12.1. Product Selection and Acquisition

Objective

12.1.1. Products providing security functions for the protection of classified information are formally evaluated in order to provide a degree of assurance over the integrity and performance of the product.

Context

Scope

12.1.2. This section covers information on the selection and acquisition of any product that provide security functionality for the protection of information. It DOES NOT provide information on the selection or acquisition of products that do not provide security functionality or physical security products.

Selecting products without security functions

12.1.3. Agencies selecting products that do not provide a security function or selecting products that will not use their security functions are free to follow their own agency or departmental acquisition guidelines.

Product specific requirements

12.1.4. Where consumer guides exist for evaluated products, agencies should identify and assess any potential conflicts with this manual. Where further advice is required, consult the GCSB.

Convergence

12.1.5. Convergence is the integration of a number of discrete technologies into one product. Converged solutions can include the advantages and disadvantages of each discrete technology.

12.1.6. Most products will exhibit some element of convergence. When products have converged elements, agencies will need to comply with the relevant areas of this manual for the discrete technologies when deploying the converged product.

12.1.7. As an example, when agencies choose to use evaluated media, such as encrypted flash memory media, the requirements for evaluated products, media and cryptographic security apply.

Assurance

12.1.8. In Common Criteria (CC), assurance is the confidence that a Target of Evaluation (TOE) meets the Security Functional Requirements (SFR) of the product.

Determining Assurance

12.1.9. In order to determine the level of assurance (the EAL), the CC standard requires tests, checks and evaluations in several areas. Higher levels of assurance require more extensive design, documentation, testing and evaluation. Determining assurance requires assessment of the following elements:

- Development;
- Guidance documents;
- Life-cycle support;
- Security Target evaluation;
- Tests; and
- Vulnerability assessment.

Augmented Assurance

12.1.10. It is possible to “augment” an evaluation to provide additional assurance without changing the fundamental assurance level. This mechanism allows the addition of assurance components not specifically required for a specific level of evaluation or the substitution of assurance components from

the specification of another hierarchically higher assurance component. Of the assurance constructs defined in the CC, only EALs may be augmented. An augmented EAL is often indicated by a "+"-sign (for example EAL4+). The concept of negative augmentation or an "EAL minus" is not recognised by the standard.

High Assurance

12.1.11. High Assurance is a generic term encompassing EAL levels 5, 6 and 7. ASD run an independent High Assurance Evaluation scheme which is not related to AISEP or an EAL rating.

Evaluated Products List

12.1.12. The Certified Products List (CPL) records products that have been evaluated through one or more of the following schemes:

- Common Criteria;
- high assurance evaluation; or
- an Australian Information Security Evaluation Program (AISEP) approved evaluation.

12.1.13. AISEP certified products can be viewed on the Common Criteria Certified Products List (CPL). IT security products that are currently undergoing an evaluation in the AISEP are listed on the AISEP webpage under the section Products in Evaluation.

Evaluation level mapping

12.1.14. The Information Technology Security Evaluation Criteria (ITSEC) and Common Criteria (CC) assurance levels used in the EPL are similar, but not identical, in their relationship. The table below shows the relationship between the two evaluation criteria.

12.1.15. This manual refers only to Common Criteria Evaluation Assurance Levels (EALs). The table below maps ITSEC evaluation assurance levels to Common Criteria EALs. EAL's are defined in the Common Criteria Standard – part 3.

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

Recognition arrangements

12.1.16. The AISEP programme has a number of recognition arrangements regarding evaluated products. Before choosing a product that has not been evaluated by the AISEP, agencies are encouraged to contact the GCSB to enquire whether the product will be recognised for New Zealand use once it has complete evaluation in a foreign scheme.

12.1.17. Two such recognition arrangements are for the Common Criteria Recognition Arrangement up to the assurance level of EAL2 with the lifecycle flaw remediation augmentation and for degausser products listed on the National Security Agency/Central Security Service's EPLD.

