Call for Views on the Code of Practice for Software Vendors

Ministerial Foreword

Viscount Camrose
Parliamentary Under Secretary of State,
Department for Science, Innovation and Technology

Software is a fundamental building block for digital technologies. It underpins all our digital devices and services and is used to create the essential applications and innovative solutions which businesses across all sectors of our economy rely on. Software is essential to keeping the day-to-day operation of businesses going, from word processors to timesheet and payment software, from operational technologies to automating processes using AI. In terms of innovation, businesses use software to deliver new products and services to the market, bringing huge economic and social opportunities to the UK. For this reason, embracing digital technologies - which are built on software - across our economy is crucial to delivering the ambitions set out in the National Cyber Strategy[1] and the UK Digital Strategy[2]. This is key to the Government's work to secure the UK's prosperity, national security, global competitiveness and geo-political standing in the world.

Software has become so widespread in day-to-day organisational operations and processes that we barely notice its presence, yet compromised or faulty software can bring organisations to a halt. Our reliance on software makes it an appealing target for malicious actors. In June 2023, an attack on MOVEit file transfer software[3], a widely used programme for business operations, allowed malicious actors to access personal details of staff and employees at a wide range of UK organisations. This caused significant disruption and demonstrated how widespread the impact of compromised software can be.

The Government outlined a package of policy measures to address the security and resilience of software in our digital supply chains in January in its response to the call for views on software resilience and security for businesses and organisations.[4] The first step in this policy package is to lay out clear expectations for how organisations selling and developing software should ensure the resilience of the software they sell. This responds to strong appetite for

[1] National Cyber Strategy, Government, 2022.
[2] UK Digital Strategy, DCMS, 2022.
[3] MOVEit hack: BBC, BA and Boots among cyber attack victims, BBC, 2023.
[4] Government response to the call for views on software resilience and security for businesses and organisations, DSIT, 2024.

government intervention to address inconsistencies in software security and resilience across the market.

I am therefore pleased to introduce this call for views on a voluntary Code of Practice for Software Vendors which is designed to ensure that software security is made fundamental to software vendors' approaches to developing and distributing their products and services. This Code builds upon work in other UK government policy areas focusing on different aspects of the technology landscape to help improve cyber resilience and reduce cyber risk at source, as set out in the National Cyber Strategy. The UK's consumer connectable product security regime comes into effect when the so far not already in force sections of Part 1 of the Product Security and Telecommunications Infrastructure (PSTI) Act 2022 come into force on 29th April 2024. This regime places legal responsibilities on relevant persons including manufacturers to ensure that internet-connectable products and embedded software are secure by design. This will make consumer connectable products more secure against cyber attacks.

The Government is also working closely with industry to ensure that voluntary codes of practice are available to guide organisations in how to develop and use both existing and emerging technologies. The Code of Practice outlined in this consultation will be a crucial part of that bigger picture which also currently includes a Code of Practice for App Store Operators and App Developers,[5] and a Cyber Governance Code of Practice which has recently undergone public consultation.

The Government must act to ensure good cyber security practices are adopted to secure both the foundations of technology products, as addressed in the proposed Code of Practice for Software Vendors, as well as emerging technologies such as AI. To address these risks together, the Government is also launching a call for views on the Cyber Security of AI at the same time. The call for views on AI outlines the proposed Code of Practice, with a view to developing an international standard to set baseline security requirements for AI Developers and System Operators.

Outputs from both these Calls for Views will have a significant impact in driving improved security behaviour across the software supply chain and providing increased confidence to organisations adopting digital products and services. The two newly proposed Codes of Practice demonstrate, and build on, the leading role that the UK plays globally in developing new cyber security and resilience policy, particularly in embedding secure by design principles as a foundation of a more secure global tech market.

The Code of Practice for Software Vendors is the product of extensive engagement with a range of stakeholders and has been co-designed with industry and academic leaders, as well as technical experts at the National Cyber Security Centre. I would like to thank all of those organisations and individuals who have shared their views on these critical issues thus far. Your contributions have been vital to shaping this draft Code of Practice.

Your responses to the questions in this call for views will help the Government to strengthen our digital supply chains by securing the most foundational aspect of the technologies we use: software. I encourage any domestic or international organisations who develop, sell or procure software as well as organisations or individuals with an interest in cyber resilience, supply chain risk management, or software security and resilience to take part. We welcome views

[5] Code of practice for app store operators and app developers, DCMS, 2023

from all sectors and businesses of any size, including academics or researchers. I thank you in advance for your valuable contributions.

Executive Summary

In January 2024, the Department for Science, Innovation and Technology (DSIT) published the government response to the call for views on software resilience and security for businesses and organisations.[6] This response outlined the Government's proposed policy package that aims to raise the baseline expectations of software security, and to improve software resilience across the UK.

This document provides businesses with the opportunity to provide feedback on the Government's primary proposed policy intervention that was developed in response to engagement with stakeholders: the Code of Practice for Software Vendors.

The Code of Practice for Software Vendors outlines the fundamental security and resilience measures that should reasonably be expected of all organisations that develop and / or sell software to organisational customers. It includes guidance on how software should be developed, built, deployed and maintained, and how vendors can communicate with effectively with customers that procure their software. In engaging with this Code of Practice, software vendors will significantly improve the cyber resilience of their product and services.

The Code of Practice is made up of 21 provisions over 4 principles:

- Principle 1: Secure design and development: this principle ensures that the product or service is appropriately secure when provided.
- Principle 2: Build environment security: this principle ensures that the appropriate steps are taken to minimise the risk of build environments becoming compromised and protect the integrity and quality of the software.
- Principle 3: Secure deployment and maintenance: this principle ensures that the product or service remains secure throughout its lifetime, to minimise the likelihood and impact of vulnerabilities.
- Principle 4: Communication with customers: this principle ensures that vendor organisations provide sufficient information to customers to enable effective risk and incident management.

The Code of Practice, co-designed with industry leaders, academics, and technical experts from the National Cyber Security Centre, has been developed to support any organisation that develops and/or sells software to be sold to organisational customers (B2B). This includes organisations that sell solely software products or services, or organisations selling digital products or services that contain software. The Government and co-creators have been mindful that organisations vary in size, capacity and resources, and organisations will have to engage in risk assessments to determine the most effective way in which they can follow this Code of Practice. Nevertheless, the Code of Practice provides clarity on key, underlying principles that represent best practices to help software vendors develop and distribute software securely.

Technical controls and implementation guidance will be published alongside the Code of Practice. This will set out the minimum set of objective controls that a software vendor should

[6] Government response to the call for views on software resilience and security for businesses and organisations, DSIT, 2024.

demonstrate to provide confidence in the resilience of their software product or service as well as guidance to support organisations in identifying the best implementation options for them.

This call for views aims to gather views on the market need for the Code of Practice for Software Vendors, the audience that this policy should be addressing, and the suitability of the Code and proposed supporting materials.

Chapter 1: Introduction

Background

1.1 Following the Government's call for views on software resilience and security for businesses and organisations,[7] DSIT has undertaken extensive stakeholder engagement to develop a package of policy interventions.[8] The interventions in this package are designed to prevent common mistakes in software development and distribution, and to improve information sharing between software vendors and their customers. Addressing these issues will reduce the likelihood and impact of software supply chain attacks and other incidents that continue to affect organisations across all sectors of our economy.

1.2 The voluntary Code of Practice for Software Vendors sets out the fundamental security and resilience measures that should be expected of all organisations that develop or sell software used by businesses and other organisations. The Code of Practice aims to strengthen the foundations of the many kinds of digital technologies that all sectors of our economy rely on.

1.3 This call for views seeks feedback on the proposed design of the Code of Practice for Software Vendors including input on how it should be implemented. The Government is also seeking input on the supporting materials and future interventions that may be needed to support both software vendors implementing the Code of Practice and organisations wishing to use this Code of Practice within their procurement processes. The Government will use the information gathered from this call for views to ensure this policy is proportionate, effective, and addresses the key concerns of those most affected.

Scope

1.4 The Code of Practice for Software Vendors will support any organisation developing and/or selling software to be sold to businesses and other organisations. This includes organisations selling solely software products or services, or organisations selling digital products or services that contain software. Examples of organisations in scope include independent software vendors, organisations selling IoT devices, or cloud services that include the provision of software.

