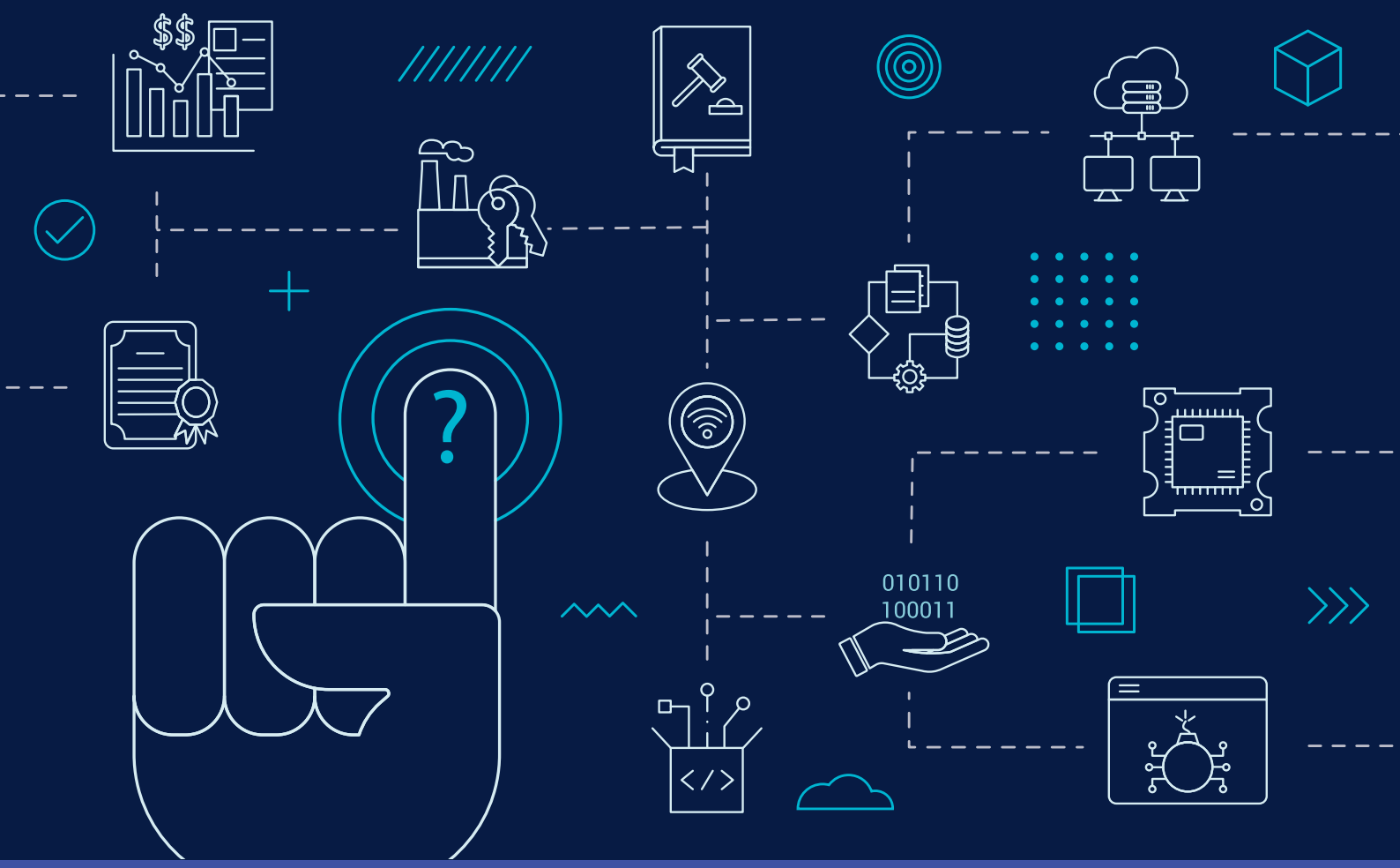
# Secure-by-Design




# Choosing secure and verifiable technologies

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

Communications Security Establishment
**Canadian Centre for Cyber Security**

Centre de la sécurité des télécommunications
**Centre canadien pour la cybersécurité**

National Cyber Security Centre
PART OF THE GCSB

National Cyber Security Centre
a part of GCHQ

**Disclaimer:**
The information herein is being provided "as is" for information purposes only. The authoring agencies do not endorse or favour any commercial entity, product, company or service, including any entities, products, companies or services linked or otherwise referenced within this document.

# Table of contents


**Introduction** ..... **4**

Audience ..... 5

Understanding Secure-by-Design ..... 5

Supporting resources ..... 6

Secure-by-Design Foundations ..... 6

IoT Secure-by-Design Guidance for Manufacturers ..... 6

Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and Default ..... 6

Minimum Viable Secure Product ..... 6

**Section One – External procurement considerations** ..... **7**

Pre-purchase ..... 8

Transparency and reporting ..... 9

Secure-by-Default ..... 12

Security requirements ..... 12

Supply chain risk management ..... 13

Open-source software usage ..... 14

Data sharing and sovereignty ..... 16

Development process ..... 17

Geopolitical risks ..... 18

Regulated industries ..... 19

Manufacturer access ..... 19

Insider threat ..... 21

Open standards ..... 22

Connected systems ..... 23

Product value ..... 24

Post-purchase ..... 26

Risk management ..... 26

Security Incident Event Management and Security Orchestration, Automation and Response ..... 27

Maintenance and support ..... 28

Contracts, licensing, and service level agreements ..... 29

Loosening guides ..... 29

End of life ..... 30

**Section Two – Internal procurement considerations** ..... **31**

Pre-purchase ..... 32

Senior management ..... 32

Policy ..... 32

Infrastructure and security ..... 33

Product owner ..... 33

Purchasing ..... 33

Senior management ..... 33

System administration ..... 33

Infrastructure and security ..... 34

Product owner ..... 34

Post-purchase ..... 34

Senior management ..... 34

System administration ..... 35

Infrastructure and security ..... 35

Product owner ..... 35

**Appendix** ..... **36**

Supporting standards ..... 36

Categories of digital products and services ..... 38

Software ..... 38

Hardware ..... 39

Cloud services ..... 39

# Introduction

With an ever-growing number of cyber threats endangering users' privacy and data, organisations must ensure they are consistently choosing secure and verifiable technologies. Customers have the responsibility for evaluating the suitability, security and risks associated with acquiring and operating a digital product or service. However, it is important that customers increasingly demand manufacturers embrace and provide products and services that are secure-by-design and secure-by-default. In this way, consumers can increase their resilience, reduce their risks, and lower the costs associated with patching and incident response.

When an organisation has determined a need to procure a digital product or service, it must consider whether the product or service is secure and that security will be maintained throughout its specified lifecycle.

**Inadequate or poor security may expose organisations to increased and possibly unmanageable risks, as well as higher operational costs.**

Proactive integration of security considerations into the procurement process can assist in managing and significantly mitigating risks and reducing costs.

While procuring organisations should endeavour to ask as many of the questions recommended in this paper as possible, it may take time for manufacturers to adapt their behaviours and practices to answer all of these questions. Ultimately, procuring organisations must ensure they have gathered sufficient information to make an informed decision.