Australian Information Security Evaluation Program (AISEP)

12.1.18. The AISEP exists to ensure that a range of evaluated products are available to meet the needs of Australian and New Zealand Government agencies.

12.1.19. The AISEP performs the following functions:

- evaluation and certification of products using the Common Criteria;
- continued maintenance of the assurance of evaluated products; and
- recognition of products evaluated by a foreign scheme with which the AISEP has a mutual recognition agreement (generally the Common Criteria Recognition Agreement – CCRA).

Protection Profiles

12.1.20. A Protection Profile (PP) describes the security functionality that must be included in a Common Criteria evaluation to meet a range of defined threats. PPs also define the activities to be taken to assess the security functions of a product. Agencies can have confidence that a product evaluated against an AISEP or GCSB approved PP addresses the defined threats. Approved PPs are published on the Certified Products List.

12.1.21. The introduction of PP's is to reduce the time required for evaluation, compared with the traditional approach to allow the AISEP to keep pace with the rapid evolution, production and release of security products and updates. Cryptographic security functionality is included in the scope of evaluation against an approved Protection Profile.

12.1.22. To facilitate the transition to AISEP approved Protection Profiles, a cap of Evaluation Assurance Level (EAL) 2 applies for all traditional AISEP (EAL

based evaluations), including for technologies with no existing approved Protection Profile. EAL 2 is considered to represent a sensible trade-off between completion time and meaningful security assurance gains.

12.1.23. Evaluations conducted in other nations' Common Criteria schemes will continue to be recognised by the GCSB under the AISEP.

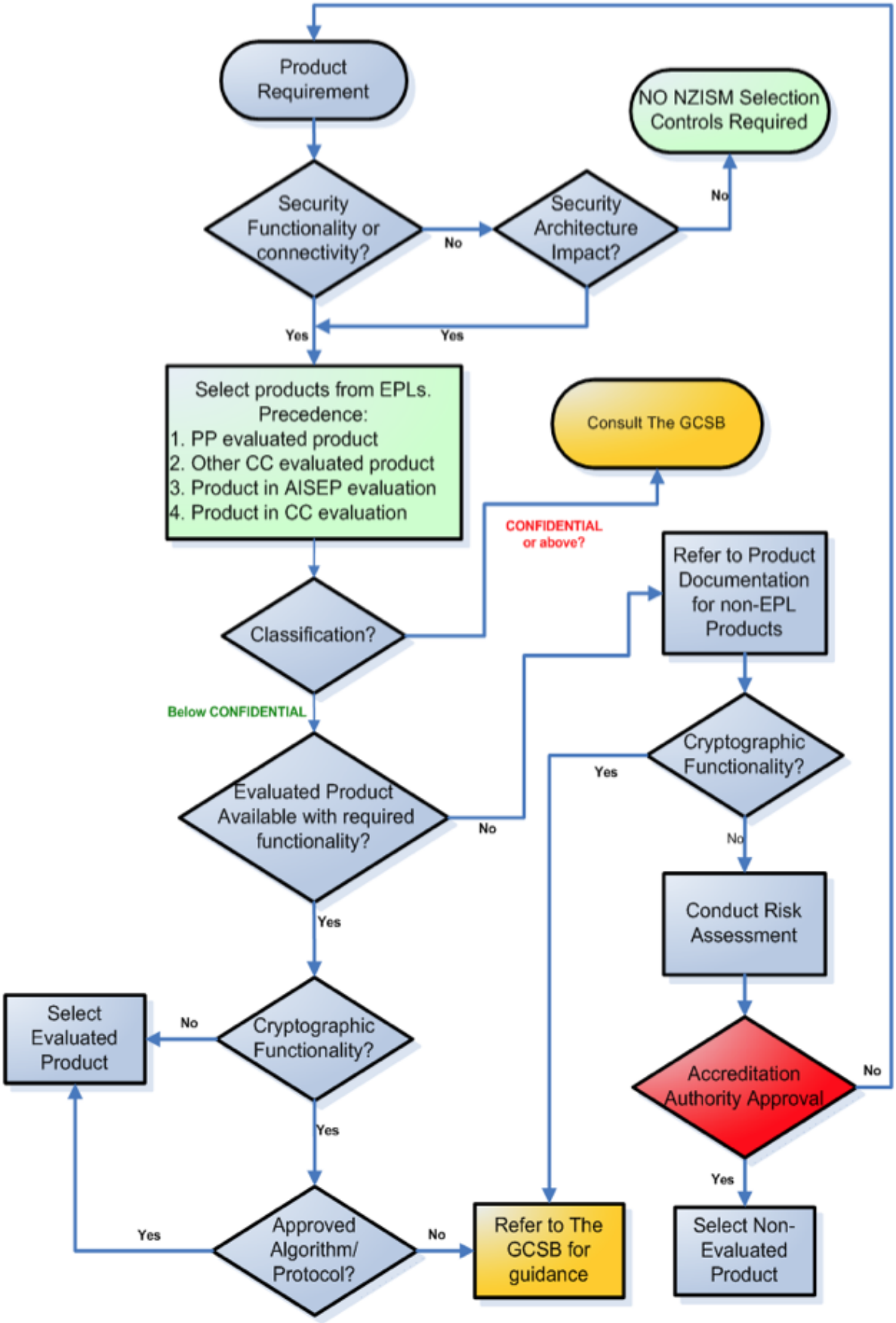
12.1.24. Some High Assurance evaluations continue to be conducted in European Approved Testing Facilities and use the EAL rating scheme. ASD run an independent High Assurance Evaluation scheme which is not related to AISEP or an EAL rating.

