



Australian Government  
Australian Signals Directorate

ACSC Australian  
Cyber Security  
Centre

# AISEP

## Policy Manual





# Forward

The internet is a critical part of our business and social lives. Electronic systems and digital information are essential for businesses and families, with most Australians using the web to bank, pay bills, buy and sell goods and services, and stay connected.

While this digital age presents enormous opportunity, connectivity also brings exposure to cybercriminal activity. The Australian Cyber Security Centre (ACSC), within the Australian Signals Directorate (ASD), provides advice and assistance to all Australians to help make Australia the safest place to connect online.

The Australian Information Security Evaluation Program (AISEP) was established to certify product evaluations that have been conducted by licensed commercial facilities, in accordance with the internationally recognised Common Criteria standard. Certified products provide end-users with a level of assurance in the security of ICT products.

In addition to AISEP's certification functions, the program influences the development of international standards for ICT products to meet national needs.

This Policy Manual governs the management and operations of the AISEP.

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

ACA Manager  
Australian Cyber Security Centre (ACSC)  
Australian Signals Directorate  
PO Box 5076  
Kingston ACT 2604  
Australia

Email: [ACA.Certifications@defence.gov.au](mailto:ACA.Certifications@defence.gov.au)

# Disclaimer

This AISEP Policy Manual (APM) has been prepared 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 of 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:

- a. any applicable legislation or law
- b. the licensing agreement between ASD and each licensed commercial facility (also known as Australian Information Security Evaluation Facility – AISEF)
- c. the APM.

# Contents

<b>Chapter 1 – Introduction</b> .....	<b>8</b>
1.1. AISEP overview .....	9
1.2. AISEP authority .....	10
1.3. Overview of AISEP policies .....	10
1.4. Mutual recognition agreements .....	11
<b>Chapter 2 – Organisation of the AISEP</b> .....	<b>12</b>
2.1. AISEP management .....	13
2.1.1 <i>AISEP governance and managerial roles</i> .....	13
2.2. ACA roles and responsibilities .....	14
2.2.1 <i>ACA management</i> .....	14
2.2.2 <i>ACA Certifiers</i> .....	15
2.2.3 <i>ACA quality assurance and compliance</i> .....	16
2.2.3.1 <i>Assessment and compliance</i> .....	16
2.2.3.2 <i>Documentation control</i> .....	16
2.2.3.3 <i>ACA dispute resolution</i> .....	17
2.2.3.4 <i>Common Criteria certificate withdrawal</i> .....	17
2.3. AISEF roles and responsibilities .....	18
2.3.1 <i>AISEF management</i> .....	18
2.3.2 <i>AISEF Evaluator</i> .....	19
2.3.2.1 <i>Principal Evaluator</i> .....	20
2.3.2.2 <i>Evaluator status</i> .....	20
2.3.3 <i>AISEF licensing requirements</i> .....	21
2.3.4 <i>NATA accreditation requirements for the AISEF</i> .....	24
2.3.5 <i>AISEF licence monitoring</i> .....	24
2.3.6 <i>Associated costs for the AISEF</i> .....	25
2.3.7 <i>AISEF impartiality</i> .....	26
2.3.8 <i>AISEF security requirements</i> .....	26
2.3.8.1 <i>AISEF information security</i> .....	27
2.3.9 <i>AISEF archiving and disposal</i> .....	27

<b>Chapter 3 – AISEP Evaluation and Operational Policy .....</b>	<b>28</b>
3.1. IT security evaluation and certification .....	29
3.1.1 <i>Plan phase</i> .....	30
3.1.1.1 Sponsorship letter for an AISEP evaluation .....	30
3.1.1.2 AISEP Acceptance Package .....	30
3.1.1.3 Acceptance requirements for an evaluation task .....	31
3.1.1.4 AISEF responsibilities to the product vendor .....	32
3.1.2 <i>Conduct phase</i> .....	33
3.1.2.1 Conduct of the certification team .....	33
3.1.2.2 Conduct of the evaluation team .....	33
3.1.2.3 Evaluation status .....	34
3.1.2.4 Product vendor initiated changes .....	35
3.1.3 <i>Conclude phase</i> .....	36
3.1.4 <i>AISEF evaluation progress rules</i> .....	36
3.2. AISEP Assurance Continuity .....	38
3.2.1 <i>AAC acceptance</i> .....	38
3.2.2 <i>AISEP assurance continuity for maintenance</i> .....	38
3.2.3 <i>AISEP assurance continuity for re-evaluation</i> .....	38
3.2.4 <i>AISEP assurance continuity for re-assessment</i> .....	39
3.2.5 <i>Non-compliance of AAC evaluations</i> .....	39
3.3. Supporting functions of program management .....	40
3.3.1 <i>AISEF progress reporting</i> .....	40
3.3.1.1 Timely evaluation progress reporting .....	40
3.3.1.2 Quarterly AISEF Progress Report .....	40
3.3.1.3 AISEF Controllers' Meeting .....	41
3.3.2 <i>Interpretations and technical alignment</i> .....	41
3.3.2.1 AISEP interpretations process .....	41
3.3.2.2 AISEP Technical Board .....	42

<b>Chapter 4 – Documents and standards</b> .....	<b>44</b>
4.1. Program standard .....	45
4.1.1 Common Criteria.....	45
4.1.2 Criteria interpretations .....	45
4.1.3 Common Criteria Recognition Arrangement .....	46
4.1.4 Conduct of mutual recognition.....	46
4.1.5 Accreditation standards .....	46
4.2. Program publications .....	47
4.2.1 Program policy and manual.....	47
4.2.2 Stakeholder guidance.....	47
4.2.3 AISEP publication updates.....	47
4.3. Program operational outputs.....	48
4.3.1 Common Criteria Portal's Certified Products List (CPL).....	48
4.3.2 Certification Report.....	49
4.3.3 Certificate.....	50
4.3.4 Maintenance report .....	51
4.3.5 Evaluation Technical Report.....	52
4.3.6 Public facing report for cPPs .....	52
<b>Chapter 5 – Reviewable decisions</b> .....	<b>54</b>
5.1. Decisions .....	55
5.1.1 Reviewable decisions.....	55
5.1.2 Non-reviewable decisions .....	55
5.2. Review process .....	56
5.2.1 Requests for review.....	56
5.2.2 Review outcomes.....	56
<b>Chapter 6 – Product vendor responsibilities</b> .....	<b>58</b>
6.1. Common Criteria logo marketing .....	59
6.2. Product vendor notification requirements .....	59

**Annex A – References and abbreviations ..... 60**

- A.1. References.....61
- A.2. Abbreviations.....62

**Annex B – AISEF applications ..... 64**

- B.1. Company information .....65
- B.2. Statement of claims .....66
- B.3. Resource capabilities .....67







# Chapter 1 – Introduction

# 1.1. AISEP overview

1. The objectives of the AISEP are:
  - to ensure that the evaluation and certification of ICT security products and Protection Profiles (PPs) are performed to high and consistent standards, in accordance with the Common Criteria (CC) and Common Criteria Recognition Arrangement (CCRA)
  - to improve the availability of evaluated ICT security products and PP
  - to set the baseline security and assurance criteria to assist with the uplift of security in ICT security products
  - to provide Australian consumers with a level of assurance in the security of ICT products and
  - to assist with the overall improvement to the national cyber security posture.
2. ASD, through the ACSC, administers the AISEP. Through ASD, financial support is provided to the AISEP.
3. ASD licenses commercial facilities, known as Australian Information Security Evaluation Facilities (AISEFs), to conduct CC evaluations under the program. ASD's function in certifying these evaluation retained through its certification body, the Australian Certification Authority (ACA).
4. An ICT 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 then collaborate on the evaluation and certification. Individuals or organisations that acquire and use certified ICT security products are known as consumers. The ACA interacts with consumers in order to understand their evaluation needs. In particular, the AISEP's primary consumers are Australian organisations, including government agencies. These entities and relationships are illustrated in Figure 1: AISEP.

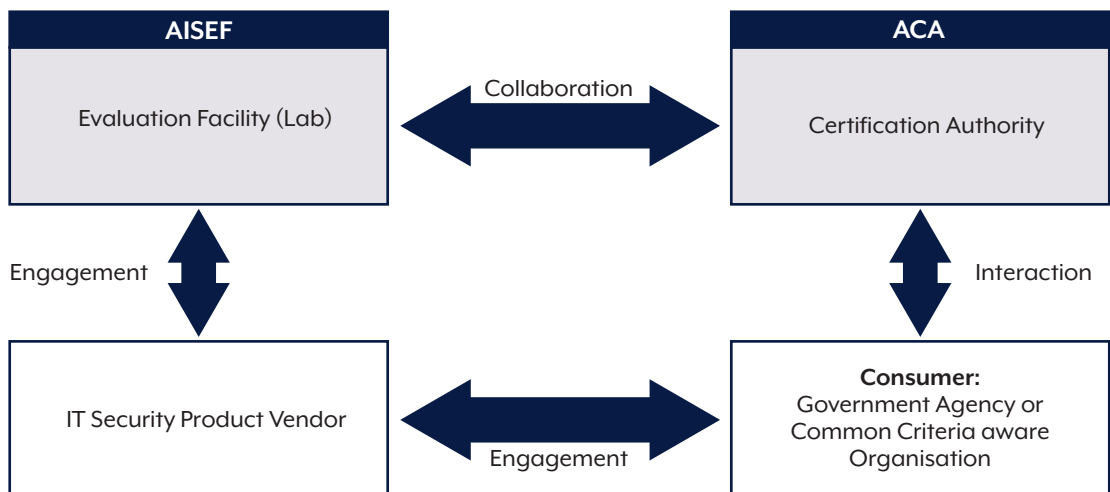


Figure 1: AISEP stakeholders

## 1.2. AISEP authority

5. The authority of the AISEP resides with the Director-General ASD (DGASD).
6. DGASD delegates this authority to the Head of the Australian Cyber Security Centre (HACSC).
7. The manager of the ACA is responsible for the management and operations of the Program, overseeing stakeholder compliance and implementing the AISEP policies.

## 1.3. Overview of AISEP policies

8. The AISEP policies provide a framework for IT security evaluations performed in Australia within the ACA.
9. The APM provides the managerial and operational policy framework. This is the parent policy document for the AISEP.
10. The APM has been organised into the following chapters:
  - Chapter 2 – Organisation of the AISEP: The key roles in the management and operations of the AISEP.
  - Chapter 3 – Operations: The day-to-day operations of the AISEP business functions of evaluation and certification, assurance continuity and mutual recognition.
  - Chapter 4 – Documents and standards: Documents, publications and standards that have an influence on the AISEP and its operations.
  - Chapter 5 – Reviewable decisions: The ACA decisions that can be reviewed.
  - Chapter 6 – Product vendor responsibilities: Information for product vendor marketing and notification responsibilities.
11. The APM is complemented by two additional policy documents that outline specific guidance for key AISEP stakeholders. These documents are not publicly available.
  - AISEP Certifier Policy (ACP): Specific guidance to the Australian Certification Authority (ACA).
  - AISEP Evaluator Policy (AEP): Specific guidance to Australian Information Security Evaluation Facilities (AISEFs).
12. The three AISEP policy documents collectively form the AISEP Quality Manual.