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) and the following international partners provide the recommendations in this guide as a roadmap for choosing secure and verifiable technologies:

- Canadian Centre for Cyber Security (CCCS) - Canada
- Cybersecurity and Infrastructure Security Agency (CISA) – United States
- National Cyber Security Centre (NCSC-UK) – United Kingdom
- National Cyber Security Centre (NCSC-NZ) – New Zealand

## Audience

This paper is written for:

- **Organisations** who procure and leverage digital products and services. Otherwise referred to as procuring organisations, purchasers, consumers and customers in this paper.
- **Manufacturers** of digital products and services.

Key personnel who should read this guidance include, but are not limited to, organisation executives, senior managers, cyber security personnel, security policy personnel, product development teams, risk advisers and procurement specialists.

This paper is designed to be read by all audiences in its entirety, to:

- Inform **organisations** of secure-by-design considerations for the procurement of digital products and services, resulting in better-informed assessments and decisions.
- Inform **manufacturers** of secure-by-design considerations for digital products and services, resulting in increased development of secure technologies. This paper provides manufacturers with key security questions and expectations they can anticipate from their customers. It is not expected that manufacturers will be able to answer every question in this paper. However, they should nonetheless endeavour to provide as much information as possible and appropriate to assist customers.

This paper is **not a checklist**, and should not be understood to provide absolute or perfect digital procurement outcomes. Rather, it is designed to assist procuring organisations to make informed, risk-based decisions within their own operational context. Every organisation is unique in its structure and approach to procurement, and as such, every item in this paper may not be relevant. Additionally, organisations may need to take other items into consideration that are not covered in this paper, that may be unique to the organisation itself, or industry or region in which it operates.

This document assumes a moderate level of computing and cyber security knowledge on the part of the reader.

## Understanding Secure-by-Design

Secure-by-design is a proactive, security-focused approach taken by software manufacturers during the development of digital products and services that requires the purposeful alignment of cyber security goals across all levels of the manufacturing organisation. Secure-by-design requires that manufacturers consider cyber threats from the outset to enable mitigations through thoughtful design, development, architecture, and security measures. Its core value is to protect user privacy and data through designing, building and delivering digital products and services with fewer vulnerabilities.

Understanding the secure-by-design principles and practices manufacturers should be applying when producing digital products and services will assist procuring organisations to make informed, secure choices.

**By investing in secure products and services, organisations can reduce operating costs over time, enhancing profitability and organisational reputation to build long-term, sustainable corporate value.**

# Supporting resources

## Secure-by-Design Foundations

The ASD's ACSC Secure-by-Design Foundations (the Foundations) have been designed for both technology manufacturers and consumers, to assist in the adoption of secure-by-design. Each Foundation identifies key areas of focus for security uplift and the key risks mitigated.

For more information, please visit Secure-by-Design Foundations | Cyber.gov.au.

## IoT Secure-by-Design Guidance for Manufacturers

The ASD's ACSC *IoT Secure-by-Design Guidance for Manufacturers* has been developed to help manufacturers implement thirteen secure-by-design principles from the AS ETSI EN 303 645 cyber security standard for consumer IoT devices.

For more information, please visit IoT Secure-by-Design Guidance for Manufacturers | Cyber.gov.au.

## Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and Default

The *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and Default* whitepaper is a co-sealed publication led by CISA. The publication focuses on providing technology manufacturers advice and guidance on developing products with both a secure-by-design and secure-by-default strategy. The publication is underpinned by three founding principles aimed at technology manufacturing leaders. Driven by the understanding that software underpins our essential services, the foundations of our economy, and our national security structures, technology manufacturing leaders must:

1. Take ownership of customer security outcomes.
2. Embrace radical transparency and accountability.
3. Lead from the top.

For more information, please visit Shifting the Balance of Cybersecurity Risk | Cyber.gov.au.

## Minimum Viable Secure Product

Minimum Viable Secure Product is a list of essential application security controls that should be implemented in enterprise-ready products and services. The controls are designed to be simple to implement and provide a good foundation for building secure and resilient systems and services.

For more information, please visit Minimum Viable Secure Product | Mvsp.dev.

# Section One – External procurement considerations

## Pre-purchase

- Transparency and reporting
- Secure-by-Default
- Security requirements
- Supply chain risk management
- Open-source software usage
- Data sharing and sovereignty
- Development process
- Geopolitical risks
- Regulated industries
- Manufacturer access
- Insider threat
- Open standards
- Connected systems
- Product value

## Post-purchase

- Risk management
- Security Incident Event Management and Security Orchestration, Automation and Response
- Maintenance and support
- Contracts, licensing, and service level agreements
- Loosening guides
- End of life

# External procurement considerations

The following considerations have been developed to assist organisations who are purchasing products and services to make informed and secure choices. When assessing a manufacturer and their product or service offering, procuring organisations should follow a two-staged approach: pre-purchase and post-purchase. Such an approach assesses the baseline security of a technology and the likelihood of security being maintained throughout the technology's lifecycle.

If at any point during assessment, the risks associated with a chosen product or service exceed an organisation's acceptable risk tolerance, the organisation should develop appropriate mitigations, or consider whether to discontinue the procurement and explore alternative options that pose less risk.

The following considerations do not represent an exhaustive list. Depending on their unique circumstances, organisations may need to account for additional matters not covered in this paper.

Manufacturers can leverage this guidance to ensure they have the necessary information and supporting artefacts to help procuring organisations make informed decisions.

For additional procurement resources, please visit Connected Communities Procurement and Implementation Guidance | Cisa.gov.

## Pre-purchase

Before purchasing a product or service, the purchaser should evaluate both the product itself and the manufacturer. The pre-purchase assessment phase is about completing low-cost checks before committing to a more extensive evaluations process. In the pre-purchase phase, the purchaser should check that the manufacturer is striving to produce secure products and the product being procured is within the purchasing organisation's risk tolerance.

It is important for the purchaser to consider the potential consequences of purchasing a product that is ***not*** secure and verifiable, and which may be outside their organisation's risk tolerance. Key consequences that should be considered include, but are not limited to:

- Costs and revenue: there are increased operating costs associated with incident response and productivity loss when a cyber incident occurs, and increased routine operating costs for managing patching schedules. Not investing in secure and verifiable products and services increases the risk of cyber incidents and requires more regular patching.
- Reputation: customer confidence in an organisation can be damaged if it is not choosing secure and verifiable products and services.
- Long-term profitability: a poor approach to cyber security can increase long-term, systemic risks impacting on profitability as threat vectors increase and more vulnerabilities are exposed.

## Transparency and reporting

Organisations should take steps to verify that the advice they are receiving from manufacturers is open, honest, and transparent.

Manufacturer transparency can take many forms. It may include attestations, industry reports, independent testing, staying abreast of security trends, conducting research, and ensuring uptake of proven security features. Transparency should extend across all incident management efforts, including business continuity and disaster recovery, when a product or service is found to be vulnerable.

Flexibility and a willingness to work within an organisation's procurement requirements and processes is often an indicator of manufacturer transparency.

