



Information security manual

Guidelines for evaluated products

Last updated: September 2026

Evaluated product procurement

Context

An evaluated product provides a level of assurance in its security functionality that an unevaluated product does not. Evaluation documentation can assist an organisation in assessing the suitability of products and making informed procurement and deployment decisions.

The Australian Certification Authority within the Australian Signals Directorate (ASD) certifies product evaluations conducted by licensed commercial facilities, in accordance with the Common Criteria (i.e. the International Organization for Standardization/International Electrotechnical Commission 15408 series), as part of the Australian Information Security Evaluation Program (AISEP).

In support of Common Criteria evaluations, a Protection Profile (PP) is a technology-specific document that defines the security functionality that must be included in a Common Criteria evaluated product to mitigate specific cyber threats. PPs can support Secure by Design principles and practices by defining security functional and assurance requirements for classes of products against which individual products can be evaluated. PPs can be published by a recognised Common Criteria Recognition Arrangement (CCRA) scheme or by the CCRA body itself. PPs published by the CCRA body are referred to as collaborative PPs. ASD recognises all collaborative PPs listed on the [Common Criteria](#) website, and will consider national PPs listed on the United States' [National Information Assurance Partnership](#) website, in addition to those listed on ASD's [AISEP](#) webpage. Where a PP does not exist, an evaluation based on an Evaluation Assurance Level (EAL) may be accepted. Such evaluations are capped at EAL2+ as this represents the best balance between completion time and meaningful security assurance gains.

In addition, some CCRA schemes leverage the [Cryptographic Algorithm Validation Program](#) for the validation of cryptographic algorithm implementations used by cryptographic modules within evaluated products. In such cases, cryptographic algorithm testing is performed by Cryptographic and Security Testing

laboratories that are accredited by the United States' National Voluntary Laboratory Accreditation Program.

Finally, ASD also performs evaluations for products used to protect SECRET and TOP SECRET data via its High Assurance Evaluation Program.

Evaluated product selection

A Common Criteria evaluation is traditionally conducted at a specified EAL, while evaluations against a PP exist outside of this scale. Although products evaluated against a PP will fulfil the Common Criteria EAL requirements, the EAL number will not be published. In addition, PP modules contain additional requirements that are complementary to or extend upon collaborative PPs. For example, a stateful traffic filtering PP module may apply to a firewall evaluated against a network device collaborative PP. As such, when procuring an evaluated product that has completed a PP-based evaluation, it is important to ensure that all applicable PP modules, as well as a software bill of materials assessment if applicable, were included as part of the product's evaluation.

Furthermore, in choosing evaluated products, an organisation should determine their suitability by reviewing their evaluation documentation. This includes the security target and certification report. Products that are undergoing a Common Criteria evaluation will not have this information publicly available; however, documentation can be obtained from ASD if a product is being evaluated through the AISEP. For a product that is in evaluation through a foreign scheme, the product's vendor can be contacted directly for further information.

The Common Criteria's [Certified Products List](#) contains a list of products that have been evaluated, certified and mutually recognised.

Where a suitable evaluated product is not available for a particular product class or use case, an organisation should consider the associated security risks and determine its security requirements when considering alternative products. Where additional product assurance is required, an organisation may also consider seeking an evaluation of a suitable product.

Finally, the [Information security manual](#) identifies a number of product classes and use cases for which evaluated products are required in certain circumstances. Further information on applicable requirements can be found in the relevant sections. For cryptographic equipment, applications and libraries, an organisation should consider the assurance preferences described in the 'Cryptographic implementation assurance' section of the [Guidelines for cryptography](#) when selecting a suitable product.

Control: ISM-0280; Revision: 9; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A

If procuring an evaluated product, a product that has completed a PP-based evaluation, including against all applicable PP modules (as well as a software bill of materials assessment if applicable), is selected in preference to one that has completed an EAL-based evaluation.

Delivery of evaluated products

It is important that an organisation ensures that products they source are the actual products that are delivered. In the case of evaluated products, if the product delivered differs from an evaluated version, then the assurance gained from the evaluation may not necessarily apply.

Packaging and delivery practices can vary greatly from product to product. For most evaluated products, standard commercial packaging and delivery practices are likely to be sufficient. However, in some cases more secure packaging and delivery practices, including tamper-evident seals and secure transportation,

may be required. In the case of the digital delivery of evaluated products, digital signatures or cryptographic checksums can often be used to ensure the integrity of the product that was delivered.

Control: ISM-0285; Revision: 1; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A

Evaluated products are delivered in a manner consistent with any delivery procedures defined in associated evaluation documentation.

Control: ISM-0286; Revision: 8; Updated: Jun-24; Applicable: S, TS; Essential 8: N/A

When procuring high assurance information technology (IT) equipment, ASD is contacted for any equipment-specific delivery procedures.

Further information

Further information on the [High Assurance Evaluation Program](#) is available from ASD.

Further information on the [AISEP](#) is available from ASD.

Further information on Common Criteria evaluated products can be found on the Common Criteria's [Certified Products List](#).

Further information on cyber supply chain risk management can be found in the 'Cyber supply chain risk management' section of the [Guidelines for procurement and outsourcing](#).

Evaluated product usage

Context

An evaluated product is operating in an evaluated configuration if:

- functionality that it uses was in the scope of the evaluation and it is implemented in the specified manner
- only product updates that have been assessed through maintenance and re-evaluation activities (known as assurance continuity) have been applied
- the environment complies with assumptions or organisational security policies stated in the evaluation documentation.

Conversely, an evaluated product is operating in an unevaluated configuration when it does not meet the requirements of the evaluated configuration and guidance provided in its certification report.

In most cases, the latest patched version of an evaluated product will be more secure than an older unpatched version. While the application of patches will not normally place an evaluated product into an unevaluated configuration, some vendors may include new functionality that has not been evaluated with their patches. In such cases, an organisation should use their judgement to determine whether this deviation from the evaluated configuration constitutes additional security risk or not.

Using evaluated products

Product evaluation provides assurance that a product and its security functionality will operate as expected when used in a clearly defined configuration. The scope of the evaluation specifies how the product is to be installed, configured, administered and operated, as well as the security functionality to be used. Using an

evaluated product in an unevaluated configuration could introduce security risks that were not considered as part of the product's evaluation.

Control: ISM-0289; Revision: 3; Updated: Jun-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A

Evaluated products are installed, configured, administered and operated in an evaluated configuration and in accordance with vendor guidance.

Control: ISM-0290; Revision: 9; Updated: Jun-24; Applicable: S, TS; Essential 8: N/A

High assurance IT equipment is installed, configured, administered and operated in an evaluated configuration and in accordance with ASD guidance.

Further information

Further information on patching or updating IT equipment can be found in the 'System maintenance' section of the [Guidelines for system management](#).

Further information on the installation, configuration, administration and operation of Common Criteria products is available from vendors and can be found in evaluation documentation on the Common Criteria's [Certified Products List](#).

Further information on the installation, configuration, administration and operation of high assurance IT equipment is available from ASD.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

© Commonwealth of Australia 2026

With the exception of the Coat of Arms and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International license (<https://creativecommons.org/licenses/by/4.0/>).

For the avoidance of doubt, this means this license only applies to material as set out in this document.



The details of the relevant license conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 license (<https://creativecommons.org/licenses/by/4.0/legalcode.en>).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (<https://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines>).



Australian Government
Australian Signals Directorate

ASD AUSTRALIAN
SIGNALS
DIRECTORATE
ACSC Australian
Cyber Security
Centre