1.5 The Code addresses risks associated with any type of software, including application or systems software. However, this Code of Practice is most relevant to the sale and distribution of proprietary software as it sets out the responsibilities of software vendors in the context of business-to-business relationships. When it comes to open-source software the developer/maintainer bears no formal commitment for the ongoing maintenance and security of products which must be managed by end-users or proprietary developers using open-source code in products made for sale. As such, aspects of this Code describing the relationship between the software vendor and procuring organisation may not be relevant to open-source. Open-source developers may find aspects of this Code of Practice useful should they choose to use it and we would encourage open-source software developers to observe the principles of this Code of Practice and the accompanying guidance where possible.

[7] Call for Views on software resilience and security for businesses and organisations, DCMS, 2023.
[8] Government response to the call for views on software resilience and security for businesses and organisations, DSIT, 2024.

1.6 This voluntary Code of Practice is designed to provide guidance and clear expectations for the security and resilience of software supplied to organisations and businesses by software vendors. For the purpose of this Code, software vendors include the following stakeholder groups:

Stakeholder	Description
Software developers and distributors Examples of these types of organisations include, but are not limited to: • Independent Software Vendors • Software as a Service (SaaS) providers • Vendors of digital products or services with a software component (e.g. organisations developing and distributing IoT products or some Managed Service Providers)	For the purpose of this Code of Practice, any organisations that both develop and sell software products or services are classed as "software developers and distributors". All principles of this Code of Practice will be relevant to software developers and distributors.
Software resellers Examples of these types of organisations may include, but are not limited to: • Organisations whose primary function is to resell software • Organisations who supply digital services and products 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". For software resellers, only principles 3 and 4 will fall within the scope of responsibility of the organisation. However, resellers should also encourage those developing the software they distribute to follow the principles of this Code.
Software developers only Examples of these types of organisations include: • Organisations that develop in-house software for proprietary use • Individual software developers	For the purpose of this Code of Practice, organisations that develop software but do not distribute software to organisational customers are classed as "software developers only" 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.

Rationale

1.7 As part of the National Cyber Strategy, the Government is committed to preventing and resisting cyber attacks more effectively by improving the management of cyber risks within UK organisations. Software insecurity poses a huge risk to the resilience and security of UK organisations, and by extension to the services which UK citizens rely upon on a daily basis. Responses to last year's call for views on software resilience and security for businesses and organisations[9] illustrated how critical the security and effective running of software is to the UK's organisational resilience. 73% of respondents advised that accidental vulnerabilities in software had a 'high' or 'very high' impact on the security and resilience of their organisations.

1.8 Currently, levels of security and resilience are inconsistent across the software market and there is considerable support for further government and industry intervention[10] to address these inconsistencies and to raise the bar of software resilience to strengthen our digital supply chains. Organisations and businesses in the UK face a complex and dynamic cyber security landscape, and there was a 742% average annual increase[11] in software supply chain attacks between 2019 and 2022. Strengthening security across the software lifecycle can help to minimise the opportunities malicious actors have to compromise organisations and could also limit the scale of the damage when attacks do occur.

1.9 This Code of Practice outlines the essential security and resilience measures required to reduce the likelihood and impact of the most commonplace software cyberattacks. The Code is aimed at senior leaders in software vendor organisations to ensure that they understand the full extent of what is required for their organisation to adequately put in place these security and resilience measures. Those senior leaders can ensure that relevant teams across their organisations take the necessary steps to put in place these measures, and have the resources, tools and knowledge they need to do so.

1.10 How compliance is managed, and how principles are implemented, will differ between organisations depending on their size and structure as well as the products and services each organisation produces. As such, the principles are designed to be flexible and adaptable rather than prescriptive, but focused on the fundamental principles that, if met, would constitute a reasonable and robust approach to software security for any software vendor.

Methodology

1.11 The Code has been developed in partnership with the NCSC and industry experts. A series of co-design workshops were held between October 2023 and February 2024. In recognition of the complexity and scope of software supply chains, the co-design group consisted of a diverse range of stakeholders, including small and large vendors, cyber and experts from industry and academia, representative bodies, and software customers.

1.12 The Code of Practice has been designed to address the key risks identified by the public in response to the call for views held last year. The code focuses on development practices, vulnerability management, and the communication of information to aid risk management throughout supply chains. This reflects the fact that respondents to the call for views were

[9] Government response to the call for views on software resilience and security for businesses and organisations, DSIT, 2024.

[10] 98% of respondents to our call for views on software resilience and security thought there was a need for greater government and/or industry intervention to address risks relating to software development security, with 65% believing that both would be needed to ensure the security and resilience in the distribution of software.

[11] State of the Software Supply Chain, Sonatype, 2022.

concerned about the high impact that software development security and low levels of transparency and communication in supply chains were having on organisational resilience. Respondents also identified accidental vulnerabilities in software code as the biggest problem relating to software resilience and security, which is addressed by provisions to encourage better monitoring and management of software vulnerabilities.

1.13 The Code of Practice for Software Vendors has been developed to limit the burden of organisations operating across borders, which is a key concern for stakeholders, including those involved in the co-creation of the Code. International approaches to software security have been taken into account when designing the Code of Practice, including the US Government's Secure Software Development Framework[12] (SSDF) which forms the basis of the US Government's new federal procurement requirements, and the regulatory requirements outlined in the EU's proposed Cyber Resilience Act.[13] Where possible, the guidance reflects internationally recognised best practices, including those outlined in the US and EU's interventions.

[12] Secure Software Development Framework, NIST, 2022.

[13] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation, EU, 2022.

Chapter 2: DSIT Activity

2.1 All cyber security codes of practice produced by DSIT are part of the Government's broader approach to improve baseline cyber security practices and cyber resilience across the UK. The Codes of Practice provide guidance ranging from the development of baseline cyber security advice which all organisations should follow, moving progressively towards more product- or domain-specific advice due to the increasing risk and evolving threat landscape. A modular approach has been developed to help organisations easily identify which Codes – and within those Codes, which provisions – are relevant to them according to both their business functions, and the types of technologies they either use or manufacture.

2.2 In the case of this Code, our expectation is that organisations in scope should, at a minimum, also adhere to the provisions in the Cyber Governance Code of Practice which sets the baseline expectations for all organisations which use digital technologies. Organisations deemed in scope of this Code would also be expected to assess whether their circumstances warrant consideration of adherence to additional Codes published by the UK Government which may cover specific products or services relevant to them.

2.3 As noted above, there is a clear overlap between the work on software and the work on AI as, like all digital technologies, software is a key component of AI technology. The Government is proposing to take forward a two-part intervention to address the cyber security risks to AI. This will be in the form of a draft voluntary Code of Practice that will be taken into a global standards development organisation for further development. A call for views on the Cyber Security of AI, which includes the draft Code, is also currently ongoing [link to be added].

The UK's Approach to Cyber Security

2.4 The UK, as a global leader in cyber security, is committed to creating a safe online environment for its citizens. A foundational pillar of this approach is to ensure that both existing and emerging technologies are secure by design. By setting baseline cyber security expectations and incorporating them into the development of digital technologies at inception, we are laying the groundwork for efforts to safeguard users and businesses against evolving cyber threats, and to provide consumers with confidence in the technologies that they use. However, security also needs to be considered throughout the lifecycle of a technology, and the distinct security challenges presented by individual technologies need to be recognised and assessed.

