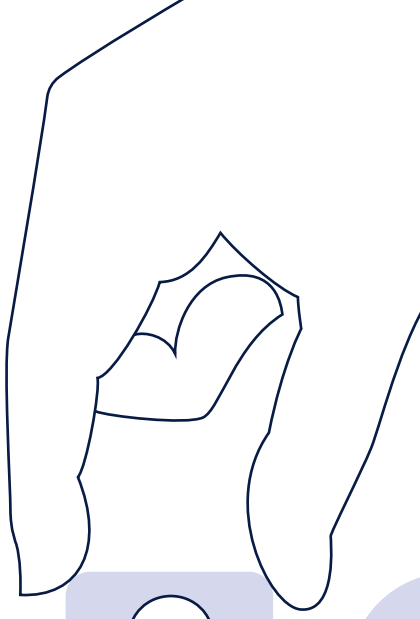
Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre



Secure-by-Design Foundations

Content Complexity
MODERATE ●●○

cyber.gov.au

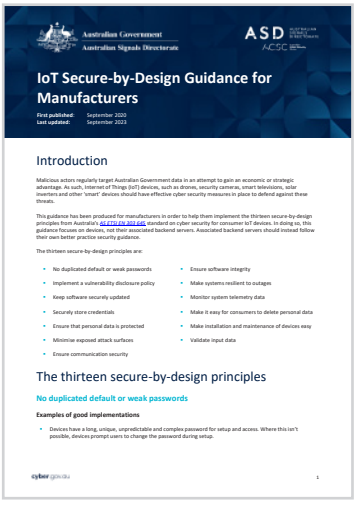
For more cyber security advice

For more information on how to improve your cyber security, see our other guides at cyber.gov.au

Shifting the Balance of Cybersecurity Risk

The Case for Memory Safe Roadmaps

IoT Secure-by-Design Guidance for Manufacturers



Choosing secure and verifiable technologies

Table of contents

Secure-by-Design Foundations

Australia's people, organisations and industries continue to be impacted by the consequences of vulnerabilities in digital products and services. Secure-by-Design offers a proactive and holistic approach to cyber security, aimed at protecting privacy and data. It institutes a security mindset from the outset, building in security throughout the design and development process, and ensuring ongoing vulnerability management through to secure deprecation. As a business practice, Secure-by-Design has relevance for technology manufacturers and technology consumers, and offers a pathway to having *secure* products, not just *security* products.

In short, Secure-by-Design is a security-focused, 'principles and practices' approach taken by technology manufacturers to develop products that are built to be as close to vulnerability-free as possible, and to be secure-by-default; that is, to be used safely 'out of the box'.

What are the Secure-by-Design Foundations:

The Australian Signals Directorate (ASD)'s Australian Cyber Security Centre (ACSC) Secure-by-Design Foundations (the Foundations) assist technology manufacturers and technology consumers to adopt secure-by-design.

Technology consumers should expect and demand products from technology manufacturers that are secure. However, products can become vulnerable if they are not managed securely, or if consumers deviate from secure settings and do not implement alternate or compensating mitigations. It is important for technology consumers to both raise expectations on technology manufacturers and keep the products they are consuming secure. Technology consumers must understand the risks associated with procuring, implementing and operating products, while proactively educating themselves on how to do so securely within their organisational context.

How do the Foundations work?

The Foundations have been designed to promote a common understanding of the responsibilities of technology manufacturers and technology consumers to develop, deploy and sustain secure digital products and services.

Under each Foundation, key risks, focus areas and benefits have been identified separately for technology manufacturers and technology consumers. This approach allows technology manufacturers and technology consumers to better work together, to ensure the products that are being developed and used are safer throughout their entire lifecycle.

The Foundations recognise that every organisation is different, and that the way they approach secure-by-design and their ability to address each Foundation will be unique. There will always be residual risks. Therefore, the goal of the Foundations is to assist organisations to follow a secure-by-design approach appropriate to their organisational context, to reduce their known risks and improve their security posture.

