread mutual recognition of evaluation results through the Arrangement on the Recognition of Common Criteria Certificates in the Field of IT Security (also known as the Common Criteria Recognition Arrangement, or CCRA).
6. The CC replaced national criteria with a worldwide standard: version 2.1 and it was accepted by the International Organisation for Standardisation (ISO) on 15 November 1998 as ISO standard 15408. Since then, it has been updated (Refs. [2], [3], [4] and [5]).
7. In 1998, the AISEP began adopting the CC as approved IT security evaluation criteria. Australia and New Zealand merged their evaluation and certification capabilities in the same year, and the program was renamed the Australasian Information Security Evaluation Program (AISEP).
8. In the Program, IT security evaluation activities are outsourced to licensed commercial evaluation facilities called Australasian Information Security Evaluation Facilities (AISEFs). The Australasian Certification Authority (ACA) is the oversight body, established through DSD.
9. On 22 September 1999, the Management Committee of the CCRA voted unanimously to accept Australia and New Zealand, through the AISEP, as certificate-producing participants of the CCRA. Also through the AISEP, Australia and New Zealand established an agreement with the United Kingdom to mutually recognise all ITSEC certificates and the maintenance of these certificates through each nation's programs.
10. In 2011, the AISEP ceased to conduct ITSEC evaluations and certificate maintenance to focus solely on CC. At this time, DSD began participating in creating technology tailored Protection Profiles (PPs) using the CC Standard.
11. PPs are documents that contain a benchmark of security requirements for a technology that a product vendor must meet to pass evaluation. CC participating governments and industry experts form technical groups to develop the PPs. Through PPs, DSD can influence industry to build security products that meet Australian government needs. DSD approved PPs are listed on the EPL.



# Chapter 1—Introduction

## 1.1 AISEP overview

12. The AISEP mission statement is:

*The Australasian Information Security Evaluation Program (AISEP) exists to ensure that a range of evaluated IT security products are available to meet the needs of Australian and New Zealand government agencies in securing their official resources.*

13. The Defence Signals Directorate (DSD), together with the New Zealand Government Communications Security Bureau (GCSB) administers the AISEP within DSD's Cyber and Information Security Division (CISD). GCSB participates through its Information Assurance (IA) and Cyber Security Division. Through DSD, financial support is provided to the AISEP.
14. DSD licenses commercial facilities to conduct Common Criteria evaluations under the Program. These are known as Australasian Information Security Evaluation Facilities (AISEFs). The function of certifying these evaluation results is retained by DSD through its certification body, the Australasian Certification Authority (ACA).
15. An IT security product vendor who wishes to have a product evaluated in the Program must engage an AISEF to conduct the evaluation. The AISEF and ACA undertake evaluation and certification activities through collaboration. Individuals or organisations that acquire and use certified IT security products are known as consumers. In particular, the AISEP's primary consumers are Australian and New Zealand government agencies. The ACA interacts with consumers to understand their needs for evaluation. These entities and relationships are illustrated in Figure 1: AISEP Stakeholders.

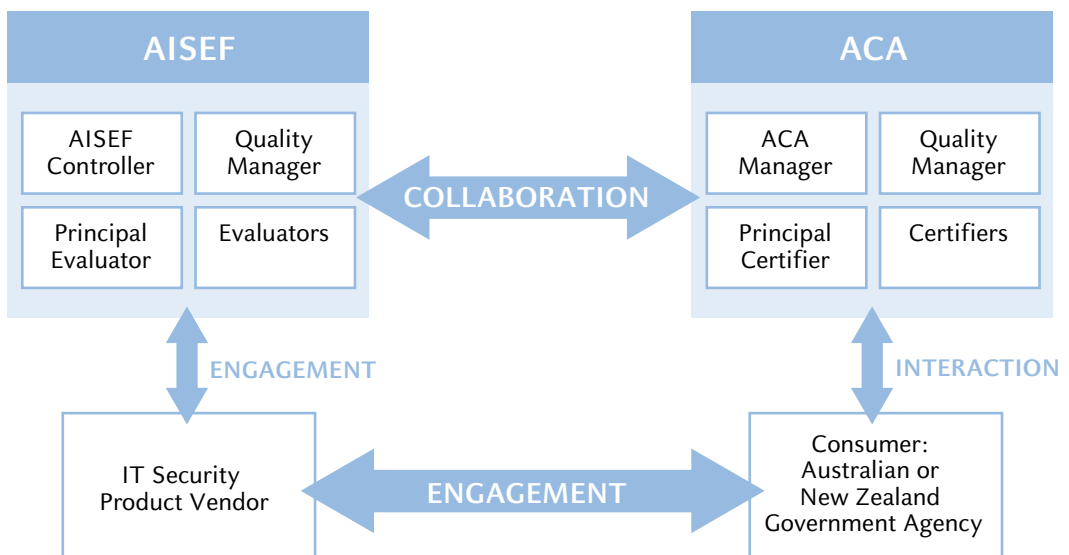


Figure 1: AISEP Stakeholders

## 1.2 AISEP authority

16. The authority of the AISEP resides with the Director of DSD (DDSD).
17. DDSD delegates this authority to the Deputy Director Cyber and Information Security (DDCIS).
18. The Director of Evaluation and Industry Coordination (DEI) is responsible for overseeing stakeholder compliance and implementation of the AISEP policies. DEI does this through the Manager of the Australasian Certification Authority (ACA).

## 1.3 Overview of AISEP policies

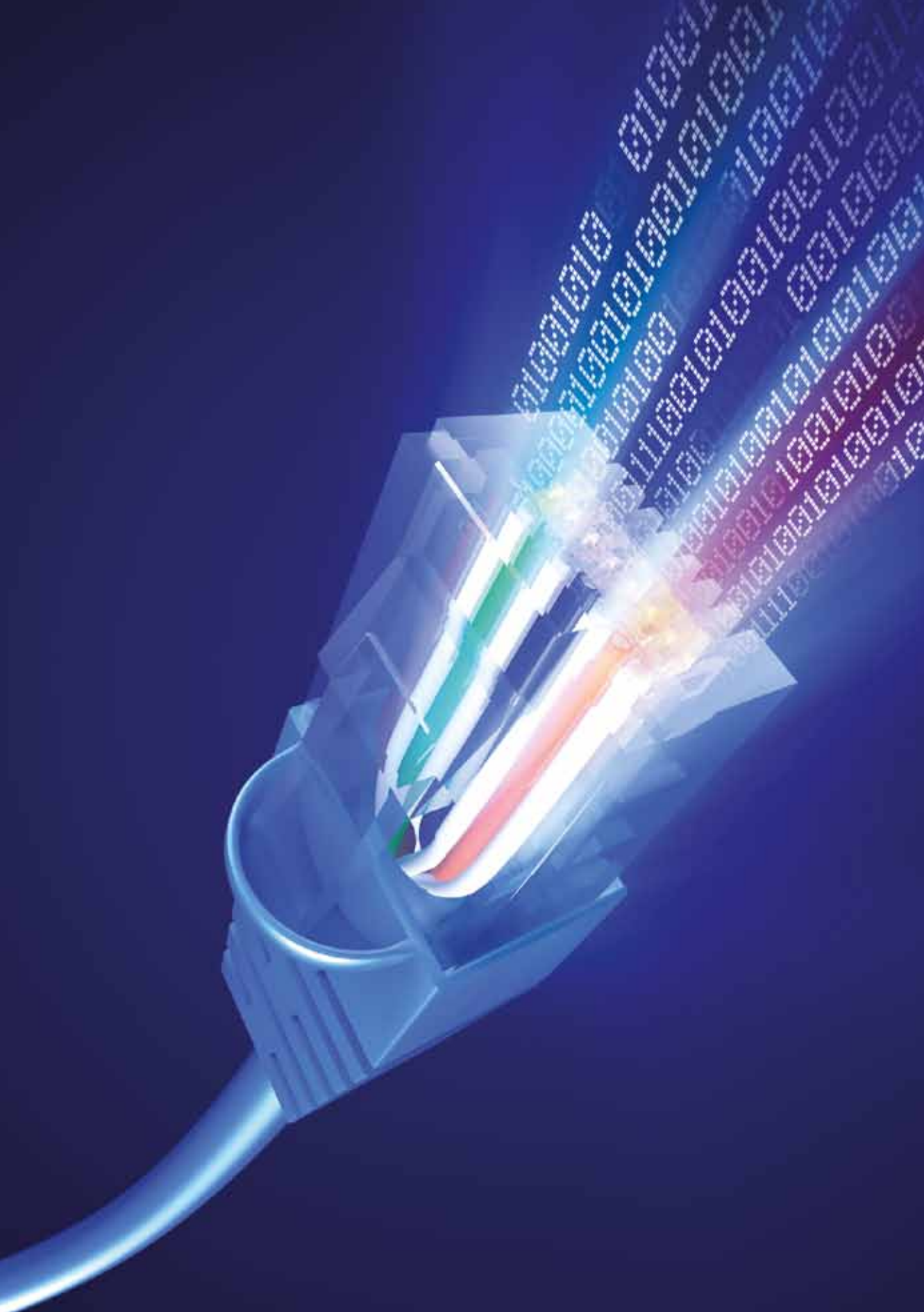
19. The AISEP Policies provide a framework for IT security evaluations performed in Australia.
20. The AISEP Policy Manual (APM) provides the managerial and operational policy framework. This is the parent policy document for the AISEP.
21. This document has been organised into the following chapters:
  - a. **Chapter 2 – Organisation of the AISEP:** The key roles in the management and operations of the AISEP.
  - b. **Chapter 3 – AISEP Evaluation and Operational Policy:** The day-to-day operations of the AISEP business functions of evaluation and certification, assurance continuity and mutual recognition.
  - c. **Chapter 4 – Documents and Standards:** Documents, publications and standards that have an influence on the AISEP and its operations.
  - d. **Chapter 5 – Reviewable Decisions:** The ACA decisions that are reviewable.
  - e. **Chapter 6 – Product Vendor Responsibilities:** Information for product vendor marketing and notification responsibilities.
22. The APM is complemented by two additional policy documents, which outline specific guidance for key AISEP stakeholders. These documents are not publically available.
  - a. **Certifier Policy:** Specific guidance to the Australasian Certification Authority (ACA).
  - b. **Evaluator Policy:** Specific guidance to Australasian Information Security Evaluation Facilities (AISEFs).

## 1.4 Mutual recognition agreements

23. DSD and GCSB have agreements in place to mutually recognise the results of IT security evaluations. Authorised arrangements and understandings are identified in section 4.1.3 and briefly described below.
24. At the time of publication, two mutual recognition arrangements exist:
  - a. **ITSEC MOU:** An arrangement with the United Kingdom to recognise all Information Technology Security Evaluation Criteria (ITSEC) certificates.
  - b. **CCRA:** The Common Criteria Recognition Arrangement, which is shared between a number of nations. See <http://www.commoncriteriaportal.org>. This arrangement relates to CC certificates of Evaluation Assurance Levels 1–4 and may include flaw remediation.
25. CC mutual recognition extends to evaluations that are compliant with a DSD approved Protection Profile.

