High assurance guidance

Introduction to high assurance principles

First published: August 2026

The high assurance principles

Purpose of the high assurance principles

This guidance provides advice for developers seeking to design, develop, and deploy high assurance products. The advice provided is generic and should not be interpreted as a prescriptive pathway for achieving a successful high assurance evaluation. Instead, this guidance defines a generalised set of principles, that can be used to inform the mindset and general approach of design controls and processes.

All developers and their contracted partners should be able to demonstrate an effective mapping between the principles defined in this guidance and the controls implemented in their manufacturing environments. While meeting the principles and controls defined in this guidance provides an essential baseline, more specific and detailed controls will be required based on the product's circumstances. Failure to adhere to these principles indicates a substantial gap in security measures, indicating that the product is far from suitable for environments requiring high assurance.

Developers seeking to build high assurance products should engage with ASD as early as possible to understand the requirements for high assurance development. For a more holistic understanding of the design, development, and deployment lifecycle, readers are encouraged to consult the following complimentary publications:

- *Protective Security Policy Framework* (PSPF)
- *Information Security Manual* (ISM)
- *Secure by Design foundations*

Threat landscape

High assurance developers are valuable targets for sophisticated attackers, as their products protect highly classified and sensitive information. To mitigate this threat, high assurance developers must implement a more comprehensive set of controls and policies to protect products over their entire lifecycle: including product design, development, deployment and destruction. This introduces substantially more time, complexity, and cost than is present in typical commercial design.

High assurance evaluation

Where a product is to be developed for Australian Government agencies to protect classified information, as defined in the Australian Government's PSPF, that product will require a high assurance evaluation; this includes assessment of its development environment.

Under the PSPF, ASD is responsible for all high assurance product evaluations and assessments via the High Assurance Evaluation Program. This program is underpinned by detailed requirements and specifications. While not a complete set of principles, the principles below provide framing on mindset and approach to high assurance.

The High Assurance Evaluation Program requirements and specifications are not available online. Developers seeking to develop high assurance products must contact ASD for further information.

High assurance principles

Design for security

Developers should clearly define and document security functionality. They should have a comprehensive understanding of the limitations of all security functionality and scenarios where protection may not be provided. The security of the product development environment must also be considered. Developers should demonstrate a strong security posture with their design, development and testing environments. Any doubt cast on the security of the information associated with the product, even retrospectively, may render high assurance unachievable.

Design for the full deployment lifecycle

Developers should demonstrate an understanding of how their product will be used throughout its lifecycle. Secure design requires consideration of not just the product but also its interfaces in deployment. Developers should ensure that security functionality remains effective outside of the development environment.

The cybersecurity threat landscape is continuously evolving. Developers must have a clear strategy for maintaining and supporting their products throughout their lifetime that reflects this evolving threat landscape.

Exercise good practices

Developers must clearly provide evidence on how they have applied ASD guidance in their processes and practices. Developer processes should adhere to the latest ASD guidance on maintaining good cyber hygiene.

Perform evidence-based assessment

Developers must be able to demonstrate proper functioning of security-enforcing claims. This includes regular systematic, independent, and evidence-based assessments of the effectiveness of implemented security functionality.

Use a trusted supply chain

Developers must source components, systems, and software used in the design, development, and deployment of a product from trusted suppliers. These suppliers should demonstrate their ability to understand and respond to high-threat environments. Developers should implement appropriate controls throughout the supply chain to ensure the confidentiality, integrity and availability of the product.

Have products operate in a trusted state

A product should be able to verify the integrity of all its hardware components, software, and internal data to maintain an accepted trust state. It should utilise robust protective mechanisms that ensure reliable and trusted operation in the event of errors, failures, or interference.

Enable users to manage risk

Technical defensive measures designed into a product may have limitations, and their effectiveness may degrade over time. Developers should ensure that advice on these limitations, along with associated mitigations and improvements, is readily available and actively advertised to both risk owners and end-users.

Users of the product should have easy access to a range of product support options throughout its lifetime. They should be notified promptly of exploitable vulnerabilities so that they can protect themselves and others, and when a product is updated, they should be advised of the security implications.

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

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