2.5 DSIT has led several initiatives that embed a "secure by design" approach, contributing to the UK's strategic advantage and global cyber security leadership. These include:

- The creation of the world's first mandatory and enforceable security requirements for consumer technology through the Product Security and Telecommunications Infrastructure (PSTI) Act.[14] This work built on the UK's Code of Practice for Consumer IoT, published in 2018.
- Delivering the world's first App and App Store Privacy and Security Code of Practice, which is being implemented by all major app store operators.[15]
- Building on the CHERI research from the University of Cambridge, we have worked with Arm to develop a processor prototype that integrates CHERI capabilities to enable

[14] The UK Product Security and Telecommunications Infrastructure (Product Security) regime, Department for Science, Innovation & Technology, 2023.
[15] Code of practice for app store operators and app developers (updated), Department for Science, Innovation & Technology, 2023 .

fine-grained protection of memory. This forms part of our Digital Security by Design programme.[16]

2.6 A secure by design approach is only the first step towards UK-wide cyber resilience. To build on this, we must also focus on cultivating the necessary cyber security skills. This entails aligning our cyber skills development initiatives more closely with the needs of Critical National Infrastructure (CNI) sectors, the specific risks associated with new and emerging technologies which are being adopted, and with the resilience measures that we expect of organisations across the economy. In doing so, we are seeking to foster a skilled workforce capable of deploying the baseline cyber security expectations we set across diverse sectors of the economy.

2.7 Another key part of building a more cyber resilient UK is identifying and mitigating cyber risks as they proliferate across digital supply chains. By providing guidance, we can help businesses and organisations better manage risks associated with the digital products and services on which they rely. Our work in this space includes:

- Cyber Essentials Certification, which is a Government backed scheme to certify that organisations have taken the minimum steps to protect themselves against the most common cyber attacks.
- The Cyber Assessment Framework, which is a framework which supports organisations as they seek to assess cyber risks to essential functions. This is aimed at critical organisations such as those in CNI sectors.
- The Cyber Governance Code of Practice, which sets the baseline expectations for all organisations using digital technologies.

2.8 Our ability to safeguard businesses and communities from cyber threats hinges upon our ability both to nurture technological and human capabilities, and to recognise and address complex risks on a macro scale. By prioritising secure by design, skill development, and targeted measures which improve resilience across all sectors of our economy, we seek to pave the way for a more secure cyber landscape in the UK.

[16] Capability Hardware Enhanced RISC Instructions (CHERI), University of Cambridge, Department of Computer Science and Technology.

Chapter 3: How organisations procuring software should use this Code of Practice

3.1 Businesses and other organisations can use this Code of Practice for Software Vendors to better understand what they can reasonably expect of their software suppliers. This awareness can help customer organisations to make appropriate requests of their suppliers during the procurement process, and to establish a clear understanding of customer and vendor security and resilience responsibilities throughout the lifetime of a product.

During the procurement process

3.2 Organisations procuring software can refer to this Code of Practice and supporting materials to inform their understanding of the risks associated with the software they are purchasing. They can use that understanding and the supporting materials which will be provided by the UK Government to request reasonable measures are taken by their software suppliers to ensure the security and resilience of the software they are purchasing. The technical controls have been developed in line with the principles and provisions within the Code of Practice and can be used by procuring organisations to ask the right questions about their suppliers' security and resilience practices.

3.3 The Government is also developing further policy to support better risk management during the procurement of software. Amongst other things, this may include standardised contractual clauses, an assurance or certification mechanism, or further guidance or education interventions on software security for non-cyber specialists such as procurement teams.

Supply chain risk management practices and responsibilities

3.4 The Code of Practice for Software Vendors focuses on the cyber security responsibilities of organisations developing and selling software, which includes making sure that the products themselves are secure, and that adequate information is provided to customer organisations to enable effective risk management. Vendors should fulfil these responsibilities, however organisations procuring and using those products and services also have certain responsibilities for the resilience and security of their own organisations. They are also responsible for using the information that vendors provide as part of their own risk management processes. Organisations procuring software are responsible for understanding their own risk exposure, and for taking an appropriate risk-based approach to identifying the products and services that meet their security needs.

3.5 Organisations procuring software should ensure they do the following:

- **Follow the Cyber Governance Code of Practice**[17]
    - The Cyber Governance Code of Practice brings together the critical governance areas that directors need to take ownership of in one place, in a form that is simple to engage with, for organisations of all sizes.
    - It establishes cyber security issues as a key focus for all organisations, putting it on an equal footing with other principal risks, such as financial and legal. As part of this, the code recommends that directors set out clear roles and responsibilities across their organisations, boosting protections for customers and safeguarding their ability to operate safely and securely.

[17] Cyber Governance Code of Practice: call for views, DSIT, 2024.

- **Take effective decisions at board level on the level of cyber security risk that is acceptable to the organisation**.
    - This includes understanding what information and assets your organisation holds that would need to be protected when dealing with suppliers. See NCSC supply chain security guidance[18] for further advice.
- **Identify suitable mechanisms to assess and review suppliers commensurate to their level of risk and how that compares to the level of risk that is acceptable to the procuring organisation.**
    - This could include referring to this Code of Practice for Software Vendors and/or other Codes of Practice produced by DSIT in relation to different types of digital products (e.g. IoT and AI).
- **Bear in mind that different sectors and software functions will have different security needs.**
    - These will need to be reflected in the organisation's internal security processes as well as their procurement processes and negotiations with suppliers.
    - For example, organisations classed as Operators of Essential Services in CNI sectors should implement the NCSC's Cyber Assessment Framework (CAF) as part of their responsibilities under the NIS regulations.

[18] Supply chain security guidance, NCSC, 2019 (updated, 2023).

Chapter 4: Voluntary Code of Practice for Software Vendors

4.1 The Code of Practice for Software Vendors contains 21 provisions split over 4 principles. Within each principle, provisions are described as either actions that senior leadership "shall" do, or actions that they "should" do. "Shall" indicates a requirement for the voluntary Code, and "should" indicates a recommendation for the voluntary Code.

4.2 Provisions classified as "shalls" can reasonably be expected of any organisations developing and selling software, regardless of size or maturity. Those classified as "shoulds" are reasonably to be expected of organisations developing and selling software, but there is a recognition that these may be more complex to carry out or demonstrate. It is expected that organisations would work towards achieving the "shoulds" even if immediate implementation is not possible.

Principle 1: Secure design and development

This principle is to ensure that the software product or service is appropriately secure when provided.

The Senior Responsible Officer in vendor organisations **shall** do the following**:**

1.1 Ensure the organisation follows an established secure development framework.

1.2 Ensure the organisation understands the composition of their software products and services and that risks linked to the ingestion and maintenance of third-party components, including open-source components, are assessed throughout the lifecycle.

1.3 Ensure the organisation has a clear process for testing software before distribution.

1.4 Ensure that the organisation follows secure by default principles[19] throughout the development lifecycle of the product.

The Senior Responsible Officer in vendor organisations **should** do the following:

1.5 Ensure secure by design principles[20] are followed throughout the development process.

1.6 Encourage the use of appropriate security tools and technologies to make sure that the default options throughout development and distribution are secure.

[19] Technology that is Secure by Default has the best security it can without you ever knowing it's there, or having to turn it on. Further detail on secure by default principles can be found here: https://www.ncsc.gov.uk/information/secure-default

[20] "Secure by design" means that software products and services are built in a way that reasonably protects against malicious cyber actors successfully gaining access. This includes identifying the key risks and building protections into product design.

Principle 2: Build environment security

This principle is to 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 Officer in vendor organisations **shall** do the following:

2.1 Ensure the build environment is protected against unauthorised access.

The Senior Responsible Officer in vendor organisations **should** do the following:

2.2 Ensure changes to the environment are controlled and logged.

2.3 Ensure you are using a build pipeline you trust.

Principle 3: Secure deployment and maintenance

This principle is to ensure that the product or service remains secure throughout its lifetime, to minimise the likelihood and impact of vulnerabilities.

The Senior Responsible Officer in vendor organisations **shall** do the following:

3.1 Ensure that software is distributed securely to customers.

3.2 Ensure the organisation implements and publishes an effective vulnerability disclosure process.

3.3 Ensure the organisation has processes in place for proactively detecting and managing vulnerabilities in software components it uses and software it develops, including a documented process to assess the severity of vulnerabilities and prioritise responses.

3.4 Ensure that vulnerabilities are appropriately reported to the relevant parties.

3.5 Ensure the organisation provides timely security updates, patches and notifications to its customers.

Senior leaders in vendor organisations **should** do the following:

3.6 Make a public affirmation that the organisation would welcome security researchers to test software products and services provided by the organisation as part of its vulnerability disclosure process.

Principle 4: Communication with customers

This principle is to ensure that vendor organisations provide sufficient information to customers to enable effective risk and incident management.