## 1.5 Compliance language

26. The language used in this document indicates the required compliance. A **MUST/MUST NOT** in bold, upper-case format is a requirement or course of action that is mandatory or prohibited, respectively. Stakeholders deviating from a '**MUST**' **MUST** seek permission from the ACA.



# Chapter 2—Organisation of the AISEP

27. This chapter contains the AISEP roles and operational policy that is performed by:
- AISEP management:** Provides strategic governance and management direction;
  - Australasian Certification Authority (ACA) roles and responsibilities:** Performs the strategic oversight and certification activities under the rules of the CCRA; and
  - AISEP roles and responsibilities:** Conduct IT security evaluations against the CC standard and in accordance with the AISEP Policies.

## 2.1 AISEP management

### 2.1.1 AISEP governance and managerial roles

28. The following officials from DSD participate in the management of the AISEP:
- Director DSD:** The authority for the AISEP.
  - Deputy Director Cyber and Information Security Division (DDCIS):** Provides strategic direction and is the delegated signatory authority for the ACA.
  - Assistant Secretary Information Security Operations (ASISO):** Coordinates the strategic direction set by DDCIS across the organisation's Information Security Operations Branch. ASISO is the signatory to this document.
  - Director Evaluations and Industry Coordination (DEI):** Distils strategic direction established by DDCIS and ASISO for AISEP alignment.
  - ACA Manager:** Manages the Program and implements the strategic direction of the AISEP with its stakeholders in collaboration with the Principal Certifier.
  - Principal Certifier:** Assists the ACA Manager and oversees the technical consistency across the Program.

### 2.1.2 GCSB support to the AISEP

29. The following officials from GCSB participate in the management of the AISEP:
- Director GCSB:** Exercises strategic direction on behalf of New Zealand, through delegation to the Deputy Director Information Assurance and Cyber Security (DDIACS).
  - Deputy Director Information Assurance and Cyber Security (DDIACS):** Executes direction from the Director GCSB, allocates GCSB resources to the program and interacts with DSD's DDCIS to establish strategic direction.

30. Figure 2: AISEP Management Framework illustrates the relationship across GCSB and DSD.

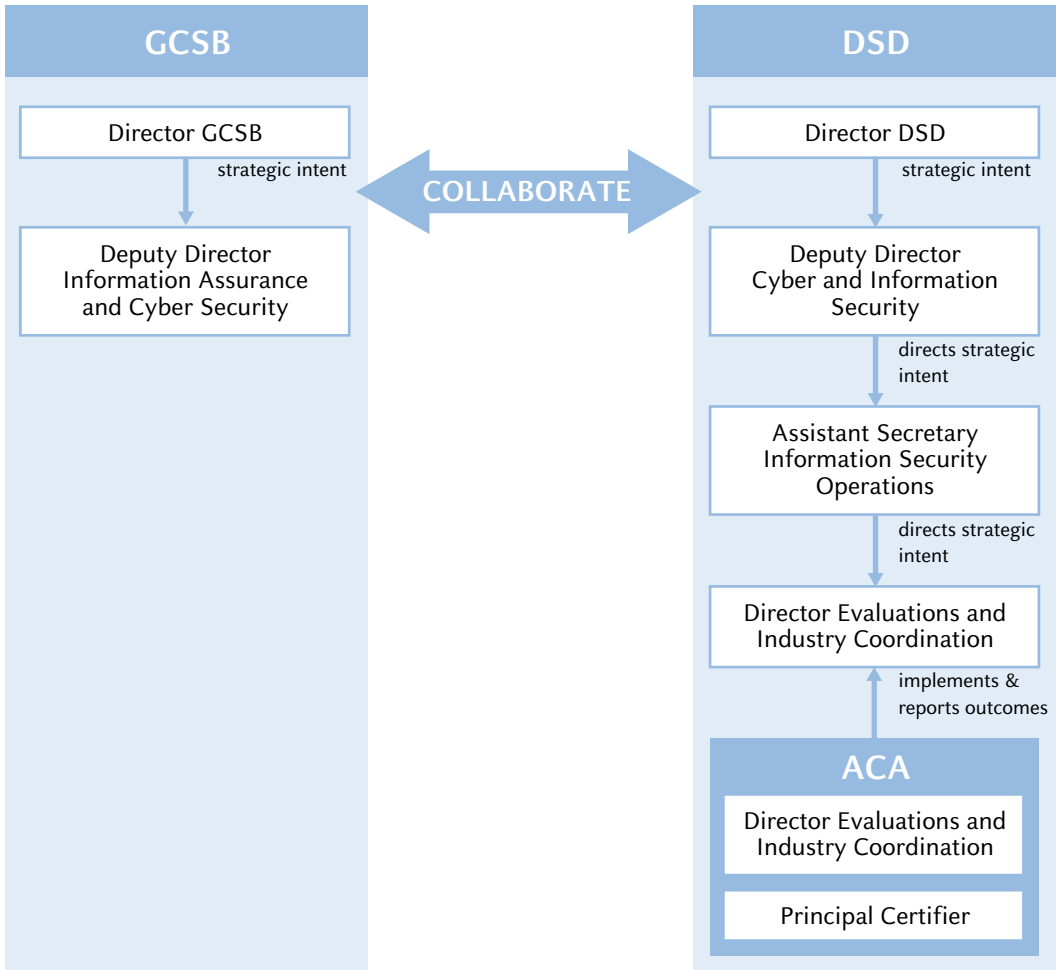


Figure 2: AISEP Management Framework

## 2.2 ACA roles and responsibilities

31. The ACA roles that oversee the day-to-day activities of the AISEP are illustrated in Figure 3: ACA Roles.

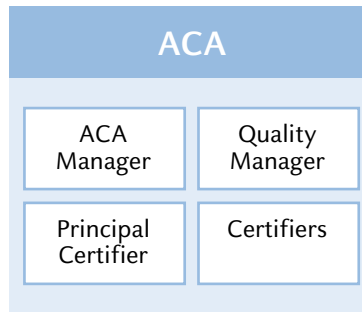


Figure 3: ACA Roles

### 2.2.1 ACA management

32. The responsibility of the ACA Manager is to:
- a. Oversee the operations of the AISEF;
  - b. Coordinate and chair the AISEF Controllers Meetings (ACM);
  - c. Oversee the operation of the ACA's quality management system with other ACA management;
  - d. Report AISEP business to senior DSD and GCSB management; and
  - e. Liaise and foster relationships with AISEP stakeholders.
33. The responsibility of the Principal Certifier is to:
- a. Manage certifications and allocate resources as required;
  - b. Report to senior DSD management on the technical operations of the AISEP;
  - c. Oversee the operation of the ACA's quality management system with other ACA management;
  - d. Ensure the technical validity and accuracy of information contained in ACA technical reports and documents;
  - e. Ensure technical alignment within the AISEP and with the international CC community; and
  - f. Manage the technical development of certification staff and associated training.

34. The responsibility of the Quality Manager is to:
- a. Administer and operate the ACA's quality management system and provide central quality control duties for the ACA;
  - b. Maintain a register of ACA certifier qualifications, training and experience;
  - c. Maintain a register of AISEF evaluator qualifications, training and experience; and
  - d. Conduct internal quality audits.

### 2.2.2 ACA certifiers

35. The ACA maintains technical staff, known as certifiers, to perform the functions of certification and certificate assurance continuity for the AISEP.
36. The ACA Certifier is to:
- a. Hold a relevant tertiary qualification in a field such as computer science, information security, networking, communications and software engineering or equivalent practical experience;
  - b. Have an understanding of IT security principles and technologies; and
  - c. Have completed the DSD and AISEP certifier training.
37. The responsibility of a Certifier is to:
- a. Manage and conduct CC certification in partnership with AISEF Evaluators;
  - b. Continue to advance skills in IT security evaluation and information security principles and technologies; and
  - c. Adhere to AISEP quality controls.
38. Certifiers perform a variety of IT security work in addition to leading or supporting certifications. Certifiers provide a leading role in a certification task through:
- a. Ongoing technical training;
  - b. Leveraging subject matter experts (SMEs) in the organisation; and
  - c. Close technical interaction with the AISEF Evaluators.
39. With the technical oversight of the Principal Certifier, certifiers lead certification tasks of EAL 1-4 and PP compliant evaluations.
40. The ACA Management ensures certifiers have clear, up to date, documented instructions regarding their duties and responsibilities. The ACA does not employ contractors to perform certification duties.

### 2.2.3 ACA quality assurance and compliance

41. The ACA manages quality assurance and compliance business functions that ensure the ACA maintains compliance with quality standards and CCRA requirements (Ref. [6]).
42. Additionally, the ACA continually assesses the AISEF through normal day-to-day involvement in the certification of evaluations. If the ACA sees the need, it may assess the AISEF regarding compliance with the *APM* (this document) as specified in section 2.3.3.1 below and the *AISEP Evaluator Policy* (Ref. [14]).

#### 2.2.3.1 Assessment and compliance

43. The ACA must undergo independent assessment by other CCRA member nations as defined in *Annex D of the CCRA* (Ref. [6]). This occurs at least once every five years and is to maintain status as a certificate producing CC scheme.
44. The ACA conducts internal self-assessments to ensure compliance with the requirements specified in *Annexes B and C of the CCRA* (Ref. [6]). In addition, peer review and documentation review procedures are in place to ensure the ACA operations are administered in a non-discriminatory manner.
45. The Quality Manager maintains an audit schedule for conducting internal audits of the ACA's compliance with particular requirements specified in Annex C of the *CCRA* (Ref. [6]).
46. The ACA maintains the results of management reviews and internal audits in accordance with Australian archives regulations and internal policies, for a period of seven years (Ref. [13]).

#### 2.2.3.2 Documentation control

47. The ACA maintains a system for the control of documentation ensuring that:
  - a. Current documentation is available to key stakeholders;
  - b. Documents are not amended or superseded without authorisation;
  - c. Changes are promulgated in such a way that those who need to know are informed promptly;
  - d. All records are stored securely and are accessible for a period of at least seven years; and
  - e. Superseded documents are declared void.

#### 2.2.3.3 ACA dispute resolution

48. A dispute resolution process is in place that enables stakeholders to identify problems and inconsistencies in the AISEP. The AISEF and/or an Evaluator may contact the ACA Manager directly to raise a concern about the Program or ACA staff.
49. The product vendor also has the opportunity to contact the ACA Manager directly should any concern arise about an AISEF, its staff or the ACA.
50. The ACA holds a raised concern or a formal complaint in the strictest confidence.

51. The ACA provides a client feedback process that allows the product vendor and the AISEF to raise suggestions for process improvement throughout an evaluation task. Items that are raised at a formal meeting are minuted and resolved.
52. The ACA exercises control regarding the use of awarded Common Criteria certificates. The ACA implements mechanisms to prevent or counter the misuse of certificates and to correct false, misleading or improper statements in relation to the certificate or the AISEP.
53. The ACA communicates in the formal meetings at the beginning and end of the evaluation task to inform and remind the product vendor of their obligation to use the certificate correctly and to refrain from misrepresenting the AISEP. The ACA Manager is responsible for taking action if AISEP certificates or marketing is found to be misused.