### Reporting

Manufacturers should be making every effort to notify customers of any vulnerabilities identified in their products and services. Notifications should be accompanied by complete, straightforward guidance on how customers can patch or mitigate identified vulnerabilities. Security patches should be supplied at no charge to the customer. Manufacturers must ensure to fulfil any legislative or regulatory reporting requirements they are subject to.

#### *Common Vulnerabilities and Exposures*

Common Vulnerabilities and Exposures (CVE) is an industry-led program which allows manufacturers, researchers and individuals to report identified vulnerabilities in a product. These vulnerabilities are catalogued and publicly disclosed.

Manufacturers should be publishing complete and timely CVEs for all published products and services as part of their reporting responsibilities.

Full details can be found at Common Vulnerabilities and Exposures | CVE.org.

### Threat modelling

Manufacturers should have a full and detailed threat model for both their organisation and the products and services they are producing. A threat model describes the ways the manufacturer expects a system might be compromised, including any identified weaknesses and the potential objectives of a malicious actor within the system. Threat models should include the security features and measures a manufacturer is implementing to reduce known risk factors.

A threat model developed early in the software development lifecycle assists the manufacturer in understanding where security features and measures should be prioritised. It is also a valuable tool throughout the development process to provide confidence that new weaknesses are not being introduced via changes in the scope or architecture of the software.

A threat model can also assist the procuring organisation in identifying potential areas to improve security resilience.

More information on threat modelling can be found at Threat Modeling Manifesto | Threatmodelingmanifesto.org
and Threat Modeling Cheat Sheet | Owasp.org.

### Reputation

Procuring organisations should take prospective manufacturers' reputation and trust within the industry into consideration when undertaking procurement. Procuring organisations can consider items including time in business, organisation ownership model, geographical locations of operations, industry and customer reviews, and whether the manufacturer is the original product manufacturer or if the technology (or a part thereof) has been bought from a third party. Manufacturers with a history of reputational and trust concerns may pose risks to a procuring organisation. These risks may include poor product quality and support, which in turn may cause damage to the procuring organisation's own reputation as a result of using disreputable products.

### Attestations

Attestations allow manufacturers to convey to consumers and industry that they are following a defined security strategy or standard.

Attestations are generally conveyed in two forms:

1. A self-attestation, completed by the manufacturer itself.
2. An independent attestation, completed by an entity independent of the manufacturer.

Attestations made against defined standards, such as those listed in the supporting standards appendix, are typically conducted to meet a particular level of maturity. Maturity can be assessed as a crawl/walk/run-style set of characteristics, practices or processes that represent the progression of capabilities in a particular discipline. It is a tool used to benchmark current capabilities and identify goals and priorities for improvement. For example, see the Cyber Capability Maturity Model | Energy.gov.

#### *Self-attestations*

Self-attestations allow manufacturers to self-assess and measure their progress toward achieving the development and delivery of secure products and services. Manufacturer self-attestations are best employed as a means for manufacturers to understand their own level of maturity.

Further information can be found at CISA Software Attestation | Cisa.gov, Supplier Declaration of Conformity | ISO.org, and Types of Conformity Assessment | IEC.ch.

#### *Independent attestations*

Independent attestations involve an impartial entity verifying the claims made by a manufacturer in relation to their organisational and product or service security. The outcome of an independent attestation is to provide procuring organisations with an objective, risk-based assessment. Controls and security measures can be assessed to varying levels of depth, from high-level desktop-based assessments through to in-depth implementation, verification, and effectiveness validation. Independent attestations can be made against a recognised industry framework, such as the Information Security Manual | Cyber.gov.au (ISM) or Secure Software Development Framework | Nist.gov (SSDF) or can be completed against the manufacturer's own policies and procedures.

**Questions to consider:**

When evaluating a manufacturer's transparency and reporting, procuring organisations should consider:

- Does the manufacturer publish threat models of the organisation and for its products and services?
- Does the manufacturer have a published vulnerability disclosure process, including public vulnerabilities and security reports?
- Does the manufacturer publish accurate and complete CVEs for identified vulnerabilities?
- Does the manufacturer publish accurate and complete CVEs for identified vulnerabilities?
- Attestation review:
  - Have the manufacturer's organisational security controls been assessed against an industry standard?
    - Which standard/s, and control objectives were followed?
    - Is the standard fit for the type of product or service and its standard use cases?
    - Was the attestation independent (conducted by who?) or self-assessed?
  - Have the product or service security controls been assessed against an industry standard and control objectives? If so, which standard and was the attestation independent or self-assessed?
  - Has the assessment been conducted as a desktop-based assessment, or performed via a thorough assessment of controls implementation, verification, and effectiveness?
  - Has the assessment of the manufacturer and product or service been made against a particular maturity model?
  - What was the date and version of the product or service assessed?
  - Is the product or service periodically re-assessed and at what frequency?
  - If the attestation was self-assessed, would the manufacturer consider a separate independent assessment?
  - Can the manufacturer provide a history of previous attestations?

## Secure-by-Default

Secure-by-default refers to products that are secure 'out of the box' with little to no additional security setup or configuration required upon deployment. It means security measures that protect against the most prevalent threats are built into a product or service 'by default' at no additional cost to the consumer. Examples of secure-by-default features include multifactor authentication, audit capabilities, security logging and default configuration settings set at their most secure values. Manufacturers should make consumers aware of the known risks that may be realised if deviations from the default configurations are made, and the increase in likelihood or impact from a compromise that could occur unless other security mitigations are implemented.

**Questions to consider:**

When validating secure-by-default, examples of questions organisations should consider include:

- Does the manufacturer provide all security features in its base product or is the procuring organisation required to purchase additional security packages?
- Are all default configuration options set to the highest levels of security?
- Does the manufacturer supply a guide detailing the risks associated with changing each configuration option, and possible compensating security measures?
- Has the manufacturer confirmed no default passwords exist in the product?
- Has the manufacturer included multifactor authentication or single sign-on (SSO) in the product?
- Does the product audit all changes to configurations and settings?

## Security requirements

Procuring organisations must establish, document and understand the predetermined security requirements they need in a product or service. This ensures that products or services being procured can be appropriately evaluated against the organisation's needs. Not all security requirements will be organisation-specific. Organisations may be bound by additional requirements under legislation/regulations.

Purchasers should consider security controls that prevent data becoming compromised such as:

- Tokenisation to replace sensitive data.
- Encryption of data (not requiring processing and using an approved encryption method relevant to the purchaser's jurisdiction) and protection of the decryption key.

**Questions to consider:**

When reviewing security requirements, examples of questions organisations should consider include:

- What encryption standards are used for data at rest, in transit and in process?
- What identity credentials and access management (ICAM) solutions and protocols are supported?
- Does the product or service offer SSO with an identity solution?
- Have auditing, security information event management (SIEM), and security orchestration, automation, and response (SOAR) integration rules and support details been provided?
- For Software as a Service (SaaS) solutions, can the data be accessed by a managed service provider (MSP) or cloud service provider (CSP)? If so, how is this controlled and audited?

