

***Changes to the EPL***  
***Relevant excerpts from the 29 September 2006 release of***  
***ACSI 33***

## **Evaluated Products List**

---

**Definition:  
Evaluated  
Products List**

3.3.3. The Evaluated Products List (EPL) consists of products that have completed Common Criteria (CC), Information Technology Security Evaluation Criteria (ITSEC) or some other form of DSD approved evaluation, as well as products in evaluation in the AISEP.

The EPL is maintained by DSD and located on the DSD website on the Internet.  
**URL:** [www.dsd.gov.au/infosec/evaluation\\_services/epl/epl.html](http://www.dsd.gov.au/infosec/evaluation_services/epl/epl.html)

---

**Definition:  
AISEP**

3.3.4. The Australasian Information Security Evaluation Program (AISEP) exists to ensure that a range of evaluated ICT products is available to meet the needs of Australian and New Zealand Government agencies.

The AISEP performs the following functions:

- evaluation and certification of ICT products using the Common Criteria (CC) and Information Technology Security Evaluation Criteria (ITSEC),
- continued maintenance of the assurance of evaluated products, and
- recognition of products evaluated by a foreign scheme with which AISEP has an agreement.

**URL:** [www.dsd.gov.au/infosec/evaluation\\_services/aisep\\_pages/aisep.html](http://www.dsd.gov.au/infosec/evaluation_services/aisep_pages/aisep.html)

---

**Evaluation level  
mapping**

3.3.5. The ITSEC and CC assurance levels are similar but not identical in their relationship. The table below shows the relationship between the two evaluation criteria.

This manual refers only to CC assurance levels. The table maps ITSEC levels to CC levels.

<b>Common Criteria</b>	N/A	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
<b>ITSEC</b>	E0	N/A	E1	E2	E3	E4	E5	E6

---

**Benefits of  
selecting an  
EPL product**

3.3.6. Choosing products listed on the EPL provides a level of assurance to agencies that the specified security functionality of the product will operate as claimed by the developer in the Security Target (ST) or similar document.

---

***Changes to the EPL***  
***Relevant excerpts from the 29 September 2006 release of***  
***ACSI 33***

## **Product Selection**

---

**Product  
selection  
standard**

3.3.7. Agencies **SHOULD** select products from the EPL whenever the product is required to enforce a security function related to the protection of official information and systems.

**Important:** Policy stated elsewhere in this manual may override this product selection standard by specifying more rigorous requirements for particular functions.

---

**Selection  
preference  
order**

3.3.8. The following order of preference applies to the selection of products:

- a. products from the EPL listed as having completed CC, ITSEC or other DSD approved evaluation, with a DSD cryptographic evaluation either completed or identified as not required,
- b. products from the EPL listed as having completed CC, ITSEC or other DSD approved evaluation, with a DSD cryptographic evaluation shown as “underway”,

**Note:** Where an evaluation assurance level (EAL) is mandated for an encryption product, products that have not completed a DSD cryptographic evaluation do not satisfy this requirement.

- c. products from the EPL listed as being either in evaluation in the AISEP, or as a certified product on the Common Criteria Portal website,
- d. products that are in evaluation by a foreign scheme with which the AISEP has a recognition agreement, and
- e. products that have had no formally recognised evaluation.

---

**Documenting  
product choice**

3.3.9. When choosing a product, agencies **MUST** document:

- a. the desired degree of assurance in the product’s key functions,
- b. the actual degree of assurance provided by the chosen product, based on the level of evaluation it has received for its key functions,
- c. justification for any decisions to drop to the next level in the defined selection order of preference, and
- d. acknowledgement and acceptance of any risk introduced by the use of a product of lower assurance than desired, particularly if using a product that has not, and may never, complete all relevant evaluation processes.

---

*Continued on next page*

***Changes to the EPL***  
***Relevant excerpts from the 29 September 2006 release of***  
***ACSI 33***

**Product Selection, Continued**

---

**Additional guidance**

- 3.3.10. DSD **RECOMMENDS** that, prior to purchase:
- a. agencies intending to use products that are listed only on the Common Criteria Portal website discuss with DSD the option of sponsoring the product through the DSD compliance process,
  - b. agencies intending to use unevaluated products contact the product vendor to discuss having the product formally evaluated, and incorporate the requirement for successful evaluation into any contracts made with the vendor,
  - c. agencies intending to use a product that the vendor claims is in evaluation in a DSD-recognised foreign scheme contact DSD to confirm this claim, if such evidence is not readily available from the foreign scheme's website.
- 

**Ongoing maintenance**

3.3.11. DSD **RECOMMENDS** that agencies choose EPL products from developers that have made a commitment to the on-going maintenance of the assurance of the product.