### 2.2.3.4 Common Criteria certificate withdrawal

54. A certificate is withdrawn when:
  - a. Serious technical inaccuracies in the evaluation or evaluation impropriety is identified after certification; or
  - b. The product vendor provided false or misleading evaluation evidence.

*Note: A decision to withdraw a certificate is a reviewable decision under Chapter 5—Reviewable decisions.*
55. The following actions are taken when the ACA withdraws a certificate:
  - a. The product vendor and AISEF are formally notified with justification for the withdrawal;
  - b. The EPL entry is removed; and
  - c. The Common Criteria Portal administrator is notified;

## 2.3 AISEF roles and responsibilities

56. The AISEF roles that undertake the evaluation activities of the AISEP are illustrated in Figure 4: **AISEF Roles**.

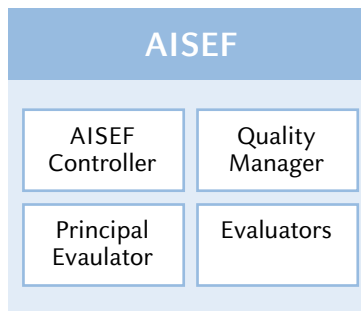


Figure 4: AISEF Roles

### 2.3.1 AISEF management

57. The AISEF management structure **MUST** have an AISEF Controller who **MUST**:
  - a. Be responsible for the management of the AISEF;
  - b. Have expertise in project and contract management and quality control;
  - c. Have a sound understanding of, and ensure compliance to, AISEP policy; and
  - d. Ensure that any conflicts of interest are managed and declared to the ACA Manager.
58. The AISEF Controller **MUST** be supported by the following roles:
  - a. AISEF Principal Evaluator: Responsible to the AISEF Controller for the effective application of accepted IT security evaluation criteria within the AISEF.
  - b. AISEF Quality Manager: Responsible for the implementation and management of the AISEF quality system.
  - c. AISEF Facility Security Officer: Responsible for AISEF security, which includes physical, personnel and information security.
59. An individual may be nominated to perform several or all of these roles, provided that person has the required experience and conflicts of interest do not arise. The ACA reserves the right to reject an individual from holding several positions where, in the reasonable opinion of the ACA, it is inappropriate.
60. The AISEF **MUST** report to the ACA if any staff member approved by the ACA to perform a defined role ceases to perform that role. This **MUST** be made in writing within one week. This **MUST** also be reflected in the next AISEF Progress Report as defined in section 3.3.1 below.

### 2.3.2 AISEF evaluator

61. The AISEF must apply in writing to the ACA for approval of AISEF evaluator status. The application must include the applicant's curriculum vitae detailing their skills, experience and training in order for the ACA to process the decision.
62. The AISEF **MUST** at all times maintain trained staff capable of undertaking evaluation tasks. The minimum number of AISEF evaluation staff should be three, with one member in the Principal Evaluator position. AISEF evaluators may seek subject matter expert advice on testing when the expertise is available in their organisation.
63. When these conditions are not met, the AISEF **MUST** inform the ACA in writing with a proposed solution in the AISEF reports as defined in section 3.3.1 below.

#### 2.3.2.1 Principal evaluator

64. The Principal Evaluator has responsibilities as defined in paragraph 58 above in addition to the requirement for an Evaluator as described below.
65. The Evaluator is to:
  - a. Hold a relevant tertiary qualification in a field such as computer science, information security, networking, communications and software engineering or equivalent practical experience; and
  - b. Have an understanding of IT security principles and technologies;

66. The Evaluator **MUST**:
- a. Have completed the DSD AISEP training;
  - b. Undergo or completed AISEF CC training;
  - c. Learn or have experience in CC evaluations;
  - d. Conduct evaluation tasks in partnership with one or more Evaluators; and
  - e. Continue to advance their skills in IT security evaluation and information security principles and technologies.

### 2.3.2.2 Evaluator status

67. Principal Evaluator and Evaluator status can lapse in the case of the individual not performing evaluation work for one year at the discretion of the ACA.
68. The ACA may reinstate a lapsed evaluator status on the Evaluator's return to an AISEF position. This will depend on the following conditions:
- a. Length of absence;
  - b. Previous Evaluator status;
  - c. Length of Evaluator service;
  - d. Relevant experience during absence; and
  - e. Demonstrable competence.

*Note: A decision not to reinstate an Evaluator's status on their return to an AISEF position is a reviewable decision under Chapter 5 — Reviewable decisions.*

69. The status of an AISEF evaluator is recognised only within the AISEP and should not be used as an ACA endorsement of the Evaluator's qualification to perform work outside the AISEP.

### 2.3.3 AISEF licensing requirements

70. The ACA does not restrict the number of licensed AISEFs. To be eligible to become an AISEF, an applicant **MUST** be:
- a. An Australian or New Zealand legal commercial entity; and
  - b. Operational within Australia and/or New Zealand.
71. An organisation wishing to apply for an AISEF licence **MUST** submit a written proposal to the ACA providing detailed information about how it intends to implement and maintain the requirements for operating as an AISEF. Required details are described in Annex B of this document.
72. On receipt of the proposal, the ACA assesses the applicant. The ACA determines the applicant organisation's ability to meet the requirements to operate an evaluation facility under the AISEP and approve or rejects the proposal.
73. The ACA may ask an applicant to clarify information contained in the proposal, or to provide additional information at any time prior to making its decision.

74. An AISEF licence is granted when the following conditions have been met:
- The applicant has submitted the proposal to the ACA;
  - The ACA has formally accepted the applicant's proposal; and
  - The applicant has agreed to the conditions of the AISEF licensing agreement.
- Note: A standard licensing agreement is available on request from the ACA.*
75. Where the ACA rejects an organisation's application for an AISEF licence, the ACA may, at its discretion, provide reasons for the decision.
- Note: The decision not to grant to an applicant an AISEF licence is NOT reviewable under Chapter 5 — Reviewable decisions.*
76. An unsuccessful applicant may reapply to become a licensed AISEF six months following the date of the ACA's decision not to grant an AISEF licence. An organisation making a second or subsequent application **MUST** undergo the process in its entirety.
77. On acceptance of an applicant's proposal to become an AISEF, the ACA will:
- Inform the organisation of its success;
  - Facilitate the signing of the licence agreement; and
  - List the facility on DSD's AISEP website and identify the AISEF as "New and preparing for NATA accreditation".

### 2.3.3.1 AISEF licence monitoring

78. The ACA assesses the AISEF's adherence to AISEP policy and licence conditions during the day-to-day activities of the conduct of evaluation work.
79. NATA carries out the following assessments of the AISEF for compliance with the NATA requirements as identified in section 2.3.4 below:
- A technical reassessment at which the ACA may attend as an observer. This occurs every three years; and
  - A surveillance visit with a focus on assessing the management system. This occurs 18 months following the technical assessment.
80. In the instance of a non-compliant AISEF, the ACA may initiate the following two stage process to discontinue the AISEF licence:
- Suspension; and
  - Termination.
81. The ACA may suspend the AISEF licence in the following circumstances:
- The AISEF is not compliant with AISEP policy;
  - NATA has suspended the AISEF accreditation;
  - The AISEF ceases to employ suitably qualified staff to maintain the required management structure or to maintain a minimum evaluation team; or
  - The AISEF fails to comply with the conditions and term specified in the licence agreement.
- Note: The decision to suspend an AISEF's licence is NOT a reviewable decision under Chapter 5 — Reviewable decisions.*

82. An AISEF with a suspended licence **MUST NOT** carry out evaluation work. The AISEF **MUST NOT**:
- Advertise its services as an AISEF; or
  - Continue to bid for evaluation work.
83. The ACA reviews the suspended status when the suspended AISEF notifies the ACA that the concerns that caused the suspension have been rectified.
84. The ACA may terminate an AISEF licence if:
- NATA has cancelled the AISEF accreditation;
  - The AISEF ceases to maintain minimum staffing levels as specified in section 2.3.2 above; or
  - The AISEF fails to rectify an issue that caused licence suspension within a reasonable timeframe considered appropriate in the opinion of the ACA.
- Note: The ACA's decision to terminate an AISEF's licence is NOT a reviewable decision under Chapter 5 — Reviewable decisions.*
85. An AISEF with a terminated licence **MUST NOT** carry out activities under the auspices of the AISEP.
86. An organisation that was a former AISEF may seek reinstatement by reapplying for a licence. In assessing a reapplication, the ACA will pay particular attention to those characteristics that caused the licence termination to ensure that Program quality is upheld.

### 2.3.5 NATA accreditation requirements for the AISEF

87. An AISEF **MUST** submit an application to NATA for accreditation as a test laboratory. Test laboratory status **MUST** be achieved:
- Within the first year of the AISEF's operation, and
  - Before the end of the conclude phase for the AISEF's first evaluation requiring recognition under the CCRA.
- Note: The conclude phase of an evaluation project is deemed to end two calendar months after ACA acceptance of the final version of the Evaluation Technical Report (ETR) associated with that evaluation.*
88. An AISEF **MUST** be accredited by NATA against the *ISO/IEC 17025: Field Application Document, Information and Communications Technology Testing, Supplementary requirements for accreditation* (Ref. [8]) within the first year of its operation.
89. An organisation wishing to maintain its AISEF licence **MUST** continue to comply with licensing requirements and **MUST** submit to continual monitoring by the ACA and NATA. A failure by an organisation to comply with the licensing agreement may result in the ACA suspending or terminating the licence.

### 2.3.6 Associated costs for the AISEF

90. The AISEF is required to pay a fee to NATA for conducting accreditation activities. AISEFs should contact NATA directly for enquiries about costs associated with obtaining and maintaining NATA accreditation.
91. The AISEF should be aware of other costs associated with operating an AISEF, which may include the following:
  - a. Training costs to maintain a level of competence for staff members;
  - b. Equipment and material costs to support testing of an evaluation; and
  - c. Operational costs associated with maintaining a secure evaluation facility.

### 2.3.6 AISEF impartiality

92. The AISEF **MUST** be able to operate as an independent, self-contained unit. It should be functionally separate from its parent organisation in its operations and administration, including separate accommodation with its own controlled access.
93. The AISEF Controller **MUST** be able to demonstrate to the ACA that the AISEF or any staff member is impartial in their conduct of an evaluation.
94. Further, an AISEF **MUST NOT**:
  - a. Evaluate a product developed and/or owned by its parent organisation or subsidiaries, or a product developed and/or owned by another organisation in which the parent organisation has a commercial or financial interest;
  - b. Allow any individual who has been involved in the development of the product and/or evaluation documentation to be involved in the evaluation of the product; or
  - c. Provide consultancy or advice to a product vendor or developer that compromises the independence of an evaluation.

*Note: The ACA permits an AISEF to provide both evaluation support consulting and evaluation services to a product developer; however, the AISEF MUST be able to demonstrate the separation of these activities from evaluation activities.*

### 2.3.7 AISEF security

95. An AISEF **MUST** be a member of the Defence Industry Security Program (DISP) with physical and ICT systems accredited to DISP requirements. AISEF personnel performing a function under the *AISEP Policy Manual* (this document) **MUST** hold the appropriate security clearance required by DISP prior to commencing work.
96. The AISEF **MUST** implement sound security practices and procedures to protect the confidentiality and integrity of commercially sensitive information.
97. The AISEF **MUST** implement mechanisms to ensure separation between evaluation tasks and to ensure that all documentation and resources associated with each task are accessed on a strictly need-to-know basis.