The Senior Responsible Officer in software vendor organisations **shall** do the following:

4.1 Ensure the organisation provides information to the customer, in an accessible way, specifying the level of support and maintenance provided for the software product/ service being sold.

4.2 Ensure the organisation provides at least 1 year's notice to customers, in an accessible way, of when the product or service will no longer be supported or maintained by the vendor.

4.3 Ensure information is made available to customers in an appropriate and timely manner about notable incidents that may cause significant impact to customer organisations.

The Senior Responsible Officer in vendor organisations **should** do the following:

4.4 Ensure that high level information about the security and resilience standards, frameworks, organisational commitments and procedures followed by the organisation is made available to customers.

4.5 Ensure that the organisation proactively supports affected customers during and following a cyber security incident to contain and mitigate the impacts of an incident. How this would be done should be documented and agreed in contracts with the customer.

4.6 Provide customer organisations with guidance on how to use, integrate, and configure the software product or service securely.

Monitoring and evaluation

4.3 The Code of Practice for Software Vendors has been developed to allow flexibility through a principles-based approach. The implementation guidance will provide specialist teams in software vendor organisations with guidance on how to identify the most suitable implementation option for their organisations, allowing space for innovative security solutions. This also allows organisations to consider the cost and benefits of different methods and tools for meeting the outcomes outlined in the principles and technical controls. This flexibility was of utmost importance to the industry partners involved in the co-design process and is central to Government's pro-innovation approach to cyber security and resilience policy.

4.4 We are seeking feedback through this call for views on a voluntary Code of Practice. Related to this Code of Practice, Government is developing further tools and guidance aimed at supporting organisations procuring software to build the principles and provisions of this Code of Practice into their procurement processes. These interventions will help to generate market demand for best practices by encouraging those purchasing software to ask their suppliers to meet the expectations laid out in this voluntary Code of Practice.

4.5 Future interventions will include standardised contractual clauses that organisations can use in their contracts with software suppliers, and work is ongoing to explore options for accreditation or assurance against this Code of Practice and to explore demand by targeting particular customer groups, such as through government procurement. The Government is also exploring further support for software vendors, including more specific guidance on more complex areas of software security and working with others across Government to bolster the skills pipeline to software development and security. Further detail on the broader package of

software resilience and security information is outlined in the Government response on software resilience and security.[21]

4.6 DSIT will review two aspects of the code, its efficacy and uptake. The Government recognises that efficacy is difficult to measure, but best efforts will be made to collect information on whether there is an improvement in the security of software. To measure uptake there will need to be a review or survey of software providers and software procurers to understand whether the code being voluntary has the required reach to remain voluntary. These will be monitored and evaluated to assess the need for further interventions, such as regulation, in the two years post implementation.

[21] Government response to the call for views on software resilience and security for businesses and organisations, DSIT, 2024.

Chapter 5: Supporting materials

5.1 The Government intends to publish technical controls and implementation guidance alongside the Code of Practice for Software Vendors. Whilst senior leaders remain accountable for ensuring the principles of the Code are followed within their organisations, the technical controls and implementation guidance are designed to provide additional support for teams responsible for delivering the provisions of the Code.

Technical controls

5.2 The technical controls set out the minimum set of actions that a software vendor needs to demonstrate to provide confidence in the software resilience of their product or service. Software vendor organisations would be able to use these technical controls to demonstrate that they are compliant with the provisions of the Code of Practice. They bring together what is widely considered good practice in software development and should be achievable for organisations of any size and sector.

5.3 The controls are objective and outcome-focused, giving organisations the flexibility to innovate and implement security solutions appropriate for their products and services. Implementation of these controls will reduce the vulnerabilities in software products, providing basic resilience against the most prevalent threats and vulnerabilities.

5.4 Demonstration against these controls will make it easier for buyers to gain confidence that the software products and services they select and operate will not increase the risk of a successful cyber-attack. Technical controls are provided for all provisions designated as “shalls” in the Code of Practice.

5.5 The technical controls are as follows:

Code of Practice Provision	**Technical controls**
Principle 1: Secure design & development	
1.1 Ensure the organisation follows an established secure development framework.	• Follow a secure development framework. *Conformance to a Secure Development Lifecycle (SDLC) Framework is documented. Detail on what the SDLC should include as a minimum is provided in the accompanying implementation guidance.*
1.2 Ensure the organisation understands the composition of their software products and services and that risks liked to the ingestion and maintenance of third-party components, including open-source components, are assessed throughout the lifecycle.	• Hold an inventory of third-party components and regularly check them for known vulnerabilities. *The organisation demonstrates an understanding of the composition and provenance of its products and services, including third-party components. These shall be risk assessed on a regular basis throughout the lifecycle of the product.*
1.3 Ensure the organisation has a clear process for testing software before distribution.	• Have a defined test plan in place. *An unambiguous test plan exists for all requirements with full coverage of the code base. Testing takes place on a regular basis.*

1.4 Ensure that the organisation follows secure by default principles throughout the development lifecycle of the product.	☐ Mandate multi-factor authentication for privileged users of the product or service. *Software products and services are deployed with multi-factor authentication by default for privileged users.* ☐ No default passwords *Software products and services are deployed with passwords that are unique and not resettable to a default value.* ☐ Validate input data. *Data input via Application Programming Interfaces (APIs) or between networks in services and products are validated.* ☐ Securely store credentials and sensitive data *Any credentials are stored securely within/by services and products. Hard-coded credentials in software are not accepted.*
Principle 2: Build environment security	
2.1 Ensure the build environment is protected against unauthorised access.	☐ Implement identity and access management in development and build environments. *Appropriate identify and access management policies and processes are in place.*
	☐ Mandate multi-factor authentication for developers. *Systems require a developer to enrol for multi-factor authentication to successfully enable their account.*
Principle 3: Distribution security & maintenance	
3.1 Ensure that software is distributed securely to customers.	☐ Only distribute software and updates through trusted channels. *The software product or service, and any updates and patches to that software, are provided in a manner that allows customers to verify the provenance and integrity of the software.*
3.2 Ensure the organisation implements and publishes an effective vulnerability disclosure process to support a transparent and open culture within the organisation.	☐ Implement a vulnerability disclosure policy. *The organisation publishes a vulnerability disclosure policy which provides a public point of contact in order that security researchers and others are able to report issues. Disclosed vulnerabilities are then reported to relevant parties (outlined in the implementation guidance) and acted on in a timely manner.*

3.3 Ensure the organisation has processes in place for proactively detecting and managing vulnerabilities in software components it uses and software it develops, including a documented process to assess the severity of vulnerabilities and prioritise responses.	□ Proactively detect and manage vulnerabilities. *The organisation has in place processes to continually identify vulnerabilities, act on them and report them to relevant parties in a timely manner.*
3.4 Ensure that vulnerabilities are appropriately reported to the relevant parties.	
3.5 Ensure the organisation provides timely security updates, patches and notifications to its customers.	□ Provide timely security updates and patches *Timely updates and patches are provided to customers at no extra cost.*
Principle 4: Communication with customers	
4.1 Ensure the organisation provides information, in an accessible way, specifying the level of support and maintenance provided for the software product/ service being sold.	□ Publish an end-of-life policy *An end-of-life policy is published which explicitly states the minimum length of time for which a product/service will receive software updates and the reasons for the length of the support period.*
4.2 Ensure the organisation provides at least 1 year's notice to customers, in an accessible way, of when the product or service will no longer be supported or maintained by the vendor.	
4.3 Ensure information is made available to customers in an appropriate and timely manner about notable incidents that may cause significant impact to customer organisations.	□ Publish an incident response plan/policy. *An incident response policy is published, including a point of contact.*

Implementation guidance

5.6 Implementation guidance will be provided to guide relevant working level teams within software vendor organisations in how to implement the principles of the Code of Practice and demonstrate the technical controls.

5.7 The implementation guidance will be based on technical guidance developed by experts in the NCSC and its partners. It will be designed to help software vendors understand how they can implement the controls in the most effective way and will signpost relevant resources including existing guidance and standards that can be used. As well as promoting a culture of transparency to support their own customers to understand their cyber security risks, we expect vendors to use this guidance against the context of their own risk assessments and risk management processes and governance. By doing this, vendors can determine the correct coverage and most appropriate way to achieve the outcomes in the Code of Practice for their organisation.