PROACTIVE

HOLISTIC

APPROACH

Key Terms:

The following terms are used throughout the Foundations:

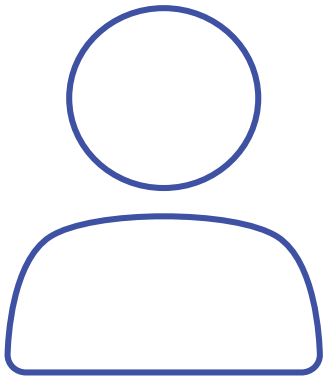
- **Technology Manufacturer:** refers to any organisation, team or individual who develops digital products or services.
- **Technology Consumer:** refers to any organisation, team or individual who is the intended consumer of a technology manufacturer's digital products and services. This can include procurement of a digital product or service, or as an internal customer of a technology manufacturer.
- **Product:** refers to any digital product or service that is developed by a technology manufacturer for technology consumers.

Feedback:

The Foundations are the next step in our drive to champion secure-by-design as a key pillar of cyber resilience. We will continue to provide technical advice and guidance to support the adoption of secure-by-design, as part of a growing international movement.

To ensure our products offer the greatest value, we continually welcome feedback on the Foundations, our current publications and other initiatives that could be developed to promote, enhance and secure products following secure-by-design practices.

Please email enquiries and comments to acsc.sda@asd.gov.au



Foundation 1: Holistic secure organisation

A great team requires all players to work together.

Secure-by-Design is a whole-of-organisation responsibility, requiring action and commitment beyond operational or technical teams. Organisations must align their business drivers and their cyber security goals, ensuring each business area understands their role in building and improving secure-by-design maturity, contributing to the delivery and selection of secure products.

Following secure-by-design practices can significantly improve the cyber security risk profile of technology manufacturers. Technology manufacturers may look to champion secure-by-design through senior stakeholders and cyber security advocates. Secure-by-Design must be seen as an enabler within all organisations. Organisational mentality must shift from viewing security as an inhibitor, to a means to realise productivity and efficiency benefits across the whole organisation. Technology manufacturers must embrace open transparency, while aligning secure-by-design to commercial outcomes to make better informed decisions and build a stronger security culture.

Technology consumers may look to champion secure-by-design through senior stakeholders and cyber security advocates and must demand secure-by-design products from the technology manufacturers they are working with. They must be able to expect baseline security in all the products they consume, while receiving support and transparency from technology manufacturers.

Our advice

To support technology manufacturers and technology consumers, the below advice outlines:

- the key risks associated with not implementing this Foundation
- the key focus areas for achieving this Foundation
- the key benefits associated with realising this Foundation

This Foundation may mitigate or reduce the impact of additional risks that are unique to each organisation.

Technology Manufacturer	Technology Consumer
Key Risks: • Malicious insider • Loss of consumer confidence • Financial and reputational damage • System downtime • Service disruptions • Employee burnout • Incident remediation costs	**Key Risks:** • Malicious insider • Loss of user confidence • Financial and reputational damage • System downtime • Service disruptions • Employee burnout • Incident remediation costs
Key Focus Areas • Senior leadership support • Cyber security risks ownership • Cyber security maturity linked to commercial success • Identify required security resources • Team structure and responsibilities • Capability tracking, reporting, and transparency • Continuous improvement	**Key Focus Areas** • Senior leadership support • Cyber security risks ownership • Business context • Contracts and tenders • Cyber security maturity linked to commercial success • Identify required security resources • Team structure and responsibilities • Continuous improvement • Risk management
Key Benefits • Reputation • Productivity • Improved risk management • Cyber maturity • Economic • Visibility • Awareness • Collaboration	**Key Benefits** • Reputation • Productivity • Improved risk management • Cyber maturity • Economic value • Visibility • Awareness • Collaboration

Foundation 2: Early and sustained security

Early and sustained progress leads to lasting achievements.

Following an early and sustained security-first approach when developing and procuring products is an investment that facilitates both technology manufacturers and technology consumers to be resilient to cyber risks. It requires a whole-of-organisation culture to ensure security risks, threats and mitigations are considered throughout the life cycle of a product.

Technology manufacturers must invest early in security practices to achieve secure, cyber-resilient products. Ensuring security requirements are reflected in the early stages of product development (inception, design and architecture) will assist in avoiding the significant cost associated with reworking inadequate security or vulnerabilities identified later in the product life cycle. This can help eliminate entire classes of vulnerabilities before development even starts, and reduce over costs.

Technology consumers need to identify secure and verifiable products and actively manage them within a security-minded culture during their life cycle.

All organisations must invest in the skills and knowledge of their employees, whilst supporting them through the implementation of technical controls, safety nets and guard rails. Organisations must prioritise a range of security activities that uplift and maintain their security posture.