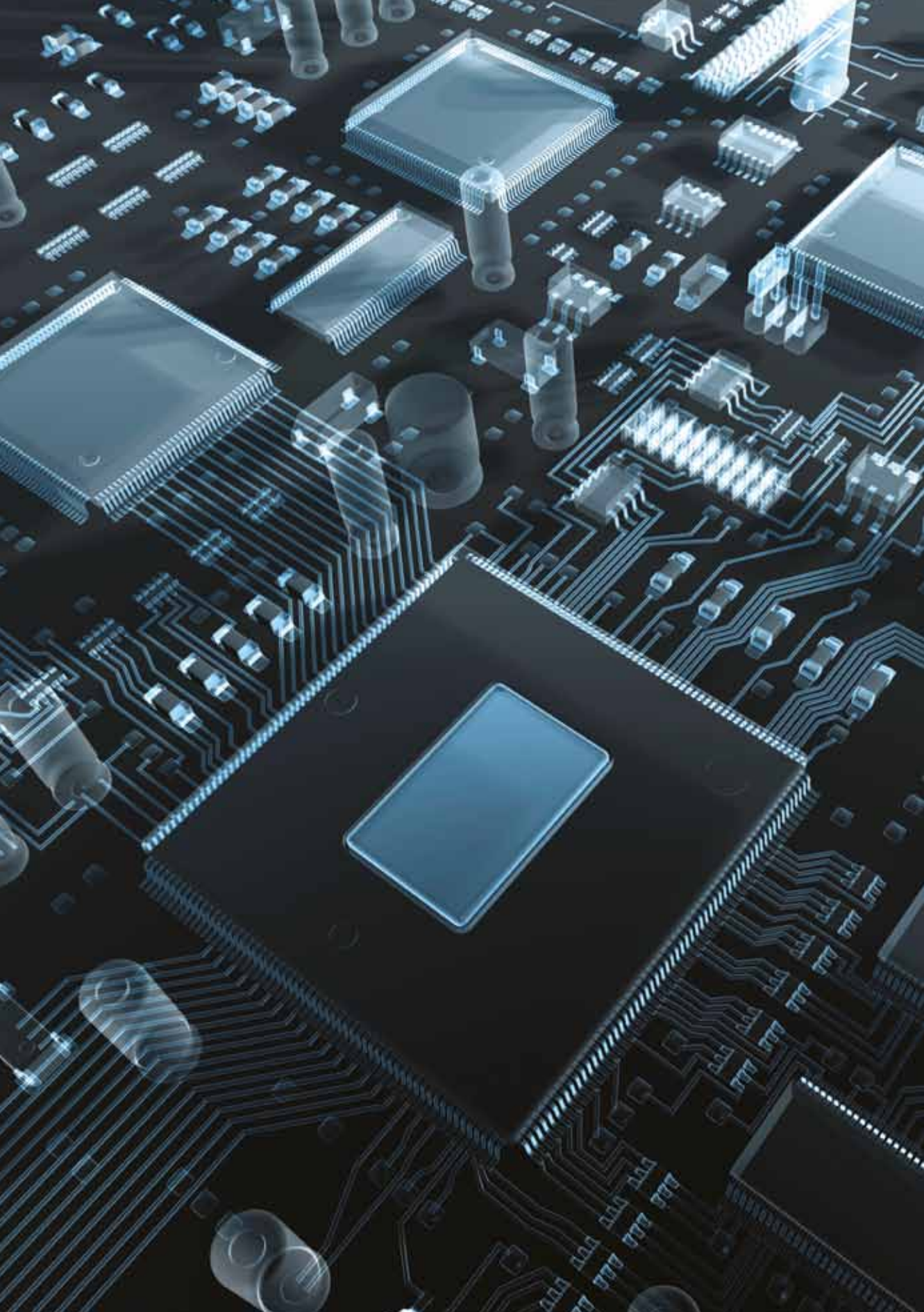
98. The AISEF **MUST** nominate a Facility Security Officer, assigned overall responsibility for security within the AISEF.
99. The AISEF **MUST** have documented security policies and supporting procedures. As a minimum, these documents **MUST** address the following:
  - a. Physical security;
  - b. Personnel security; and
  - c. Information security.

### 2.3.7.1 AISEF information security

100. The AISEF **MUST** use DSD approved cryptographic algorithms and protocols as specified in the *Australian Government Information Security Manual (ISM)* (Ref. [10]) for the protection of evaluation and commercially sensitive information. Cryptographic protocols and algorithms are used when evaluation material is stored and/or transmitted over a public network.
101. Evaluation and commercially sensitive information and material **MUST** be marked with the appropriate label. DSD uses Dissemination Limiting Markers (DLM) for information whose disclosure may be limited or prohibited by legislation, or which may otherwise require special handling.
102. In the AISEP, evaluation information and material **MUST** be marked with the appropriate DLM and **MUST NOT** be distributed beyond AISEF and ACA staff without the express written permission of the ACA. In addition, a label of **EVALUATION-IN-CONFIDENCE** and **COMMERCIAL-IN-CONFIDENCE** **MUST** be used with the DLM to indicate who the limited distribution applies to. Guidance on the use of DLMs is provided in the *AISEP Evaluator Policy* (Ref: [14]).
103. Evaluation information and material that is marked with a DLM that is exposed outside the Evaluator and Certifier relationship, may compromise:
  - a. The outcome of an evaluation or certification;
  - b. The integrity of the AISEP;
  - c. The intellectual property of the ACA or an AISEF; and/or
  - d. The intellectual property of the product vendor.

### 2.3.8 AISEF archiving and disposal

104. At the completion of an evaluation task, the AISEF **MUST** archive or dispose of all material supplied for the evaluation as agreed at the Task Start-up Meeting (TSM).
105. Adequate records **MUST** be retained by both the ACA and AISEF to ensure the reproducibility and repeatability of the task, and to comply with the requirements of the *Australian Archives Act* (Ref. [13])
106. The AISEF **MUST** maintain for a period of seven years those records that demonstrate adherence to:
  - a. Quality processes;
  - b. Security policies and procedures; and
  - c. Evaluation activities.



# Chapter 3—AISEP Evaluation and Operational Policy

## 3.1 IT security evaluation and certification

107. The AISEP's evaluation and certification workflow of activities comprises five major phases. Figure 5: AISEP Evaluation and Certification Workflow of Activities illustrates the phases of Initiate, Plan, Conduct, Conclude and Continuity.
108. The Initiate phase precedes IT security evaluation and certification and enables stakeholders to discuss evaluation needs. The Plan, Conduct and Conclude phases are described in this chapter. The Continuity phase exists for product vendors when they are seeking to extend their CC certificate to cover minor changes from the original evaluation. Assurance continuity is described in section 3.2 below.

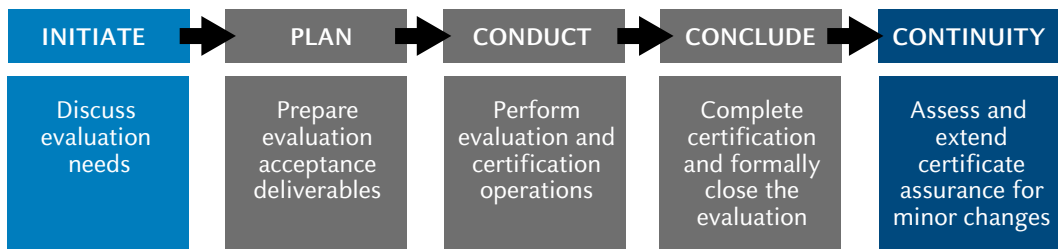


Figure 5: AISEP Evaluation and Certification Workflow of Activities

109. This chapter describes the following three major phases:
- Plan phase:** Stakeholders plan evaluation and support activities.
  - Conduct phase:** Evaluators and certifiers conduct their respective activities and ensure compliance with AISEP policies and IT evaluation criteria.
  - Conclude phase:** Evaluation activities are completed and certification may be granted.

### 3.1.1 Plan phase

#### 3.1.1.1 Letter of recommendation for evaluation

110. AISEP evaluation requires an Australasian government agency need to be identified through a *Letter of Recommendation for Evaluation*. Government agency need is already established where a DSD approved Protection Profile exists for product technologies.

111. The *Letter of Recommendation for Evaluation* may be submitted by an AISEF, product vendor or government agency. A template for this letter is available from the DSD website.
112. The *Letter of Recommendation for Evaluation* forms part of the AISEP Acceptance Package (AAP). Early submission of the Letter is desirable as it enables the ACA to engage the Government agency on their evaluation needs prior to the ACA's review of the evaluation task for acceptance.

### 3.1.1.2 AISEP acceptance package

113. The AISEF submits an evaluation task into the AISEP for acceptance through an AISEP Acceptance Package (AAP).
114. The AISEF **MUST** submit a paper and electronic copy of the specified AAP to the ACA for each evaluation request. The ACA will only commence review of an AAP on receipt of both the paper and electronic copy. The AAP **MUST** contain:
  - a. A covering letter that identifies the evaluation task and a statement of suitability. This details the steps that the AISEF has taken to ensure that the evaluation request is suitable for entry into the AISEP as specified in paragraph 115 below and that the product vendor has been made aware of its obligations. This deliverable is supplied by the AISEF.
  - b. An Evaluation Work Plan (EWP) that documents the deliverables required in the *AISEP Evaluator Policy* (Ref. [14]) including a unique task identifier for the evaluation. The proposed evaluation timeframe **MUST** be achievable by the AISEF and the product vendor. This deliverable is supplied by the AISEF with input from the product vendor.
  - c. The EWP **MUST** include a proposal of the evaluation team that includes the Principal Evaluator as the technical oversight and a nominated lead Evaluator as a minimum. The AISEF may decide on any number of additional evaluators. This deliverable is supplied by the AISEF.
  - d. The Security Target (ST) and the approved PP if applicable to the proposed evaluation. This deliverable is supplied by the product vendor via the AISEF.
  - e. A completed ST review using any guidelines provided by the ACA. This deliverable is supplied by the AISEF.