## Supply chain risk management

Manufacturers will most likely have existing suppliers and supply chains on which they depend. The risks associated with a manufacturer's supply chain are inherited risks to the procuring organisation. Accountability resides with the procuring organisation, throughout the lifecycle of a product, to ensure that the supply chain of the preferred manufacturer aligns with the procuring organisation's expectations for security and availability, and any risks do not exceed acceptable tolerances. Manufacturers should have a supply chain risk management (SCRM) plan in place to assist in managing supply chain risks.

Additional information is available at Guidelines for Procurement and Outsourcing | Cyber.gov.au, Cyber Supply Chain: An Approach to Assessing Risk | Cyber.gc.ca, Supply Chain Security | Ncsc.gov.uk, Protecting your Organization from Software Supply Chain Threats (ITSM.10.071) | Cyber.gc.ca and The Threat from Cyber Supply Chains | Cyber.gc.ca.

### Manufacturer's supply chain

The suppliers in a manufacturer's supply chain can be assessed on their transparency through their policies and whether they offer documents such as software bill of materials (SBOM) and hardware bill of materials (HBOM). These are valuable resources that aid in determining potential supply chain risks as they detail what components and dependencies these suppliers use.

Additional information is available at Cybersecurity Supply Chain Risk Management Practices for Systems and Organisations | Nist.gov.

### Single supplier reliance

Single supplier reliance can be an issue for both procuring organisations and manufacturers. Procuring organisations should consider the level of reliance they have on any single manufacturer when making a purchase and whether the reliance risk can be mitigated. Manufacturers may face similar risks where they are reliant on a single upstream supplier. Organisations should consider both their own single supplier risk, as well as any upstream single supplier risk on the part of the manufacturer from whom they are purchasing.

**Questions to consider:**

When assessing supply chain risk management, examples of questions organisations should consider include:

- Does the manufacturer have a SCRM plan in place? Is the plan periodically reviewed and updated?
- Has the manufacturer implemented additional security controls or mitigations to manage supply chain risks?
- Has the manufacturer completed their supply chain due diligence to ensure their suppliers are following a secure-by-design process?
- Has the manufacturer identified any single supplier reliance risks within their upstream supply chain? If yes, have risk mitigations been put in place?
- Has the manufacturer identified and disclosed potential supply chain risks which may affect consumers?
- Does the product audit all changes to configurations and settings?

## Open-source software usage

Open-source software (OSS) allows software manufacturers to develop software at an increased speed and scale, fostering significant innovation. Software manufacturers must manage risks of OSS as they would for any third-party software. Due to its widespread deployment, security flaws in widely used OSS components can have cascading security effects. Additionally, OSS can be a target of supply chain attacks that seek to compromise upstream open-source dependencies. Manufacturers must own and mitigate risks associated with using OSS.

Manufacturers should exercise due diligence when selecting OSS. For example, manufacturers should avoid OSS components that do not have a community actively monitoring and responding to vulnerabilities.

Manufacturers should be transparent and actively disclose any OSS that is used in their products and services, such as by publishing an SBOM. Procuring organisations should look for manufacturers who maintain an internal secure OSS repository that ensures OSS components (and any dependent components) undergo initial scanning and testing and are continuously checked for updated versions and vulnerabilities. Manufacturers may need to update unsupported OSS components themselves when vulnerabilities are identified or look to replace/remove the vulnerable components.

Additional information is available at Enduring Security Framework | Nsa.gov and Securing the Software Supply Chain: Recommended Practices for Managing Open-Source Software and Software Bill of Materials | Defense.gov.

**Questions to consider:**

When assessing OSS usage, examples of questions organisations should consider include:

- Have all OSS libraries and components been code reviewed, scanned and tested for malicious content?
- Have all OSS components been included in an SBOM?
- Does the SBOM include all possible inherited components?
- Does the SBOM meet a required specification to support automated monitoring?
- Do all OSS libraries and components have an active community supporting continued development? If not, does the manufacturer have an OSS support plan?
- Has the manufacturer committed to supporting any customised or modified open-source components it uses?
- Has the manufacturer committed to supporting the communities of open-source components it uses?
- Does the manufacturer provide evidence on their OSS management, such as policies, procedures, training, approval and rejection?
- Does the manufacturer have a continued monitoring plan for all open-source components used?
- Has the manufacturer risk assessed the OSS component repositories used, including how contributions and contributors are assessed?

## Data sharing and sovereignty

Procuring organisations must have visibility of what organisational and customer data is shared and used by the manufacturer during the procurement process and during use of the product or service. Procuring organisations will need to ensure that data protection security controls pertaining to the manufacturer are sufficient, and meet or exceed the same standard they set for themselves.

Consideration should be given to the geographical location/s where data is captured, processed and stored by the manufacturer. This is particularly so for procuring organisations who are subject industry-specific legislative or regulatory requirements on data sovereignty.

### Cloud computing

Cloud computing services should be assessed to identify the physical location/s where all data is processed and stored, and locations from where data may be accessed, including by remote cloud administrators and support staff. Many CSPs use geographically diverse infrastructure to deliver scalable and reliable services. This means the exact geographical area or region where data is being captured, processed and stored is not always transparent. This may become even less transparent when organisations use SaaS or go through an MSP, as this adds an additional layer of abstraction.

### Backups and storage solutions

When using backup services, such as archival offsite storage or cloud provider storage, organisations need to be assured of the final resting place of their own and customer data. Production/live data being stored and processed in one location does not guarantee the location of archived data, which may be stored in a different, cheaper, or more convenient location.

**Questions to consider:**

When reviewing data sharing and sovereignty, examples of questions organisations should consider include:

- What data will be shared during the procurement process?
- Will the manufacture be collecting data while the purchaser is using the product and service? If so, for what purpose?
- What data protection controls does the manufacturer have in place?
- Has the geographical location of all data, including logs, been specified in the contract or configuration? If so, has this been verified?
- Are all backup copies of data, including logs, held in the region specified in the contract or configuration? If so, has this been verified?

## Development process

If not managed carefully, there are many activities during the development process that may lead to vulnerabilities or introduce malicious content into products and services. Procuring organisations must be vigilant in ensuring manufacturers are providing sufficient evidence of their development procedures and processes. The evidence provided will assists purchasers in assessing risks and verifying that products and services have been built in line with industry security standards.

**Questions to consider:**

When reviewing a manufacturer's development process, examples of questions organisations should consider include:

- Is the manufacturer developing products or services following a secure-by-design methodology or framework?
- Has the manufacturer developed the product or service in a secure development environment? Are they following a defined standard, such as CSA/ANSI T200:22?
- Is the manufacturer providing an attestation against an industry product development standard such as ISM or SSDF?
- What percentage of the product or service has code written in a non-memory safe language? Does the manufacturer have a memory safe roadmap (1-3 years) to reduce or completely remove memory unsafe code?
- Can the manufacturer provide evidence of the testing regime the product has gone through? For example, penetration testing, unit and integration test coverage, and field testing.

## Geopolitical risks

Manufacturers must remain vigilant of geopolitical risks that could impact their products and services. Such risks may include trade disputes, changes to import/export laws and regulations, sanctions and political instability, all of which could affect a manufacturer's supply chain, security and business operation.

Procuring organisations should consider whether a manufacturer actively maintains an awareness of the geopolitical environment and implements mitigation measures against impacting situations, as this provides greater assurance regarding the security and continuity of products and services.