5.8 For each provision of the Code of Practice for Software Vendors, the implementation guidance will provide detail on the following

- **Objectives:** What a good outcome looks like.
- **Description:** Further detail on the provision and technical control and the context in which they should be implemented, including a more detailed explanation of the risks and threats and potential consequences if these are not mitigated.
- **Implementation options:** Measures that vendors can put in place to achieve the objectives.
- **Risk assessment:** Questions to support vendors in understanding how to make the best decisions for mitigating risks in their organisations.

- **Signposts:** Links to existing resources such as guidance and standards.

5.9 A snapshot example of what this implementation guidance will look like for parts of principle 1 is provided in Annex B.

Chapter 6: How to respond to the call for views

6.1 Please take this opportunity to shape our future work by responding to the online survey. To help us analyse the responses, please use the online consultation system wherever possible.

6.2 If you are unable to submit your response using the online survey, you can also submit an email response to cyber.resilience.consultations@dsit.gov.uk or a hard copy by post to:

Code of Practice for Software Vendors call for views
Cyber Resilience Team – 4/48
DSIT
100 Parliament Street
London
SW1A 2BQ

6.3 The call for views will be open for 8 weeks, from the 15th May 2024. The closing date for responses is 11.45pm on 10th July 2024.

6.4 When providing your response, you are also able to provide contact details if you are open to the department seeking further information or clarification on your views.

6.5 Should you require access to the consultation in Welsh or in an alternative format (e.g. Braille, large font or audio) please contact us at cyber.resilience.consultations@dsit.gov.uk

6.6 The information you provide will be used to shape future policy development and may be shared between UK Government departments and agencies for this purpose. Personal information will be removed in such instances. Copies of responses, in full or in summary, may be published after the call for views closing date on the Department's website. You can also read the privacy notice associated with this call for iews.

Freedom of information

6.7 Information provided in the course of this call for views, including personal information, may be published or disclosed in accordance with access to information regimes, primarily the Freedom of Information Act 2000 (FOIA) and the Data Protection Act 2018 (DPA).

6.8 The Department for Science, Innovation and Technology will process your personal data in accordance with the DPA and, in the majority of circumstances, this will mean that your personal data will not be disclosed to third parties. This consultation follows the UK Government's consultation principles.

6.9 If you want the information you provide to be treated confidentially, please be aware that, in accordance with the FOIA, public authorities are required to comply with a statutory Code of Practice which deals, amongst other things, with obligations of confidence. In view of this, it would be helpful if you could explain to us why you wish that information to be treated confidentially. If we receive a request for disclosure of that information, we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances.

Annex A: Full Code of Practice

Principle 1: Secure design and development

This principle ensures that the software product or service is appropriately secure when provided.

The Senior Responsible Officer in vendor organisations **shall** do the following**:**

1.1 Ensure the organisation follows an established secure development framework.

1.2 Ensure the organisation understands the composition of their software products and services and that risks linked to the ingestion and maintenance of third-party components, including open-source components, are assessed throughout the lifecycle.

1.3 Ensure the organisation has a clear process for testing software before distribution.

1.4 Ensure that the organisation follows secure by default principles throughout the development lifecycle of the product.

The Senior Responsible Officer in vendor organisations **should** do the following:

1.5 Ensure secure by design principles are followed throughout the development process.

1.6 Encourage the use of appropriate security tools and technologies to make sure that the default options throughout development and distribution are secure.

Principle 2: Build environment security

This principle ensures 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 Officer in vendor organisations **shall** do the following:

2.1 Ensure the build environment is protected against unauthorised access.

The Senior Responsible Officer in vendor organisations **should** do the following:

2.2 Ensure changes to the environment are controlled and logged.

2.3 Ensure you are using a build pipeline you trust.

Principle 3: Secure deployment and maintenance

This principle ensures that the product or service remains secure throughout its lifetime, to minimise the likelihood and impact of vulnerabilities.

The Senior Responsible Officer in vendor organisations **shall** do the following:

3.1 Ensure that software is distributed securely to customers.

3.2 Ensure the organisation implements and publishes an effective vulnerability disclosure process.

3.3 Ensure the organisation has processes in place for proactively detecting and managing vulnerabilities in software components it uses and software it develops, including a documented process to assess the severity of vulnerabilities and prioritise responses.

3.4 Ensure that vulnerabilities are appropriately reported to the relevant parties.

3.5 Ensure the organisation provides timely security updates, patches and notifications to its customers.

Senior leaders in vendor organisations **should** do the following:

3.6 Make a public affirmation that the organisation would welcome security researchers to test software products and services provided by the organisation as part of its vulnerability disclosure process.

Principle 4: Communication with customers

This principle ensures that vendor organisations provide sufficient information to customers to enable effective risk and incident management.

Senior Responsible Officers in software vendor organisations **shall** do the following:

4.1 Ensure the organisation provides information to the customer, in an accessible way, specifying the level of support and maintenance provided for the software product/ service being sold.

4.2 Ensure the organisation provides at least 1 year's notice to customers, in an accessible way, of when the product or service will no longer be supported or maintained by the vendor.

4.3 Ensure information is made available to customers in an appropriate and timely manner about notable incidents that may cause significant impact to customer organisations.

Senior Responsible Officers in vendor organisations **should** do the following:

4.4 Ensure that high level information about the security and resilience standards, frameworks, organisational commitments and procedures followed by the organisation is made available to customers.

4.5 Ensure that the organisation proactively supports affected customers during and following a cyber security incident to contain and mitigate the impacts of an incident. How this would be done should be documented and agreed in contracts with the customer.

4.6 Provide customer organisations with guidance on how to use, integrate, and configure the software product or service securely.

Annex B: Implementation guidance example

Below is an example of how the implementation guidance will be designed and structured. Work on the accompanying implementation guidance is ongoing, but the guidance will be published alongside the Code of Practice and technical controls detailed above.

Principle 1: Secure design & development

Good security engineering means building technologies that remain usable and resilient throughout their lifetime, even in the face of a cyber attack. Achieving this outcome needs to begin in the design and development phase so that user need and security are baked into the product or service. Ensuring that engineering processes and practices minimise both the likelihood and possible impact of a security compromise plays an essential part in gaining assurance in vendor competence and the products and services producing.

Developers are not necessarily security experts and the security toolbox available to them can make it difficult to navigate cyber security technical complexities, leading to implementation mistakes that could have been avoided. The selection of the toolbox available to developers should therefore consider its usability and maintenance, as well as functionality and cost. This support to developers can be through access to experts, training, positive security cultures and processes as well as the availability of up-to-date tools.

By implementing the provisions in the Software Vendor Code of Practice, not only will the software product or service be more cyber resilient by default, but it will also be more stable and easier to maintain.

1.1 Ensure the organisation follows an established secure development framework.

Technical control: Follow a secure development framework.

Using a secure development framework across your engineering projects will provide a consistent and repeatable way to support developers to ensure security has been considered at the right time. They are proactive approaches to building security into a product or service that incorporate people, processes and technology aspects. By not following a secure development framework, important cyber security decisions may #be missing# and inevitably will need to be bolted on at the end of the development process and/or cause more cost during deployment.

You may wish to publish a description of which framework you are using, and which controls have been implemented. You should be able to demonstrate conformance to a secure development framework across your development and deployment activities.

A good secure development framework should include the following topics as a minimum:

- **Threat modelling** – techniques used to understand how the product or service might be attacked or otherwise fail.
- **Requirements capture** – understanding and recording security and user needs.
- **Governance & roles** – how the approach to ensuring secure design & development is controlled and directed.
- **Test strategy** – consistent approaches to verification that have sufficient rigour and coverage.

- **Data management** – understanding what data exists and how it should be appropriately protected throughout its lifecycle.
- **Configuration management** – consistent approaches to tracking changes, implementing version control, and enabling reproducibility.