### 3.1.1.3 Acceptance requirements for an evaluation task

115. The following **MUST** be adequately satisfied for the ACA to accept an evaluation task into the AISEP:
  - a. An adequate Australasian government *Letter of Recommendation for Evaluation* has been provided to the ACA in the case of an evaluation that is not compliant with a DSD approved Protection Profile;
  - b. The submitted AAP includes the required information and documents as defined in paragraph 114 above;
  - c. The submitted ST provides a technically sound basis for the commencement of the evaluation;
  - d. The submitted ST has sufficient relevance to, and presents sufficient benefits for Australasian government use;
  - e. The submitted ST complies with an approved PP that exists for that technology where applicable;

- f. The proposed evaluation plan contains the level of detail required, is of adequate quality, and is able to abide by AISEP policies and procedures;
  - g. The AISEF is able to meet the requirements for specialist technical skills, independence and impartiality;
  - h. The product is *NOT* currently being evaluated in another Scheme that would be covered by a mutual recognition arrangement or understanding with DSD upon evaluation completion. See section 4.1.3 below for relevant mutual recognition arrangements and understandings;
  - i. A contractual agreement exists between the product vendor and the AISEF to have the product evaluated under the AISEP.
116. The ACA authorises acceptance of an evaluation task into the Program through the formal notification of a letter. Evaluation activity may not commence until the evaluation task has been formally accepted and notified by the ACA. When an evaluation task commences, the ACA will publish the product on the EPL.
117. The ACA may reject an evaluation task for the following reasons:
- a. All the requirements specified in paragraph 115 above have not been adequately met; or
  - b. The evaluation does not meet the national security needs of Australasian government agencies in protecting their official communication and information systems.
118. The ACA will notify the AISEF if an evaluation task has not been accepted.
- Note: A decision to reject an evaluation task is a reviewable decision under Chapter 5 — Reviewable decisions.*
119. The ACA enforces the following additional acceptance requirement for products that contain cryptographic functionality in scope of the evaluation. Consumers **MUST** be able to configure the evaluated product so that DSD Approved Cryptographic Algorithms (DACAs) and DSD Approved Cryptographic Protocols (DACPs) are used for all cryptographic functions.
- Note: DSD Approved Cryptographic Algorithms (DACAs) and DSD Approved Cryptographic Protocols (DACPs) are specified in the Australian Government Information Security Manual (ISM) (Ref. [10]).*
120. The ACA will consider a request from the product vendor for an evaluation to be conducted discretely and not be listed on the EPL until the task has completed. However, task progress goals **MUST** still be met. The ACA **MUST** be able to inform Australasian government consumers of the discrete evaluation should a need arise. The ACA will inform the AISEF and product vendor if this occurs.

#### 3.1.1.4 AISEF responsibilities to the product vendor

121. Prior to the AAP submission, the product vendor **MUST** be informed of:
- a. The Program's evaluation process;
  - b. The role of the AISEF;
  - c. The role of the ACA;
  - d. The product vendor's responsibilities throughout the evaluation as defined in paragraph 122 below; and
  - e. The location of the relevant AISEP Policy documents on the DSD website.

122. The AISEF **MUST** inform the product vendor that they are responsible for and agree to the following during the evaluation:
  - a. Provide personnel and financial resources to fully support the conduct of the evaluation and to progress the task sufficiently;
  - b. Provide the necessary equipment and deliverables required for the evaluation This may include the provision of evaluation deliverables to the ACA; and
  - c. Allow DSD to provide draft versions of the ST to potential Australasian government consumers while the product is in evaluation.

### 3.1.2 Conduct phase

#### 3.1.2.1 Conduct of the certification team

123. The ACA allocates at least two certifiers to an evaluation task, where one Certifier is identified as the Lead Certifier. Additional support Certifiers may also be assigned.
124. Certifiers conduct oversight activities and gain assurance that the evaluation is being conducted accurately by:
  - a. Conducting Certifier Assurance Meetings (CAMs) with the evaluation team;
  - b. Discussing technical details with the evaluation team, the Principal Certifier and subject matter experts;
  - c. Reviewing evaluation reports; and
  - e. Maintaining certification records.
125. Should the ACA be unable to maintain suitably qualified employees to complete certification work, the ACA may, in discussion with the AISEF:
  - a. Control the introduction of new evaluation tasks;
  - b. Negotiate later start times for new evaluation tasks;
  - c. Negotiate later completion times for existing evaluation tasks; and
  - d. Prioritise ACA work effort for current tasks.

#### 3.1.2.2 Conduct of the evaluation team

126. The AISEF **MUST** assign at least two evaluators to each evaluation task, subject to the following provisions:
  - a. The Principal Evaluator is assigned as the oversight;
  - b. One Evaluator **MUST** be assigned as the Lead Evaluator; and
  - c. At least one or more evaluators as a minimum **MUST** be allocated to provide support.
127. Changes to personnel during the evaluation **MUST** be agreed to by the ACA. The AISEF **MUST** inform the ACA within a week of the change in writing.
128. Should the AISEF be unable to maintain suitably qualified staff to complete a particular evaluation, the ACA may suspend the evaluation, giving it a status of 'inactive', until agreement is reached between the parties to resume evaluation.

### 3.1.2.4 Evaluation status

129. The ACA maintains a monthly reporting period for evaluation tasks. The AISEF **MUST** report to the ACA on the progress of each evaluation task for each reporting period. The report **MUST** describe progress as at the first workday of the calendar month.
130. The ACA recognises evaluation activity as progress for the evaluation task. An AISEF **MUST NOT** identify evaluation support consulting, training, AISEP policy or licence compliance activities as evaluation progress or as a contribution to evaluation progress.
131. The ACA is responsible for assessing and determining the status of current AISEP evaluation tasks and this is reflected on the EPL through progress indicators.
132. The ACA uses one of the following progress indicators for a current evaluation task:
  - a. **Progressing**: Used to indicate that the evaluation task is progressing as agreed in the EWP contained in the Evaluation Progress Statement (EPS).
  - b. **Inactive**: Used for an evaluation task that is not being maintained acceptably, precipitating remedial action by the ACA in accordance with AISEP policy as defined in Section 3.1.4 below.
  - c. **Concurrent**: Used for an evaluation task where the product is undergoing development concurrently with the evaluation.

*Note: The ACA does not place standard evaluation progress requirements as outlined in Section 3.1.4 below, on a product that is being developed concurrently with the evaluation.*
133. For an evaluation task to be considered concurrent, the product **MUST NOT** be available for purchase by consumers. However, if during the course of a concurrent evaluation the product becomes available for purchase, the AISEF **MUST** ensure that the task complies with the standard evaluation progress requirements as outlined in this section.

### 3.1.2.4 Product vendor initiated changes

134. During the course of an evaluation, product vendors may propose changes to the evaluation scope. Changes in scope **MUST** be assessed to determine the impact on the evaluation schedule, evaluation activities already conducted, and standard acceptance criteria to enable the ACA to make an informed decision prior to committing to the change.
135. If the proposed scope change does not resolve a security issue discovered through the evaluation process, the product vendor **MUST** provide sufficient information so that the ACA and the AISEF can assess the impact on the evaluation. Minor changes may be approved by the Lead Certifier on the evaluation task.
136. A proposed scope change that incurs a significantly adverse impact that is not sufficiently counterbalanced by enhanced security and/or product version currency may be rejected by the ACA. Major changes to the scope of evaluation **MUST** be approved by the Principal Certifier in writing.
137. The following changes to the scope of evaluation **MUST** be approved by the Principal Certifier in writing:
  - a. The removal of a Security Functional Requirement (SFR) or claims from the AAP approved ST;
  - b. The removal or amendment of an SFR dependency from the AAP approved ST; and
  - c. A change in the ST Objectives, Threats and/or Assumptions from the AAP approved ST.

138. In some cases, the cost and timeliness implications associated with a change in scope would be seen as counterproductive to both product vendor and consumer objectives. An option would be to complete the existing evaluation and then engage in AISEP Assurance Continuity (AAC) for changes to the product after certification. AAC is described in section 3.2 below.

### 3.1.3 Conclude phase

139. On completion of evaluation activities, the AISEF **MUST** submit a draft Evaluation Technical Report (ETR) to the ACA for review. The ETR content requirements are described in section 4.3.5 below.
140. The ACA will provide formal ETR comments if required. The AISEF **MUST** ensure that the evaluation team addresses the ACA comments and a final ETR **MUST** be delivered to the ACA.
141. On final ETR agreement, the ACA will:
- Finalise a Certification Report for the product's completed evaluation as defined in Section 4.3.2 below;
  - Create a DSD signed certificate for the evaluation;
  - Update the EPL listing to reflect an evaluation status of certified and include the Certification Report, Security Target and/or Protection Profile documents; and
  - Post an update to the Common Criteria Portal with the details of the certification.
142. The AISEF **MUST** ensure that the task is closed down in a controlled manner through a formal Task Close-down Meeting (TCM). This provides evaluation stakeholders the opportunity to present feedback and ensures that all information is appropriately distributed or disposed of. The possibility of AISEP Assurance Continuity (AAC) may also be discussed at the Task Closedown Meeting. AAC is described in section 3.2 below.

### 3.1.4 AISEF evaluation progress rules

143. Best practice project and contract management controls **MUST** be employed throughout the conduct of an evaluation to ensure undue delays are avoided. The AISEF formally reports evaluation progress to the ACA once a month.
144. If the ACA determines there is insufficient evaluation progress made in a calendar month, the ACA will contact the AISEF to discuss any progress issues. If progress issues are not resolved through this initial discussion, the ACA may call an Evaluation Progress Meeting (EPM). The AISEF is required to coordinate the EPM between all relevant stakeholders no later than five working days after the ACA calls the EPM.
145. When sufficient evaluation activity has not occurred in two consecutive reporting periods, the ACA will issue a warning letter to the product vendor and inform the AISEF. The AISEF **MUST** acknowledge the letter and provide reasons for the lack of evaluation progress.
146. The ACA may consider the evaluation task 'inactive' when an evaluation task has not progressed sufficiently over two consecutive reporting periods. The ACA notifies the AISEF and the product vendor of the status change, modifies the EPL listing accordingly, and initiates an investigation of the situation.

147. During the investigation, the AISEF may be required to provide additional information on what actions it has taken or proposes to take, in order to progress the task. The product vendor may be required to provide information to the ACA to assist it in deciding whether to remove the listing from the EPL.
148. Should there be insufficient evaluation progress across three consecutive reporting periods; the ACA will remove the EPL listing for the task. The ACA will formally notify the AISEF and the product vendor through a letter following the EPL listing removal. The task will not be re-listed until the AISEF can demonstrate one month of sufficient evaluation progress.
149. The ACA reserves the right to terminate the task if sufficient evaluation progress is not demonstrated three months consecutively from the issue of the warning letter.
- Note: A decision to terminate an evaluation task, after the product vendor has provided relevant information to the ACA (show-cause process), is a reviewable decision under Chapter 5 — Reviewable decisions.*
150. On termination of a task, the ACA will:
- Remove the task's EPL entry;
  - Provide formal notification to the product vendor and the AISEF of the termination of the task;
  - Provide formal notification to the government agency that provided the *Letter of Recommendation for Evaluation*; and
  - Notify known consumers.
151. A task that the ACA has terminated is not permitted to recommence. To continue a previously terminated evaluation, the task **MUST** be treated as a new evaluation and the product vendor renegotiates a contract with an AISEF. The AISEF **MUST** submit a new AISEP Acceptance Package (AAP) for the task. However, the ACA may recognise previous evaluation effort in accordance with re-evaluation policy defined in section 3.2.3 below.
152. If during the course of the evaluation process, the ACA determines the product is unable to meet evaluation requirements, the ACA will terminate the task.
- Note: A decision to terminate an evaluation task, where the product is unable to meet evaluation requirements, is a reviewable decision under Chapter 5 — Reviewable decisions.*

## 3.2 AISEP assurance continuity

153. This section provides the ACA's policy on maintaining assurance for a product that has undergone changes. AISEP Assurance Continuity (AAC) allows the product vendor to conduct discrete maintenance or re-evaluation activities to extend the original certification. AAC only accommodates AISEP certified Common Criteria products.
154. A product vendor wishing to maintain an upgraded product's certification in a cost effective manner should approach the ACA, either directly, or via an AISEF.