**Questions to consider:**

When evaluating geopolitical risks, examples of questions procuring organisations should consider include:

- Does the manufacturer operate in any capacity, including within its supply chain, in regions of high risk? Note, what is considered 'high risk' will vary according to organisation, industry and country protocols.
- Are there any trade restrictions, tariffs or similar that may affect the cost, availability or security of the product or service?
- Has the manufacturer assessed and developed mitigations for potential geopolitical tension or military conflict impacting their supply chain?
- Does the manufacturer provide advice and assurance on their geopolitical risk management? This may include geopolitical forecasting and long-term stability assessments.

## Regulated industries

Some industries may need to comply with legislative or regulatory requirements. This can be driven by the sensitivity of data stored or transmitted, or if the technology or industry is critical to human safety or national security.

Where applicable, procuring organisations must ensure to validate products and services against relevant legislative and/or regulatory requirements. For example, many organisations in the financial sector handle payment information and must comply with the Payment Card Industry Data Security Standard (PCI DSS). Similarly, healthcare entities must ensure their procurement is compliant with any laws and/or regulations governing the collection and storage of patient health information.

**Questions to consider:**

When evaluating products and services in a regulated industry, examples of questions organisations should consider include:

- Are there legislative, regulatory, or other factors that may impact the manufacturer's import/export of necessary technologies, components etc.?
- Has the manufacturer provided evidence of legislative or regulatory compliance? If so, how recent is the evidence?
- Will adherence with legislative and/or regulatory requirements have significant impacts on functionality or security of the product or service? If so, does the impact on functionality or security create a potential loss of value?

## Manufacturer access

Procuring organisations will need to determine whether the manufacturer of a product or service requires physical or virtual access to the procuring organisation's premises, network or data. The level of access and the associated risks will need to be assessed with consideration given to any required security vetting of the manufacturer's personnel.

**Questions to consider:**

When assessing manufacturer access, examples of questions procuring organisations should consider include:

- Is remote access required?
  - What authentication and authorisation process will be used?
  - Who will be given access?
  - Frequency and time of access?
  - What data and systems will be accessed?
  - How will the access be supervised, do the supervisors have knowledge of the product or service?
  - Is multifactor authentication mandated for 100% of remote access? If not, what are the exceptions?
  - How will access be audited?
- Is physical access required?
  - Who will be given access?
  - Frequency and time of access?
  - What data and systems will be accessed?
  - How will the access be supervised, do the supervisors have knowledge of the product or service?
  - How will access be audited?
- What relevant vetting processes have the manufacturer's personnel undergone?
- What auditing standards and practices are to be followed?
  - Will all actions be audited?
  - Can the procuring organisation conduct its own audits?
- Is any data access retained by the manufacturer?
  - What data is retained?
  - How long is the data retained?
  - How is the data secured?
  - How is the data disposed?
- Will the manufacturer consent to confidentiality and non-disclosure agreements covering all access to systems and data?

## Insider threat

When procuring a product or service, procuring organisations should consider the potential for manufacturer insider threat. In particular, the following types of insider threat have the possibility to cause harm to organisations:

- **Application contributor:** has access to alter the code base or configuration of a product prior to it being released to customers.
- **SaaS application administrator:** has administrative rights to the product and the data it holds.
- **Manufacturer installation and support staff:** may require remote or on-site access to install, configure or troubleshoot a product or service.

Manufacturers can reduce the likelihood of an insider threat through various controls, such as robust hiring practices, monitoring and change control processes.

For more information, please visit Defining Insider Threats | Cisa.gov.

**Questions to consider:**

When reviewing insider threat possibilities, examples of questions organisations should consider include:

- Does the manufacturer have review and change control processes in place?
- Are administration actions for SaaS products immutably logged and audited?
- Do the manufacturer's employees go through a security vetting and training process?
- Can the manufacturer provide evidence of workplace culture and training requirements for their employees?

## Open standards

Open standards are publicly available specifications or protocols that are developed collaboratively and are not owned, controlled, or restricted by any single organisation. They are accessible to the public, and anyone can implement them. Open standards should employ the following characteristics:

- Transparency: openly available, allowing for scrutiny by the public and the cybersecurity community.
- Interoperability: compatibility and interoperability between different products and systems.
- Manufacturer-neutrality: no single manufacturer has exclusive control over standards, reducing the risk of manufacturer lock-in.

Open standards facilitate trust between manufacturers and customers by ensuring products and services are built transparently, can be made interoperable and according to known levels of security.

**Questions to consider:**

When validating open standards, examples of questions organisations should consider include:

- Is the manufacturer using open standards within their product or service?
- Does the product or service provide interoperability with other industry products and services?
- Does use of the product or service restrict integration or have any manufacturer lock-in impacts?
- Is the manufacturer monitoring the open standards they use for disclosed vulnerabilities?

## Connected systems

Modern IT systems are increasingly interconnected, requiring both internally and externally connected systems. Examples of internally connected systems include authentication and log administration. Examples of externally connected (via the internet) functions include transferring or receiving data for actions such as cloud processing. When purchasing a product or service, organisations must consider all systems to which the product or service will be connected. Each layer of interconnectivity increases the product's risk profile and potential attack surface and will require assessment and possible risk mitigations. Managing many interconnected systems can increase an organisation's administrative overheads and add additional risk.

**Questions to consider:**

When evaluating connected systems, examples of questions organisations should consider include:

- Does the manufacturer provide a detailed architecture of all interconnected systems?
- Has the manufacturer completed risk assessments against all possible connected systems?
- Does the product make clear mandatory requirements for connected systems and the security controls in place?

## Product value

Procuring organisations will need to assess the value of a product or service to their unique requirements. While many of the considerations for valuing a product or service are not directly security related, they may have an indirect impact on the security posture of the procuring organisation. Any aspect of a product or service which adds complexity, adds to the risks faced by a procuring organisation. If a manufacturer can mitigate or reduce these risks, then a product or service will have greater value to the procuring organisation.

There are multiple criteria which can be used to assist organisations in determining the value of the product to their organisation, these criteria can include:

- The purchasing costs of the product or service, and/or ongoing licence fees.
- Anticipated lifetime of the product or service.
- The administration costs of running the product or service.
- Complexity of integration into the environment.
- The value of the efficiency gains, productivity or functionality made to the organisation with the purchasing and implementation of the product or service.
- The value of the assets (data) managed by the product or service.

### Contracts, Licensing, and Service Level Agreements

When assessing a product or service contract, licensing, and service level agreements (SLAs), the purchaser must consider both the contractual obligations and associated security risks that may impact the organisation and their customers. In particular, the purchaser should consider the potential impact if an obligation cannot be fulfilled by the manufacturer or if an element was to fail or not be upheld post purchase.

Considerations:

- Limits of liability.
- Confidentiality requirements for data and information.
- Right to request an audit.
- SLAs and rectification or compensation.
- Contractor financial reporting.
- Preventing data loss.
- Contractor insurance.
- Contractor business continuity/ disaster recovery plans.
- Backup guarantees.
- Warranties.
- Breach notification.
- Vulnerability Disclosure Program | Cyber.gov.au (commitment to complete and timely CVEs).
- Requirements on contract negotiation.
- Privacy.
- Security functional requirements.
- Security strength requirements.
- Security-related documentation.
- Security assurance and attestations, including penetration testing, risk assessments, etc.
- Goods/services acceptance criteria.
- Governance oversight and leadership involvement.
- Termination capability and data removal.
- Maintenance, support and reporting obligations.