## 1.4. Mutual recognition agreements

13. Australia, through ASD, has an agreement in place to mutually recognise the results of IT security evaluations. Authorised arrangements and understandings are identified in section 4.1.3 and briefly below.
  14. At the time of publication, one mutual recognition arrangement exists:
    - the Common Criteria Recognition Arrangement (CCRA): which is shared between participants of this arrangement. See About The Common Criteria : CC Portal ([commoncriteriaportal.org](http://commoncriteriaportal.org)) The CCRA covers certificates with claims of compliance against CC assurance components of either:
      - i. a collaborative Protection Profile (cPP), developed and maintained in accordance with CCRA Annex K, with assurance activities selected from Evaluation Assurance Levels (EAL) up to and including level 4 and ALC\_FLR (Flaw Remediation), developed through an International Technical Community and endorsed by the Management Committee, or
      - ii. EAL 1 through 2 and ALC\_FLR (Flaw Remediation).
    - Where a CC certificate claims compliance with EAL 3 or higher, but does not claim compliance with a cPP, then for the purposes of mutual recognition under the CCRA, the CC certificate should be treated as equivalent to EAL 2.
    - CC certificates will remain on the CC Portal for five years unless the validity period is extended using the appropriate procedures.
- Note: EAL is an increasing evaluation assurance scale (from EAL1 to 7) that specifies the rigor of evaluation assurance requirements.**
15. The ACA recognises PPs from other schemes, as deemed necessary, based on the demand of vendors and Australian consumers.
  16. There are two types of CC evaluations that are conducted within the AISEP; these are an evaluation against a specific Target of Evaluation (TOE) at an EAL-based evaluation or against a PP. For the purpose of selecting evaluations against a PP, the ACA maintains a list of endorsed PPs on the AISEP website.



# **Chapter 2 – Organisation of the AISEP**

17. This chapter contains the AISEP roles and operational policy that is performed by:
- AISEP management: Provides strategic governance and management direction
  - ACA roles and responsibilities: Performs the strategic oversight and certification activities under the rules of the CCRA
  - AISEF roles and responsibilities: Conducts IT security evaluations against the CC standard in accordance with the AISEP Policies.

## 2.1. AISEP management

### 2.1.1 AISEP governance and managerial roles

18. The following officials from ASD participate in the management of the AISEP:
- DGASD: The authority for the AISEP.
  - HACSC: Coordinates the strategic direction set by DGASD in relation to the organisation's cyber security mission and is the signatory authority for the ACA. This authority may be delegated to its respective division or branch heads, as appropriate or necessary.
  - 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.
19. The ACA is a resource provided by the Australian Government that facilitates the operation of the AISEP in the interest of both the public and private sectors. The ACA resides within the ACSC, which itself is part of ASD. An overview of this structure is provided in Figure 2: AISEP management framework.

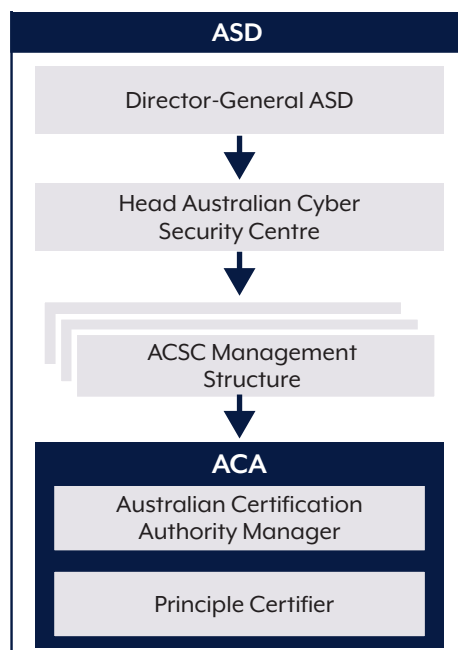


Figure 2: AISEP management framework

## 2.2. ACA roles and responsibilities

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

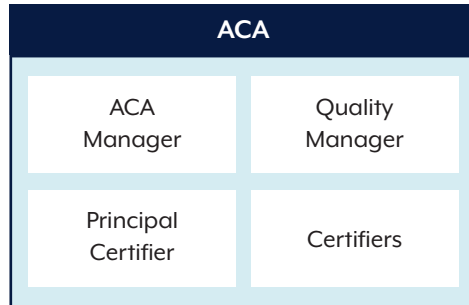


Figure 3: ACA roles

### 2.2.1 ACA management

21. The responsibility of the ACA Manager is to:
- oversee the operations of both the ACA and AISEFs
  - coordinate and chair the AISEF Controllers Meetings (ACMs)
  - oversee the operation of the ACA's quality management system with other ACA management
  - report AISEP business to senior ASD management
  - liaise and foster relationships with AISEP stakeholders.
22. The Principal Certifier, who is a special instance of an ACA Certifier (section 2.2.2 below), is to have:
- experience in the interpretation of the CC and in the development of relevant international standards deemed sufficient by ASD management
  - skills and/or experience in the management of technical work and staff.
23. The Principal Certifier has the following additional responsibilities:
- manage certifications and allocate resources as required
  - report to senior ASD management on the technical operations of the AISEP
  - oversee the operation of the ACA's quality management system with other ACA management
  - ensure the technical validity and accuracy of information contained in ACA technical reports and documents
  - ensure technical alignment within the AISEP and with the international CC community
  - lead the ACA's effort in the development of PPs and other relevant international standards, as required
  - foster relationships and liaise with AISEP technical stakeholders
  - manage the technical development of certification staff and associated training.



24. The responsibility of the Quality Manager is to:
- administer and operate the ACA's quality management system and provide central quality control duties for the ACA
  - maintain a register of ACA certifier qualifications, training and experience
  - maintain a register of AISEF evaluator qualifications, training and experience
  - conduct internal quality audits.

## 2.2.2 ACA Certifiers

25. The ACA maintains technical staff, known as Certifiers, to perform the functions of certification and certificate assurance continuity for the AISEP. Certifiers are also involved in the development of standards, including PPs.
26. The ACA Certifier is to:
- hold a relevant tertiary qualification in a field such as computer science, information security, networking, communications and software engineering, or equivalent practical experience
  - have an understanding of IT security principles and technologies
  - have completed the ASD and AISEP certifier training.
27. The responsibility of a Certifier is to:
- manage and conduct CC certification in partnership with AISEF Evaluators
  - continue to advance their skills in IT security evaluation and information security principles and technologies
  - adhere to AISEP quality controls
  - participate in standards development work, including PPs.
28. 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:
- ongoing technical training
  - leveraging subject matter experts (SMEs) in the organisation
  - close technical interaction with the AISEF Evaluators.
29. With the technical oversight of the Principal Certifier, Certifiers lead certification tasks for EAL-based and PP-compliant evaluations.
30. The ACA management ensure Certifiers have clear, up-to-date, documented instructions regarding their duties and responsibilities. The ACA does not employ contractors to perform certification duties.
31. The ACA is staffed by ASD personnel and a staff member can take on more than one ACA role.

## 2.2.3 ACA quality assurance and compliance

32. The ACA manages quality assurance and compliance business functions that ensure the ACA maintains compliance with quality standards and CCRA requirements (Ref. [5]).
33. 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's compliance with the APM (this document), as specified in section 2.3.5 below and the AEP (Ref. [13]).

### 2.2.3.1 Assessment and compliance

34. The ACA must undergo independent assessment by other CCRA member nations as defined in Annex D of the CCRA (Ref. [5]). This occurs at least once every five years and is necessary to maintain status as a certificate-producing CC scheme.
35. The ACA conducts internal self-assessments to ensure compliance with the requirements specified in Annexes B and C of the CCRA (Ref. [5]). In addition, peer review and documentation review procedures are in place to ensure the ACA operations are administered in a non-discriminatory manner.
36. The Quality Manager conducts Periodic Management Reviews (PMRs) to ensure ACA's compliance with the requirements specified in Annex C of the CCRA (Ref. [5]).
37. The ACA maintains the results of management reviews in accordance with Australian archives legislation, regulations and internal policies, for a period of seven years (Ref. [12]).

### 2.2.3.2 Documentation control

38. The ACA maintains a system for the control of documentation, ensuring that:
  - current documentation is available to key stakeholders
  - documents are not amended or superseded without authorisation
  - changes are promulgated in such a way that those who need to know are informed promptly
  - all records are stored securely and are accessible for a period of at least seven years
  - superseded documents are declared void.

### 2.2.3.3 ACA dispute resolution

39. 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.
40. 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.
41. The ACA holds a raised concern or a formal complaint in the strictest confidence.
42. 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.
43. The ACA exercises control regarding the use of awarded CC 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.
44. The ACA, in the formal meetings at the beginning and end of the evaluation task, informs and reminds 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 have been misused.

### 2.2.3.4 Common Criteria certificate withdrawal

45. A certificate is withdrawn when:
  - serious technical inaccuracies in the evaluation, or evaluation impropriety, are identified after certification
  - the product vendor provided false or misleading evaluation evidence
  - the certified product contains known security-relevant vulnerabilities that are not mitigated by the vendor.

**Note: A decision to withdraw a certificate is a reviewable decision under section 5.1.1 Reviewable decisions.**

46. The following actions are taken when the ACA withdraws a certificate:
  - the product vendor and AISEF are formally notified, with justification for the withdrawal included
  - the ACA then issues an announcement of the CC certificate withdrawal on the ACSC's AISEP webpage. The CC Portal entry is removed.

## 2.3. AISEF roles and responsibilities

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

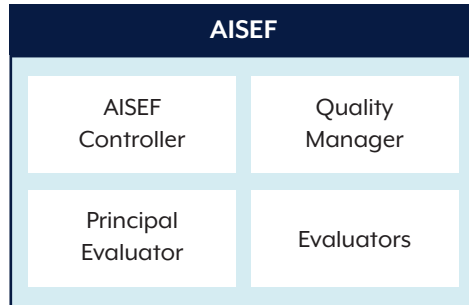


Figure 4: AISEF roles

### 2.3.1 AISEF management

48. The AISEF management structure must have an AISEF Controller who:
- is responsible for the management of the AISEF
  - has expertise in project and contract management and quality control
  - has a sound understanding of, and ensures compliance with, AISEP policy
  - ensures that any conflicts of interest are managed and declared to the ACA Manager.
49. The ACA will consider whether to accept the nomination for AISEF Controller, based on the criteria in paragraph 48 above. The ACA will confirm the approval of the AISEF Controller and notify the AISEF in writing.
50. The AISEF Controller must be supported by the following roles:
- AISEF Principal Evaluator: Responsible for the effective application of accepted IT security evaluation criteria within the AISEF.
  - AISEF Quality Manager: Responsible for the implementation and management of the AISEF quality system.
  - AISEF Facility Security Officer: Responsible for AISEF security, which includes physical, personnel and information security.
51. 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.
52. The AISEF is required to report to the ACA if any staff member approved by the ACA to perform a defined role ceases to perform that role. This notification is to be made in writing within one week. This must also be reflected in the next AISEF Progress Report (APR) as defined in section 3.3.1 below.