### 3.2.2 AAC acceptance

155. AAC follows the Common Criteria format of assurance continuity, as described in *Assurance Continuity: CCRA Requirements* (Ref.[7]). The AISEP requires an *Impact Analysis Report (IAR)* to form the basis for continuity activity.
156. The ACA reviews the IAR to determine whether the documented changes to the certified product are:
  - a. 'Major' and warrant independent investigation by an AISEF (re-evaluation); or
  - b. 'Minor' and are accepted by the ACA as a maintenance update to the product's original certificate.
157. The ACA is the sole adjudicator on the impact of changes to a certified product.

*Note: The decision on the impact of changes to a certified product is NOT reviewable under Chapter 5 — Reviewable decisions.*

### 3.2.2 AISEP assurance continuity for maintenance

158. For a product to be considered for AAC, the following must occur:
  - a. The product **MUST** have completed evaluation through the AISEP;
  - b. An *Impact Analysis Report (IAR)* is submitted to the ACA; and
  - c. A covering letter is provided to the ACA with the product vendor details.
159. Where the ACA determines that changes can be accommodated under maintenance and is satisfied that all requirements have been met, the ACA updates the EPL listing for the certified product to include:
  - a. An updated maintenance addendum to the CR; and
  - b. An AISEP Maintenance Report.
160. If the ACA considers the changes described in an IAR to be major, the product vendor will be notified and will have the option of submitting the product for re-evaluation.
161. A product vendor is permitted to directly enter into re-evaluation if they believe that the modification to the certified product is major or the aggregate of changes warrant a re-evaluation.

### 3.2.3 AISEP assurance continuity for re-evaluation

162. Alternatively, a product vendor may choose to submit a product directly for re-evaluation without an IAR. Re-evaluation tasks are conducted in a similar fashion to normal evaluation tasks.
163. Re-evaluation tasks are subject to the same acceptance rules as normal evaluation tasks, except as follows.
164. For a submitted evaluation proposal to be considered a 're-evaluation', the product vendor **MUST** ensure that the AISEF has access to the *Impact Analysis Report (IAR)* and following documents from the previous certification:
  - a. Security Target (ST);
  - b. Evaluation Technical Report (ETR); and
  - c. Certification Report (CR).

165. The AISEF contracted to conduct the re-evaluation **MUST** determine the level of effort required to re-establish assurance. The product vendor should ensure that the AISEF has access to all previous evaluation deliverables to ensure the task is performed effectively.
166. The AISEF **MUST** schedule a meeting with the ACA to discuss and finalise the required level of effort agreed for the re-evaluation task.
167. A re-evaluation task concludes in the same manner as an evaluation task. Unlike a maintenance task, a re-evaluation results in a new certificate being issued.

*Note: Product vendors MUST seek advice from the ACA for AISEP Assurance Continuity options where the original evaluation was against a DSD approved Protection Profile.*

### 3.2.4 Non-compliance of AAC evaluations

168. The ACA retains the ability to conduct an audit in order to verify AAC related claims by the product vendor.
169. The ACA reserves the right to rescind findings and adjust the maintenance addendum accordingly, or reject product vendor claims, depending on the result of an AAC audit.
170. All non-compliance rules for evaluation tasks apply equally to re-evaluation tasks.

## 3.3 Supporting functions of program management

171. The ACA implements Program management functions to:
- a. Ensure the efficiency of AISEP operations and effective management of evaluation task progress;
  - b. Provide a forum for the ACA to disseminate AISEP-relevant information to the AISEFs; and
  - c. Provide a forum for AISEF Controllers to raise Program issues and concerns with the ACA.

### 3.3.1 AISEF progress reporting

#### 3.3.1.1 Monthly evaluation progress statement

172. The AISEF **MUST** ensure that the evaluation team submit to the ACA a monthly Evaluation Progress Statement (EPS) that reports the progress of the evaluation task. The EPS ensures visibility of an evaluation task and if a problem occurs, allows for early identification and resolution.
173. The EPS reports are due the last working day of each calendar month. The first EPS is due the calendar month after the Task Start-up Meeting (TSM). The last EPS is to be submitted after the Task Close-down Meeting (TCM) minutes has been received by the ACA. The ACA deems the absence of an EPS to indicate that progress has not occurred and AISEP progress rules are applied as described in section 3.1.4 above.

### 3.3.1.2 Quarterly evaluation progress report

174. The AISEF **MUST** submit a quarterly AISEF Progress Report (APR) to inform the ACA of future evaluation tasks and to raise any changes or issues relating to the AISEF. The APR **MUST** be signed by the AISEF Controller. The reporting periods for the APR are outlined in the AISEP Evaluator policy (Ref [14]).
175. The APR **MUST** include:
  - a. Prospective business or relevant new contacts made;
  - b. Changes to current AISEF staff or their role in the facility;
  - c. Changes to the current licensing and accreditation status of the AISEF. If there is a change, the report **MUST** be made within one week of the change; and
  - d. General issues in relation to the AISEP that the AISEF wishes to bring to the attention of the ACA.

### 3.3.1.3 AISEF controllers' meeting

176. The ACA convenes the AISEF Controllers' Meetings (ACM) to provide a forum for disseminating AISEP management information collectively to AISEF Controllers. These meetings are generally held two to four times a year.
177. The ACA uses this forum to:
  - a. Disseminate strategic and program information decided by DSD management; and
  - b. Disseminate information from international CC meetings that DSD attends.

## 3.3.2 Interpretations and technical alignment

178. The ACA implements the interpretations and technical alignment functions to conduct the following process and forum:
  - a. **AISEP interpretations process:** A national interpretation process for the ACA to provide timely interpretations of IT security evaluation criteria and AISEP policies for AISEP stakeholders.
  - b. **AISEP technical board:** A forum for the ACA to discuss and disseminate to AISEF evaluators, technical knowledge and promote evaluation and certification technical alignment within the AISEP.

### 3.3.2.1 AISEP interpretations process

179. An AISEP Request for Interpretation (ARI) of accepted IT security evaluation criteria or of an AISEP policy can be submitted to the ACA.

- 
- 180. An AISEF, government agency or product vendor may submit an ARI if they:
    - a. Have difficulty interpreting a component of accepted IT security evaluation criteria, supporting document or PP;
    - b. Have difficulty interpreting AISEP policy or a process;
    - c. Cannot find sufficient guidance in order to perform a required AISEP activity; or
    - d. Find an error in the current version of an AISEP policy or accepted IT security evaluation criteria or a supporting document.
  - 181. The ACA assigns a unique identifier and issues an acknowledgement to the originator on receipt of an ARI.
  - 182. In response to an ARI, the ACA will, via email or letter:
    - a. Provide a resolution to the ARI; or
    - b. Explain why the ACA has determined that the matter in question is not required to be resolved through an interpretation.
  - 183. The ACA publishes an AISEP interpretation for a resolution that involves interpreting accepted IT security evaluation criteria. The ACA distributes the AISEP interpretation for comment before it is finalised.
  - 184. The ACA submits a final AISEP interpretation that relates to IT security evaluation criteria to the appropriate criteria authorities for submission to the relevant international interpretation process.
  - 185. The ACA withdraws the superseded AISEP interpretation after the international bodies have reviewed scheme interpretation and the response is final.
  - 186. A resolution to the ARI that may involve interpreting or modifying an AISEP policy or procedure is posted on the AISEP website. An ARI resolution is incorporated in the next release. See section 4.2.3 below describes the update cycle for AISEP policies.

### 3.3.2.2 AISEP technical board

- 187. The AISEP Technical Board (ATB) is a forum for interpretation and technical alignment activities within the AISEP.
- 188. The ACA uses the ATB to:
  - a. Openly discuss technical issues with AISEF evaluators;
  - b. Disseminate technical knowledge to the leading AISEF evaluators; and
  - c. Discuss AISEP requests for interpretations of IT security evaluation criteria and AISEP publications.
- 189. The ACA may convene the ATB between two to four times a year, or as needed.
- 190. The ACA Principal Certifier or a nominated delegate chairs the ATB, and each AISEF's Principal Evaluator should participate as a member of the board. The ACA and AISEFs are permitted to have other evaluation staff attend ATB meetings; however, the AISEF Principal Evaluator is its official member.
- 191. The ACA may disseminate documents and knowledge articles in advance of the meeting so that members have the opportunity to prepare for the technical subjects to be discussed.



# Chapter 4—Documents and Standards

192. This chapter provides information on the following documents and standards that play a role in the management and operations of the AISEP:
- Program standards:** Standards used in the operations and management of the Program, including approved IT security evaluation criteria.
  - Program publications:** Formal AISEP publications issued and controlled by the ACA.
  - Program operational outputs:** Documents and other outputs produced in conducting core business functions.

## 4.1 Program standard

### 4.1.1 Common Criteria

193. The AISEF **MUST** employ the following standard for conducting IT security evaluations under the AISEP:  
*Common Criteria for Information Security Technology Evaluation* (Refs. [2], [3], [4] and [5]).
194. The AISEF **MUST** utilise the following parts of the CC when conducting evaluation tasks against the CC:
- Part 1: Introduction and general model* (Ref. [2])
  - Part 2: Security functional components* (Ref. [3])
  - Part 3: Security assurance components* (Ref. [4]).
195. The AISEF **MUST** use the accepted IT security evaluation methodology that supports the correct application of the CC. The accepted CC methodology is the *Common Methodology for Information Technology Security Evaluation*, commonly known as the *Common Evaluation Methodology (CEM)* (Ref. [5]).
196. For a DSD approved PP for a technology, the AISEF **MUST** also follow the additional methodology provided within the PP or from a relevant supporting document where applicable.
197. Current versions of the CC are listed in Annex A. As a participant in the CCRA, the ACA will always use the official current version of the CC.
198. The authority body for the CCRA has a mechanism for releasing interpretations of the criteria. The AISEF **MUST** incorporate into its evaluation activities all final interpretations as published by the CCRA authority.

### 4.1.2 Criteria interpretations

199. The ACA recognises all 'final' interpretations of accepted IT security evaluation criteria by the relevant CCRA authorities.
200. The AISEF **MUST** incorporate all final national and international interpretations into evaluation activities if they are published as final before the evaluation task is begun.  
*Note: See section 3.3.2.1 above for more information on the AISEP interpretation process.*
201. The AISEF **MUST NOT** use 'draft' interpretations without receiving authorisation from the ACA.