### Asset protection

Consideration should be given to the data that the product or service will collect, process and store. Data must be assessed based on its value to both the procuring organisation and its customers, as well as the classification or sensitivity of that data. These factors will determine the value and the associated risk the product brings to an organisation, and can be used to determine the mitigations and controls needed to manage risk to an acceptable level. Products that have been identified as built following secure-by-design methodologies will bring less risk to the purchaser.

**Questions to consider:**

When evaluating product or service value, examples of questions procuring organisations should consider include:

- What is the classification or sensitivity of data that the product or service will handle?
- Will the product or service handle customer or user data?
    - Will this include sensitive data, such as personally identifiable information?
- Are the product or service inbuilt security controls adequate for the classification or sensitivity of the data being handled?
- Is the manufacturer able to provide a data model of all data and metadata handled by the product or service?
- Does the cost of the product or service present good value for the data being handled?
- Will the manufacturer commit to the anticipated lifetime need for the product or service?
- Does the product or service require significant administration or management?
- What is the complexity of integration into the procuring organisation's information environment?

# Post-purchase

Following the purchase of a product or service, the procuring organisation needs to ensure that their purchase continues to provide the same level of security as originally assessed.

## Risk management

Procuring organisations must ensure that the manufacturer is conducting ongoing risk management of its products and services, as well as its organisational security posture. A product or manufacturer may not have been compromised during initial purchase, but that does not mean they will not become a target in the future. Procuring organisations need to ensure manufacturers are continuously assessing the security of their products and are providing timely updates if issues are identified. Manufacturers should provide ongoing assurance to customers that they are maintaining their security posture.

**Questions to consider:**

When evaluating risk management, examples of questions organisations should consider include:

- Does the manufacturer provide evidence of its risk management strategies?
- Does the information provided by the manufacturer support continuous improvement and risk mitigation?
- Are manufacturer reports and attestations re-evaluated at defined periods? Are these being provided?
- Does the manufacturer have a history of continual maintenance and support for its existing products and services?

## Security Incident Event Management and Security Orchestration, Automation and Response

The integration of SIEM and SOAR solutions is important to enable detection and rectification of malicious activities. Both SIEM and SOAR products need detailed logs from an application. It is recommended that manufacturers work with SIEM and SOAR providers to validate that their products are logging sufficient information. Manufacturers and procuring organisations will have different responsibilities depending on whether the product or service is purchaser-hosted or manufacturer-hosted.

### Purchaser-hosted

In the purchaser-hosted model, the procuring organisation will be responsible for SIEM and SOAR management. In this model, the manufacturer should provide a list of all events that can be raised by the product, including metadata, such as severity, reason code and a correlation identifier. This will enable the procuring organisation to integrate the product effectively into their own SIEM and SOAR systems.

### Manufacturer-hosted

The manufacturer-hosted model generally consists of SaaS products or services that a procuring organisation is consuming, or their own customers may be accessing. In this model, the manufacturer is responsible for managing SIEM and SOAR handling for all incidents and events raised. The manufacturer should be providing an SLA, which outlines the types of events that are tracked and how they will respond and allow for independent or consumer audits.

**Questions to consider:**

When evaluating SIEM and SOAR, examples of questions organisations should consider include:

- Have SIEM and SOAR rules been defined for the model being employed, either purchaser-hosted or manufacturer-hosted?
- Are the defined rules periodically reviewed for effectiveness?

## Maintenance and support

Procuring organisations must ensure that manufacturers are adhering to maintenance and support commitments made during the pre-purchase phase of procurement. The security posture of products and services will change throughout their lifecycle as malicious actors discover new vulnerabilities and new exploitation tactics, techniques and procedures (TTPs). Manufacturers should support consumers by providing monitoring and maintenance schedules with relevant policies, procedures, supply chains and vulnerability disclosure programs. More information is available at Vulnerability Disclosure Programs Explained | Cyber.gov.au.

### Supply chain monitoring

Procuring organisations will need to monitor as much of the upstream supply chain as possible. In this regard, manufacturers should be supplying documentation on their upstream monitoring capabilities to downstream consumers, including public reporting and notifications on events.

### Change management

A robust change management strategy is comprised of multiple strategies that provide ongoing security and business continuity to products and services. Change management will assist in both ensuring that insider threats are less likely, and will help reduce other vulnerabilities from being introduced into a product, by ensuring that all changes are reviewed. Manufacturers should provide details of the change management policies and procedures to potential customers as part of their secure-by-design disclosure.

### Incident management

Manufacturers should provide their incident management policies and procedures. These policies and procedures should be made available as part of the SLAs agreed to between the manufacturer and the purchaser.

**Questions to consider:**

When validating maintenance and support, examples of questions organisations should consider include:

- Does the manufacturer have vulnerability monitoring and reporting in place for both their product and their supply chain?
- Does the manufacturer have notification/reporting policy and procedures in place? If so, are the specified timeframes suitable?
- Is vulnerability reporting included in the licence or SLA?
- Does the manufacturer provide timely support to maintenance requests?
- Does the manufacturer have policies and procedures in place to respond to identified vulnerabilities, such as a vulnerability disclosure program? If so, are the responses and timeframes suitable?
- Does the manufacturer provide a product roadmap of planned patching and enhancements?

## Contracts, licensing, and service level agreements

Procuring organisations must ensure that manufacturers are maintaining adherence to all commitments made in the procurement contract, licensing, and SLAs. Specific attention to adherence to security and data assurances is recommended.

**Questions to consider:**

When validating contracts, licensing and SLAs, examples of questions organisations should consider include:

- Have contracts, licensing or SLAs been changed or updated?
- Is the manufacturer adhering to the agreed contracts, licensing and SLAs?

## Loosening guides

Loosening guides detail the configuration settings users can change within a product. Loosening guides should provide sufficient detail such that users can make an informed, risk-based decision when changing settings.

Guides should highlight the risks the product or service and/or user are exposed to for each change and offer suggestions on possible mitigations. Where possible, products should alert or prompt users and administrators periodically or during certain actions that the current configuration is less than optimal.

**Questions to consider:**

When validating loosening guides, examples of questions organisations should consider include:

- Is a loosening guide provided with the purchased product?
- Is the product secure-by-default or will the product require additional configuration to make it secure?
- Are all configuration options detailed, including the level of security they provide?
- Does the manufacturer provide a list of recommended mitigations for when a configuration is altered from its default to ensure a minimum level of security is maintained?

## End of life

When a product is no longer in use by a customer, either through the product reaching end of life or the customer has decided to no longer continue with the product, the manufacturer must have appropriate off-boarding procedures in place. The manufacturer must make the customer aware of the data they are still in possession of and if they will be deleting or storing that data. The manufacturer should provide detailed guidance for securely removing the product and guidance for data handling and removal if necessary.