Which secure development framework you decide to use is a business decision based on what will fit best with the culture and existing processes of your organisation. There are many secure development frameworks available "off-the-shelf", examples include:

- **NIST Secure Software Development Framework:** https://csrc.nist.gov/projects/ssdf[22]
- **Microsoft Security Development Lifecycle:** https://www.microsoft.com/en-us/securityengineering/sdl[23]
- **OWASP Secure Software Development Lifecycle:** https://owasp.org/www-pdf-archive/Jim_Manico_(Hamburg)_-_Securiing_the_SDLC.pdf & The Model (owaspsamm.org)[24]
- **Cisco Secure Development Lifecycle:** https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-secure-development-lifecycle.pdf[25]

Useful links:
CyBoK for Secure Software Lifecycle[26]
Securing the Software Supply Chain: Recommended Practices Guide for Developers (cisa.gov)[27]
https://www.ncsc.gov.uk/collection/risk-management/threat-modelling[28]
https://www.ncsc.gov.uk/collection/risk-management/cyber-security-governance[29]
https://www.ncsc.gov.uk/information/gdpr[30]
https://www.security.gov.uk/guidance/secure-by-design/principles/[31]
https://www.gov.uk/service-manual[32]

1.2 Ensure the organisation understands the composition of their software products and services and that risks linked to the ingestion and maintenance of third-party components, including open-source components, are assessed throughout the lifecycle.

Technical control: Hold an inventory of third-party components and regularly check them for known vulnerabilities.

[22] Secure Software Development Framework, NIST, 2022.
[23] Microsoft Security Development Lifecycle, Microsoft.
[24] OWASP Securing the software development lifecycle, OWASP.
[25] Cisco Secure Development Lifecycle, Cisco, 2024.
[26] CyBoK for Secure Software Lifecycle, NCSC 2019.
[27] Securing the software supply chain, CISA, 2022.
[28] Risk management, NCSC, 2023.
[29] Risk management, NCSC, 2023.
[30] GDPR, NCSC, 2018.
[31] Secure by Design Principles, NCSC, 2024.
[32] Government service manual, UK Government Service Manual Team.

Often, software vendors will rely upon suppliers and third-party libraries (for example as an aspect of their activities to leverage existing Application Programming Interface (API) capabilities) to deliver their products and services. These dependencies can be complex and effectively securing the supply chain can be hard because vulnerabilities can be inherent, introduced or exploited at any point within it.

In recent years there has been a significant increase in the number of cyber-attacks resulting from vulnerabilities within the supply chain.[33] These attacks can result in devastating, expensive and long-term ramifications for affected organisations, their supply chains, and customers.

In software development, dependency chains relate to the set of packages (including internal, direct third-party and transitive dependencies) that a software product or service requires to function. An attacker can take advantage of these dependencies and a successful attack can result in the execution of malicious code from an attacker-controlled package or by exploiting a flaw that has been introduced in error by the original developers.

To mitigate these risks, as a software vendor, the first step is to know what is in your software supply chain. You should understand what components you use in all your products or services. That inventory should be documented, used to ensure that security requirements are being met and that they are being regularly checked for known vulnerabilities and used for any incident management events that may occur.

You should ensure that:

- You capture the third-party components that your product is comprised of. Your software product or service will be comprised of many third-party components: either internally generated or external commercial components. Third party components may come from a supplier with whom you have a contractual relationship, or they may be Free Open-Source Software (FOSS). Selection of these components will initially be focussed on capability and ease of integration - however, it is important to consider security attributes such as provenance of the software, frequency of updates, how many maintainers, and geographic location of contributors. An inventory can take any format that suits the processes and culture of the organisation. A Supply Chain Bill of Materials (SBOM) is an approach that can be used for this purpose.

- You share security requirements with your suppliers. Having an inventory of all your integrated third-party components is a crucial first step, but it is not enough on its own to ensure your supply chain is secure. Your inventory should be validated and regularly updated as needed.

If required, you should be able to share your inventory with your customers so that they can be provided with a validated and up-to-date list of all the third-party components in your software product and service for their own supply chain security needs. Considering the best format to enable your developers and customers to be able to use the information effectively is an important consideration in how you record and document your third-party components inventory.

[33] Supply Chain Security Guidance, NCSC 2023.

- The components are regularly checked for vulnerabilities for the lifespan of the product. Not all your components will be provided through a contractual arrangement by a supplier who provides you with confidence that they have supply chain security measures in place. Therefore, to ensure your supply chain is secure, regular testing of all your third-party components and dependencies needs to be in place. You should be able to demonstrate that adequate testing (more explanation on what this means can be found in Section 1.3) has been carried out on each component.

If a new vulnerability or attack be discovered outside of your regular testing cadence, you should be able to prioritise and test for these in a timely way to minimise the risk of the vulnerability being exploited.

- You carry out any remediation required in a timely way. Hopefully, vulnerabilities that are possible to exploit will not be discovered but it is an inevitable part of software development and cyber security that they will. Responding to these instances, and effectively communicating with others, is as important as discovery. You should carry out any remediation required (e.g. developing and issuing updates and patches) in a timely way and report these to your customers. More details on this can be found in Section 4.

Useful links:
Securing the Software Supply Chain: Recommended Practices Guide for Developers (cisa.gov)[34]
https://www.ncsc.gov.uk/collection/supply-chain-security/third-party-software-providers[35]
https://www.ncsc.gov.uk/collection/assess-supply-chain-cyber-security[36]

Several specifications define the format of an SBOM: 1. The Linux Foundation Projects "Software Package Data eXchange (SPDX)." 2. OWASP "CycloneDX." 3. NIST "Software Identification (SWID) tags."

[34] Securing the software supply chain, CISA, 2022.
[35] Supply Chain Security Guidance, NCSC 2023.
[36] How to assess and gain confidence in your supply chain cyber security, NCSC, 2022.

Annex C: Call for views Survey Questionnaire

Demographics

- Q1.Are you responding as an individual or on behalf of an organisation?
    - Individual
    - Organisation

- Q2.[if individual] Which of the following statements best describes you?
    - Cyber security/IT professional
    - Professional
    - Software developer
    - Software tester
    - Senior leader in a company
    - Consumer expert
    - Academic
    - Interested member of the public
    - Government official (including regulator)
    - Other [if selected, then a please specify text box appears]

- Q3. [if Q1 = organisation] Which of the following statements best describes your organisation? Select all that apply [check boxes]
    - Organisation/Business
        - That is involved in the sale or development of software
        - That develops standard software for the business market
        - That develops standard software for the consumer market
        - That develops bespoke software for clients
        - That plans to develop software
        - That has no plans to produce software
        - That resells software (with or without value added features
    - A organisation that procures software
    - A cyber security provider
    - An educational institution
    - Government
    - Other [if selected, then a please specify text box appears]

- Q4 [if Q3 = “Organisation/Business that is involved in the sale or development of software”] Which of these statements apply to your organisation? Select all that apply.
    - That develops standard software for the business market
    - That develops standard software for the consumer market
    - That develops bespoke software for clients
    - That plans to develop software
    - That has no plans to produce software
    - That resells software (with or without value added features)

- Q5.[if Q1 = organisation], What is the size of your organisation?
    - Micro (fewer than 10 employees)
    - Small (10-49 employees)
    - Medium (50-499 employees)

    - Large (500+ employees)

- Q6.[if Q1 = individual], Where are you based?
    - United Kingdom
    - Europe (excluding the United Kingdom)
    - North America
    - South America
    - Africa
    - Asia
    - Oceania (Australia and surrounding countries)
    - Other [if selected, then a please specify text box appears]

- Q7.[if Q1= organisation], Where is your organisation headquartered?
    - United Kingdom
    - Europe (excluding the United Kingdom)
    - North America
    - South America
    - Africa
    - Asia
    - Oceania (Australia and surrounding countries)
    - Other [if selected, then a please specify text box appears]

Questions relating to Chapter 1: Introduction

- Q8: Do you agree with any of the following statements? [checkboxes]
    - The market is currently operating with appropriate levels of secure by design principles.
    - The Government should produce guidance that will show software vendors what “good” cyber security looks like.
    - There should be an assurance / certification scheme for software.
    - There should be mandated security regulations for all software.
- Q9: Are there any types of organisations for which this Code of Practice would not be suitable? [open text]
- Q10: Do you agree that senior leaders in software vendor organisations should be the target audience of this Code of Practice?
    - Yes
    - No
    - Don’t know

Questions relating to Chapter 3: How organisations procuring software should use this Code of Practice

- Q11: If one was available, how likely would your organisation be to use to a voluntary Code of Practice for software vendors to inform
    - a) Procurement?
        - Very likely
        - Likely
        - Neutral
        - Not likely
        - Definitely won’t use
        - Don’t know
    - b) Supplier management processes?
        - Very likely

- Likely
- Neutral
- Not likely
- Definitely won't use
- Don't know

Questions on Chapter 4: Voluntary Code of Practice for Software Vendors

The next questions are going to ask you specifically about the Code of Practice that has been designed and proposed by DSIT. The questions will be ~~asked about~~focused on individual actions asked by the Code.