### 4.1.3 Common Criteria Recognition Arrangement

202. Australia and New Zealand through the AISEP are signatories to the CCRA (Ref. [6]). Common Criteria certificates for IT security evaluations at EAL 1 to 4 inclusive are mutually recognised by the CCRA.
203. Participation in the CCRA entails the following operational Program obligations:
  - a. **Voluntary periodic assessment:** The ACA must undergo independent assessment by other CCRA member nations at least once every five years. This is to maintain status as a certificate producing CC scheme.
  - b. **Quality system:** The ACA and AISEFs implement and comply with a quality system. DSD ensures that the AISEFs operate in accordance with *ISO standard 17025* (Refs. [8]) and the ACA operates in accordance with Annex C of the CCRA (Ref. [6]).
  - c. **Effective program management:** DSD ensures that a suitably qualified management team leads the AISEP and implements effective business processes and procedures that maintain compliance with requirements identified in international agreements.
  - d. **Effective oversight:** DSD ensures that a suitable number of qualified staff is maintained to provide technical leadership for the AISEP. DSD has also put in place effective oversight techniques to ensure that evaluators are applying criteria effectively and consistently.

### 4.1.4 Conduct of mutual recognition

204. As part of the CCRA mutual recognition, the ACA recognises the certification of products from other CC certificate producing schemes, up to and including EAL 4. Common Criteria certified products, from Evaluation Assurance Level 1 – 7 may be performed and listed on the Common Criteria Portal.
205. A certificate above EAL 4 certified by another certificate producing scheme is mutually recognised in the AISEP at EAL 4 (eg. An EAL 5 firewall certified by another certificate producing scheme would be recognised as an EAL 4 firewall by the AISEP). Evaluations that are augmented with flaw remediation are also mutually recognised in the AISEP.
206. A CC certificate for an evaluation that is compliant with a DSD approved PP follows the same mutual recognition rules described in paragraphs 204 and 205 above.

### 4.1.5 Accreditation standards

207. The ACA implements processes and procedures to ensure compliance with Annexes B and C of the *Arrangement on the Recognition of Common Criteria Certificates in the Field of IT Security (CCRA)* (Ref. [6]).
208. An AISEF **MUST** comply with and be accredited against the following quality standard and supplementary requirements:
- ISO/IEC 17025: Field Application Document, Information and Communications Technology Testing, Supplementary requirements for accreditation*, National Association of Testing Authorities, Australia. (Ref. [8]).

## 4.2 Program publications

### 4.2.1 Program policy and manual

209. The ACA publishes AISEP policy through this document, the *AISEP Policy Manual*.

### 4.2.2 Stakeholder guidance

210. The ACA publishes a series of policy documents for key AISEP stakeholders:
- AISEP Certifier Policy**: This document is for DSD internal use only. (Ref. [15]).
  - AISEP Evaluator Policy**: This document is for AISEF evaluators and is not available publicly. (Ref. [14]).

### 4.2.3 AISEP publication updates

211. The ACA updates AISEP publications periodically for quality control purposes. New AISEP publication releases will incorporate relevant AISEP Request for Interpretation responses concluded since the previous AISEP publication release, as appropriate. See section 3.3.2.1 above for more information on the AISEP interpretations process.
212. New releases of the AISEP policy is:
- Amended according to the ACA version control system;
  - Authorised by DSD Management;
  - Forwarded to licensed AISEFs as appropriate;
  - Forwarded to NATA representatives where relevant; and
  - Published on the DSD website with an associated 'New' announcement.
213. An AISEF **MUST** use the latest version of the *AISEP Policy Manual* and *AISEP Evaluator Policy*. (Ref. [14]).

## 4.3 Program operational outputs

214. This section provides information on the outputs produced by the ACA and AISEFs.

### 4.3.1 Evaluated Products List (EPL)

215. The ACA maintains a list of evaluated and certified IT security products, known as the Evaluated Products List (EPL). The EPL is published on the DSD website.
216. The '**Completed**' section of the EPL comprises products and systems that:
- a. Have successfully completed an AISEP evaluation; or
  - b. Have successfully completed a DSD approved evaluation.
217. The '**In Evaluation**' section of the EPL comprises IT security products that are currently undergoing CC evaluation in the AISEP.
218. The EPL listing varies depending on the status, type, and method of evaluation. The following information is included for all AISEP-certified product related EPL entries:
- a. A brief description of the IT product and the security functionality evaluated;
  - b. A general category or product type;
  - c. The ST and CR;
  - d. The relevant assurance level;
  - e. The criteria or methodology that was used to evaluate the product;
  - f. Details of the AISEF that performed the evaluation; and
  - g. Product vendor details including contact information.
219. Other information may also be included where relevant, such as that listed below:
- a. A DSD Consumer Guide;
  - b. An indicator for an associated DSD Cryptographic Evaluation (DCE);
  - c. An indication of the current status of the task;
  - d. The PP (evaluated or conformant);
  - e. History of a certified product's assurance maintenance; and
  - f. A list of documents associated with the product that is publicly available.
220. The ACA maintains a historical EPL for those certified products that are:
- a. Unavailable in their original form;
  - b. Not supported by the product vendor;
  - c. Not available for purchase by consumers; or
  - d. No longer in compliance with the *Australian Government Information Security Manual (ISM)* (Ref. [10]).

### 4.3.2 Certification report

221. The ACA reports the final results of the certification effort of an evaluation task with a formal CR.
222. The ACA ensures that the contents of the CR comply with requirements specified in Annex I of the CCRA (Ref. [6]). For product evaluations the CR includes the following major areas:
  - a. An executive summary;
  - b. A section identifying the evaluated IT product;
  - c. A description of the IT product's security policy;
  - d. Assumptions and clarification of scope in relation to the evaluation;
  - e. Architectural information for the evaluated IT product;
  - f. A description of the testing effort performed during the evaluation;
  - g. A description of the evaluated configuration;
  - h. The results of the evaluation;
  - i. Certifier comments and/or recommendations;
  - j. Annexes, including a glossary and/or bibliography if required; and
  - k. Reference to the complete and sanitised version of the ST for the evaluated product. A sanitised version means that commercially sensitive information has been removed from the ST.

### 4.3.3 Certificate

223. The ACA ensures that the content of the certificate complies with the requirements specified in Annex J of the CCRA (Ref. [6]). The certificate for AISEP evaluations includes the following details:
  - a. Product vendor name;
  - b. Product name;
  - c. Product type;
  - d. Version and release numbers;
  - e. Protection Profile conformance (if applicable);
  - f. Evaluation platform (optional);
  - g. AISEP name;
  - h. The IT security evaluation criteria that was used;
  - i. Certificate number;
  - j. Date issued; and
  - k. EAL including any augmentations.

224. For AISEP certificates, the following statement is included:

*The IT product identified in this certificate has been evaluated at an accredited and licensed evaluation facility of the Australasian Information Security Evaluation Program using the Common Methodology for IT Security Evaluation, [insert version number], for conformance to the Common Criteria for IT Security Evaluation, [insert version number].*

*This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report. The evaluation has been conducted in accordance with the provisions of the Australasian Information Security Evaluation Program, and the conclusions of the evaluation facility in the Evaluation Technical Report are consistent with the evidence adduced.*

*This certificate is not an endorsement of the IT product by the AISEP or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the AISEP or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.*

225. The CCRA logo is included in CC certificates, as defined in Annex E of the CCRA (Ref. [6]).
226. An EPL addendum is created in instances of successful maintenance activities in order to specify details of accepted changes to the certified IT security product.

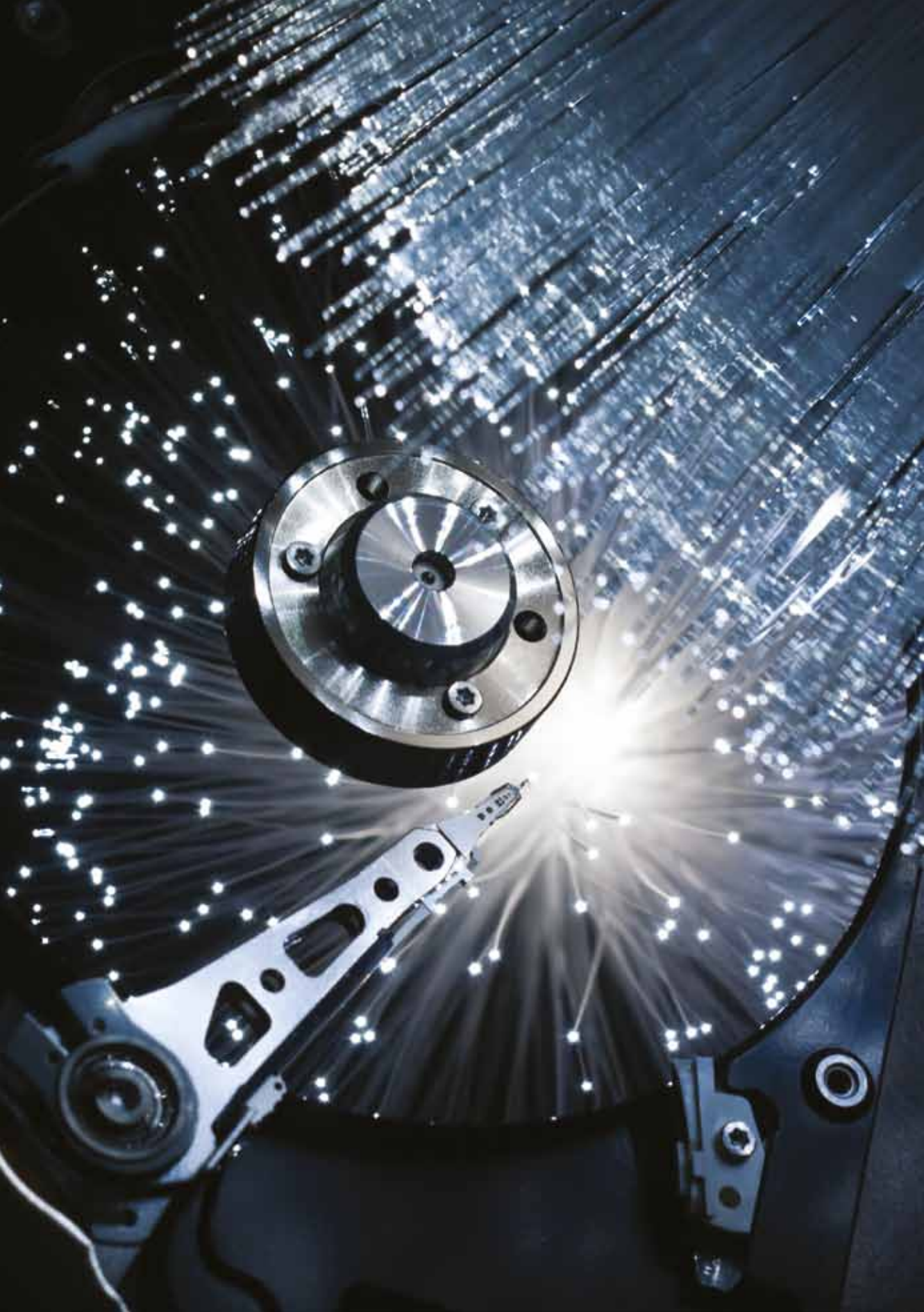
#### 4.3.4 Maintenance report

227. The ACA reports the final results of maintenance activities with an AISEP Maintenance Report.
228. The contents of the AISEP Maintenance Report include the following:
- a. Description of changes to the certified product; and
  - b. Affected evaluation evidence.