12.1.25. It is important that Agencies check the evaluation has examined the security enforcing functions by reviewing the target of evaluation/security target and other testing documentation.

12.1.26. The UK utilises several product evaluation schemes such as the CESG Assisted Products Service (CAPS), CESG Assured Service (CAS) and IT Security Evaluation Criteria (ITSEC). Agencies should consult the GCSB if further clarity on the utilisation of these evaluation schemes and products is required.

Product Selection

12.1.27. The UK utilises several product evaluation schemes such as the CESG Assisted Products Service (CAPS), CESG Assured Service (CAS) and IT Security Evaluation Criteria (ITSEC). Agencies should consult the GCSB if further clarity on the utilisation of these evaluation schemes and products is required.



References

12.1.28.

Reference	Title	Publisher	Source
	AISEP Policy Manual, August 2022	ASD	2022_AUG_REL_AISEP_Policy_Manual_6.3.pdf (cyber.gov.au)
	Australian Information Security Evaluation Program (AISEP)	ASD	https://www.cyber.gov.au/acsc/view-all-content/programs/australasian-information-security-evaluation-program
	Common Criteria	CC	https://www.commoncriteriaportal.org
	Common Criteria Certified Products	CC	https://www.commoncriteriaportal.org/products
	Product & Services Marketplace	NCSC, UK	https://www.ncsc.gov.uk/marketplace
	National Information Assurance Partnership (NIAP)	NIAP	https://ww.niap-ccevs.org
	Government Rules of Sourcing	Ministry of Business Innovation & Employment (MBIE)	Government Procurement Rules - Rules for sustainable and inclusive procurement Government Procurement Rules | New Zealand Government Procurement and Property
	Commonwealth Procurement Rules	Department of Finance and deregulation (Financial Management Group)	Commonwealth Procurement Rules | Department of Finance https://www.finance.gov.au/sites/default/files/2022-06/CPRs 1 July 2022.pdf

PSR references

12.1.29. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV5, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2	Home | Protective Security Requirements Security governance (GOV) | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements/ Physical security (PHYSEC) | Protective Security Requirements

Rationale & Controls

Evaluated product selection preference order

12.1.30.R.01. **Rationale**

In selecting products for use, agencies should note that completed evaluations provide greater assurance than those products that are still undergoing evaluation or have not completed any formal evaluation activity. This assurance gradation is reflected in the preference order for selecting security products. If an agency selects a product that is ranked lower in the preference order, the justification for this decision MUST be recorded.