## 2.3.2 AISEF Evaluator

53. The Evaluator is to:
  - hold a relevant tertiary qualification in a field such as computer science, information security, networking, communications and software engineering or equivalent practical experience
  - have an understanding of IT security principles and technologies.
54. The Evaluator must:
  - have completed the AISEP overview training
  - undergo or have completed AISEF CC training
  - learn or have experience in CC evaluations
  - conduct evaluation tasks in partnership with one or more evaluators
  - continue to advance their skills in IT security evaluation and information security principles and technologies.
55. The AISEF must apply in writing to the ACA for approval of AISEF Evaluator status.
56. For a new AISEF Evaluator, the AISEF must first notify the ACA, in writing, of the new candidate and submit a copy of the applicant's curriculum vitae detailing their skills and experience. The AISEF is to provide a proposed training plan with an evaluation work schedule for the new candidate.
57. Prior to the approval of an AISEF Evaluator by the ACA, the candidate must have completed the training plan with an experienced evaluator. A statement of training completion and training records (including details of evaluation tasks involved) is then forwarded to the ACA to make the decision. The completed training plan should be submitted within six months or at an agreed time from the initial notification.
58. Alternatively, for ACA approval of a new AISEF Evaluator candidate, the AISEF can provide any evidence detailing the candidate's past experience when the AISEF notifies the ACA of the candidate, as per paragraph 57 above.
59. The ACA will confirm the approval of the AISEF Evaluator and notify the AISEF in writing.
60. The AISEF must at all times maintain trained staff capable of undertaking evaluation tasks. The minimum number of AISEF evaluation staff should be two, with one member in the Principal Evaluator position. AISEF Evaluators may seek advice on testing from SMEs when that expertise is available in their organisation.
61. When these conditions are not met, the AISEF must inform the ACA, in writing, with a proposed solution as soon as practicable, and record this in the AISEF reports, as defined in section 3.3.1 below.

### 2.3.2.1 Principal Evaluator

62. Acceptance of nomination for the Principal Evaluator role is considered by the ACA based on the criteria in paragraphs 67, 68 and 69 above. The ACA will confirm the approval of the AISEF Principal Evaluator and notify the AISEF in writing.

### 2.3.2.2 Evaluator status

63. The Principal Evaluator and evaluator status can lapse, at the discretion of the ACA, when the individual has not performed evaluation work for one year.
64. The ACA may reinstate a lapsed evaluator status on the evaluator's return to an AISEF position. This will depend on the following conditions:

- length of absence
- previous evaluator status
- length of evaluator service
- relevant experience during absence
- demonstrable competence.

65. The reinstatement of AISEF evaluator's status will be determined by the ACA on a case-by-case basis and the ACA will notify the AISEF in writing.

**Note: A decision not to reinstate an evaluator's status on their return to an AISEF position is a reviewable decision under section 5.1.1 Reviewable decisions.**

66. 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

67. Australian legal commercial entities operating within Australia can apply to become an AISEF.
68. An applicant for an AISEF licence provides a written proposal to the ACA, with information about how it intends to implement and maintain the requirements for operating as an AISEF. This includes an ISO/IEC 17025 accreditation. Required details are described in Annex B.
69. 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.
70. 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.
71. An AISEF licence is granted when the following conditions have been met:
  - the applicant has submitted the proposal to the ACA
  - the applicant has fulfilled the AISEF licensing criteria outlined in this manual and agreed to the conditions of the AISEF licensing agreement
  - the ACA has formally accepted the applicant's proposal.

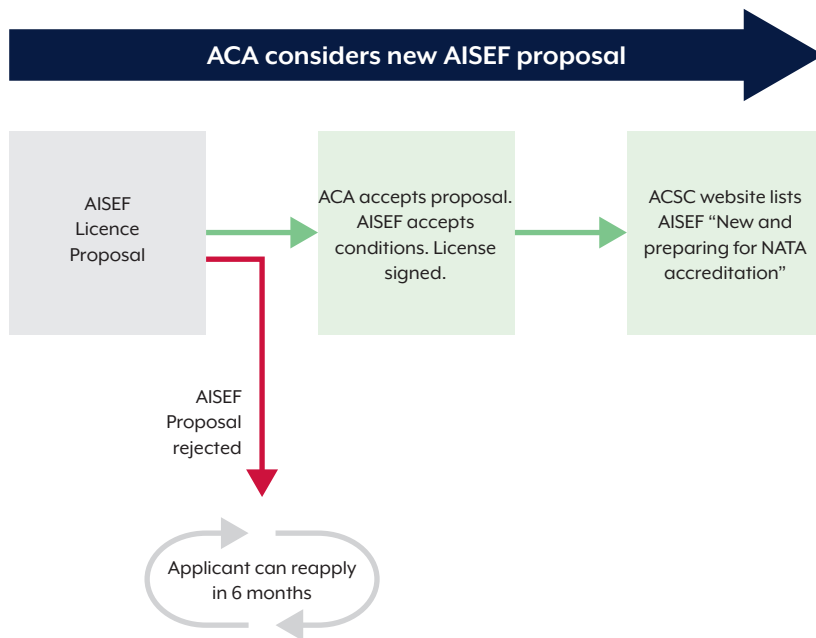
**Note: A standard licensing agreement is available from the ACA on request.**

72. 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 section 5.1.2 Non-Reviewable decisions.**

73. An unsuccessful applicant may re-apply to become a licensed AISEF six months after 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.

74. 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
  - list the facility on ACSC's AISEP website and identify the AISEF as "New and preparing for National Association of Testing Authorities (NATA) accreditation".

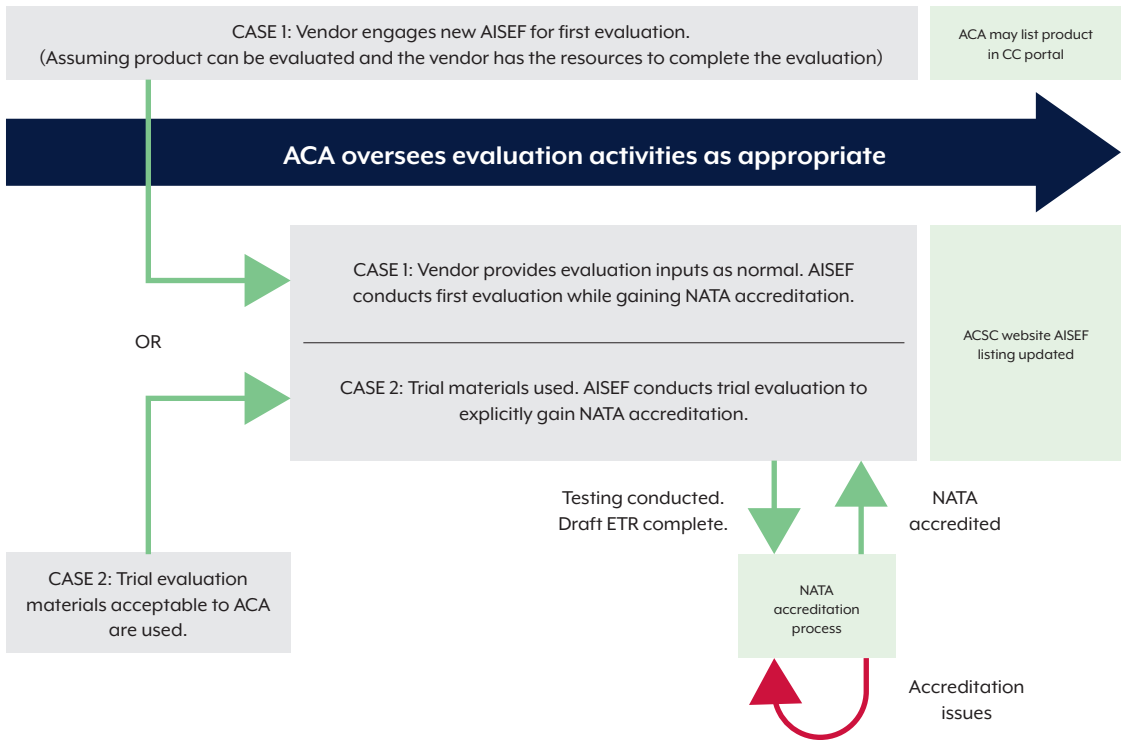


**Figure 5 AISEF proposal**

75. There are two possible pathways for an AISEF to gain NATA accreditation:
- One, an evaluation is performed in parallel with gaining NATA accreditation. Evaluations successfully completed by the licensed AISEF may be certified for mutual recognition, at the discretion of the ACA, once the licensed AISEF achieves its NATA accreditation. This is shown as 'CASE 1' in Figure 6.
  - Two, an evaluation can be performed based on trial inputs accepted by the ACA. This is shown as 'CASE 2' in Figure 6. The AISEF may gain NATA accreditation based on the completed work.



76. More details are provided in Section 2.3.4.



**Figure 6: NATA accreditation and first evaluation**

## 2.3.4 NATA accreditation requirements for the AISEF

77. An AISEF must submit to NATA an application for accreditation as a test laboratory. Test laboratory status must be achieved within the first year of the AISEF's operation. NATA accreditation is completed against requirements of ISO/IEC 17025 and the ISO/IEC 17025 Application Document, Manufactured Goods – Annex, Software and information system performance testing (Ref [7]).
78. For a product aiming for CCRA mutual recognition, NATA accreditation must be achieved prior to the end of the conduct phase with ACA acceptance of the final Evaluation Technical Report (ETR).

**Note: Evaluation successfully completed by the licensed AISEF for the purpose of a NATA accreditation may be certified at the discretion of the ACA, once the licensed AISEF achieves its NATA accreditation.**

79. An AISEF wishing to maintain its AISEF licence must continue to comply with NATA accreditation requirements, including continual monitoring by the ACA and NATA. Any failure by an AISEF to comply with these requirements may result in the ACA suspending or terminating the licence.