### Information disposal or secure storage

When a product or service reaches its end of life, the purchaser must be conscious of the data they have shared with the manufacturer. This data may include company, end user or customer information. If possible, the purchaser should consider asking the manufacturer to securely dispose of all non-essential data. The power to instruct the manufacturer to delete data should be included in the original contract or licence.

### SaaS data destruction

SaaS products present many additional risks to procuring organisations when trying to decommission a product. Without clear visibility of all data that has been collected or created as part of using the SaaS product, it may be impossible to verify that all data has been securely deleted. Ensuring robust clauses in the contract or licence can help give assurances to the procuring organisation.

**Questions to consider:**

When validating end of life, examples of questions organisations should consider include:

- Does the manufacturer disclose the end of life and end of support for the product or service?
  Is there a policy in place to notify the consumer prior to end of life?
- Does the manufacturer have data disposal policies and procedures?
- Does the manufacturer provide data destruction certificates?

# Section Two – Internal procurement considerations

## Pre-purchase

- Senior management
- Policy
- Infrastructure and security
- Product owner

## Post-purchase

- Senior management
- System administration
- Infrastructure and security
- Product owner

## Purchasing

- Senior management
- System administration
- Infrastructure and security
- Product owner

# Internal procurement considerations

When considering procurement of product or service, in addition to assessing the manufacturer, the purchasing organisation should assess itself. This assessment can be conducted across three stages: pre-purchase, purchase and post-purchase.

If at any point during assessment, the risks associated with a chosen product or service exceed an organisation's acceptable risk tolerance, the organisation should develop appropriate mitigations, or consider whether to discontinue the procurement and explore alternative options that pose less risk.

The following considerations do not represent an exhaustive list. Depending on their unique circumstances, organisations may need to account for additional matters not covered in this paper.

## Pre-purchase

During the pre-purchase phase of self-assessment, the purchaser should be consulting with the following areas of their organisation: senior management, policy, infrastructure and security, and the product owner. Each of these areas will have specific requirements and insights that will ultimately determine if the product or service is suitable and of low enough risk for the organisation to purchase.

### Senior management

The following questions should be asked of senior management during the pre-purchase phase:

- Has an organisational risk threshold been established?
- Has senior management been provided with a risk assessment and accepted the risks associated with the proposed procurement?
- Has senior management approved the adding of the product or service to the organisation's incident response plan?

### Policy

The following questions should be asked of the policy area during the pre-purchase phase:

- Does the proposed purchase conflict with any existing policies?
- Does the level of risk exceed the accepted thresholds for the organisation?
- Does the product or service meet logging and auditing requirements (legislative or regulatory)?
- Does the organisation have a plan in place for conducting periodic re-assessment?

## Infrastructure and security

The following questions should be asked of the infrastructure and security areas during the pre-purchase phase:

- What are the current security control catalogues or frameworks that the organisation is willing to accept?
- Has a security impact assessment been completed?
- Has a threat model been completed, relevant threats and risks identified, and the risks managed to an acceptable level?
- Is the product or service compatible with the organisation's infrastructure?

## Product owner

The following questions should be asked of the internal product owner during the pre-purchase phase:

- Does the product meet business needs without exceeding risk tolerance?
- What risk level or security classification level does the purchase need to meet?
- What privacy implications does the purchase introduce?
- Does the proposed contract cover a level of risk and risk mitigation suitable to the organisation?
- Has a risk mitigation plan been established?

Note: If the organisation does not have an assigned business owner for products or services, it is recommended that a business owner be appointed for the product or service to work with the IT team and across their organisation.

# Purchasing

During the purchasing phase of self-assessment, the purchaser should be consulting with the following areas of their organisation: senior management, system administration, infrastructure and security, and the product owner. Each of these areas will have specific requirements and insights that need to be addressed before the final product is chosen and implemented.

## Senior management

The following questions should be asked of senior management during the purchasing phase:

- Have all residual risks been accepted?
- Has the final contract been signed and accepted?

## System administration

The following questions should be asked of the system administration area during the purchasing phase:

- Have all logging and auditing outputs been verified?
- Have all ICAM requirements been identified, assessed and implemented?
- Have all role-based access controls (RBAC) and attribute-based access controls (ABAC) requirements been documented and verified if applicable?
- Has the delivered product or service been scanned for potential compromises?

## Infrastructure and security

The following questions should be asked of the infrastructure and security areas during the purchasing phase:

- Have infrastructure security controls have been implemented, e.g., service accounts with least privilege, isolated networks with only the required resources?
- Are monitoring systems in place? Are they pre-tuned or in learning mode, or has post-tuning been arranged?
- Are third parties being used for operations? If so, what assurance can they provide?

## Product owner

The following questions should be asked of the product owner during the purchasing phase:

- Has the delivered product and version been verified (digital signature)?
- Does the final contract meet the organisation's security requirements?
- Has all assessment and security documentation been provided and verified?
- Is secure default configuration being followed? Have risks and associated explanations been assessed and documented for each deviation?

# Post-purchase

During the post-purchase phase of self-assessment, the purchaser should be consulting with the following areas of their organisation: senior management, system administration, infrastructure and security, and the product owner. Each of these areas will have specific requirements and insights that will need to be addressed during the ongoing administration and management of a product.

## Senior management

The following questions should be asked of senior management during the post-purchase phase:

- Has continuous or periodic acceptance and review of product risks been established?
- Have system security plans and business continuity plans been accepted?
- Have legacy technology risks been added to and managed on an organisation risk register?

## System administration

The following questions should be asked of the system administration area during the post-purchase phase:

- Is monitoring and notification in place for patches, CVEs, and product updates for the full supply chain?
- Has product monitoring been provisioned within a SIEM?
- Does the organisation have SOAR capabilities for the product? Have they been provisioned?
- Are procedures set up for data management, e.g., disposal, editing, and back-up?
- Has the new product or service been written into the organisation's incident response plan, has an incident response plan been established specifically for the product or service?

## Infrastructure and security

The following questions should be asked of the infrastructure and security areas during the post-purchase phase:

- Are authorisations and privilege accounts being periodically reviewed?
- Are the manufacturer's security attestations being periodically reviewed for updates?
- Does the technology used by the product or service have a roadmap or legacy support plan,
  and has this been identified in the organisation legacy support plan?

## Product owner

The following questions should be asked of the product owner during the post purchase phase:

- Is the manufacturer still adhering to claims made during purchase?
- Are periodic contract reviews in place?
- Are changes to the product being risk assessed, e.g., configuration updates, and user access?
- Has a business continuity plan been developed?
- Has a system security plan been developed?
- Are regulatory and legislative requirements being periodically reviewed?
- Does the product or service have a legacy technology roadmap or plan?

# Appendix

## Supporting standards

The following standards can be used by manufacturers to assist in the development of secure and verifiable technologies. Manufacturers following one or more of these standards should be able to provide evidence to procuring organisations to support product or service claims.

1. **ASD ACSC Information Security Manual (ISM)**
   The purpose of the ISM is to outline a cyber security framework that an organisation can apply, using their risk management framework, to protect their systems and data from cyber threats. ISM | Cyber.gov.au.