12.1.30.R.02. **Rationale**

For products that are currently in evaluation, agencies should select those that are undergoing evaluation through AISEP in preference to those being conducted in a recognised foreign scheme. If a major vulnerability is found during the course of an AISEP evaluation, the GCSB may advise agencies on appropriate risk reduction strategies.

12.1.30.R.03.

Rationale

It is important to recognise that a product that is under evaluation has not, and might never, complete all relevant evaluation processes.

12.1.30.R.04. **Rationale**

Agencies should be aware that while this section provides a product selection preference order, policy stated elsewhere in this manual, or product specific advice from the GCSB, could override this standard by specifying more rigorous requirements for particular functions and device use.

12.1.30.R.05. **Rationale**

Additionally, where an EAL rating is mandated for a product to perform a cryptographic function for the protection of data at rest or in transit, as specified within Chapter 17 – Cryptography, products that have not completed an Approved Evaluation do not satisfy the requirement.

12.1.30.C.01. **Control System Classifications(s): Confidential, Top Secret, Secret; Compliance: Must** [CID:3284]

Agencies MUST select products in the following order of preference:

- a protection profile (PP) evaluated product;
- products having completed an evaluation through the AISEP or recognised under the Common Criteria Recognition Arrangement (CCRA);
- products in evaluation in the AISEP;
- products in evaluation in a scheme where the outcome will be recognised by the GCSB when the evaluation is complete; or
- If products do not fall within any of these categories, contact the GCSB.

12.1.30.C.02. **Control System Classifications(s): Top Secret, Secret, Confidential; Compliance: Must** [CID:3286]

When choosing a product, agencies MUST document the justification for any decision to choose a product that is still in evaluation and accept any security risk introduced by the use of such a product.

12.1.30.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3287]

Agencies SHOULD select products in the following order of preference:

- a protection profile (PP) evaluated product;
- products having completed an evaluation through the AISEP or recognised under the Common Criteria Recognition Arrangement (CCRA);
- products in evaluation in the AISEP;
- products in evaluation in a scheme where the outcome will be recognised by the GCSB when the evaluation is complete; or
- If products do not fall within any of these categories, normal selection criteria (such as functionality and security) will apply.

Evaluated product selection

12.1.31.R.01. **Rationale**

A certified product might not meet the security requirements of an agency. This could occur for a number of reasons, including that the scope of the evaluation is inappropriate for the intended use or the operational environment differs from that assumed in the evaluation. As such, an agency should ensure that a product is suitable by reviewing all available documentation. In the case of Common Criteria certified products list, this documentation includes the protection profile, target of evaluation, security target, certification report, consumer guide along with any qualifications and limitations.

12.1.31.R.02. **Rationale**

Products that are in evaluation will not have a certification report and may not have a published security target. A protection profile will, as a rule, exist. A draft security target can be obtained from the GCSB for products that are in evaluation through AISEP. For products that are in evaluation through a foreign scheme, the vendor can be contacted directly for further information.

12.1.31.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3294]

Agencies SHOULD select products that have their desired security functionality within the scope of the product's evaluation and are applicable to the agency's intended environment.

Product specific requirements

12.1.32.R.01. **Rationale**

Whilst this manual may recommend a minimum level of assurance in the evaluation of a product's security functionality not all evaluated products may be found suitable for their intended purpose even if they pass their Common Criteria evaluation. Typically such products will have cryptographic functionality that is not covered in sufficient depth under the Common Criteria. Where products have specific usage requirements, in addition to this manual, or supersede requirements in this manual, they will be outlined in the product's consumer guide.