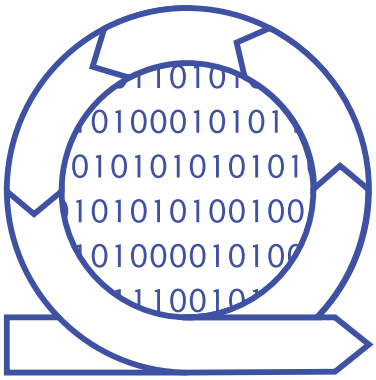
Our advice

To support technology manufacturers and technology consumers, the below advice outlines:

- the key risks associated with not implementing this Foundation
- the key focus areas for achieving this Foundation
- the key benefits associated with realising this Foundation

This Foundation may mitigate or reduce the impact of additional risks that are unique to each organisation.

Technology Manufacturer	Technology Consumer
Key Risks: • Poor vulnerability identification • Insecure code • Costly security additions • Increased attack surface • System design flaws • Emerging threats	**Key Risks:** • Attestations and assurance • Authority to operate • Supply chain compromise • Privilege/access accumulation • Security misconfigurations
Key Focus Areas • Organisational cyber security awareness, culture, and training • Role specific cyber security awareness and training • Security architecture • Product threat modelling • Organisation threat modelling • Customer threat modelling • Security controls and mitigations • System boundaries • Security patterns • Keys and secrets management • Secure hosting environment • Reporting and complete Common Vulnerability Exposurers (CVE) creation • Defence in depth • Privilege and access management	**Key Focus Areas** • Choosing secure and verifiable technologies • Organisational cyber security awareness, culture, and training • Role specific cyber security awareness and training • Security architecture • Security controls and mitigations • System boundaries • Keys and secrets management • Secure operating environment • Configuration management • Privilege and access management • System administration • Baseline configuration
Key Benefits • Quality • Sustainability • Proficiency • Awareness • Preparedness	**Key Benefits** • Verifiable technology • Collaboration • Awareness • Preparedness



Foundation 3. Secure product development

Quality means doing the work that no one sees.

Secure product development starts with quality design and considered architecture, as well as an understanding of the attack surface and threats that a product must be protected against. It is critical to understand the data a product will consume, create and store to know what to protect. This includes understanding data flows, storage locations and classification. Having a clear and comprehensive picture will assist in securing a product and its data in all 3 states: at-rest, in-transit and in-use.

Technology manufacturers must develop their products to be secure-by-default, meaning security features are included without charge, with the most secure settings configured by default, to protect against the most prevalent threats. Products need to make technology consumers aware that if settings deviate from the secure default, the likelihood of compromise may increase. Technology manufacturers must provide guidance on how technology consumers can securely manage their products and maintain a high level of security by implementing additional compensating controls. This will assist technology consumers in maintaining a high level of security throughout the life cycle of a product.

A secure development environment aids in protecting products from unauthorised, vulnerable or malicious changes throughout the development life cycle. By maturing development environments, technology manufacturers can start to automate and shift the responsibility of security assurance away from developers to enhance productivity and security. Technology manufacturers must take steps to protect their unique supply chains, including AI-generated code, open-source code and all transitive dependencies.

Secure-by-Demand encourages technology consumers to demand products that have been designed, built and delivered with fully considered and included security mitigations and features. Technology consumers should seek out technology manufacturers who are open and transparent about how they are implementing and following secure-by-design practices in their product development.

Our advice

To support technology manufacturers and technology consumers, the below advice outlines:

- the key risks associated with not implementing this Foundation
- the key focus areas for achieving this Foundation
- the key benefits associated with realising this Foundation

This Foundation may mitigate or reduce the impact of additional risks that are unique to each organisation.

Technology Manufacturer	Technology Consumer
Key Risks: • Malicious source code • Vulnerable source code • Supply chain compromise • Poor code quality • Security misconfigurations • Unauthorised changes • Consuming vulnerable third-party components	**Key Risks:** • Increased attack surface • Weak or vulnerable products • Supply chain compromise
Key Focus Areas • Secure development environment • Critical and security component review • Developer led security reviews • Secure and defensive coding • Memory safe language use • Code review • Security and audit logging • Data, flows and data boundaries • Cryptography • Third-party component assessment • Software Bill of Materials (SBOM) • Verifiable artefacts • Architectural blueprints • Logging • Authentication and authorisation • Error handing • Source code scanning	**Key Focus Areas** • Secure-by-Demand • Evaluating assertions • Log ingestion • Identity, credential and access management • Privacy impact assessments • Personal identifying information collections and retention requirements
Key Benefits • More secure products • Confidentiality, Integrity, Availability • Development agility • Supply chain resilience	**Key Benefits** • Confidentiality, Integrity, Availability • Trust • Attack surface mitigations • Secure configuration • Configuration warnings • Supply chain resilience

Foundation 4. Testing

Prevention is better than cure.