[Each principle to be displayed on one page.]

Principle 1: Secure design and development
The Senior Responsible Officer in vendor organisations **shall** do the following:

- Ensure the organisation follows an established secure development framework.

- Q12: Do you agree with this provision?
  - Yes – I think this action should be included as a "shall"
  - Yes – I think this action should be included as a "should"
  - No – I think this action should not be included in this Code of Practice
  - I don't know

Principle 1: Secure design and development
The Senior Responsible Officer in vendor **organisations shall** do the following:

- Ensure the organisation understands the composition of their software products and services and that risks linked to the ingestion and maintenance of third-party components, including open-source components, are assessed throughout the lifecycle.

- Q13: Do you agree with this action?
  - Yes – I think this action should be included as a "shall"
  - Yes – I think this action should be included as a "should"
  - No – I think this action should not be included in this Code of Practice
  - I don't know

Principle 1: Secure design and development
The Senior Responsible Officer in vendor organisations **shall** do the following:

- Ensure the organisation has a clear process for testing software before distribution.

- Q14: Do you agree with this action?
  - Yes – I think this action should be included as a "shall"
  - Yes – I think this action should be included as a "should"
  - No – I think this action should not be included in this Code of Practice
  - I don't know

Principle 1: Secure design and development
The Senior Responsible Officer in vendor organisations **shall** do the following:

- Ensure that the organisation follows secure by default principles throughout the development lifecycle of the product.

- Q15: Do you agree with this action?
  - Yes – I think this action should be included as a "shall"
  - Yes – I think this action should be included as a "should"
  - No – I think this action should not be included in this Code of Practice
  - I don't know

Principle 1: Secure design and development

The Senior Responsible Officer in vendor organisations **should** do the following:

- Ensure secure by design principles are followed throughout the development process.

- Q16: Do you agree with this action?
  - Yes – I think this action should be included as a “shall”
  - Yes – I think this action should be included as a “should”
  - No – I think this action should not be included in this Code of Practice
  - I don’t know

Principle 1: Secure design and development

The Senior Responsible Officer in vendor organisations **should** do the following:

- Encourage the use of appropriate security tools and technologies to make sure that the default options throughout development and distribution are secure.

- Q17: Do you agree with this action?
  - Yes – I think this action should be included as a “shall”
  - Yes – I think this action should be included as a “should”
  - No – I think this action should not be included in this Code of Practice
  - I don’t know

We have asked you questions on the following provisions of principle 1:

Principle 1: Secure design and development

This principle ensures that the product or service is appropriately secure when provided.

The Senior Responsible Officer in vendor organisations **shall** do the following**:**

1.1 Ensure the organisation follows an established secure development framework.

1.2 Ensure the organisation understands the composition of their software products and services and that risks linked to the ingestion and maintenance of third-party components, including open-source components, are assessed throughout the lifecycle.

1.3 Ensure the organisation has a clear process for testing software before distribution.

1.4 Ensure that the organisation follows secure by default principles throughout the development lifecycle of the product.

The Senior Responsible Officer in vendor organisations **should** do the following:

1.5 Ensure secure by design principles are followed throughout the development process.

1.6 Encourage the use of appropriate security tools and technologies to make sure that the default options throughout development and distribution are secure.

- Q18: Do you think there is anything missing from this Principle? If so, what? [free text]
- Q19: Do you have any other comments or feedback relating to this Principle? [free text]

Principle 2: Build environment security

Senior Responsible Officers in vendor organisations **shall** do the following:

- Ensure the build environment is protected against unauthorised access.

- Q20: Do you agree with this action?
  - Yes – I think this action should be included as a “shall”
  - Yes – I think this action should be included as a “should”
  - No – I think this action should not be included in this Code of Practice
  - I don’t know

Principle 2: Build environment security

Senior Responsible Officers in vendor organisations **should** do the following:

- Ensure changes to the environment are controlled and logged.

- Q21: Do you agree with this action?
  - Yes – I think this action should be included as a “shall”
  - Yes – I think this action should be included as a “should”
  - No – I think this action should not be included in this Code of Practice
  - I don’t know

Principle 2: Build environment security

Senior Responsible Officers in vendor organisations **should** do the following:

- Ensure you are using a build pipeline you trust.

- Q22: Do you agree with this action?
  - Yes – I think this action should be included as a “shall”
  - Yes – I think this action should be included as a “should”
  - No – I think this action should not be included in this Code of Practice
  - I don’t know

Principle 2: Build environment security

This principle ensures that the appropriate steps are taken to minimise the risk of build environments becoming compromised and protect the integrity and quality of the software.

Senior Responsible Officers in vendor organisations **shall** do the following:

2.1 Ensure the build environment is protected against unauthorised access.

Senior Responsible Officers in vendor organisations **should** do the following:

2.2 Ensure changes to the environment are controlled and logged.

2.3 Ensure you are using a build pipeline you trust.

- Q23: Do you think there is anything missing from this Principle? If so, what? [free text]
- Q24: Do you have any other comments or feedback relating to this Principle? [free text]

Principle 3: Secure deployment and maintenance

The Senior Responsible Officer in vendor organisations **shall** do the following:

1. Ensure that software is distributed securely to customers.

- Q25: Do you agree with this action?
  - Yes – I think this action should be included as a “shall”
  - Yes – I think this action should be included as a “should”
  - No – I think this action should not be included in this Code of Practice
  - I don’t know

Principle 3: Secure deployment and maintenance

The Senior Responsible Officer in vendor organisations **shall** do the following:

2. Ensure the organisation has processes in place for proactively detecting and managing vulnerabilities in software components it uses and software it develops, including a documented process to assess the severity of vulnerabilities and prioritise responses.

- Q26: Do you agree with this action?

- Yes – I think this action should be included as a “shall”
- Yes – I think this action should be included as a “should”
- No – I think this action should not be included in this Code of Practice
- I don’t know

Principle 3: Secure deployment and maintenance

TThe Senior Responsible Officer in vendor organisations **shall** do the following:

3. Ensure the organisation implements and publishes an effective vulnerability disclosure process.

- Q27: Do you agree with this action?
  - Yes – I think this action should be included as a “shall”
  - Yes – I think this action should be included as a “should”
  - No – I think this action should not be included in this Code of Practice
  - I don’t know

Principle 3: Secure deployment and maintenance

The Senior Responsible Officer in vendor organisations **shall** do the following:

4. Ensure the organisation provides timely security updates, patches and notifications to its customers.

- Q28 Do you agree with this action?
  - Yes – I think this action should be included as a “shall”
  - Yes – I think this action should be included as a “should”
  - No – I think this action should not be included in this Code of Practice
  - I don’t know

Principle 3: Secure deployment and maintenance

The Senior Responsible Officer in vendor organisations **shall** do the following:

5. Ensure that vulnerabilities are appropriately reported to the relevant parties.

- Q29: Do you agree with this action?
  - Yes – I think this action should be included as a “shall”
  - Yes – I think this action should be included as a “should”
  - No – I think this action should not be included in this Code of Practice
  - I don’t know

Principle 3: Secure deployment and maintenance

Senior leaders in vendor organisations **should** do the following:

6. Make a public affirmation that the organisation would welcome security researchers to test software products and services provided by the organisation as part of its vulnerability disclosure process.