12.1.32.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3299]

Agencies MUST check consumer guides for products, where available, to determine any product specific requirements.

12.1.32.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3304]

Where product specific requirements exist in a consumer guide, agencies MUST comply with the requirements outlined in the consumer guide.

12.1.32.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3306]

Agencies selecting high assurance products and HACE MUST contact the GCSB and comply with any product specific requirements, before any purchase is made.

Sourcing non-evaluated software

12.1.33.R.01. **Rationale**

Software downloaded from websites on the Internet can contain malicious code or malicious content that is installed along with the legitimate software. Agencies need to confirm the integrity of the software they are installing before deploying it on a system to ensure that no unintended software is installed at the same time.

12.1.33.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3310]

Agencies SHOULD:

- obtain software from verifiable sources and verify its integrity using vendor supplied checksums; and
- validate the software's interaction with the operating systems and network within a test environment prior to use on operational systems.

Delivery of evaluated products

12.1.34.R.01. **Rationale**

It is important that agencies ensure that the selected product is the actual product received. If the product differs from the evaluated version, then NO assurance can be gained from an evaluation being previously performed.

12.1.34.R.02. **Rationale**

For products evaluated under the ITSEC or the Common Criteria scheme at EAL2 or higher, delivery information is available from the developer in the delivery procedures document.

12.1.34.R.03. **Rationale**

For products that do not have evaluated delivery procedures, it is recommended that agencies assess whether the vendor's delivery procedures are sufficient to maintain the integrity of the product.

12.1.34.R.04. **Rationale**

Other factors that the assessment of the delivery procedures for products might consider include:

- the intended environment of the product;
- likely attack vectors;
- the types of attackers that the product will defend against;
- the resources of any potential attackers;
- the likelihood of an attack;
- the level of importance of maintaining confidentiality of the product purchase; and
- the level of importance of ensuring adherence to delivery timeframes.

12.1.34.R.05. **Rationale**

Delivery procedures can vary greatly from product to product. For most products the standard commercial practice for packaging and delivery can be sufficient for agencies requirements. More secure delivery procedures can include measures to detect tampering or masquerading. Some examples of specific security measures include tamper evident seals, cryptographic checksums and signatures, and secure transportation.

12.1.34.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3318]

Agencies procuring high assurance products and HACE MUST contact the GCSB and comply with any product specific delivery procedures.

12.1.34.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3320]

Agencies SHOULD ensure that products are delivered in a manner consistent with any delivery procedures defined in associated documentation.

Delivery of non-evaluated products

12.1.35.R.01. **Rationale**

When a non-evaluated product is purchased agencies should determine if the product has arrived in a state that they were expecting it to and that there are no obvious signs of tampering.

12.1.35.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3325]

Agencies SHOULD 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 that they expect to receive in an unaltered state, including checking:

- any labelling changes;
- any damage; and
- any signs of tampering.

Leasing arrangements

12.1.36.R.01. **Rationale**

Agencies should consider security and policy requirements when entering into a leasing agreement for IT equipment in order to avoid potential information security incidents during maintenance, repairs or disposal processes.

12.1.36.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3330]

Agencies SHOULD ensure that leasing agreements for IT equipment takes into account the:

- difficulties that could be encountered when the equipment needs maintenance;
- control of remote maintenance, software updates and fault diagnosis;
- if the equipment can be easily sanitised prior to its return; and
- the possible requirement for destruction if sanitisation cannot be performed.

Ongoing maintenance of assurance

12.1.37.R.01. **Rationale**

Developers that have demonstrated a commitment to ongoing maintenance or evaluation are more likely to be responsive to ensuring that security patches are independently assessed.

12.1.37.R.02. **Rationale**

A vendor's commitment to assurance continuity can be gauged through the number of evaluations undertaken and whether assurance maintenance has been performed on previous evaluations.

12.1.37.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3337]

Agencies SHOULD choose products from developers that have made a commitment to the ongoing maintenance of the assurance of their product.