## 2.3.5 AISEF licence monitoring

80. The ACA assesses the AISEF's adherence to AISEP policy and licence conditions continuously and in particular during the day-to-day conduct of the evaluation work.
81. NATA carries out the following assessments of the AISEF for compliance with the NATA requirements, as identified in section 2.3.4:
  - a technical reassessment at which the ACA may attend as a technical assessor or as an observer; this occurs every three years
  - a surveillance visit with a focus on assessing the management system. This occurs 18 months following the technical assessment.
82. In the instance of a non-compliant AISEF, the ACA may initiate the following two-stage process to discontinue the AISEF licence:
  - suspension
  - termination.
83. The ACA may suspend the AISEF licence if:
  - 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
  - the AISEF fails to comply with any terms and conditions specified in the licence agreement.

**Note: The decision to suspend an AISEF's licence is NOT a reviewable decision under section 5.1.2 Non-Reviewable decisions.**

84. An AISEF with a suspended licence is not authorised to carry out AISEP evaluation work. The AISEF must not:
- advertise its services as an AISEF or
  - continue to bid for evaluation work.
85. The ACA reviews the suspended status when the suspended AISEF notifies the ACA that the relevant concerns have been rectified.
86. When an AISEF's licence is suspended, the ACA will indicate this status on the ACSC's AISEP website.
87. 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, within a reasonable timeframe, to rectify the licence suspension issue to the satisfaction of the ACA.

**Note: The ACA's decision to terminate an AISEF's licence is NOT a reviewable decision under section 5.1.2 Non-Reviewable decisions.**

88. An AISEF with a terminated licence is not authorised to carry out activities under the auspices of the AISEP.
89. An organisation that was a former AISEF may seek reinstatement by re-applying for a licence. In assessing a re-application, the ACA will pay particular attention to those characteristics that caused the licence termination in order to ensure that program quality is upheld.
90. The ACA will remove the listing of the AISEF with the terminated licence from the ACSC's AISEP website and the CC Portal.

### 2.3.6 Associated costs for the AISEF

91. 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.
92. The AISEF should be aware of other costs associated with operating an AISEF, which may include:
- training costs to maintain a level of competence for staff members
  - equipment and material costs to support testing of an evaluation
  - operational costs associated with maintaining a secure evaluation facility.

**Note: The ACA does not charge any fees associated with the establishment of an AISEF or for a product certification.**

## 2.3.7 AISEF impartiality

93. The AISEF must operate as an independent, self-contained unit. When part of a larger parent organisation, its operations and administration should be functionally separate from its parent organisation, and ensure separate accommodation with its own controlled access.
94. The AISEF Controller must be able to demonstrate to the ACA that the AISEF – or any of its staff members – is impartial in the conduct of an evaluation. Individuals involved in developing a product or evaluation documentation are to be kept separate from evaluation activities involving that product.
95. Further, an AISEF is not authorised to:
  - evaluate a product developed and/or owned by its parent organisation or subsidiaries
  - evaluate a product developed and/or owned by another organisation in which the parent organisation has a commercial or financial interest
  - provide any consultancy or advice to a product vendor or developer that compromises the independence of an evaluation.

**Note: The ACA permits an AISEF to provide to a vendor both consultation in support of evaluation and evaluation services; however, the AISEF must be able to demonstrate the separation of these activities from evaluation activities.**

## 2.3.8 AISEF security requirements

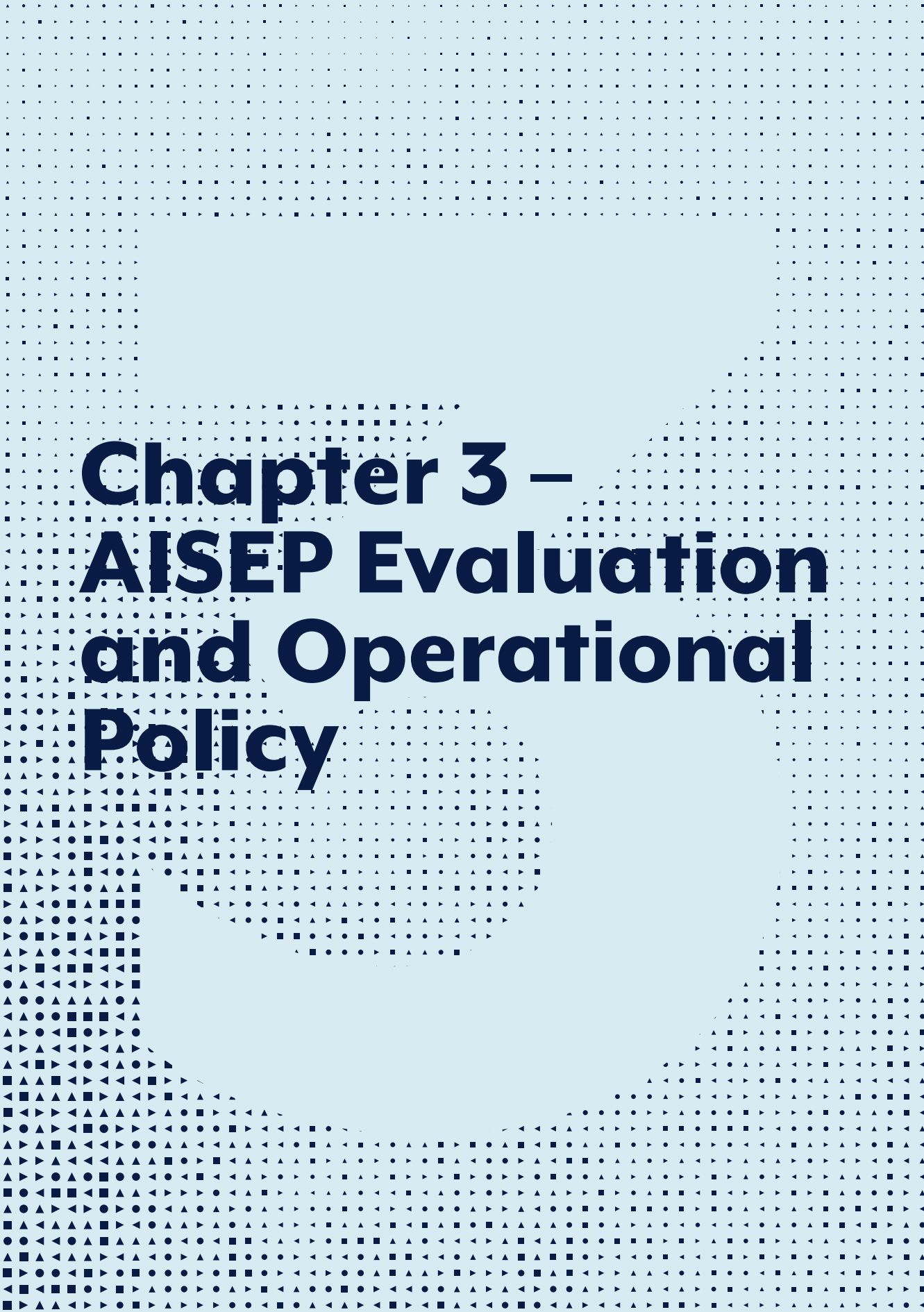
96. An AISEF must comply with all physical and ICT systems security requirements, as per the Protective Security Policy Framework (PSPF) (Ref. [9]), up to OFFICIAL: Sensitive.
97. The AISEF must implement sound security practices and procedures to protect the confidentiality and integrity of commercially sensitive information.
98. 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.
99. The AISEF must nominate a Facility Security Officer, assigned overall responsibility for security within the AISEF.
100. The AISEF must have documented security policies and supporting procedures. At a minimum, these documents must address the following:
  - physical security
  - personnel security
  - information security.

### 2.3.8.1 AISEF information security

101. The AISEF must use ASD-approved cryptographic algorithms (AACAs) and protocols, as specified in the Australian Government Information Security Manual (ISM) (Ref. [9]), 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.
102. Evaluation and commercially sensitive information and material must be marked with the appropriate label. ASD uses protective markers for information of which disclosure may be limited or prohibited by legislation, or which may otherwise require special handling.
103. In the AISEP, evaluation information and material must be marked with the appropriate Information Management Markers (IMMs) and must not be distributed beyond AISEF and ACA staff without the express written permission of the ACA. In addition, a label of OFFICIAL or OFFICIAL: Sensitive must be used with the protective markers to indicate who the limited distribution applies to. Guidance on the use of protective markers is provided in the AEP (Ref. [13]).
104. Evaluation information and material carrying protective markers must be contained within the Evaluator and Certifier relationship, as any external exposure may compromise:
  - the outcome of an evaluation or certification
  - the integrity of the AISEP
  - the intellectual property of the ACA or an AISEF
  - the intellectual property of the product vendor.

### 2.3.9 AISEF archiving and disposal

105. At the completion of an evaluation task, the AISEF is responsible for archiving or disposing of all material supplied for the evaluation, as agreed at the Task Start-up Meeting (TSM).
106. Adequate records must be retained by both the ACA and AISEF to ensure the repeatability of the task, and to comply with the requirements of the Australian Archives Act 1983 (Ref. [12]).
107. The AISEF retention period of seven years pertains to all records that adhere to:
  - quality processes
  - security policies and procedures
  - evaluation activities.



# **Chapter 3 – AISEP Evaluation and Operational Policy**

# 3.1. IT security evaluation and certification

- 108. The AISEP's evaluation and certification workflow of activities comprises five major phases. Figure 7: AISEP Evaluation and Certification Workflow of Activities illustrates the major phases of Initiate, Plan, Conduct, Conclude and Continuity.
- 109. 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 allows product vendors to extend their CC certificate to cover minor changes to the original evaluation. Assurance continuity is described in section 3.2 below.

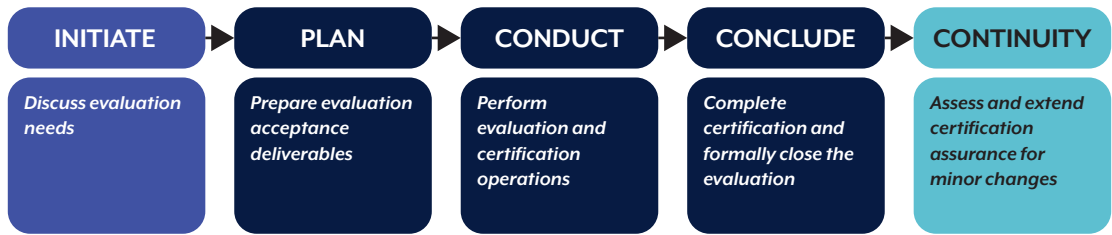


Figure 7: AISEP Evaluation and Certification Workflow of Activities

- 110. This chapter describes the following 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.
  - **Continuity phase:** Process for the maintenance, re-evaluation and re-assessment of CC certified products.