2. **ASD ACSC Infosec Registered Assessors Program (IRAP)**
   IRAP endorses individuals from the private and public sectors to provide security assessment services. Endorsed IRAP assessors assist in securing your systems and data by independently assessing your cyber security posture, identifying security risks, and suggesting mitigation measures. IRAP | Cyber.gov.au.

3. **ISO/IEC 20243-1:2018 Open Trusted Technology Provider Standard (O-TTPS)**
   ISO/IEC 20243-1:2018 O-TTPS is a set of guidelines, requirements and recommendations that address specific threats to the integrity of commercial off-the-shelf (COTS) hardware and software products throughout the product lifecycle. ISO/IEC 20243-1 | Iso.org.

4. **NIST Special Publication (SP) 800-218.**
   The Secure Software Development Framework (SSDF) is a set of fundamental, sound and secure software development practices based on established secure software development practice documents from various organisations. SSDF | Nist.gov.

5. **Open Web Application Security Project (OWASP) - Application Security Verification Standard (ASVS)**
   The OWASP ASVS provides a basis for testing web application technical security controls and provides developers with a list of requirements for secure development. ASVS | Owasp.org.

6. **Open Web Application Security Project (OWASP) - Comprehensive, Lightweight Application Security Process (CLASP)**
   The OWASP CLASP is an activity-driven, role-based set of process components whose core contains formalised best practices for building security into existing or new-start software development lifecycles in a structured, repeatable, and measurable way. CLASP | Owasp.org.

7. **Open Web Application Security Project (OWASP) - Software Assurance Maturity Model (SAMM)**
   The mission of OWASP SAMM is to be the prime maturity model for software assurance that provides an effective and measurable way for all types of organisations to analyse and improve their software security posture. SAMM | Owasp.org.

8. **CISA Cyber Performance Goals (CPGs)**
   CISA's CPGs are a subset of cybersecurity practices, selected through a thorough process of industry, government, and expert consultation, aimed at meaningfully reducing risks to both critical infrastructure operations and people. CPG | Cisa.gov.

9. **NIST SP 800-53 Rev. 5 - Security and Privacy Controls for Information Systems and Organisations**
   This publication provides a catalogue of security and privacy controls for information systems to protect organisational operations and assets from a diverse set of threats and risks, including cyber attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. SP800-53 | Nist.gov.

10. **Common Criteria (CC) - Common Criteria for Information Technology Security Evaluation**
    The CC is the driving force for the widest available mutual recognition of secure IT products. Products can be evaluated by competent and independent licensed laboratories to determine the fulfilment of particular security properties, to a certain extent or assurance.
    Common Criteria | Commoncriteriaportal.org.

11. **CSA/ANSI T200:22**
    This Standard describes a methodology for assessing the product software and cybersecurity control maturity of an organisation. It covers the entire product system life cycle from conception to full commissioning and until the end of life. It supports effective executive business decisions that establish a comprehensive maturity model approach to cybersecurity.
    CSA/ANSI T200:22 | Csagroup.org.

12. **Cybersecurity Capability Maturity Model C2M2**
    The Cybersecurity Capability Maturity Model (C2M2) is a free tool to help organizations evaluate their cybersecurity capabilities and optimize security investments.
    Cyber Capability Maturity Model | Energy.gov.

# Categories of digital products and services

## Software

Software covers all types of programs/applications, operating systems, embedded systems and firmware. Software is either proprietary (licensed) or open-source (freely available).

### Proprietary software

Proprietary or 'closed source' software is software that has been developed by a manufacturer and is not freely distributed but made available through a licensing or purchasing agreement. Manufacturers may impose restrictions on proprietary software, such as restricting the number of users or prohibiting resale, redistribution or reverse engineering.

### Open-source software

Open-source software (OSS) is a type of software, often including source code, that is distributed with an open license for anyone to view, use, study or modify. Source code is the human-readable language that the software has been written in. OSS is generally managed by a community of volunteers dedicated to its ongoing development and refinement. There are many benefits to using OSS, including the speed with which new products can be built.

### Embedded software and firmware

Embedded software refers to software that is written to control embedded systems. These are systems that are purpose-built to perform specific functions or tasks within larger systems. They are typically limited by processing resources available and designed to operate in real time. Examples include car engine management units, and smart devices like home thermostats.

Firmware is a type of embedded software that is designed to be permanently stored in the non-volatile memory (memory which is retained after power is removed) of a hardware device, such as Read Only Memory (ROM) or flash memory. Firmware provides low-level control for a device's specific hardware components. Examples include micro controllers and PC BIOS.

### Software Bill of Materials

A Software Bill of Materials (SBOM) is a formatted way of describing the software components or libraries that comprise a software package. An SBOM is applicable to all software types, including proprietary, open-source, embedded and firmware. An SBOM allows both manufacturers and consumers to easily identify the components included in a product and their versions. The information in an SBOM enables organisations to monitor manufacturers and public sources for software updates and reported vulnerabilities. There are many industry formats for SBOMs, with most being machine readable to allow for automation of monitoring and reporting.

For more information please visit SBOM | Cisa.gov

## Hardware

Hardware covers any physical device that is designed to process, store, or transmit data. This includes network devices, such as firewalls, routers, load balancers and network security products (e.g. network intrusion detection (NID) and network intrusion prevention (NIP)), storage items, such as network attached storage (NAS), and any device that processes data, including physical servers. Most hardware will contain software including firmware and/or embedded software which must be taken into consideration during procurement.

### Hardware Bill of Materials

A Hardware Bill of Materials (HBOM) is a formatted way of describing the physical components and materials that comprise a piece of hardware. There are several industry standards for HBOMs, with the CISA *Framework for Supply Chain Risk Management* being one such example.

For more information, please visit HBOM | Cisa.gov.

### Internet of Things

The Internet of Things (IoT) is generally considered a subset of hardware. It covers a multitude of devices and sensors that must be connected to a network or the internet to exchange data and provide functionality. IoT devices include general consumer products (IP cameras, temperature and humidity sensors, home automation devices, etc.), medical and health devices (pacemakers, fall monitors, etc.), and operational technologies (OT) (sensors, control units, etc.).

## Cloud services

Cloud service providers (CSPs) offer computing resources that organisations can access on demand. In general, CSPs offer infrastructure, platform, storage, networking, and processing as services. When procuring cloud services, organisations should apply the same security considerations as when purchasing software or hardware.

### Software as a Service

Software as a Service (SaaS) is a way of offering software to consumers without the need for the consumer to install or manage/administer the software themselves. SaaS offers many advantages, including reduced management overheads, maintenance, and infrastructure costs (such as patching). SaaS can be offered under a purchasing/licensing agreement or can be offered as free access (this does not necessarily mean it is offered as OSS).

### Managed service providers

Managed service providers (MSPs) offer a range of specialised services assisting organisations to effectively leverage cloud computing resources. MSPs take on the responsibility of managing, securing, and optimising a client's cloud infrastructure, enabling the client to focus on their core business activities rather than the intricacies of cloud management. Key MSP service offerings include cloud infrastructure management, monitoring, performance optimisation, security and compliance, data backup and recovery.

**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 2024
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 licence (www.creativecommons.org/licenses).

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

The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

**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 (www.pmc.gov.au/government/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