**Note:** These products will be indicated as such within the EPL.

---

**Assessing the suitability of EPL products**

- 3.3.12. In assessing an EPL product for its suitability to meet the security objectives of the agency, the agency **SHOULD** review the product's Security Target (ST) and Certification Report (CR) or similar documents, and any caveats contained in the product's entry on the EPL, for the following:
- a. its applicability to the intended environment,
  - b. that the version and configuration of the product matches that of the evaluated product,
  - c. that the required functionality was evaluated and certified,
  - d. that the level of assurance is adequate for its needs, and
  - e. for any constraints or caveats DSD may have placed on the product's implementation and use.

**Note:** Products that are in evaluation will not have a CR and may not have a published ST.

---

**High Grade Equipment**

3.3.13. Agencies intending to use High Grade Equipment (HGE) **SHOULD** contact DSD.

---

*Changes to the EPL*  
*Relevant excerpts from the 29 September 2006 release of*  
*ACSI 33*

## **Acquiring Products**

---

**Purchasing and delivery** 3.3.14. When acquiring products for use in a sensitive environment, it may be important to limit opportunities for the products to be accidentally or maliciously replaced or altered during the purchase and delivery process.

---

**Delivery of EPL products** 3.3.15. Agencies **SHOULD** ensure that EPL products are delivered in a manner consistent with any delivery procedures defined in associated documentation.

**Note:** For ITSEC products, and products evaluated under the CC at EAL2 or higher, delivery information is available from the developer in the delivery procedures document.

---

**Delivery of non-EPL products** 3.3.16. DSD **RECOMMENDS** that agencies ensure that products purchased without the delivery assurances provided through the use of formally evaluated procedures are delivered in a manner that provides confidence that they receive the product they expect to receive.

---

**Leasing arrangements** 3.3.17. Agencies **SHOULD** ensure that leasing agreements for ICT equipment take into consideration the:

- a. difficulties that may be encountered when the equipment requires maintenance,
- b. sanitisation of the equipment prior to its return, and
- c. possible requirement for destruction of the equipment if sanitisation cannot be performed.

---

*Changes to the EPL*  
*Relevant excerpts from the 29 September 2006 release of*  
*ACSI 33*

## Installing and Using Products

---

**Introduction** 3.3.18. This section discusses the installation, configuration, administration and use of ICT products.

---

**Installing and configuring EPL products** 3.3.19. Agencies **SHOULD** ensure that products are installed and configured in a manner consistent with the evaluated configuration of the product.

**Note:** For products evaluated under the CC and ITSEC, this information is available from the developer in the installation, generation and start-up documentation. Further information is also available in the ST and CR.

---

**Use of EPL products in unevaluated configurations**

3.3.20. An EPL product is outside of its evaluated configuration if:

- functionality is used that was not within the scope of the evaluation,
- functionality is used that was within the scope of evaluation but is not implemented in the specified manner,
- patches not covered by a formal assurance continuity process are applied to resolve vulnerabilities, and/or
- the environment does not comply with assumptions and/or Organisational Security Policies stated in the product's ST or similar document.

Products that have a High Grade level of assurance **MUST NOT** be used in unevaluated configurations.

If an agency intends to use an EPL product in an unevaluated configuration the agency **MUST** undertake a risk assessment. To be effective, the risk assessment **MUST**, at a minimum, be based on the following considerations:

- a. the necessity of the functionality or patch,
  - b. the testing of the functionality or patch, and
  - c. the environment in which the product is to be used.
- 

**Operation of EPL products**

3.3.21. Agencies **SHOULD** ensure that products are operated and administered in accordance with the user and administrator guidance. This guidance is generally available from the developer.

Agencies **MUST** ensure that High Grade products are configured, operated and administered in accordance with all DSD standards applicable to the product. These standards are usually contained in a separate, product-specific ACSI.

---

*Changes to the EPL*  
*Relevant excerpts from the 29 September 2006 release of*  
*ACSI 33*

## Cryptographic Requirements

---

**Use of EPL products**

3.9.4. Where this manual expresses a minimum assurance requirement for a cryptographic product as an EAL, agencies **MUST** use an EPL product that has completed a DSD cryptographic evaluation in addition to meeting the stated assurance level.

**See:** ‘Evaluated Products List’ on page 3-xxx.

---

**EPL products, DACAs and DACPs**

3.9.5. Agencies **SHOULD** use an EPL product that has completed a DSD cryptographic evaluation whenever cryptography is being used to protect official information. This applies even when the use of a DACA or DACP is given as the minimum assurance level required to satisfy a “MUST” statement.

**Example:** An agency using an unevaluated product employing SSL to encrypt PROTECTED information travelling over an IN-CONFIDENCE network is complying with the “MUST” statement requiring the use of a DACP for this scenario, avoiding the need for a waiver. However, they are not using an EPL product, and are therefore required to complete the documentation relating to deviations from a “SHOULD” statement.

**See:**

- ‘DSD Approved Cryptographic Algorithms (DACAs)’ on page 3-xxx.
- ‘DSD Approved Cryptographic Protocols (DACPs)’ on page 3-xxx.