- Q30: Do you agree with this action?
  - Yes – I think this action should be included as a “shall”
  - Yes – I think this action should be included as a “should”
  - No – I think this action should not be included in this Code of Practice
  - I don’t know

Principle 3: Secure deployment and maintenance

This principle ensures that the product or service remains secure throughout its lifetime, to minimise the likelihood and impact of vulnerabilities.

The Senior Responsible Officer in vendor organisations **shall** do the following:

3.1 Ensure that software is distributed securely to customers.

3.2 Ensure the organisation implements and publishes an effective vulnerability disclosure process.

3.3 Ensure the organisation has processes in place for proactively detecting and managing vulnerabilities in software components it uses and software it develops, including a documented process to assess the severity of vulnerabilities and prioritise responses.

3.4 Ensure that vulnerabilities are appropriately reported to the relevant parties.

3.5 Ensure the organisation provides timely security updates, patches and notifications to its customers.

Senior leaders in vendor organisations should do the following:

3.6 Make a public affirmation that the organisation would welcome security researchers to test software products and services provided by the organisation as part of its vulnerability disclosure process.

- Q31: Do you think there is anything missing from this Principle? If so, what? [free text]
- Q32: Do you have any other comments or feedback relating to this Principle? [free text]

Principle 4: Communication with customers

Senior Responsible Officers in software vendor organisations **shall** do the following:

1. Ensure the organisation provides information to the customer, in an accessible way, specifying the level of support and maintenance provided for the software product/ service being sold.

- Q33: Do you agree with this action?
    - Yes – I think this action should be included as a “shall”
    - Yes – I think this action should be included as a “should”
    - No – I think this action should not be included in this Code of Practice
    - I don’t know

Principle 4: Communication with customers

Senior Responsible Officers in software vendor organisations **shall** do the following:

2. Ensure the organisation provides at least 1 year’s notice to customers, in an accessible way, of when the product or service will no longer be supported or maintained by the vendor.

- Q34: Do you agree with this action?
    - Yes – I think this action should be included as a “shall”
    - Yes – I think this action should be included as a “should”
    - No – I think this action should not be included in this Code of Practice
    - I don’t know

Principle 4: Communication with customers

The aim of this principle is to ensure that vendor organisations provide sufficient information to customers to enable effective risk and incident management.
Senior Responsible Officers in software vendor organisations **shall** do the following:

3. Ensure information is made available to customers in an appropriate and timely manner about notable incidents that may cause significant impact to customer organisations.

- Q35: Do you agree with this action?
    - Yes – I think this action should be included as a “shall”
    - Yes – I think this action should be included as a “should”
    - No – I think this action should not be included in this Code of Practice
    - I don’t know

Principle 4: Communication with customers

The aim of this principle is to ensure that vendor organisations provide sufficient information to customers to enable effective risk and incident management.
Senior Responsible Officers in vendor organisations **should** do the following:

4. Ensure that high level information about the security and resilience standards, frameworks, organisational commitments and procedures followed by the organisation is made available to customers.

- Q36: Do you agree with this action?
    - Yes – I think this action should be included as a “shall”
    - Yes – I think this action should be included as a “should”
    - No – I think this action should not be included in this Code of Practice
    - I don’t know

Principle 4: Communication with customers

Senior Responsible Officers in vendor organisations **should** do the following:

5. Ensure that the organisation proactively supports affected customers during and following a cyber security incident to contain and mitigate the impacts of an incident. How this would be done should be documented and agreed in contracts with the customer.

- Q37: Do you agree with this action?
    - Yes – I think this action should be included as a “shall”
    - Yes – I think this action should be included as a “should”
    - No – I think this action should not be included in this Code of Practice
    - I don’t know

Principle 4: Communication with customers

Senior Responsible Officers in vendor organisations **should** do the following:

6. Provide customer organisations with guidance on how to use, integrate, and configure the software product or service securely.

- Q38: Do you agree with this action?
    - Yes – I think this action should be included as a “shall”
    - Yes – I think this action should be included as a “should”
    - No – I think this action should not be included in this Code of Practice
    - I don’t know

Principle 4: Communication with customers

This principle ensures that vendor organisations provide sufficient information to customers to enable effective risk and incident management.

Senior Responsible Officers in software vendor organisations **shall** do the following:

4.1 Ensure the organisation provides information to the customer, in an accessible way, specifying the level of support and maintenance provided for the software product/ service being sold.

4.2 Ensure the organisation provides at least 1 year's notice to customers, in an accessible way, of when the product or service will no longer be supported or maintained by the vendor.

4.3 Ensure information is made available to customers in an appropriate and timely manner about notable incidents that may cause significant impact to customer organisations.

Senior Responsible Officers in vendor organisations **should** do the following:

4.4 Ensure that high level information about the security and resilience standards, frameworks, organisational commitments and procedures followed by the organisation is made available to customers.

4.5 Ensure that the organisation proactively supports affected customers during and following a cyber security incident to contain and mitigate the impacts of an incident. How this would be done should be documented and agreed in contracts with the customer.

4.6 Provide customer organisations with guidance on how to use, integrate, and configure the software product or service securely.

- Q39: Do you think there is anything missing from this Principle? If so, what? [free text]
- Q40: Do you have any other comments or feedback relating to this Principle? [free text]
- Q41 [if Q3 = "Organisation/Business that is involved in the sale or development of software"]: As a software vendor/developer/reseller, do you consider this Code of Practice feasible to implement?
    - Yes
    - No
    - Don't know
-
- Q42 [if Q3 = "Organisation/Business that is involved in the sale or development of software"]: What barriers would your organisation face if asked to implement this Code as a software vendor?
    - No barriers. The actions listed in this Code of Practice are within my organisations' capability
    - This Code of Practice would be too expensive to implement
    - Staff do not have the required skills to implement this Code of Practice
    - The actions in this Code of Practice are too difficult to scale up across the organisation.
    - My organisation does not have the necessary staff to implement this Code of Practice.
    - Senior leaders in my organisation are not likely to engage with this Code of Practice.
    - Other [please specify]
    - N/A - my organisation does not develop or sell software

- Q43[if Q3 = “Organisation/Business that is involved in the sale or development of software”]:: As a software vendor/developer/reseller, would this Code cause excessive hindrance to innovation?
    - Yes
    - No
    - Don’t know
- Q44 [if Q3 = “An organisation that procures software”]: As an organisation procuring software, do you consider that it would be feasible to use this Code of Practice in your procurement processes?
    - Yes
    - No
    - Don’t know
-
- Q45: What barriers would your organisation face if asked to request that software suppliers to your organisation meet this Code of Practice?
    - No barriers. My organisation would not face any significant challenges in using this Code of Practice in procurement processes.
    - This Code of Practice would be too expensive to incorporate into procurement processes.
    - This Code of Practice would be incompatible with my organisation’s procurement processes.
    - Staff responsible for procurement would not have the necessary skills to use this Code when negotiating with suppliers.
    - Staff do not have the necessary skills to understand any attestation or proof provided by software vendors of adherence to this Code of Practice.
    - Other [please specify]

Questions on Chapter 5: Supporting materials

- Q46: Are the proposed technical controls suitable for measuring compliance with the Code of Practice for software vendors?
    - Yes
    - No
    - Don’t know
- Q46b [if Q44=”no”]: Why is it not suitable? [open text]
- Q49: Do you have any other comments about the technical controls outlined above and the implementation guidance example (attached in B)? [Free text]
- Q50[if Q3 = “An organisation that procures software”]: As a customer procuring software, what other supporting materials would be helpful to enable you to request adherence to this Code of Practice from your suppliers? [check boxes]
    - Standardised contractual clauses
    - Guidance on how to assess suppliers’ adherence to the Code
    - Standardised templates for supplier attestation of compliance with the Code
    - Training for non-cyber specialists
    - An assurance scheme or certification
    - Product security testing labs
    - N/A - my organisation does not procure software
    - Other [please specify]
- Q51 [if Q3 = “Organisation/Business that is involved in the sale or development of software”]: As a software vendor, what other supporting materials would be helpful to enable you to follow the Code of Practice?
    - An assurance or certification scheme

- Product security testing labs
- Further guidance on how to manage the use open-source software in development
- Skills interventions to secure the talent pipeline in software development
- Other [please specify]
-

Survey close

- Q52: Do you have any other feedback on our Code of Practice? [open text]