Secure-by-Design aims for early detection of vulnerabilities and weaknesses through quality assurance and continuous security testing. With automation and repeatable processes, technology manufacturers can reduce the time, effort and resources needed to resolve issues throughout a product's life cycle.

Testing by technology manufacturers must cover both positive and negative use cases and must target critical code, security components and threats identified in the product's threat model. Any identified vulnerabilities must be analysed and be addressed at the root cause. Technology manufacturers must ensure that any analysis is fed back into the development process to ensure mistakes are not repeated.

To improve the chances of finding vulnerabilities and weaknesses early, technology manufacturers could implement the following key testing strategies:

- **In-house**: Testing performed by both the development and dedicated software testing teams.
- **Automated**: Dynamic Application Security Testing (DAST) and Static Application Security Testing (SAST), along with unit and integration tests.
- **External**: Independent code review, manual and automated testing and focused security testing including penetration tests.
- **Field testing**: Simulated real-world testing, focusing on integrations and customer scenarios.

It is important for technology consumers to be able to independently verify the products they may be procuring to make risk-informed choices. Technology manufacturers can consider allowing technology consumers, security researchers and members of the public to test and report on their products using the following strategies:

- **Bug bounties**: Bug bounties incentivise ethical external parties to test for and report vulnerabilities.
- **Client testing**: Allow technology consumers to conduct their own testing; this may include user acceptance and penetration tests.
- **Vulnerability disclosure program**: Allowing public testing and safe harbour for reporting vulnerabilities.

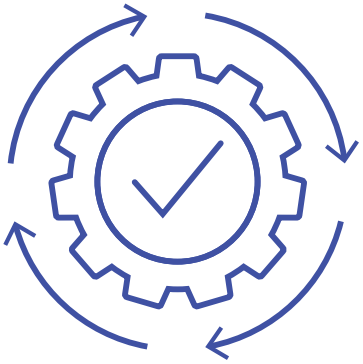
Our advice

To support technology manufacturers and technology consumers, the below advice outlines:

- the key risks associated with not implementing this Foundation
- the key focus areas for achieving this Foundation
- the key benefits associated with realising this Foundation

This Foundation may mitigate or reduce the impact of additional risks that are unique to each organisation.

Technology Manufacturer	Technology Consumer
Key Risks: • Regression defects • Late-stage weaknesses • Poor user experience • Performance issues • Functional defects • Security defects • Compatibility issues.	**Key Risks:** • Evolving threats • Resource constraints
Key Focus Areas • Critical and security component assurance • Repeatable testing • Automated testing • Red teaming • Field testing • Scaling through automation • Vulnerability disclosure	**Key Focus Areas** • Client focussed testing • Consumer threat model testing • Vulnerability reporting
Key Benefits • Early vulnerability identification • Consumer confidence • Industry acceptance • Transparency	**Key Benefits** • Independent assurance • User experience • Transparency



Foundation 5. Continuous assurance

You can't know what you don't know until you know it.

The continued revision of digital products and services is essential to ensuring products stay secure throughout their life cycle. Technology manufacturers and technology consumers must document changes to their environments and threat landscapes to assist in monitoring, incident management, maintenance and assurance.

Technology manufacturers should build automated detection and defence into their products to enable technology consumers to gather quality evidence of intrusion or compromise. Having effective monitoring and incident response will significantly reduce the impact of malicious activity by attempting to block this activity from accessing systems, or before any negative effects are realised.

Products can become vulnerable over time and need to be maintained to ensure they are secure and free from vulnerabilities, increasing a malicious actor's costs and time to exploit. Technology consumers must ensure they are protected from such vulnerabilities by apply defence-in-depth principles. Additionally, technology consumers must apply patches, when available, to the products they are consuming.