## 3.1.1 Plan phase

### 3.1.1.1 Sponsorship letter for an AISEP evaluation

111. A request for an EAL-based AISEP evaluation requires an organisation to complete a Sponsorship letter for an AISEP evaluation. The security priorities are already established where an ACA-endorsed PP exists for product technologies; in this case, a Sponsorship letter for an AISEP evaluation is not required. An evaluation can only be sponsored by a consumer and may not be self-sponsored by the vendor.
112. A Sponsorship letter for an AISEP evaluation is completed by a relevant organisation. The letter indicates the consumer's interest in the product, but does not oblige the consumer to purchase the product once it has been certified. It will also allow the ACA to contact the sponsor about the intended use of the product or to discuss any issues raised during its evaluation. A template for this letter is available from the ACSC website.
113. The Sponsorship letter for an AISEP evaluation forms part of the AISEP Acceptance Package (AAP) submitted by an AISEF. The letter may be submitted prior to the AAP as it enables the ACA to engage the relevant organisation on its evaluation needs prior to the ACA's review of the evaluation task.

### 3.1.1.2 AISEP Acceptance Package

114. The AISEF submits an evaluation task to the AISEP for acceptance through an AAP.
115. The AISEF submits an electronic copy of the specified AAP to the ACA for each evaluation request. The AAP contents include:
  - 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 116 below, and that the product vendor has been made aware of its obligations. This deliverable is supplied by the AISEF
  - an Evaluation Work Program (EWP) that documents the deliverables that are required by the AEP (Ref. [13]), including a unique task identifier for the evaluation. The EWP specifies that the evaluation team comprises the Lead Evaluator (which can be the Principal Evaluator) and a nominated Evaluator, at a minimum. The AISEF may decide on any number of additional Evaluators. The EWP will also specify the Evaluation Supporting Consultant (ESC) arrangements. This deliverable is supplied by the AISEF
  - the requirement that the proposed evaluation timeframe be achievable by the AISEP and the product vendor. This deliverable is supplied by the AISEF, with input from the product vendor
  - the Security Target (ST) for the proposed evaluation. This deliverable is supplied by the product vendor via the AISEF.
  - a completed cursory 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

116. The following criteria must be adequately satisfied for the ACA to accept an evaluation task into the AISEP:
- An Australian organisation completed the Sponsorship letter for an AISEP evaluation, with adequate justification for an evaluation that is not compliant with an ACA-endorsed PP.
  - The submitted AAP includes the required information and documents, as defined in paragraph 115 above.
  - The submitted ST provides a technically sound basis for the commencement of the evaluation.
  - The submitted ST has sufficient relevance to, and presents sufficient benefits for, Australian consumer use.
  - The submitted ST complies with an ACA-endorsed PP that exists for that technology, where applicable.
  - The proposed evaluation plan contains the level of detail required, is of adequate quality, and is able to abide by AISEP policies and procedures.
  - The AISEF is able to meet the requirements for specialist technical skills, independence and impartiality.
  - The product is NOT currently being evaluated in another scheme that would be covered by a mutual recognition arrangement. See section 4.1.3 below for relevant mutual recognition arrangements and understandings.
  - A contractual agreement exists between the product vendor and the AISEF to have the product evaluated under the AISEP.
117. The ACA authorises acceptance of an evaluation task into the program through the formal notification of an acceptance letter. Evaluation activity may not commence until the evaluation task has been formally accepted and notified by the ACA. When an accepted evaluation task commences, the ACA will publish the product on the AISEP's website as 'In evaluation'.
118. The ACA may reject an evaluation task if:
- any of the requirements specified in paragraph 116 above have not been adequately met
  - the evaluation does not meet the ICT security needs of Australian consumers in protecting their communication and information systems
  - the evaluation does not meet Australia's national interests.
119. 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 section 5.1.1 Reviewable decisions.**

120. For products that contain cryptographic functionality in the scope of the evaluation, the ACA enforces the following additional acceptance requirement:
- Consumers must be able to configure the evaluated product to use AACAs and ASD-approved Cryptographic Protocols (AACPs) for designated cryptographic functions, as specified by the ACA.

**Note: AACAs and AACPs are specified in the Australian Government Information Security Manual (ISM) (Ref. [9]).**

121. The ACA will consider a request from the product vendor for an evaluation to be conducted discreetly and not be listed on the CC Portal until the task is completed. However, task progress goals still apply. The ACA must be able to inform relevant organisations of the discreet evaluation, should the need arise. The ACA will inform the AISEF and product vendor if this occurs.

#### **3.1.1.4 AISEF responsibilities to the product vendor**

122. Prior to the AAP submission, the product vendor must be informed of:
- the program's evaluation process
  - the role of the AISEF
  - the role of the ACA
  - the product vendor's responsibilities throughout the evaluation as defined in paragraph 123 below
  - the location of the relevant AISEP policy documents on the ACSC website.
123. The AISEF must inform the product vendor that, during the evaluation, they are responsible for and agree to the following:
- to provide personnel and financial resources to fully support the conduct of the evaluation and to progress the task sufficiently
  - to provide the necessary equipment and deliverables required for the evaluation. This may include the provision of evaluation deliverables to the ACA
  - to allow the ACA to provide draft versions of the ST to potential Australian consumers while the product is in evaluation, if deemed appropriate.

## 3.1.2 Conduct phase

### 3.1.2.1 Conduct of the certification team

124. The ACA allocates a Lead Certifier to an evaluation task. Additional support certifiers may also be assigned.
125. Certifiers conduct oversight activities to gain assurance that the evaluation is being conducted accurately by:
  - conducting Certification Assurance Meetings (CAMs) with the evaluation team
  - discussing technical details with the evaluation team, the Principal Certifier and SMEs
  - reviewing evaluation materials, including reports
  - maintaining certification records.
126. Should the ACA be unable to maintain suitably qualified employees to complete certification work, the ACA may, in discussion with the AISEF:
  - control the introduction of new evaluation tasks
  - negotiate later start times for new evaluation tasks
  - negotiate later completion times for existing evaluation tasks
  - prioritise ACA work effort for current tasks.

### 3.1.2.2 Conduct of the evaluation team

127. The AISEF must assign at least two evaluators to each evaluation task, subject to the following provisions:
  - one evaluator is assigned as the Lead Evaluator
  - at least one or more evaluators are allocated to provide support.

**Note: The Principal Evaluator has oversight of all active evaluations.**

128. Changes to personnel during the evaluation must be agreed to by the ACA. The AISEF informs the ACA of any changes in writing.
129. 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.

### 3.1.2.3 Evaluation status

130. The ACA requires timely information in order to progress evaluation tasks. The AISEF reports to the ACA on the progress of each evaluation at least monthly, or as progress is made or issues arise.
131. The ACA recognises evaluation activity as progress for the evaluation task. Supporting consultation, training, AISEP policy or licence compliance activities do not count as evaluation progress or as a contribution to evaluation progress.
132. The ACA is responsible for assessing and determining the status of current AISEP evaluation tasks, and this is reflected on the AISEP website through progress indicators.
133. The ACA uses one of the following progress indicators for a current evaluation task:
  - Progressing: Used to indicate that the evaluation task is progressing as agreed in the EWP.
  - Inactive: Used for an evaluation task that is not being maintained acceptably, prompting remedial action by the ACA in accordance with AISEP policy as defined in section 3.1.4 below.
  - 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.**

134. Products not yet available for purchase can be listed as concurrent evaluations. However, if, during the course of a concurrent evaluation, the product becomes available for purchase, the normal progress rules are applied by the ACA.

### 3.1.2.4 Product vendor initiated changes

135. 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, in order to enable the ACA to make an informed decision prior to committing to the change.
136. 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 evaluation task's Lead Certifier.
137. Major scope changes or those that resolve a security issue discovered through the evaluation process must be approved by the Principal Certifier in writing.
138. Examples of these scope changes include:
  - the removal of a Security Functional Requirement (SFR) or claims from the AAP-approved ST
  - the removal or amendment of an SFR dependency from the AAP-approved ST
  - a change in the ST objectives, threats and/or assumptions from the AAP-approved ST.
139. 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.
140. On completion of evaluation activities, the AISEF submits a draft ETR to the ACA for review. The AISEF also submits evaluation evidence and relevant documentation along with the ETR. The ETR content requirements are described in Section 4.3.5 below. When an evaluation has been conducted against a cPP, there is an additional requirement to report on the cPP assurance activities. This may be in the form of an Assurance Activity Report (AAR).
141. The ACA will provide formal ETR comments. The AISEF must address the ACA comments before a final ETR is delivered to the ACA.

### 3.1.3 Conclude phase

142. On final ETR agreement, the evaluation is deemed to be complete, and the ACA will:
  - finalise a Certification Report (CR) for the product evaluation as defined in section 4.3.2 below. The certification is deemed to be complete when all parties agree on the final CR. The date on the final CR is the official certification date to mark the end of a certification.
  - post a listing of the certification to the CC Portal, including the CR and ST document
  - create CC certificates for the completed evaluation and publish a copy of the certificate once signed.
143. The issue date on the certificate is used for the purpose of certificate validity and archiving on the CC Portal.
144. An important AISEF role is to ensure that the task is closed down in a controlled manner through a formal Task Closedown Meeting (TCM). This provides evaluation stakeholders the opportunity to present feedback and discuss the evaluation information to be distributed or disposed of. The possibility of AAC may also be discussed at the TCM. AAC is described in section 3.2 below.
145. After the TCM, evaluation and certification records are to be archived as described in section 2.3.9 of this document.

### 3.1.4 AISEF evaluation progress rules

146. Best practice project and contract management controls must be employed throughout the conduct of an evaluation to ensure undue delays are avoided. The ACA will check evaluation progress at least once a month.
147. 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.
148. When sufficient evaluation activity has not occurred in two months, 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.
149. The ACA may consider the evaluation task 'inactive' when an evaluation task has not progressed sufficiently over two consecutive months. The ACA notifies the AISEF and the product vendor of the status change, modifies the AISEP website listing accordingly, and initiates an investigation of the situation.

150. During the investigation, the AISEF is required to provide additional information on what actions it has taken or proposes to take, in order to progress the task. The product vendor is expected to provide information to the ACA to assist it in deciding whether to remove the listing.
151. Should there be insufficient evaluation progress across three consecutive months; the ACA will remove the listing for the task. The ACA will formally notify the AISEF and the product vendor, by letter, following the listing removal. The task will not be re-listed until the AISEF can demonstrate one month of sufficient evaluation progress.
152. The ACA reserves the right to terminate the task if sufficient evaluation progress is not demonstrated over three consecutive months 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 section 5.1.1 Reviewable decisions.**

153. On termination of a task, the ACA will:
  - remove the task's 'In evaluation' entry on the ACSC's AISEP webpage
  - provide formal notification to the product vendor and the AISEF of the termination of the task
  - provide formal notification to the organisation that provided the sponsorship letter for an AISEP evaluation
  - notify known consumers.
154. A task that the ACA has terminated is not permitted to recommence. To continue a previously terminated evaluation, the task will be treated as a new evaluation. The AISEF must submit a new AAP for the task. However, the ACA may recognise previous evaluation effort in accordance with re-evaluation policy defined in section 3.2.2 below.
155. 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 section 5.1.1 Reviewable decisions.**

156. The ACA expects all evaluations against PPs to be completed within six months of AAP acceptance. More details of the expected evaluation timeline are described in the AEP.

## 3.2. AISEP Assurance Continuity

157. 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.
158. 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.

### 3.2.1 AAC acceptance

159. AAC follows the Common Criteria format of assurance continuity, as described in Assurance Continuity: CCRA Requirements (Ref.[6]). For changes to the certified Target of Evaluation (TOE), the AISEP requires an Impact Analysis Report (IAR) to form the basis of continuity activity. For changes to the threat environment, the product vendor needs to consult the ACA for re-assessment activity.
160. 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 section 5.1.2 Non-reviewable decisions.**

### 3.2.2 AISEP assurance continuity for maintenance

161. For a product to be considered for AAC, the following must occur:
  - the product must originally have been evaluated through the AISEP
  - an Impact Analysis Report (IAR) has been submitted to the ACA
  - a covering letter has been provided to the ACA with the product vendor details.
162. For any changes to the development environment assurance measures, an AISEF will be required to conduct a subset evaluation of the applicable assurance components in the ST.
163. Where the ACA determines that the changes are minor, it can be accepted as a maintenance update to the product's original certificate.
164. When all requirements have been met, the ACA updates the CC Portal listing for the certified product to include:
  - an updated maintenance addendum to the CR
  - an AISEP Maintenance Report.

**Note: No new CC certificate will be issued and the certificate validity remains unchanged.**

### 3.2.3 AISEP assurance continuity for re-evaluation

165. When 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. Major changes will warrant independent investigation by an AISEF.



166. A product vendor may choose to submit a product directly for re-evaluation without an IAR if they believe that the modification to the certified product is major or the aggregate of changes warrants a re-evaluation. A re-evaluation task is conducted in a similar fashion to a normal evaluation task.
167. Re-evaluation tasks are subject to the same acceptance rules as normal evaluation tasks. In addition, the AISEF must have access to the following documents from the previous certification:
- Certificate for the TOE (including maintenance addendum)
  - Certification Report (CR)
  - Evaluation Technical Report (ETR)
  - Security Target for the Certified TOE
  - Impact Analysis Report (IAR) if applicable
  - previous evaluation deliverables.
168. The AISEF schedules a meeting with the ACA to agree on the required level of effort for the re-evaluation task.
169. A re-evaluation task concludes in the same manner as an evaluation task. Unlike a maintenance task, a re-evaluation results in a new certification report and certificate being issued.

**Note: Product vendors will need to seek advice from the ACA for AISEP Assurance Continuity options where the original evaluation was completed against an ACA endorsed PP. This is to ensure the currency of any PP used.**

### 3.2.4 AISEP assurance continuity for re-assessment

170. A product vendor is permitted to directly enter into re-assessment if they believe that the threat environment has changed sufficiently. If this is the case, assurance activities concerning the vulnerability assessment are conducted again. Relevant product lifecycle activities are also repeated unless the product vendor provides sufficient justification to the ACA.
171. A new ETR is produced and a re-assessment report is generated. If the re-assessment report indicates that the TOE continues to meet the changed threat environment, the validity of the initial certificate is extended if the re-assessment is made public. As described in Assurance Continuity: CCRA Requirements (Ref. [6]), if the re-assessment report indicates the certified TOE no longer meets the changed threat environment and is made public, the initial certificate validity is unchanged.

### 3.2.5 Non-compliance of AAC evaluations

172. The ACA retains the ability to conduct an audit in order to verify AAC-related claims by the product vendor.
173. 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.
174. All non-compliance rules for evaluation tasks apply equally to re-evaluation and re-assessment tasks.

## 3.3. Supporting functions of program management

175. The ACA implements Program management functions to:
- ensure the efficiency of AISEP operations and effective management of evaluation task progress
  - provide a forum for the ACA to disseminate AISEP-relevant information to the AISEFs
  - 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 Timely evaluation progress reporting

176. The AISEF reports evaluation progress at least monthly via submission of an evaluation progress report. This is to ensure visibility of an evaluation task and, if a problem occurs, allows for early identification and resolution.
177. Progress information is continually checked by the ACA during each calendar month. The first progress reporting commences at the end of the month of the TSM. The ACA deems the absence of progress reporting to be an indication that progress has not occurred and AISEP progress rules are applied as described in section 3.1.4 above. After receipt of the final ETR, progress reporting is no longer required.

#### 3.3.1.2 Quarterly AISEF Progress Report

178. The AISEF submits a quarterly APR to inform the ACA of future evaluation tasks and to raise any changes or issues relating to the AISEF. The APR is released by the AISEF Controller. The reporting periods for the APR are outlined in the AEP (Ref [13]).
179. The APR includes:
- prospective business or relevant new contacts made
  - changes to current AISEF staff or their role in the facility
  - changes to the current licensing and accreditation status of the AISEF.

**Note: in addition to reporting in the APR, these changes must also be reported, in writing, to the ACA within one week.**

- 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

180. The ACA convenes the ACM to provide a forum for disseminating AISEP management information collectively to AISEF Controllers. These meetings are generally held once or twice per year.
181. The ACA uses this forum to:
  - disseminate strategic and program information decided by ASD management
  - disseminate information from international CC meetings that ASD attends
  - openly discuss programmatic issues with the AISEFs.

## 3.3.2 Interpretations and technical alignment

182. The ACA implements the interpretations and technical alignment functions to conduct the following process and forum:
  - 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.
  - AISEP Technical Board (ATB): 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

183. An AISEP Request for Interpretation (ARI) of an IT security evaluation criteria or of an AISEP policy can be submitted to the ACA.
184. An AISEP, Australian consumer or product vendor may submit an ARI if they:
  - have difficulty interpreting a component of an IT security evaluation criteria, PP, cPP or supporting document
  - have difficulty interpreting an AISEP policy or process
  - cannot find sufficient guidance in order to perform a required AISEP activity
  - find an error in the current version of an AISEP policy or an IT security evaluation criteria, PP, cPP or supporting document.
185. The ACA assigns a unique identifier and issues an acknowledgement to the originator on receipt of an ARI.
186. In response to an ARI, the ACA will, via email or letter:
  - provide a resolution to the ARI or
  - explain why the ACA has determined that the matter in question is not required to be resolved through an interpretation.
187. The ACA publishes an AISEP interpretation for a resolution that involves interpreting an IT security evaluation criteria. The ACA distributes the AISEP interpretation for comment before it is finalised.
188. The ACA submits a final AISEP interpretation, which relates to IT security evaluation criteria, to the appropriate criteria authorities for submission to the relevant international interpretation process.
189. The ACA withdraws the superseded AISEP interpretation after the international bodies have reviewed the scheme interpretation and their response is finalised.
190. 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 that describes the update cycle for AISEP policies.
191. The ACA submits, to relevant international technical communities, an interpretation that relates to cPPs. The ACA also considers interpretations from other CCRA certificate authorising nations.

### 3.3.2.2 AISEP Technical Board

192. The ATB is a forum for interpretation and technical alignment activities within the AISEP.
193. The ACA uses the ATB to:
  - openly discuss technical issues with AISEF evaluators
  - disseminate technical knowledge to the AISEF evaluators
  - discuss AISEP requests for interpretations of IT security evaluation criteria and AISEP publications.
194. The ACA may convene the ATB meeting once or twice per year, or as needed.
195. 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.
196. 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**

197. 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

198. The AISEF must employ the security evaluation criteria and methodology for conducting IT security evaluations under the AISEP as approved by the ACA and listed on the AISEP website.
199. For an ACA endorsed PP, the requirements and the methodology that the AISEF uses are contained in the cPP and supporting document.
200. Current versions of the CC are listed on the AISEP website. As a participant in the CCRA, the ACA will always use the official current version of the CC.
201. 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

202. The ACA recognises all final interpretations of an IT security evaluation criteria by the relevant CCRA authorities.
203. The AISEF must incorporate all interpretations of an IT security evaluation criteria into evaluation activities if they are published as final at the time of the submission of the AAP.
- Note: See section 3.3.2.1 above for more information on the AISEP interpretation process.**
204. The AISEF must not use 'draft' interpretations without receiving authorisation from the ACA.
205. For a PP from other national schemes or cPP, the AISEF must apply all relevant technical interpretations up to the date of the submission of the draft ETR.

### 4.1.3 Common Criteria Recognition Arrangement

206. Australia, through the ACA, is a signatory to the CCRA (Ref. [5]). CC certificates for IT security evaluations, up to EAL2 and against ACA endorsed PPs with assurance requirements up to EAL4, are mutually recognised by the CCRA.
207. Participation in the CCRA entails the following operational program obligations:
- 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.
  - Quality system: The ACA and AISEFs implement and comply with a quality system. NATA ensures that the AISEFs operate in accordance with ISO standard 17025 (Ref. [7]) and the ACA operates in accordance with Annex C of the CCRA (Ref. [5]).
  - Effective program management: ASD 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.
  - Effective oversight: ASD ensures that a suitable number of qualified staff is maintained to provide operational and technical leadership for the AISEP. ASD has also put in place effective oversight techniques to ensure that evaluators are applying criteria effectively and consistently.
  - Management review The ACA, undertakes PMRs in order to assess the effectiveness and relevance of scheme policies and procedures, whether the scheme is continuing to meet the needs of the Australian consumers, and whether it continues to share the objectives of the CCRA (Preamble) (Ref. [5]). The review will be in the form of a meeting held at yearly intervals.

### 4.1.4 Conduct of mutual recognition

208. As part of the CCRA mutual recognition, the ACA recognises the certification of products from other CC certificate authorising nations, up to and including EAL 2 as well as against a cPP.
209. A certificate above EAL 2 that has been certified by another certificate authorising nation is mutually recognised in the AISEP at EAL 2 (e.g. An EAL 4 firewall certified by another certificate authorising nation would be recognised as an EAL 2 firewall by the AISEP). Evaluations that are augmented with flaw remediation are also mutually recognised in the AISEP.

### 4.1.5 Accreditation standards

210. 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. [5]).
211. An AISEF must comply with and be accredited against the requirements of ISO/IEC 17025 and the ISO/IEC 17025 Application Document, Manufactured Goods – Annex, Software and information system performance testing (Ref [7])



## 4.2. Program publications

### 4.2.1 Program policy and manual

212. The ACA publishes AISEP policy through this document, the APM.

### 4.2.2 Stakeholder guidance

213. The ACA publishes a series of policy documents for key AISEP stakeholders:

- AISEP Certifier Policy (ACP): This document is for ASD internal use only.
- AISEP Evaluator Policy (AEP): This document is for AISEF evaluators and is not available publicly.

### 4.2.3 AISEP publication updates

214. The ACA updates AISEP publications periodically for quality control purposes. New AISEP publication releases will incorporate relevant ARI 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.

215. A new release of an AISEP policy is:

- amended according to the ACA version control system
- authorised by ASD management
- forwarded to licensed AISEFs
- forwarded to NATA representatives where relevant
- published on the AISEP website with an associated 'New' announcement.

216. An AISEF must use the latest version of the APM and AEP.

## 4.3. Program operational outputs

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

### 4.3.1 Common Criteria Portal's Certified Products List (CPL)

218. The ACA maintains a list of evaluated and certified IT security products on the CC Portal's Certified Products List (CPL).

219. The 'In Evaluation' section of the AISEP's website comprises IT security products that are currently undergoing an evaluation in the AISEP. A product listing contains:

- a brief description of the IT product and the security functionality evaluated
- a general category or product type
- details of the AISEF performing the evaluation
- product vendor details including contact information
- the criteria or methodology that is being used to evaluate the product
- an indication of the current status of the task
- the ACA endorsed PP(s) and any applicable annexes or addenda.

220. The CC Portal's CPL listing includes the following information for all AISEP-certified product entries:

- a general category or product type
- the ST, CR and a copy of the CC certificate
- the relevant assurance level or ACA endorsed PP(s)
- the history of a certified product's assurance maintenance
- the certification and archive dates.

221. The CC Portal maintains an Archived CPL for those certified products with a CC certificate that are either more than five years old or that are:

- unavailable in their original form
- not supported by the product vendor
- not available for purchase by consumers
- no longer in compliance with the Australian Cyber Security Centre policies.

222. When a vulnerability is discovered in a certified product, the ACA will work with the vendor for a resolution. At the discretion of the ACA, the entry may be removed from the CC Portal's CPL. An announcement is made on the AISEP website.

**Note: The decision on the removal of a CC Portal's CPL entry is reviewable under section 5.1.1 Reviewable decisions.**

## 4.3.2 Certification Report

223. The ACA reports the final certification results of a product or PP evaluation task with a formal CR.
224. The ACA ensures that the contents of the CR comply with requirements specified in Annex I of the CCRA (Ref. [5]). The CR includes the following major components:
- an executive summary
  - a section identifying the evaluated IT product or PP
  - a description of the IT product or PP security policy
  - assumptions and clarification of scope in relation to the evaluation
  - the architectural information and product documentation listing for an evaluated IT product
  - a description of the testing effort performed during the evaluation
  - a description of the evaluated configuration
  - the results of the evaluation
  - the evaluator and certifier comments and/or recommendations
  - any annexes, including a glossary and/or bibliography if required
  - any 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
  - any extra information specified by any collaborative PP supporting documents, which should either be included in the CR or available and referenced. For example, the network device collaborative PP supporting document specifies extra reporting from the vulnerability analysis as part of the evaluation.

### 4.3.3 Certificate

225. The ACA ensures that the content of the certificate complies with the requirements specified in Annex J of the CCRA (Ref. [5]). The certificate for AISEP evaluations includes the following details:

- certification identification, including:
  - i. scheme or Certification Body (CB) name
  - ii. evaluation criteria used
  - iii. year of issue and number.
- product name
- version and release numbers
- product manufacturer
- type (category) of product.
- for a cPP-based certification, the cPP conformance – including name, version and certification ID – is specified. For EAL type certification, the contents include a conformance of functionality statement (where the SFRs come from), a statement on the assurance package and, if applicable, any PP conformance claims.
- signature of issuing CB
- date issued
- CR identifier:
  - i. CB name
  - ii. evaluation criteria used
  - iii. report number
  - iv. year of issue.
- detailed disclaimer (the small print) copied from Ref. [5] Annex J Section 1 for cPP based certification, or Annex J Section 2 for non-cPP based certification
- marks and logos:
  - i. CC certification mark: globe with C shapes
  - ii. scheme logo
  - iii. recognition arrangement service mark: bold red rectangle and words 'Common Criteria'
  - iv. for EAL based certifications, if the EAL assurance package includes components above CC Part 3 EAL2 (and ALC\_FLR (Flaw Remediation)), then the following text must appear on the certificate: 'CCRA recognition for components up to EAL2 and ALC\_FLR only'.

226. CCRA (Ref [5]) Annex J Section I contains these optional items

- e) evaluation platform
- g) evaluation sponsor
- i) AISEF name
- o) expiry date

which are omitted in an AISEP certificate.

227. After successful maintenance activities, a CC Portal's CPL addendum is created in order to specify details of accepted changes to the certified IT security product. The original certificate remains unchanged.

### 4.3.4 Maintenance report

228. The ACA reports the final results of maintenance activities with an AISEP Maintenance Report.

229. Successful maintenance activities are recorded in the Common Criteria Portal. A Maintenance Report and Maintenance ST are added to the product entry.

230. The contents of the AISEP Maintenance Report include details of accepted changes to the certified IT security product, and satisfy Assurance Continuity CCRA reporting requirements (Ref. [6]) that include the following:

- an introduction or overview, including:
  - i. an IAR identifier
  - ii. the current TOE and ST identifiers
  - iii. the certified TOE, ETR, CR and ST identifiers
  - iv. the vendor identity.
- a description of changes to the certified product:
  - i. changes to the product
  - ii. changes to the development environment.
- any affected vendor evidence:
  - i. a list of affected items associated with the product
  - ii. a list of affected items associated with the development environment.

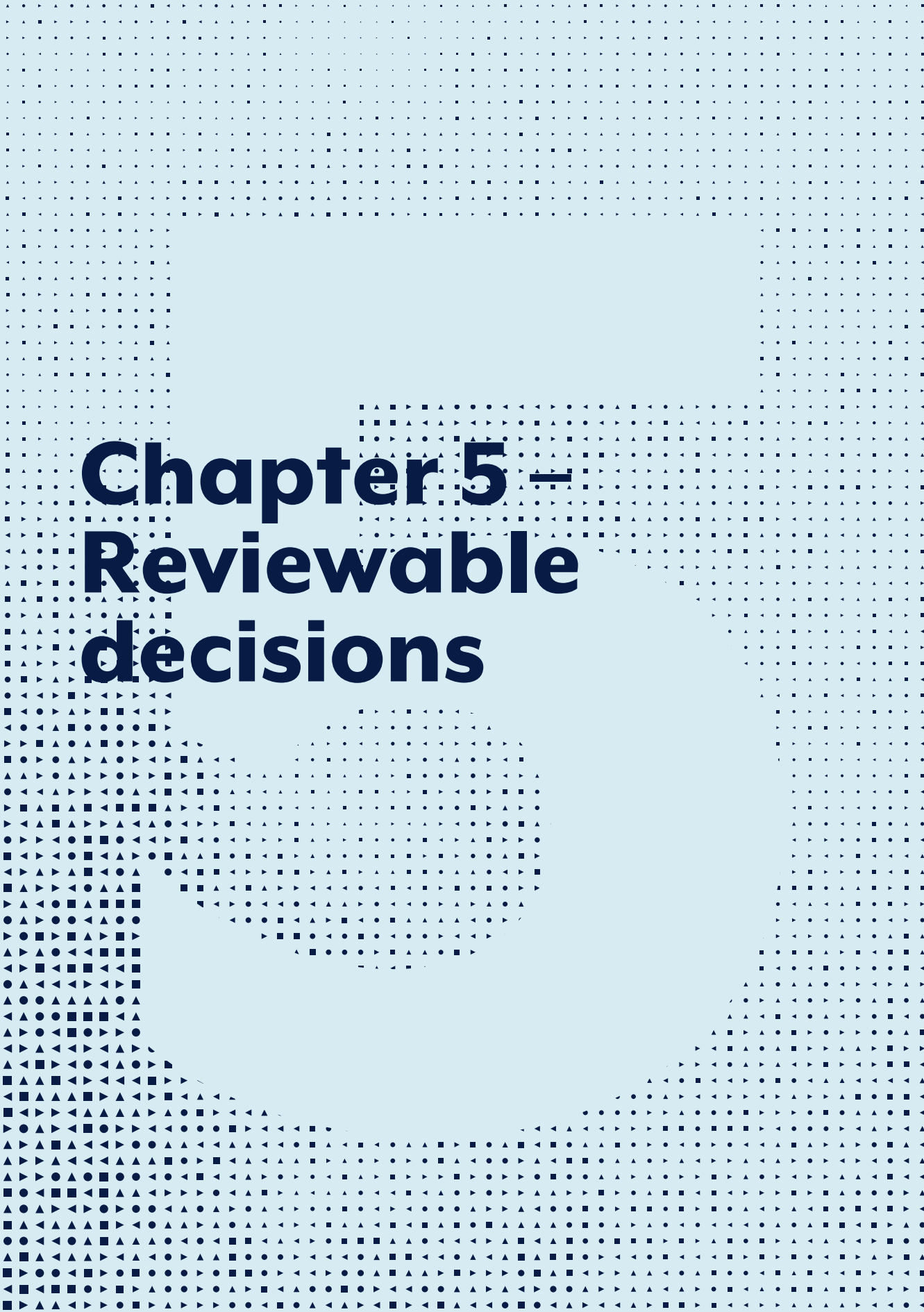
## 4.3.5 Evaluation Technical Report

231. The AISEF must formally report the results of the evaluation task to the ACA for approval in the ETR.
232. The ETR must present all verdicts, justifications and findings derived during the evaluation activity.
233. The ACA ensures that the contents of the ETR comply with requirements specified in the CEM document (Ref. [5]).
234. The AISEF must apply appropriate security markings to share evaluation results with the ACA.
235. 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.
236. The AISEF must include the following information in the ETR for PP and product evaluations:
  - executive summary
  - introduction
  - evaluation results
  - conclusions and recommendations
  - evaluation documentation
  - problem reports and resolutions.
237. For product evaluations, the additional information below is also included:
  - product description (to include an overview, usage and environmental assumptions), threats, organisational security policies and a clarification of scope
  - the evaluation context, including the evaluated configuration, security policy, product architecture and testing efforts. The ETR must identify any use of external test results, identify the testing entity, location and dates of testing along with the external test evidence as applicable
  - Product delivery and installation.

## 4.3.6 Public facing report for cPPs

Additional reporting requirements specified in the cPP supporting document can be included in an annex of the AISEP certification report or in other reports, such as the AAR from the AISEF.





# **Chapter 5 – Reviewable decisions**



238. The purpose of this chapter is to:

- outline the ACA decisions that are reviewable under this policy document
- state those decisions that are not reviewable under this policy document
- outline the process for requesting a decision review.

## 5.1. Decisions

### 5.1.1 Reviewable decisions

239. The following decisions are reviewable:

- 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
- a decision to reject an evaluation task as described in section 3.1.1.3 above
- 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 for an evaluation as described in section 3.1.1.2 above and 3.1.1.3 above
- a decision to withdraw a certificate as described in section 2.2.3.4 above
- a decision to withdraw a certificate due to the discovery of a vulnerability in the product as described in section 4.3.1.

240. A person or organisation whose interests are affected by a reviewable decision may request the ACA to reconsider the decision.

### 5.1.2 Non-reviewable decisions

241. Some decisions described in this document are not reviewable under the review process outlined in this chapter.

242. The decisions that are not reviewable under the process outlined in this chapter are:

- a decision on the impact of changes to a certified product as described in section 3.2.1 above
- a decision not to grant to an applicant an AISEF licence as described in section 2.3.3 above
- a decision to suspend an AISEF's licence as described in section 2.3.5 above
- a decision to terminate an AISEF's licence as described in section 2.3.5 above.

## 5.2. Review process

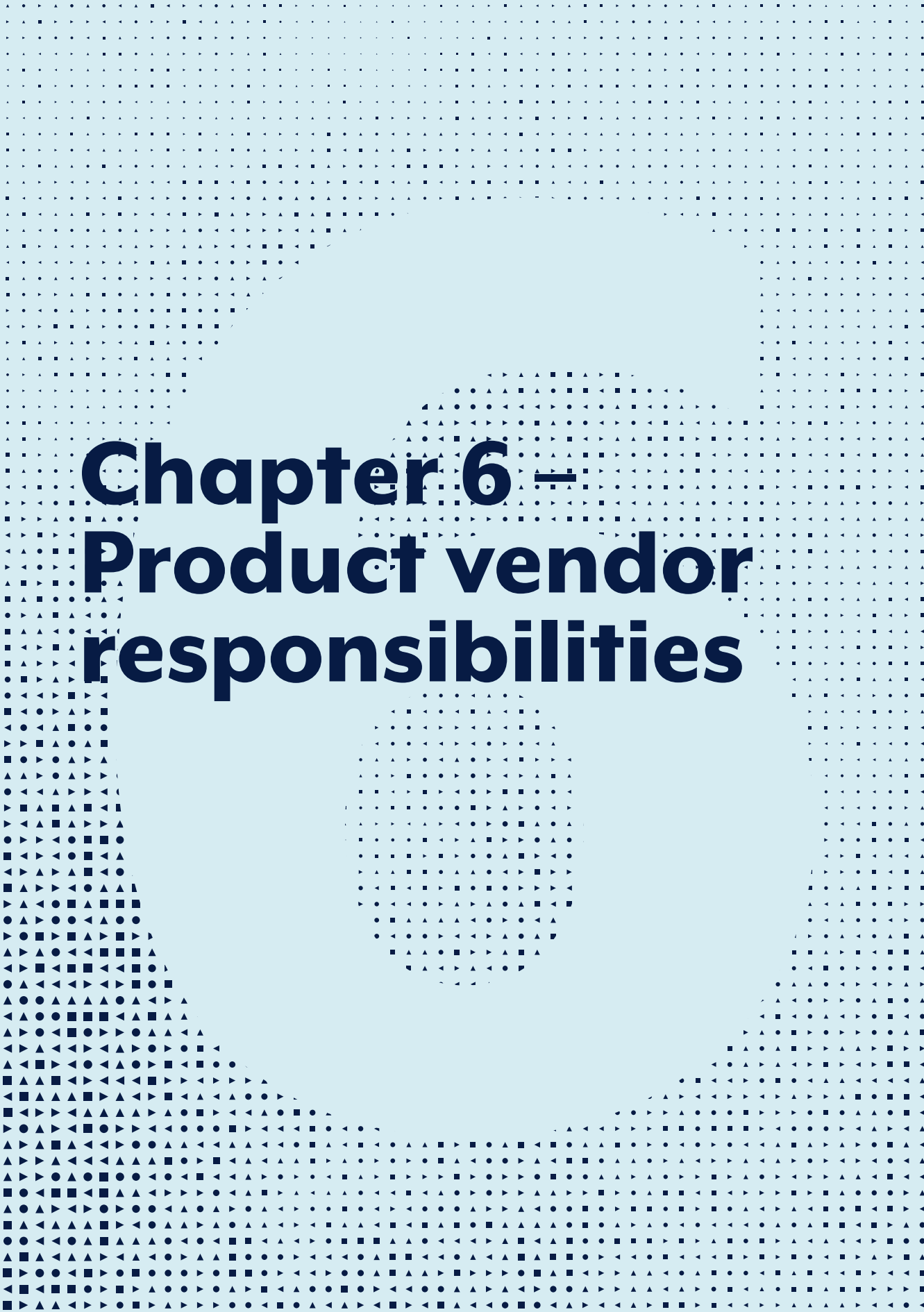
### 5.2.1 Requests for review

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

### 5.2.2 Review outcomes

245. After the ACA has considered the information provided by the complainant, the following may occur:
  - the ACA will uphold the original decision
  - the ACA will change the original decision or
  - the ACA will further investigate the matter.
246. The ACA will endeavour to complete the review within 28 days, and will send the complainant a letter advising of the outcome of the review.
247. a decision will be reviewed once only.





# **Chapter 6 – Product vendor responsibilities**

## 6.1. Common Criteria logo marketing

248. Upon receipt of an ACA issued CC certificate, the product vendor is entitled to use the mark shown at Figure 8: Common Criteria Certification Mark (CCCM). This may be used in conjunction with advertising, marketing and sales of the product for which the certificate is issued.



**Figure 8: Common Criteria Certification Mark**

249. To prevent the misuse of the CCCM, it is registered in Australia with the trade mark office of Intellectual Property (IP) Australia, in classes 9, 16 and 42.
250. 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 8: Common Criteria Certification Mark – until certification is achieved.
251. The product vendor must seek ACA approval prior to publicly releasing material that makes reference to the AISEP, ACA, ACSC or ASD.

## 6.2. Product vendor notification requirements

252. 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 or conduct a new evaluation as part of the product release strategy as described in 3.2 above.
253. The product vendor should notify the ACA when their contact details change to ensure that such information on the AISEP website remains current.
254. 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] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017
- [2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
- [3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, CCMB-2017-04-003, Version 3.1, Revision 5, April 2017
- [4] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, CCMB-2017-04-004, Version 3.1, Revision 5, April 2017
- [5] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, July 2, 2014
- [6] Assurance Continuity: CCRA Requirements [current release]
- [7] ISO/IEC 17025 and Specific Accreditation Criteria – ISO/IEC 17025 Application Document – Manufactured Goods – Annex – Software and information system performance testing [current release]
- [8] The Protective Security Policy Framework (PSPF), Australian Government, Attorney-General's Department [current release]
- [9] Australian Government Information Security Manual (ISM), Australian Signals Directorate, [current release]
- [10] New Zealand Information Security Manual (NZISM), Government Communications Security Bureau, [current release]
- [11] Intelligence Services Act 2001, Commonwealth of Australia
- [12] Archives Act 1983, Commonwealth of Australia, 1983
- [13] AISEP Evaluator Policy, Australian Signals Directorate, Version 5.0, Dated: October 2016
- [14] AISEP Certifier Policy, Australian Signals Directorate, Version 5.0, Dated: October 2016

## A.2. Abbreviations

AAC	AISEP Assurance Continuity
AAR	Assurance Activity Report
ABN	Australian Business Number
ACA	Australian Certification Authority
ACM	AISEF Controllers Meeting
ACN	Australian Company Number
ACT	Australian Capital Territory
ACSC	Australian Cyber Security Centre
AGSCS	Australian Government Security Classification System
AISEF	Australian Information Security Evaluation Facility
AISEP	Australian Information Security Evaluation Program
APM	AISEP Policy Manual
APR	AISEF Progress Report
APS	AISEP Progress Statement
ARI	AISEP Request for Interpretation
ASD	Australian Signals Directorate
ATB	AISEP Technical Board
CAM	Certification Assurance Meeting
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
CPL	Certified Products List
cPP	Collaborative Protection Profile
CR	Certification Report
DGASD	Director-General Australian Signals Directorate
EAL	Evaluation Assurance Level



EPM	Evaluation Progress Meeting
ESC	Evaluation Supporting Consultant
ETR	Evaluation Technical Report
EWP	Evaluation Work Package
HACSC	Head Australian Cyber Security Centre
IAR	Impact Analysis Report
IEC	International Electrotechnical Commission
ISM	Australian Government Information Security Manual
ISO	International Organization for Standardization
IT	Information Technology
ICT	Information Communication Technology
MOU	Memorandum of Understanding
NATA	National Association of Testing Authorities, Australia
NIAP	National Information Assurance Partnership
PCL	Product Compliant List
PMR	Periodic Management Review
PP	Protection Profile
PSPF	Protective Security Policy Framework
ST	Security Target
TCM	Task Closedown Meeting
TOE	Target of Evaluation
TSM	Task Start-up Meeting
VPA	Voluntary Periodic Assessment



# **Annex B** — **AISEF** **applications**

# B.1. Company information

255. The applicant must provide the following details in their application to become an AISEF:

- the organisation's full name
- the organisation's trading or business name
- the organisation's registered office and principal place of business
- the organisation's date and place of incorporation
- the names of individual shareholders who hold 20 per cent or more of issued share capital
- the particulars of foreign nationals or organisations in a position to exercise control or influence over the applicant
- the particulars of related companies within the meaning of section 50 of the Corporations Act 2001
- for a foreign-owned company, the details of registration, incorporation and place of business in Australia, and the name of Australian representatives
- the Australian Company Number (ACN) and, if in Australia, the Australian business number (ABN)
- the 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
- the 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
- the details of an order, contract, joint venture, collaboration or other commitments with another firm or company, and the resources that would derive therefrom that are relevant to the applicant's ability to meet the requirements of being an AISEF
- the 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

256. The Applicant should submit a statement of claims with the following organisation's details:

- the background and structure
- the technical, financial and managerial capacity to provide IT security evaluation services
- a curricula vitae of proposed evaluation staff, covering previous evaluation or testing work
- any staff experience using IT security evaluation related skills, such as experience in the use of formal methods or functional and vulnerability testing
- 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
- any other factors the applicant believes will support its position through demonstrating its ability to perform the role of an AISEF
- the 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 outlined quality plan for the conduct of IT security evaluations
  - v. a plan for supervising and mentoring new evaluators.
- Agree to the conditions of the AISEF licensing agreement and state how the applicant intends to maintain these conditions once the licence has been granted.

## B.3. Resource capabilities

257. Applicants should submit details of the resources the organisation will draw upon, including descriptions of:
- proposed office accommodation
  - proposed physical access control mechanisms
  - management arrangements for coordinating with the Australian Certification Authority (ACA)
  - equipment that will be used to conduct IT security evaluations
  - proposed administrative support to the AISEF
  - proposed travel support for AISEF personnel to attend ACA meetings, if the AISEF personnel are located outside the Australian Capital Territory (ACT)
  - proposed methods for ensuring communication and coordination with the ACA
  - proposed charging regime for IT security evaluations
  - 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
  - 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 of the company and the elements of work to be subcontracted.





