Department for Science, Innovation & Technology

National Cyber Security Centre
a part of GCHQ

Communications Security Establishment Canada
Canadian Centre for Cyber Security

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

# Software Security Code of Practice

May 2025

# Background

This document outlines a voluntary Software Security Code of Practice. The Code of Practice has been developed to improve the security and resilience of software that organisations and businesses rely on.

The Software Security Code of Practice is designed to support software vendors and their customers in reducing the likelihood and impact of software supply chain attacks and other software resilience incidents. Often, these kinds of attacks and disruptions are caused by avoidable weaknesses in software development and maintenance practices. The impact of these kinds of incidents can also be exacerbated by poor communication between organisations and their software suppliers.[1]

This Code is the product of extensive engagement and has been co-designed with technical experts at the National Cyber Security Centre (NCSC) and a group of industry and academic experts. It has also been refined using feedback from a public call for views undertaken from May to August 2024. It consists of 14 principles that software vendors are expected to implement to establish a consistent baseline of software security and resilience across the market.

The principles that form the Code of Practice are relevant to any type of software supplied to business customers. Divided into 4 themes, the government has identified these principles as fundamental and achievable measures that should be reasonably expected from organisations of any size, type or sector. If carried out, these principles would represent a robust approach to software security and resilience, helping to secure the foundations of the digital technologies and services that connect digital supply chains.

The Software Security Code of Practice should be considered as part of the broader suite of cyber security guidance issued by the Department for Science, Innovation and Technology, and read in parallel with other codes of practice. Organisations deemed in scope should also adhere to other relevant security measures, and particularly the Cyber Governance Code of Practice, which sets the baseline expectations for all organisations using digital technologies. Organisations deemed in scope should also consider whether they should adhere with further technology-specific codes of practice, such as those relating to AI and App Stores, depending on their business function.

This voluntary code of practice is designed to be complementary to relevant international approaches and existing standards in this space to limit the compliance burden for organisations operating across borders. Where possible, the Code reflects internationally recognised best practices, which includes those outlined in the US Secure Software Development Framework (SSDF) and the EU's Cyber Resilience Act, as well as existing guidance and formal standards in this space.

---

[1] Beyond these baseline expectations, organisations operating in more sensitive sectors or environments or with a larger customer base may require more advanced measures to protect against more sophisticated threat actors.

# Audience and scope

The Software Security Code of Practice sets out the fundamental security and resilience measures that should be reasonably expected from all organisations that develop and/or sell software to businesses or other organisations. This includes those that supply standalone software or software services, or organisations selling goods or services that contain software. The software or software component may be any kind of software, including application or systems software. However, this Code of Practice is most relevant to the sale and distribution of proprietary software in the context of business-to-business commercial relationships.

Table 1 below gives examples of different types of organisations for whom this voluntary code of practice may be relevant.

## Table 1 – Stakeholder Groups and Guidance

| Stakeholder Groups | Guidance |
|---|---|
| ***Software developers and distributors***<br><br>Examples of these types of organisations include, but are not limited to:<br>• Independent Software Vendors<br>• Software as a Service (SaaS) providers<br>• Vendors of goods or services with a software component (e.g. organisations developing and distributing IoTs or some Managed Service Providers) | For the purpose of this Code of Practice, any organisations that both develop and sell software or software services are classed as "software developers and distributors".<br><br>Software developers and distributors would be expected to follow all principles of this Code of Practice. |
| ***Software resellers***<br><br>Examples of these types of organisations may include, but are not limited to:<br>• Organisations whose primary function is to resell software.<br>• Organisations who supply goods and services and resell software as part of this offering (e.g. some managed service providers) | For the purpose of this Code of Practice, organisations that sell software but do not develop the software themselves are classed as "software resellers".<br><br>For software resellers, only principles 3 to 4 will fall within the scope of a reseller's responsibility. However, where possible, resellers should encourage those developing the software they distribute to follow the principles of this Code. |
| ***Software developers only***<br><br>Examples of these types of organisations include:<br>• Organisations that develop in-house software for proprietary use<br>• Individual software developers | For the purpose of this Code of Practice, organisations that develop software but are not involved in the sale or distribution of software are classed as "software developers only".<br><br>For software developers only, principles 1 and 2 will be relevant, as well as principle 3 where it is in the scope of responsibility of the organisation/ individual. |
| ***Open-source developers and maintainers*** | For the purpose of this Software Security Code of Practice, open-source developers and maintainers are not considered the primary audience.<br><br>This Code of Practice is most relevant to the sale and distribution of proprietary software as the Code aims to set out the responsibilities of software vendors in the context of business-to-business commercial relationships. For open-source software, the developer/maintainer bears no formal commitment to their onwards supply chain or for the ongoing maintenance and security of their code. Any risks associated with open-source code must be managed by end-users or proprietary developers using open-source code in their software. Open-source developers may find aspects of this Code of Practice useful, but principles relating to vendor-customer relationships may not be relevant for this audience. |

The Code is aimed at senior leaders in software vendor organisations to ensure that the measures outlined in the Code of Practice are prioritised and followed through within the organisation. With clarity on the software vendor's responsibilities, those senior leaders can ensure that relevant teams across their organisations take the necessary steps to meet those expectations, and have the resources, tools and knowledge they need to do so.

To support the technical teams who are responsible for implementing these principles, the Software Security Code of Practice is supplemented by implementation guidance. This guidance provides more detailed information about how the principles of the Code of Practice can be implemented. Implementation may vary depending on the size or sector of the organisation or the type of software being produced, but the guidance provided will help organisations to find the right implementation option for them. It will also signpost to existing guidance and frameworks where possible.

Table 2 below outlines how different stakeholder groups are expected to interact with the Code of Practice and implementation guidance.

## Table 2 – Stakeholder and Description

| Stakeholder | Description |
|---|---|
| ***Senior Leaders in Software Vendor organisations*** | Senior leaders are the primary target audience for this Code of Practice. A Senior Responsible Owner (SRO) should be appointed at the top-tier leadership level of an organisation. This individual will be accountable for ensuring the principles of the Software Security Code of Practice are followed by relevant teams and individuals within their organisations. Job titles may vary depending on organisational structure, but this individual could be a senior executive, board member, a C-Suite member, President, Vice President, Director, Department Head or equivalent. They would not require a deep, technical understanding of software security but would need to ensure that adherence to the Code of Practice is prioritised and that the relevant teams throughout the organisation have the resources and tools needed to implement the Code. |
| ***Specialist and technical Teams/ roles*** | The principles of the Code of Practice will be relevant to a range of functions and roles within a software vendor organisation. These include those who design and develop software, those responsible for maintaining software, and those responsible for communicating with business customers. Depending on the size and structure of the software vendor organisation, these may fall in separate teams or departments or could be implemented by the same team/ individual(s).<br><br>The implementation guidance provides support for these individuals on how they can identify the most appropriate implementation options for their organisation, including signposting to more detailed technical guidance where needed. |
| ***Organisations procuring software*** | Businesses and organisations that procure software can use this Code of Practice to inform negotiations with suppliers. Customer organisations may refer to the principles of the Code in negotiations or use them to inform agreements and contracts with their suppliers. DSIT is also developing software supplier management guidance to provide additional support on holding suppliers accountable which will be published in due course. |

## Assurance and self-assessment

The UK Government is providing a self-assessment form to accompany this Code of Practice. This form can be used for internal compliance monitoring or can be shared with customers to provide software security assurance.

The assurance approach for this Code of Practice has been developed to follow the NCSC's Principles Based Assurance approach. This breaks the Code of Practice down into a set of Assurance Principles and Claims (APCs). Using the Code of Practice as the core principles, the APCs derive a set of ideal-scenario claims that, if met, mean the software vendor is achieving the principles of the Software Security Code of Practice. The kind of evidence provided may vary depending on the specific processes used by each organisation, which provides flexibility in how organisations can demonstrate compliance using the form provided.

The UK Government is currently working to develop a certification scheme based on this compliance process. Further information about this certification process will be shared in due course.

## Skills

Senior leaders should be accountable for ensuring that the organisation fulfils the requirements of this Code of Practice. Part of that responsibility is to ensure that the relevant teams and individuals implementing the below measures have the necessary skills and resources. This includes formal qualifications as well as on-the-job training and exposure to relevant knowledge (e.g. secure coding standards). Supporting the development of software security skills is essential to creating an internal culture that promotes software security as an organisational priority.

In addition to industry training provisions and qualifications, the following government schemes are helping to bolster the cyber security ecosystem and can help organisations recognise appropriate skills or provide development routes for existing staff:

- The UK Cyber Security Council represents a first port of call for cyber security professional standards in the UK. The Council, recognised by Royal Charter, sets out the knowledge, skill and experience that cyber security professional should demonstrate in their roles. This is intended to make the cyber career pathway, for employers and practitioners alike, easier to navigate and access.
- The NCSC certified degree programme recognises courses in computing and cyber security run by UK Higher Education Institutions (HEIs) that provide well-defined and relevant cyber security content and that are delivered to an appropriate standard. NCSC certified degrees help universities attract talent and employers recruit skilled staff and develop the cyber skills of existing employees, as well as enable prospective students to make better informed choices when looking for a highly valued qualification.
- In 2025 the NCSC plans to launch a revised undergraduate degree certification standard which will incentivise the teaching of Software Security and Secure Software Lifecycle (SSL) knowledge areas, as defined in the Cyber Security Body of Knowledge (CyBOK). The aim is to increase the numbers of graduates from computing and cyber security related degree courses entering the tech workforce with the knowledge and skills to meet the Software Code of Practice.

# The Software Security Code of Practice

The Software Security Code of Practice contains 14 principles split across 4 themes. A Senior Responsible Owner should be appointed at senior leadership level to hold accountability for the principles being followed within their organisations.

## 1. Secure design and development

These principles ensure that the software is appropriately secure when provided.

The Senior Responsible Owner in vendor organisations shall gain assurance that their organisation achieves the following in relation to any software or software services sold by their organisation:

1.1 Follow an established secure development framework.

1.2 Understand the composition of the software and assess risks linked to the ingestion and maintenance of third-party components throughout the development lifecycle.

1.3 Have a clear process for testing software and software updates before distribution.

1.4 Follow secure by design and secure by default principles throughout the development lifecycle of the software.

## 2. Build environment security

These principles ensure that the appropriate steps are taken to minimise the risk of build environments becoming compromised and protect the integrity and quality of the software.

The Senior Responsible Owner in vendor organisations shall gain assurance that their organisation achieves the following in relation to any software or software services sold by their organisation:

2.1 Protect the build environment against unauthorised access.

2.2 Control and log changes to the build environment.

## 3. Secure deployment and maintenance

These principles ensure that the software remains secure throughout its lifetime, to minimise the likelihood and impact of vulnerabilities.

The Senior Responsible Owner in vendor organisations shall gain assurance that their organisation achieves the following in relation to any software or software services sold by their organisation:

3.1 Distribute software securely to customers.

3.2 Implement and publish an effective vulnerability disclosure process.

3.3 Have processes and documentation in place for proactively detecting, prioritising and managing vulnerabilities in software components.

3.4 Report vulnerabilities to relevant parties where appropriate.

3.5 Provide timely security updates, patches and notifications to customers.

## 4. Communication with customers

These principles ensure that vendor organisations provide sufficient information to customers to enable effective risk and incident management.

The Senior Responsible Owner in vendor organisations shall gain assurance that their organisation achieves the following in relation to any software or software services sold by their organisation:

4.1 Provide information to the customer specifying the level of support and maintenance provided for the software being sold.

4.2 Provides at least 1 year's notice to customers of when the software will no longer be supported or maintained by the vendor.

4.3 Make information available to customers about notable incidents that may cause significant impact to customer organisations.

# Table 3 – Glossary of key terms

| Term | Definition |
|---|---|
| **Assurance, Principles & Claims (APCs)** | An APC is a document containing a complete set of Principles and Claims that describe an ideal baseline for a technology, system, service, or process. The claims in an APC can be evidenced to help assess where the baseline is met, or where improvements can be made.<br><br>The APC deconstructs the set of principles into claims using a Claims Argument Evidence method described on the NCSC's Principles Based Assurance page.<br><br>An APC has been created for the Code of Practice based on the themes and principles the Code lays out. The claims it contains form the basis for a self-assessment of a software producers practices against the Code of Practice |
| **Build Environment** | The environment where software is compiled, built and packaged ready for release. This should be logically or physically separate from areas where code is written and tested. |
| **Digital service** | The provision of services (such as banking or online shopping) via the internet, or an electronic network. |
| **Enterprise customer** | For the purpose of this Code of Practice an enterprise customer is defined as any business or other organisation that procures software or software services. |
| **Implementation guidance** | Implementation guidance supports software vendors to achieve the security outcomes in the Code of Practice. The implementation guidance also signposts to other guidance or frameworks where these may be relevant. This guidance is aimed at technical and other specialist teams or individuals responsible for carrying out work to meet the actions of the Code of Practice. |
| **Incident** | A cyber incident as relevant to this Software Security Code of Practice is defined as unauthorised access (or attempted access) to an organisation's IT systems. These may be malicious attacks (such as a software supply chain attack, malware infection or ransomware attack), or could be accidental incidents (such as incidents where disruption is caused by vulnerabilities in software or updates). |

| Term | Definition |
|---|---|
| **Lifecycle** | A software development lifecycle (SDLC) is a formal or informal methodology for designing, creating, and maintaining software (including code built into hardware). There are many models for SDLCs, but they typically contain a variation of these 7 stages: Requirements gathering, analysis, design, implementation or coding, testing, deployment, and maintenance/support. |
| **Principles Based Assurance (PBA)** | Principles Based Assurance (PBA) is an NCSC framework for assurance best practice. It is designed to help customers gain confidence that the technology they use every day is resilient to an acceptable level. It provides an adaptable and holistic process and structure that allows vendors to demonstrate evidence against a set of principles (in this case the Code of Practice). |
| **Relevant parties (action 3.4)** | This action refers to parties external to the organisation who would benefit from knowledge of the identified vulnerability. These could be software vulnerability databases, customers, regulators or supply chains. Software vendors would need to conduct a risk assessment to ascertain when and to whom reports would be appropriate. |
| **Secure by Default** | This approach ensures that technology is developed so that security is embedded from its inception and is frictionless for the user. Security is treated as a core fundamental rather than a follow-up activity, and the most secure configurations are enabled by default. |
| **Secure by Design** | "Secure by design" means that software and goods containing software are built in a way that reasonably protects against malicious cyber actors successfully gaining access to devices, data and connected infrastructure. Software vendors should perform a risk assessment to identify and enumerate prevalent cyber threats to critical systems and then include protections in the blueprints that account for the evolving cyber threat landscape. |
| **Secure development framework** | A secure development framework provides a structured approach to integrating security throughout the software development life cycle. An established secure development framework should include the following topics as a minimum: threat modelling, secure coding practices, requirements capture, governance and roles, test strategy, data management, and configuration management (see implementation guidance for further detail). |
| **Self-assessment form** | A self-assessment form is available. Software vendors can use this form to evidence that they meet the requirements of the Software Security Code of Practice. The self-assessment form uses APCs to provide structure whilst supporting a variety of forms of evidence. |

| Term | Definition |
|---|---|
| **Senior Leader** | A senior leader is someone at the top of the hierarchy of an organisation. They hold an executive or upper management function and provide high-level leadership and direction for an organisation. Depending on each organisation's size and structure, the specific roles could vary but may include CEO, President, Vice President, C-Suite, Director, a General Manager, or Department Head. |
| **Senior Responsible Owner** | A Senior Responsible Owner is an individual appointed at senior leadership level to hold accountability for ensuring each action of the Code of Practice is achieved by the organisation. This includes ensuring that relevant teams have the appropriate resources, knowledge and tools to achieve each action. |
| **Shall** | In this Code of Practice, "shall" represents a requirement of the Code of Practice. This language reflects the language used in government standards, which will facilitate assurance against this Code of Practice. |
| **Software** | Software is code, programmes and applications that run on devices. Software runs on both IT and OT hardware devices and via cloud services (Saas, see below). |
| **Software service (Software as a Service – SaaS)** | A business model where customers access centrally hosted software applications over the internet. |
| **Software Vendor** | Software vendors are organisations that develop and sell software or software services. |
| **Third-party component** | A third-party software component is a component of software developed by a party that is external to the software vendor organisation. They can be open source, or owned or licensed by third parties. |
| **Vulnerability** | A weakness, or flaw, in software. An attacker may exploit these to (for example) gain unauthorised access to a computer system. |
| **Vulnerability disclosure process** | A process whereby individuals can, safely and accessibly, report vulnerabilities to the organisation. This should be backed up by a vulnerability disclosure policy which details how reports should be handled internally (see implementation guidance for more detail). |