Secure-by-Design builds assurance through several initiatives including verifiable builds, attestations against industry frameworks and disclosure. Assurance is supported by a continued commitment to transparency through technology manufacturers reporting how they are enhancing their security by following secure-by-design practices. Assurance is not a one-off, but a continual process that is enacted throughout the product life cycle. Technology consumers should be regularly engaged with technology manufacturers to get assurance on the products they are consuming.

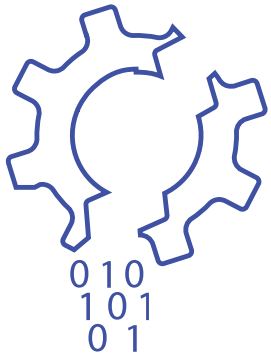
Our advice

To support technology manufacturers and technology consumers, the below advice outlines:

- the key risks associated with not implementing this Foundation
- the key focus areas for achieving this Foundation
- the key benefits associated with realising this Foundation

This Foundation may mitigate or reduce the impact of additional risks that are unique to each organisation.

Technology Manufacturer	Technology Consumer
Key Risks: • Increased time to identify incidents and vulnerabilities • Increased time to recover from compromise • Loss of reputation.	**Key Risks:** • Asset mappings • Threat detection • Configuration drift • Vulnerability detection.
Key Focus Areas • Immutable and secure centralised logging • log and telemetry analytics • Incident response; isolation, recovery, and remediation • Software Bill of Materials (SBOM) monitoring • Situational threat awareness • Review schedules • Patches and updates • Security before backwards compatibility • Change management • Customer support • Continued maturity	**Key Focus Areas** • Application monitoring • Vendor/supplier monitoring • Change management • User support • Immutable and secure centralised logging • Applying patching • Defence in depth • Continuous authority to operate • Continued maturity
Key Benefits • Consumer confidence • Reputation	**Key Benefits** • Notifications and alerting • Threat informed identification • Incident response



Foundation 6. Secure deprecation

Dispose securely or protect indefinitely.

Security does not end when a product or feature is decommissioned, is no longer required or the product becomes legacy. Both technology manufacturers and technology consumers must consider how they will manage products through the end-of-life stage of the product life cycle.

Exploitation of deprecated or legacy systems is common and can be used to perform lateral movement within an information environment; perform data exfiltration; or compromise valid credentials that could be used to access other systems.

To securely deprecate a product, technology manufacturers must provide clear guidance to technology consumers. In the case of Software as a Service (SaaS) or managed service providers, clear communications must be provided to technology consumers about how their implementation will be deprecated, including details on what data will be deleted or retained. All data controlled by a product must be securely archived or securely destroyed; accounts and access must be removed or updated; and, for deprecated systems, the software must be removed completely to prevent living off the land (LotL) attacks.

Our advice

To support technology manufacturers and technology consumers, the below advice outlines:

- the key risks associated with not implementing this Foundation
- the key focus areas for achieving this Foundation
- the key benefits associated with realising this Foundation

This Foundation may mitigate or reduce the impact of additional risks that are unique to each organisation.

Technology Manufacturer	Technology Consumer
Key Risks: • Privilege accumulation • Unsecured credentials • Vulnerable legacy products • Data compromise (confidentiality, integrity, and availability) • Unauthorised access.	**Key Risks:** • Unsecured credentials • Vulnerable legacy products • Data compromise (confidentiality, integrity, and availability) • Unauthorised access.
Key Focus Areas • Secure archiving • Data destruction • Accounts and permissions reviews • System and software removal • Regulatory and legislative requirements • Feature addition and removal • Data geography • Data retention regulations or legislation	**Key Focus Areas** • Secure archiving • Data destruction • Data loss prevention • Right to be forgotten • Transition between technology or products • Data retention regulations or legislation • Accounts and permissions reviews
Key Benefits • Attack surface reduction • Data protection	**Key Benefits** • Attack surface reduction • Data protection

Glossary

Abbreviation	Name
ACSC	Australian Cyber Security Centre
ASD	Australian Signals Directorate
CVE	Common Vulnerabilities Exposures
DAST	Dynamic Application Security Testing
LotL	Living off the land
SaaS	Software as a Service
SAST	Static Application Security Testing
SBOM	Software Bill of Materials

Notes

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 In the Department of the Prime Minister and Cabinet website (www.pmc.gov.au/honours-and-symbols/commonwealth-coat-arms).

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371).

Australian Government

Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre