Department for
Science, Innovation
& Technology

Code of Practice for Software Vendors: Government Response to the Call for Views

CP 1281

Code of Practice for Software Vendors: Government Response to the Call for Views

Presented to Parliament by the Parliamentary Under-Secretary of State for AI and Digital Government by Command of His Majesty

March 2025

CP 1281

This publication is available at www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at cyber.resilience.consultations@dsit.gov.uk

ISBN 978-1-5286-5441-8

E03293157 03/2025

Printed on paper containing 40% recycled fibre content minimum

Printed in the UK by HH Associates Ltd. on behalf of the Controller of His Majesty's Stationery Office

Contents

Ministerial Foreword

This government is committed to ensuring businesses can safely harness the benefits of technology and help drive growth and innovation. As the Minister for AI and Digital Government, I want to ensure new and existing technologies are safely deployed across the UK, with the benefits more widely shared. As modern businesses are increasingly interconnected and reliant on new and existing technologies, it is important they understand the risks these technologies pose, not only to their own organisations, but also to their customers and wider supply chains.

Software here plays a crucial role. It is the foundation of digital technology. It is in all digital devices and services which organisations across all sectors rely on for innovation and growth. However, software is now so widespread in business operations and processes that its fundamental role is often taken for granted. When software is compromised or malfunctions, it can halt organisational operations entirely, and this reliance makes software a prime target for malicious actors. In recent months and years, the UK has witnessed cyber attacks and disruption from incidents such as those on Advanced (2022) and MOVEit (2023) software, demonstrating the widespread impact attacks that take advantage of software vulnerabilities can have across the economy. In fact, 59% of organisations globally[1] are believed to have been impacted by a software supply chain attack or exploit. Even so, the government's Cyber Security Breaches Survey shows that only 11% of businesses assess the risks posed by their immediate suppliers.

It is within our power to limit the likelihood of avoidable weaknesses and vulnerabilities which are being exploited by malicious actors or causing disruption through software failure. We can do this by ensuring those who develop and sell software embed best practices for software security and resilience within their organisations. We can also encourage more organisations to assess risks in their supply chains and demand better security provision from their suppliers. Today I am pleased to announce the government has published its response to the Call for Views on a draft Code of Practice for Software Vendors. This will address the risks that can lead to these types of incidents.

The proposed code of practice, being developed in collaboration with the National Cyber Security Centre and a group of experts from industry and academia, seeks to ensure security and resilience are embedded into the development and distribution of products and services. The code comprises a set of voluntary measures that software vendors would be expected to implement to establish a consistent baseline of security and resilience across the market, raising the bar across our digital supply chains.

This code of practice is just a part of this government's work to ensure that all businesses can benefit safely from new and existing technologies. This government has committed to improving the security of critical sectors through the Cyber Security & Resilience Bill, but cyber security is a multi-faceted issue which requires more than just legislation. We must also ensure all organisations across the economy are resilient and prepared to face cyber incidents. Our work to improve the cyber security of software is therefore part of a wider set of work to drive up cyber resilience across the economy and society.

This effort includes the introduction of other codes of practice which formalise the government's expectations around cyber governance and the cyber security of Artificial Intelligence (AI). The government also continues to work to close the skills gap through our cyber skills programmes, including CyberFirst and to raise the bar for cyber resilience across the economy through schemes like Cyber Essentials.

I would like to thank everyone who responded to the Call for Views on the Code of Practice for Software Vendors. I would also like to thank those who hosted or participated in one of the events, workshops, and webinars that DSIT officials held during the call for views period. All of this input and support has provided invaluable insight that has helped us improve the code and ensure its effectiveness. Your feedback forms the basis of this government response and has helped us define our next steps to drive uptake and ensure the code of practice is impactful and effective. Your views on this policy and future initiatives will help us strengthen the digital supply chains which the UK's 5.6 million businesses rely on, enabling growth and innovation across all sectors.

Feryal Clark MP
Parliamentary Under-Secretary of State for AI and Digital Government
Department for Science, Innovation and Technology

1. Executive summary

Software is the backbone of the digital economy. It has become an integral component of the day-to-day operations and processes upon which organisations rely and is therefore crucial in supporting economic growth and resilience. The widespread use of software, however, exposes this technology and its supply chains to disruptive risks. When software is compromised or faulty, it can bring organisations to a halt, and reliance on such technology makes it an appealing target for malicious actors.

The impact of attacks can spread quickly through supply chains and between sectors, with 59% of organisations globally estimated to have been impacted by a software supply chain attack[1]. With software at the root of all technology, action must be taken by those responsible for developing and selling software to make software a more difficult target for malicious actors and to protect our supply chains from unnecessary disruption.

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. The stakeholders that took part in this call for views in 2023 highlighted the following key themes:

- The Government should set clear expectations for software vendors;
- There is a need to strengthen software vendor accountability in the software supply chain;
- Secure software development is key to strengthening the resilience of UK organisations and the UK economy;
- Greater transparency and better communication are needed across software supply chains.

Consequently, a range of policy interventions were announced, including the development of a Code of Practice for Software Vendors. The draft code was co-designed with industry leaders, academics, and technical experts from the National Cyber Security Centre (NCSC) to support any organisation that develops and/or sells software to organisational customers (B2B). This includes organisations that sell software and software services, or organisations selling products or services that contain software.

The code of practice outlines the fundamental security and resilience measures that should be reasonably expected of all organisations that develop and / or sell software to organisational customers. It provides guidance on how software should be developed, built, deployed and maintained, and how vendors can communicate effectively with customers that procure their software. Engagement with this code of practice can enable software vendors to improve the cyber resilience of their products and services.

[1] https://www.blackduck.com/resources/analyst-reports/software-supply-chain-security.html?cmp=pr-sig&utm_medium=referral (this statistic refers to research conducted on organisations in North America, EMEA, and Japan.)

The draft Code of Practice for Software Vendors was published as part of a call for views in May 2024. Through this call for views, the government invited feedback from industry and any other interested parties to inform its policy approach to software security.

The draft code presented in the call for views was addressed to senior leaders in the targeted organisations and was made up of 21 provisions over 4 principles. The principles address the secure design and development of software, build environment security, the secure deployment and maintenance of software, and effective customer communication to facilitate better risk management.

The Call for Views on the Code of Practice for Software Vendors ran for 12 weeks from **15 May 2024** to **9 August 2024.** During this period, DSIT also co-hosted workshops with multiple stakeholders from a wide range of organisations and sectors, including industry, academia, local government organisations, and trade and professional associations. Submissions to the call for views were received from 87 respondents. Of these, 47 were organisations. Most of the organisations responding are involved in the sale or development of software, procurement of software, and cyber security. The remaining 40 respondents identified themselves as individual cyber security/IT professionals, software developers, senior leaders, academics, and one interested member of the public. Their views formed the basis of the analysis presented below and contribute to informing the government's approach to software security and resilience moving forward.

This document provides an overview of the feedback on the draft Code of Practice for Software Vendors, the themes that emerged. It also presents the government's response to the feedback. This is structured around the following six key themes from responses to the call for views:

A. There is strong support for the creation of a Code of Practice for Software Vendors;
B. There is overall support for the code's proposed principles and provisions;
C. There is demand for more supporting materials describing technical controls and implementation guidance for the code;
D. There was interest in aligning the code with existing standards, regulation and guidance;
E. There was interest in the government accompanying the code with a form of assurance, auditing or attestation;
F. There is a need for clarity on certain aspects of the code's language and terminology.

The document ends with an outline of next steps which summarises the government response to the call for views.

2. Background

DSIT is committed to ensuring that new and existing technologies are deployed safely across the UK. This includes ensuring that security and resilience are prioritised in their development and distribution, as well as providing organisations with the tools they need to understand cyber risk and feel confident in their use of technologies. The development of a Code of Practice for Software Vendors is an important step towards achieving these objectives by improving levels of security and resilience in the technology market and providing a supply chain management tool for businesses.

Data from the 2023 Call for Views on Software Resilience and Security for Businesses and Organisations suggested that disruption and harm caused by software supply chain attacks and incidents are enabled by both inconsistent security practice by those who develop and sell software, and poor market demand due to low awareness from enterprise customers. This means that government policy and guidance need to address both suppliers and enterprise customers to ensure that reasonable levels of security and resilience become standard across the market and that good security and resilience can become a point of market differentiation.

On the supply side, stakeholders argued that software vendors - whether small or large organisations - are not incentivised to prioritise security or resilience when developing software. This is partially because there’s a lack of clear expectations for software vendors to act as a market baseline, leading to security and resilience often being overlooked in favour of cost or innovation. However, risks relating to software security and resilience are clearly a concern for software vendors and their business customers alike. The 2023 consultation demonstrated clear demand for a multi-staged government intervention to improve software security and resilience to strengthen digital supply chains. Risks caused by inconsistent software development practices and a lack of transparency in software supply chains were both highlighted as key concerns for industry.

On the demand side, despite the prevalence of software supply chain attacks and disruption from software failure, few organisations are actively assessing cyber risks in their supply chain, and cyber security often is not a top priority when procuring software and software services. The UK government’s Cyber Breaches Survey 2024 reports that only one in ten (11%) organisations are taking the necessary steps to review cyber risks derived from their direct suppliers. The number is even lower (6%) when it comes to looking at their wider supply chain. This underlines the need for a greater understanding and awareness of supply chain risks such as those related to software, and for new or better supply chain management tools.

These challenges can start to be addressed if relevant actors in the supply chain, like software vendors, follow established best practices for the design, development, and distribution of software. Software is not a new or emerging technology, but it is becoming increasingly complex due to the rapid evolution of innovative technologies. It is therefore essential that fundamental security and resilience measures are taken by technology developers to ensure that the foundations of our technology ecosystem are secure. It is also essential that these expectations are understood and communicated by both vendors and their business customers to ensure that risks are managed consistently throughout supply chains.

The Code of Practice for Software Vendors provides those baseline expectations by outlining the security and resilience measures that should ideally be taken by organisations which develop and distribute software. This document summarises and provides a government response to the recent call for views on the draft code of practice. The draft code shared for views can be referred to in Annex A of this government response.

The code is aimed at senior leaders in software vendor organisations to ensure that these measures are prioritised across their organisations. With knowledge of these baseline expectations, senior leaders can then ensure that relevant teams across their organisations take the necessary steps to enact these measures, and have the resources, tools and knowledge they need to do so.

The measures outlined in this code of practice can be applied to the development of any software that is sold to a business customer. This includes software, software services, or software within digital products or services. The code outlines the fundamental software security principles that should ideally be observed to appropriately secure software components of any technology to the level needed by enterprise customers. These principles have therefore been designed as a set of technology-agnostic actions that can be adapted for organisations of any size, sector, or technology-type to implement. The measures were also split into “shalls” and “shoulds”, where a “shall” indicates a requirement, whereas a “should” indicates a recommendation.

The principles in the draft code of practice were co-designed by DSIT, the NCSC and a group of industry and academic experts which included software vendors (large and small), cyber security experts, standards professionals, supply chain security experts, procurers, and academic researchers. The broader views collected through the public call for views and outlined in this document will be used to further refine the principles to ensure they are proportionate and feasible for any relevant organisation to implement. Views will also be used to inform next steps in driving uptake of the code of practice.

Policy context

This work is part of DSIT’s wider technology security programme. Within this programme, DSIT promotes a secure by design approach across all digital technologies which places the responsibility on those that develop technology to build robust cyber security into their systems. This year, the PSTI Act came into force which aims to enhance the security of consumer connectable products against cyber threats by mandating minimum security requirements.

Beyond regulation, the Code of Practice for Software Vendors is an integral part of a wider package of voluntary codes of practice being developed by DSIT. The product security regulations themselves were derived from a Code of Practice for Consumer IoT. These codes set out voluntary measures that act as a shorthand for what government expects from organisations across a range of technologies and sectors. This is part of the government’s broader approach to improve baseline cyber security practices and increase the cyber resilience of the economy. Other codes include those on cyber governance, the cyber security of AI, enterprise device security and the Code of Practice for App Stores. The Code of Practice for Software Vendors has been designed as part of a modular approach so that stakeholders can apply this code in tandem with other codes depending on which technology areas are relevant to their business[2].

3. Methodology

The call for views was open from 15th May to 9th August 2024. The survey was open to the public and responses were received from individuals and organisations. Respondents were invited to participate via an online survey or to submit responses by email.

The consultation asked respondents 52 questions on the draft code of practice, including both closed and open questions. Respondents did not have to answer every question. For some questions, respondents were offered the opportunity to expand on answers and provide more detail with qualitative open text boxes.

A minor error was found in the questionnaire after the call for views was closed: Q44 was originally written for organisations procuring software, however, the survey was incorrectly routed so this question appeared for organisations/businesses involved in the sale or development of software (based on responses to Q3). This issue has been noted where relevant statistics are referenced, but it has not negatively impacted the results.

In total, 87 responses were included in the analysis. This was made up of 69 online responses and 18 email responses. Responses were excluded from the analysis if they only answered the demographics questions. Some responses were also excluded because they were duplicates.

For open response questions, every response was reviewed, and while not every point that was made by each respondent can be reflected, responses were coded to identify common themes.

A Privacy Notice was provided containing information for participants on their rights and how their responses will be used. All personally identifiable information has been removed from the analysis.

4. Key themes and government response

a. Strong support for the creation of the Code of Practice for Software Vendors

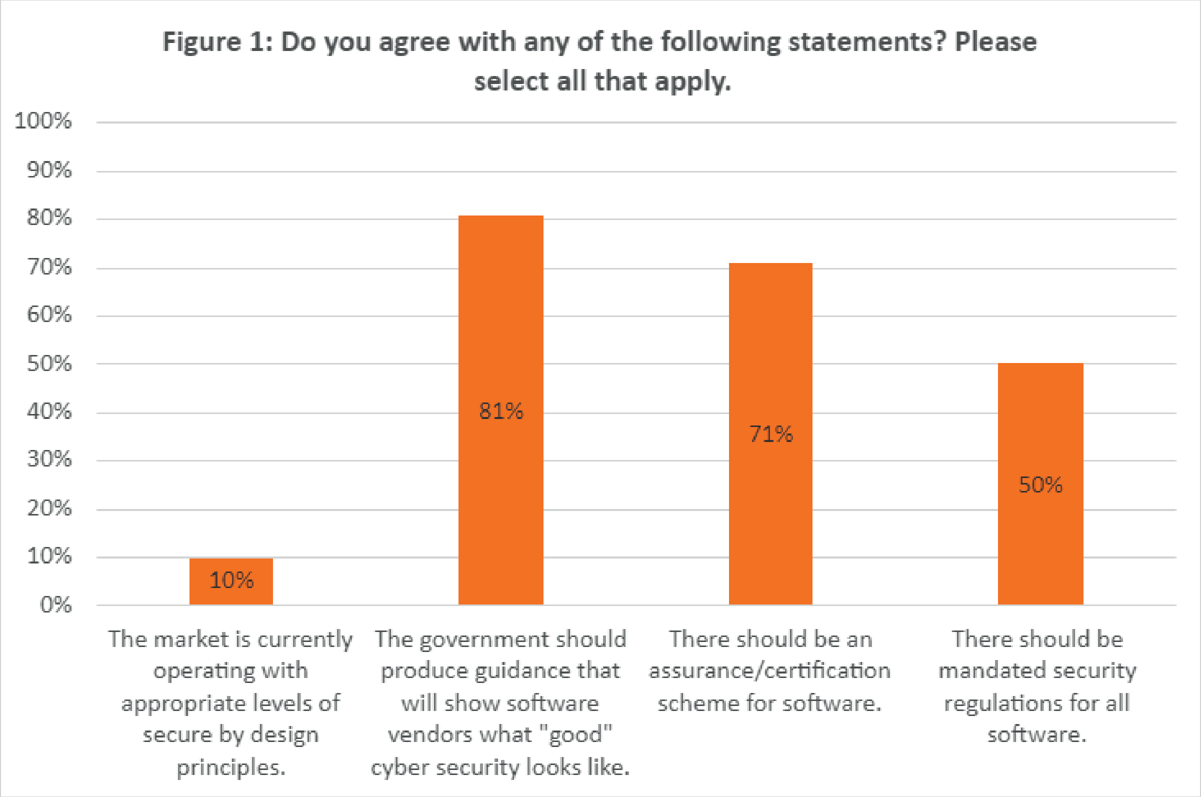
Analysis of responses

The call for views showed strong support for a Code of Practice for Software Vendors. Figure 1 shows that the majority of respondents are in favour of government action on software vendors. Of the 72 respondents, 81% agreed that the government should produce guidance that will show software vendors what “good”

[2] https://www.gov.uk/government/collections/cyber-security-codes-of-practice

cyber security looks like. Only 10% of respondents to the call for views thought that the market currently operates with the appropriate levels of secure by design principles.

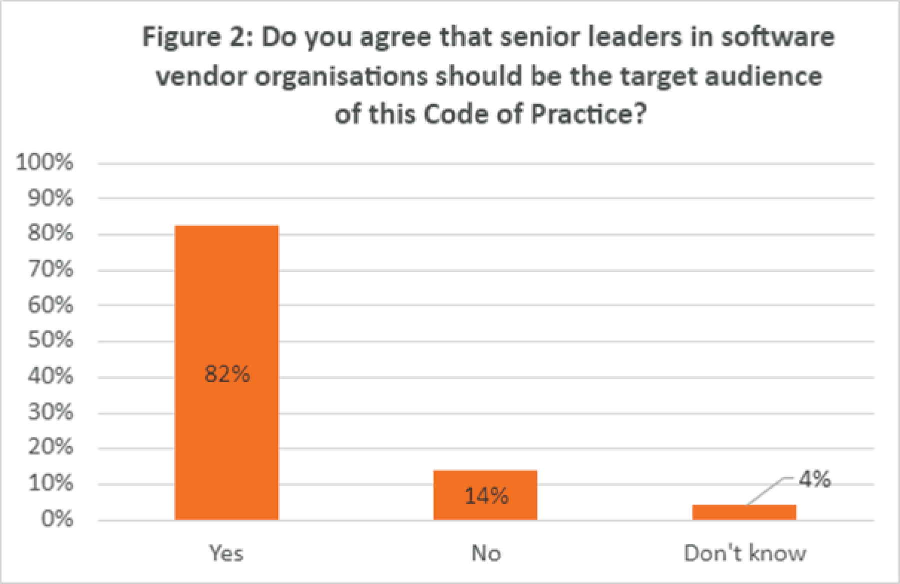
Figure 1 – Do you agree with any of the following statements? Please select all that apply.



Base: 72

Additionally, respondents showed support for the proposed target audience of the Code of Practice. As Figure 2 shows, 82% agree that senior leaders should be the target audience for the Code of Practice. 14% said they did not agree with this target audience, and 4% said they don’t know.

Figure 2 – Do you agree that senior leaders in software vendor organisations should be the target audience of this Code of Practice?



Base: 73

Respondents to the call for views generally considered the code of practice to be widely applicable across different types of organisations. When asked, most respondents did not identify any organisations for which the code of practice would be unsuitable. A small minority of respondents stated that the code of practice would not be suitable for small and medium-sized enterprises (SMEs) or startups, or that a maturity model would be needed to accommodate different organisations. Some respondents also pointed to open-source software projects as an area where the code of practice would not be applicable although, again, this was a small minority.

Most respondents also stated that they would be likely or very likely to use a code of practice, further indicating the overall support found in the call for views. Table 1.1 shows that 46% said they were very likely to use a voluntary code of practice to inform procurement. A further 27% said they were likely to use the code.

Table 1.1 - If one was available, how likely would your organisation be to use a voluntary Code of Practice for Software Vendors to inform procurement?

Response	Number of responses	%
Very likely	31	46%
Likely	18	27%
Neutral	9	13%
Not likely	5	7%
Definitely won't use	1	1%
Don't know	3	4%

Base: 67

Furthermore, Table 1.2 shows that most respondents said they were very likely (43%) or likely (35%) to use a voluntary Code of Practice for Software Vendors to inform supplier management processes.

Table 1.2 - If one was available, how likely would your organisation be to use a voluntary Code of Practice for Software Vendors to inform supplier management processes?

Response	Number of responses	%
Very likely	29	43%
Likely	24	35%
Neutral	8	12%
Not likely	4	6%
Definitely won't use	0	0%
Don't know	3	4%

Base: 68

The call for views has shown there is support for the government to publish a Code of Practice for Software Vendors aimed at senior leaders and across the software sector. Additionally, the results shown in Tables 4.1 and 4.2 suggest that a code of practice would be a helpful supply chain management tool for organisations procuring software.

b. Overall support for the code’s proposed principles and provisions

Analysis of responses

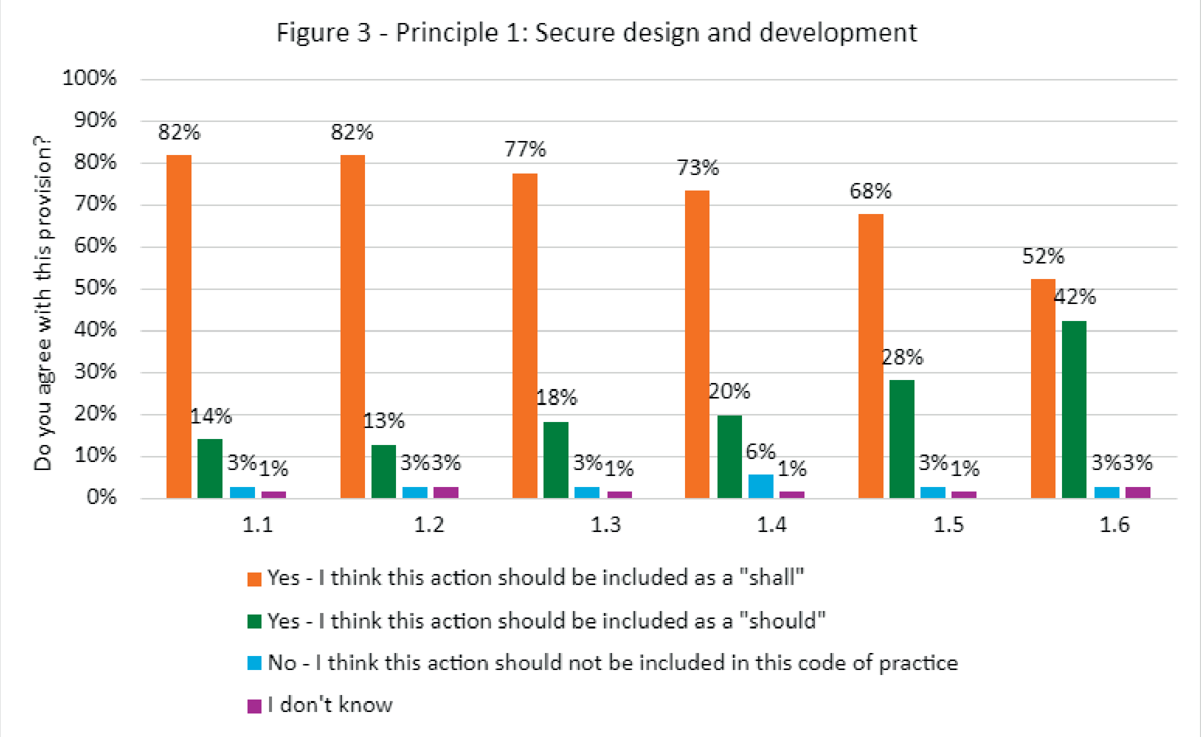
Overall, respondents to the call for views demonstrated support for the code’s proposed principles. Respondents showed a clear preference for the provisions to be included as a “shall” rather than “should”. Here, provisions falling under “shall” pointed to a requirement expected of organisations that would adopt the Code of Practice for Software Vendors. The “should”, on the other hand, pointed to a recommendation.

Principle 1

The call for views survey asked respondents about the proposed principles and associated provisions for the code of practice in turn (see Annex A for a full copy of the code of practice presented in the call for views). Respondents were asked if they agree with each provision, and if so, if it should be included as a “shall” (requirement) or a “should” (recommendation) in the code of practice. Respondents could also select that they thought the provision should not be included, or that they don’t know. Figures 3-6 presented below show the results for each provision by the four proposed principles in the code.

Figure 3 shows that for each provision under Principle 1 a majority of respondents thought that they should be included as a “shall”. The next most common response was for the provision to be included as a “should”. Across all provisions, 6% or fewer thought the provision should not be included in the code. In comparison to other provisions under Principle 1, respondents were more split over their preference to include provision 1.6 as a requirement (shall) or a recommendation (should). 52% of the respondents preferred “shall”, while 42% preferred “should”. For provisions 1.1-1.5, 68% or more respondents indicated a preference for “shall” over “should”. This suggests there is slightly less certainty on the provision to “encourage the use of appropriate security tools and technologies to make sure that the default options throughout development and distribution are secure” (Provision 1.6 – see Annex A; see also the government response section below).

Figure 3 – Support for Principle 1 (Secure design and development)



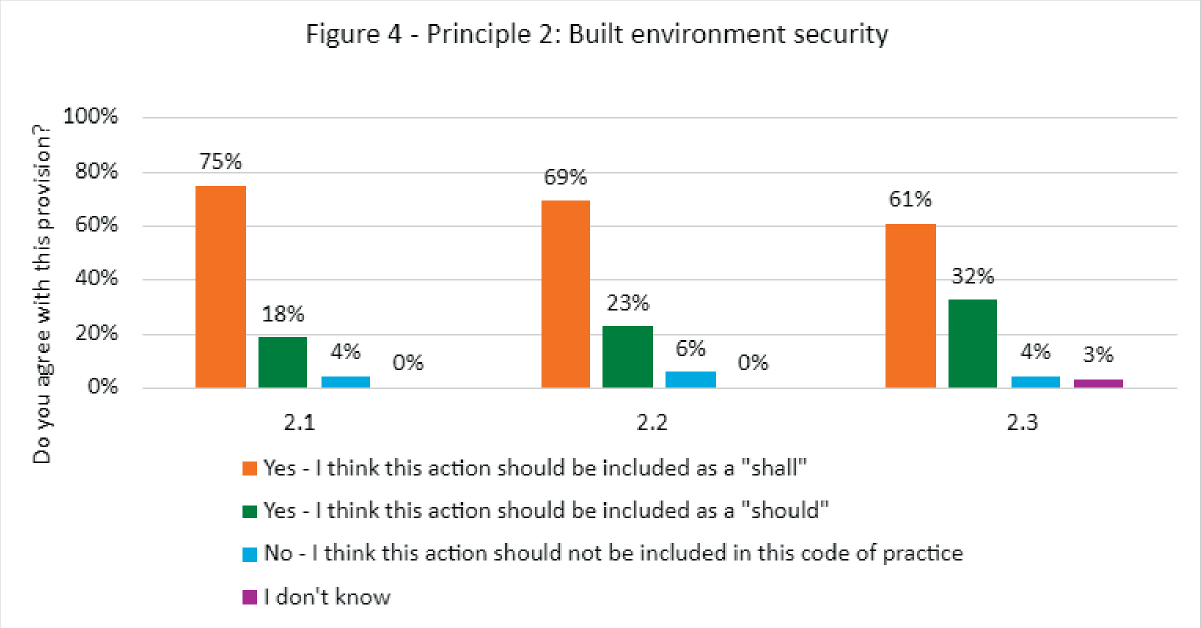
Bases: Provision 1.1 - 71, Provision 1.2 - 71, Provision 1.3 - 71, Provision 1.4 - 71, Provision 1.5 - 71, Provision 1.6 - 71

Qualitative feedback on the code showed there is interest in additional provisions to the code, and this was particularly notable for Principle 1. Suggestions were very broad, from information on software development to a provision on staff responsibilities and skills. Several respondents also commented specifically on provision 1.3 (“ensure the organisation has a clear process for testing software before distribution”) and suggested that adding explicit guidance on threat modelling and red teaming would be beneficial.

Principle 2

Principle 2 also received strong support for the proposed provisions to be included as a “shall”. Figure 4 shows 61% or more of respondents thought they should be included as a “shall”. The next most common response was for the provisions to be included as a “should”. For each provision, 6% or fewer thought it should not be included in the code of practice.

Figure 4 – Support for Principle 2 (built environment security)



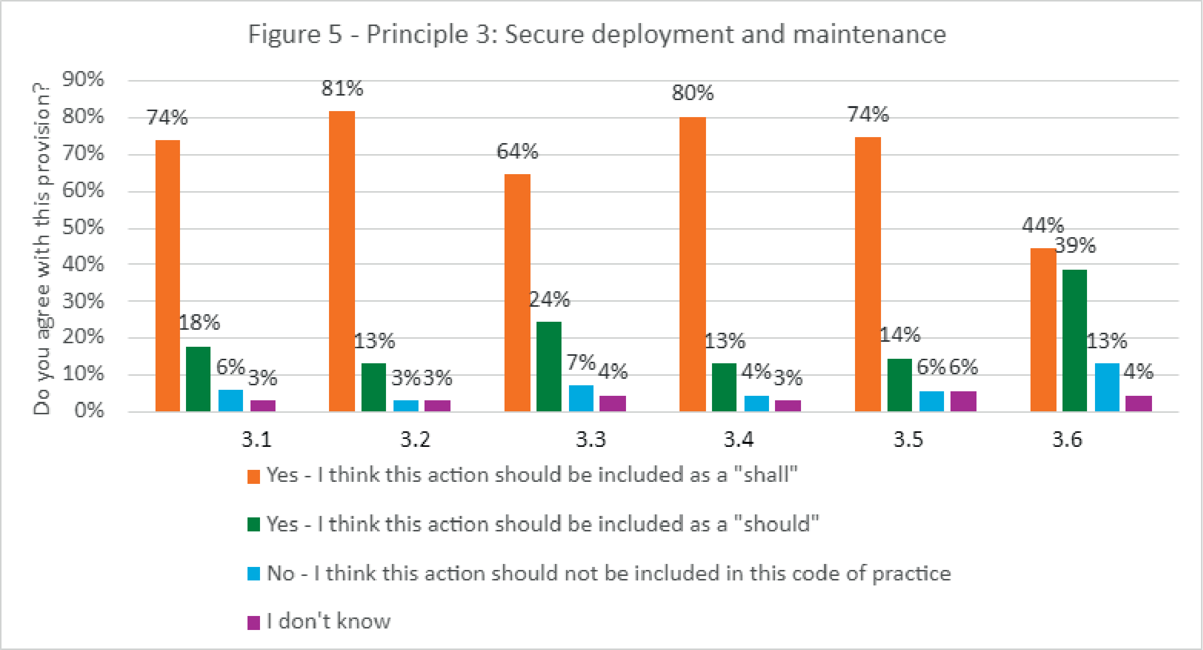
Bases: Provision 2.1 - 71, Provision 2.2 - 71, Provision 2.3 - 71

Qualitative feedback on Principle 2 shows that there is interest in additional provisions, as well as further detail on those proposed in the draft code. A recurrent theme in the qualitative feedback on Principle 2 was interest in having auditing, assurance or attestation against the code.

Principle 3

Figure 5 reports responses to the question on Principle 3 of the code. 64% or more of respondents for provisions 3.1 to 3.5 thought the provision should be included as a “shall”. The next most common response for each provision under Principle 3 was for the provision to be included as a “should”. Across these provisions, 7% or fewer thought the provision should not be included in the code. Compared to the other provisions under Principle 3 of the code, feedback on provision 3.6 (“Make a public affirmation that the organisation would welcome security researchers to test software and software services provided by the organisation as part of its vulnerability disclosure process”) was more divided: 44% of the respondents said the provision should be included as a “shall” and 39% said it should be included as a “should”. 13% also said that provision 3.6 should not be included in the code. Furthermore, some responses in the qualitative data put forward requests to define and / or amend the provision in question.

Figure 5 – Support for Principle 3 (secure deployment and maintenance)



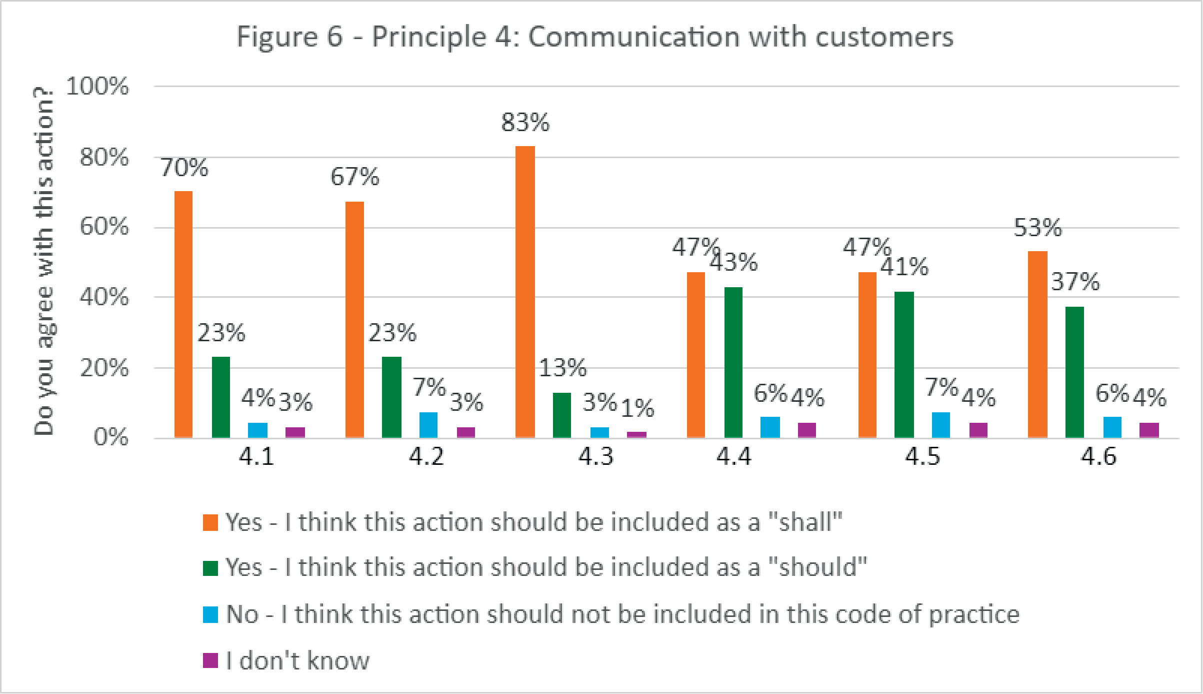
Bases: Provision 3.1 - 68, Provision 3.2 - 70, Provision 3.3 - 70, Provision 3.4 - 70, Provision 3.5 - 70, Provision 3.6 - 70

Principle 4

Figure 6 shows that while the level of support for the provisions under Principle 4 to be included as a “shall” is lower compared to Principles 1, 2 and 3, there is support from the majority of respondents for the provisions’ inclusion in the code. For provisions 4.1-4.3, 67% or more respondents thought the provision should be included as a “shall”.

Feedback on the other provisions under Principle 4 was more divided. 53% thought that provision 4.6 should be included as a “shall”, while 37% thought it should be included as a “should”. Feedback on provisions 4.4 and 4.5 was more closely split between those who thought that the provision should be included as a “shall” (47% for both provisions) and a “should” (43% in 4.4 and 41% in action 4.5). This suggests there is slightly less clarity than for other principles as to whether organisations providing high level information and supporting affected customers during and following a cyber security incident (provision 4.4 and 4.5 respectively) should be included in the code as a “shall” or a “should”. For each provision, 7% or fewer of respondents thought that it should not be included in the code of practice.

Figure 6 – Support for Principle 4 (communication with customers)



Bases: Provision 4.1 - 70, Provision 4.2 - 70, Provision 4.3 - 70, Provision 4.4 - 70, Provision 4.5 - 70, Provision 4.6 - 70

Support across different business sizes
For most provisions, organisations of all sizes support their inclusion as a “shall” in the code of practice. There were some exceptions to this, whereby smaller organisations were more divided in their support for “shall” versus support for “should” than organisations with 500+ employees for certain provisions. Support for each provision by size of organisations is laid out in detail in Annex B.

Organisations with 0-499 employees were slightly more in favour of provision 3.6 and 4.4 being included as a “should”. Table 2.1 shows that support for provision 3.6 was more strongly in favour of “should” in organisations with 0-499 organisations (32% for shall vs. 58% for should), compared to organisations with 500+ employees (50% for shall vs. 29% for should).

Table 2.1 - Type of support for provision 3.6 by size of organisation.

Response	0 to 499 (combined)	500+
Yes - I think this action should be included as a "shall"	32%	50%
Yes - I think this action should be included as a "should"	58%	29%
No - I think this action should not be included in this code of practice	11%	7%
I don't know	0%	14%
Total	**19**	**14**

Bases: 19 organisations with 0-499 employees (Q5 = micro; small; medium), 14 organisations with 500+ employees (Q5 = large).

Table 2.2 shows that organisations with 0-499 organisations slightly more strongly support provision 4.4 to be included as a “should” (45% for shall vs. 50% for should), compared to organisations with 500+ employees (50% for shall vs. 29% for should).

Table 2.2 - Type of support for provision 4.4 by size of organisation.

Response	0 to 499 (combined)	500+
Yes - I think this action should be included as a "shall"	45%	50%
Yes - I think this action should be included as a "should"	50%	29%
No - I think this action should not be included in this code of practice	0%	7%
I don't know	5%	14%
Total	**20**	**14**

Bases: 20 organisations with 0-499 employees (Q5 = micro; small; medium), 14 organisations with 500+ employees (Q5 = large).

This suggests that for some provisions, smaller organisations are more hesitant to include them in the code of practice as a “shall” than large organisations. Overall, however, support was generally in favour for provisions to be included as a “shall” by organisations of different sizes (see Annex B).

Government response

The call for views confirmed the need to improve levels of security and resilience of software and software services, and that government intervention in this space is necessary. The government recognises the critical role that software plays in maintaining UK businesses’ operations and security. To protect organisations, the government will publish and promote the Code of Practice for Software Vendors to drive improvements in the security and resilience of digital supply chains and the UK’s organisational resilience.