#### 4.3.5 Evaluation technical report

229. The AISEF **MUST** formally report the results of the evaluation task to the ACA for approval in the Evaluation Technical Report (ETR).
230. The ETR **MUST** present all verdicts, justifications and findings derived during the evaluation activity.
231. The ACA ensures that the contents of the ETR comply with requirements specified in the CCRA (Ref. [6]).
232. Initially, the AISEF **MUST** only distribution evaluation results to the ACA using the appropriate DLM.
233. The AISEF is able to distribute a sanitised version of the evaluation results to interested government agencies when the ACA has approved the results of the evaluation.

234. The AISEF **MUST** include the following major areas within the ETR for product evaluations:
- a. Executive summary;
  - b. Introduction;
  - c. Product description (to include an overview, usage and environmental assumptions) threats, organisational security policies and a clarification of scope;
  - d. The evaluation context, including the evaluated configuration, security policy, product architecture and testing efforts;
  - e. Evaluation results;
  - f. Product delivery and installation;
  - g. Conclusions and recommendations;
  - h. Evaluation documentation; and
  - i. Problem reports and resolutions.



---

# Chapter 5—Reviewable Decisions

235. The purpose of this chapter is to:
- a. Outline the DSD decisions that are reviewable under this policy document;
  - b. State those decisions that are not reviewable under this policy document; and
  - c. Outline the process for requesting a decision review.

## 5.1 Decisions

### 5.1.1 Reviewable decisions

236. The following decisions are reviewable:
- a. A decision not to reinstate an evaluator's status on return to an AISEF position after an absence as described in section 2.3.2.2 above;
  - b. A decision to reject an evaluation task as described in section 3.1.1.3 above;
  - c. A decision to terminate an evaluation task, after the show-cause process as described in section 3.1.4 above; or where the product is unable to meet the stated requirements as described in section 3.1.1.2 above and 3.1.1.3 above; and
  - d. A decision to withdraw a certificate as described in section 2.2.3.4 above.
237. A person or organisation whose interests are affected by a reviewable decision may request DSD to reconsider the decision.

### 5.1.2 Non- reviewable decisions

238. Some decisions described in this document are not reviewable under the review process outlined in this chapter.
239. The decisions that are not reviewable under the process outlined in this chapter are:
- a. A decision on the impact of changes to a certified product as described in section 3.2.1 above;
  - b. A decision not to grant to an applicant an AISEF licence as described in section 2.3.3 above;
  - c. A decision to suspend an AISEF's licence as described in section 2.3.3.1 above;
  - d. A decision to terminate an AISEF's licence as described in section 2.3.3.1 above.

## 5.2 Review process

### 5.2.1 Requests for review

240. A request for review **MUST** be made in writing to DSD within 28 days of the date DSD advised the decision.
241. The decision review request **MUST** provide specific reasons as to why it is thought the DSD decision is wrong. DSD will consider this information and decide whether or not to review the decision. DSD will advise the decision to the complainant within 30 days.

### 5.2.2 Review outcomes

242. After DSD has considered the information provided by the complainant, the following may occur:
  - a. DSD will uphold the original decision;
  - b. DSD will change the original decision; or
  - c. DSD will further investigate the matter.
243. DSD will endeavour to complete the review within 28 days. DSD will send the complainant a letter advising of the outcome of the review.
244. A decision will be reviewed once only.



# Chapter 6—Product Vendor Responsibilities

## 6.1 Common Criteria logo marketing

245. Upon receipt of an AISEP-issued CC certificate, the product vendor is entitled to use the mark shown in Figure 6: Common Criteria Certification Mark. This may be used in conjunction with advertising, marketing and sales of the product for which the certificate is issued.



Figure 6: Common Criteria Certification Mark

246. During the **In-Evaluation** stage, the product vendor may indicate in marketing material that the product is undergoing evaluation, but **MUST NOT** use the logo associated with a certified product, as shown in Figure 6: Common Criteria Certification Mark, until certification is achieved.
247. The product vendor **MUST** seek ACA approval prior to publicly releasing material that makes reference to the AISEP, ACA or DSD.

## 6.2 Product vendor notification requirements

248. The product vendor should inform the ACA when there is a new release of the certified TOE. In this situation, the product vendor is strongly encouraged to engage in AAC activities as part of the product release strategy as described in 3.2 above.
249. The product vendor should notify the ACA when their contact details change to facilitate the currency of such information on the EPL.
250. The product vendor should also notify the ACA when there is a firm intent to cease sales and/or technical support of a certified product.

# Annex A—References and Abbreviations

## A.1 References

1. Information Technology Security Evaluation Criteria (ITSEC), Commission of the European Communities CD-71-91-502-EN-C, Version 1.2, June 1991.
2. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CCMB-2009-07-001, Version 3.1 Revision 3, July 2009.
3. Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, CCMB-2009-07-002, Version 3.1, Revision 3, July 2009.
4. Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, CCMB-2009-07-003, Version 3.1, Revision 3, July 2009.
5. Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, CCMB-2009-07-004, Version 3.1, Revision 3, July 2009.
6. Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.
7. Assurance Continuity: CCRA Requirements, CCIMB-2004-02-009, Version 1.0, February 2004.
8. ISO/IEC 17025: Field Application Document, Information and Communications Technology Testing, Supplementary requirements for accreditation, National Association of Testing Authorities, Australia.
9. Memorandum of Understanding between Australasian Information Security Evaluation Program and United Kingdom Information Security Evaluation and Certification Scheme, 20 November 2002.
10. Australian Government Information Security Manual (ISM), Defence Signals Directorate, [annual release].
11. New Zealand Information Security Manual (NZISM), Government Communications Security Bureau, [annual release].
12. Intelligence Services Act 2001, Commonwealth of Australia.
13. Archives Act 1983, Commonwealth of Australia, 1983.
14. AISEP Evaluator Policy, Defence Signals Directorate, Version 4.0, August 2011.
15. AISEP Certifier Policy, Defence Signals Directorate, Version 4.0, August 2011.

## A.2 Abbreviations

AAC	AISEP Assurance Continuity	DDSD	Director Defence Signals Directorate
ACA	Australasian Certification Authority	DGCSB	Director Government Communications Security Bureau
ACM	AISEF Controllers Meeting	DEI	Director ICT Evaluations and Industry Coordination, DSD
ACT	Australian Capital Territory	DSD	Defence Signals Directorate (Australia)
AISEF	Australasian Information Security Evaluation Facility	DLM	Dissemination Limiting Marker
AISEP	Australasian Information Security Evaluation Program	EPL	Evaluated Products List
APM	AISEP Policy Manual	ETR	Evaluation Technical Report
APR	AISEF Progress Report	GCSB	Government Communications Security Bureau (New Zealand)
APS	AISEP Progress Statement	IAR	Impact Analysis Report
ARI	AISEP Request for Interpretation	ISM	Australian Government Information Security Manual
ASISO	Assistant Secretary Information Security Operations	ISO	International Organization for Standardization
ATB	AISEP Technical Board	ITSEC	Information Technology Security Evaluation Criteria
CAM	Certifier Assurance Meetings	MOU	Memorandum of Understanding
CC	Common Criteria	NATA	National Association of Testing Authorities, Australia
CCRA	Common Criteria Recognition Arrangement	PP	Protection Profile
CEM	Common Evaluation Methodology	REF	Reference
CISD	Cyber and Information Security Division	SFR	Security Functional Requirement
CR	Certification Report	SME	Subject Matter Expert
DACA	DSD Approved Cryptographic Algorithm	ST	Security Target
DACP	DSD Approved Cryptographic Protocol	TCM	Task Close Down Meeting
DDCIS	Deputy Director, Cyber and Information Security	TSM	Task Start Up Meeting
DDIACS	Deputy Director Information Assurance and Cyber Security		

## Annex B— AISEF Applications

### B.1 Company information

251. The applicant **MUST** provide the following details in their application to become an AISEF:
- a. Organisation's full name;
  - b. Organisation's trading or business name;
  - c. Organisation's registered office and principal place of business;
  - d. Organisation's date and place of incorporation;
  - e. The names of individual shareholders that hold 20 per cent or more of issued share capital;
  - f. The particulars of foreign nationals or organisations in a position to exercise control or influence over the applicant;
  - g. The particulars of related companies within the meaning of section 50 of the *Corporations Act 2001*;
  - h. If a foreign-owned company, details of registration, incorporation and place of business in Australia or New Zealand, and the name of Australian or New Zealand representatives;
  - i. The Australian or New Zealand company number (ACN/NZCN) and, if in Australia, the Australian business number (ABN);
  - j. Details of indemnity by the company or its directors or auditor in respect of liability provided to officers of the company and insurance cover provided to them in respect of that liability;
  - k. Particulars of a petition, claim, action, judgment or decision that is likely to adversely affect the applicant's ability to provide IT security evaluation services;
  - l. Details of an order, contract, joint venture, collaboration or other commitments with another firm or company, and the resources that would derive there from relevant to the applicant's ability to meet the requirements of being an AISEF; and
  - m. Details of a potential or existing conflict of interest that would affect the applicant's ability to become an AISEF or to perform the function of an AISEF.

## B.2 Statement of claims

252. The Applicant should submit a statement of claims with the following organisation's details:
- a. Background and structure;
  - b. Technical, financial and managerial capacity to provide IT security evaluation services;
  - c. A curricula vitae of proposed evaluation staff, covering previous evaluation or testing work;
  - d. Staff experience using IT security evaluation related skills, such as experience in the use of formal methods or functional and vulnerability testing;
  - e. A summary of projects satisfactorily completed within the past two years that are similar in nature and complexity to evaluation projects, including the names of clients and other trade references and the applicant's experience in adhering to schedules for similar projects;
  - f. Any other factors the applicant believes will support its position through demonstrating its ability to perform the role of an AISEF;
  - g. Details of quality arrangements, including:
    - i. NATA accreditation, or how it will be acquired;
    - ii. The management structure that will achieve and maintain the quality, security and confidentiality of security evaluations;
    - iii. The organisation's quality assurance system;
    - iv. An outline quality plan for the conduct of IT security evaluations;
    - v. A plan for supervision and mentoring of new evaluators.

## B.3 Resource capabilities

253. Applicants should submit details of the resources the organisation will draw upon, including descriptions of:
- a. Proposed office accommodation;
  - b. Proposed physical access control mechanisms;
  - c. Management arrangements for coordinating with the Australasian Certification Authority (ACA);
  - d. Equipment that will be used to conduct IT security evaluations;
  - e. Proposed administrative support to the AISEF;
  - f. Proposed travel support for AISEF personnel to attend meetings at DSD, if the AISEF personnel is located outside the Australian Capital Territory (ACT);
  - g. Proposed methods for ensuring communication and coordination with the ACA;
  - h. Proposed charging regime for IT security evaluations
  - i. Details of insurance policies for public liability and workers compensation (including the type of cover, the insurance provider, any specific exclusions and the value of the policy), and evidence of such policies;
  - j. Details of any subcontractors that the applicant proposes to use to conduct IT security evaluations, including (for each proposed subcontractor) the name and ACN/ABN/NZCN of the company and the elements of work to be subcontracted.

---

Intentionally blank