To address the insights from the call for views, the government will make minor revisions to the code of practice. The government recognises that although there was strong support for the scope and content of the draft code, views on a few provisions of the code were more divided than others. There were also some concerns in open-text responses that some provisions may be challenging for smaller organisations to comply with. This was reflected in the data concerning whether provisions should be “shalls” (requirements) or “shoulds” (recommendations).

To ensure the code is feasible for any software vendor, DSIT and the NCSC will reassess the provisions where smaller organisations were more divided over whether they should be “shalls” or “shoulds”. Although these provisions will be revised, it is clear that there is general support for the outcomes given the low number of respondents who thought draft provisions should not be included. As far as possible, therefore, these outcomes will be maintained either in redrafted provisions or within the technical controls or implementation guidance.

The principles have been designed to be flexible and adaptable for organisations of different sizes and sectors, focusing on the fundamental principles that, if met, would constitute a proportionate and robust approach to software security. This approach will be maintained in the upcoming revision of the code. Qualitative feedback indicating where actions may be more challenging for SMEs will be used to ensure the final draft meets this objective.

The call for views document provided a sample of the implementation guidance that will accompany the code of practice. The final version of the implementation guidance will cover all provisions and will provide additional detail to guide software vendors in identifying the most appropriate implementation options for their organisation. This will be particularly useful for SMEs.

In relation to the scope of the code of practice, some respondents noted concerns about the impact on the open-source community. The government recognises the value of open-source software to the technology ecosystem and the importance of minimising the burden on open-source developers and maintainers. The code of practice will apply primarily to organisations that develop, distribute, and maintain software and software services that are sold for profit. The code sets out expectations for organisations that make a business of selling software (or products or services containing software) to business customers (B2B). The open-source community can consult the code as a useful tool for the development and maintenance of secure software if they choose.

c. Technical controls and implementation

Analysis of responses

Respondents to the call for views often requested further implementation guidance and raised some concerns about the cost of implementing the code. However, overall, there was support for the code's proposed technical controls and implementation guidance.

a. *Support for implementation of the code of practice*

The call for views asked software vendors, developers and resellers about the implementation of the code. Most of these organisations said that the code is feasible to implement (84%), as shown in Table 3.1. 16% said the code is not feasible to implement.

Table 3.1 - As a software vendor/developer/reseller, do you consider this code of practice feasible to implement?

Response	Number of responses	%
Yes	16	84%
No	3	16%
Don't know	0	0%

Base: 19 organisations/businesses involved in the sale or development of software (Q3 = "organisation/business that is involved in the sale or development of software").

The code was also seen as feasible to implement by most organisations procuring software (64%), as shown in Table 3.2. 36% said it would not be feasible to implement.

Table 3.2 - As an organisation procuring software, do you consider that it would be feasible to use this code of practice in your procurement processes?

Responses	Number of responses	%
Yes	14	64%
No	8	36%
Don't know	0	0%
Base	**22**	**100%**

Base: 22 organisations/businesses involved in the sale or development of software (Q3 = "organisation/business that is involved in the sale or development of software").[3]

Additionally, software vendors were asked what barriers they would face if asked to implement the code. As shown in Table 3.3, most of these organisations said the actions are within their organisations' capability to implement (68%).

Table 3.3 - What barriers would your organisation face if asked to implement this code as a software vendor?

Barrier	Number of responses	%
No barriers. The actions listed in this code of practice are within my organisations' capability.	13	68%
This code of practice would be too expensive to implement.	0	0%
Staff do not have the required skills to implement this code of practice.	1	5%
The actions in this code of practice are too difficult to scale up across the organisation.	0	0%
My organisation does not have the necessary staff to implement this code of practice.	1	5%
Senior leaders in my organisation are not likely to engage with this code of practice.	1	5%
N/A - my organisation does not develop or sell software.	1	5%
Other	2	11%

Base: 19 organisations/businesses involved in the sale or development of software (Q3 = "organisation/business that is involved in the sale or development of software").

[3] Please note that this question (Q44) was originally written for organisations procuring software, however, the survey was incorrectly routed so this question appeared for organisations/businesses involved in the sale or development of software (based on responses to Q3).

All respondents to the call for views were also asked about potential barriers if asked to request that software suppliers meet the code's measures. Table 3.4 shows that 37% of respondents said their organisation would not face any significant challenges in using the code of practice in procurement processes. However, unlike for software vendors, most respondents did identify that requesting software suppliers to meet the code of practice would result in a barrier for their organisation (63%).

Table 3.4 - What barriers would your organisation face if asked to request that software suppliers to your organisation meet this code of practice?

Barriers	Number of responses	%
No barriers. My organisation would not face any significant challenges in using this code of practice in procurement processes.	25	37%
This code of practice would be too expensive to incorporate into procurement processes.	7	10%
This code of practice would be incompatible with my organisation's procurement processes.	4	6%
Staff responsible for procurement would not have the necessary skills to use this code when negotiating with suppliers.	6	9%
Staff do not have the necessary skills to understand any attestation or proof provided by software vendors of adherence to this code of practice.	5	7%
Other (please specify)	20	30%

Base: 67

For those respondents who did face a barrier to using the code of practice, the most common option selected was 'other' (30%), as shown in Table 3.4. Respondents highlighted in qualitative feedback that the cost of compliance for vendors or products for customers would be a barrier if they were required to ensure their software suppliers meet the code. This is supported by the 10% of respondents who selected in the closed text question that the code would be too expensive to incorporate into procurement processes, shown in Table 3.4, suggesting that cost is a key concern in implementing the code within organisations' software procurement.

b. Requests for further implementation guidance

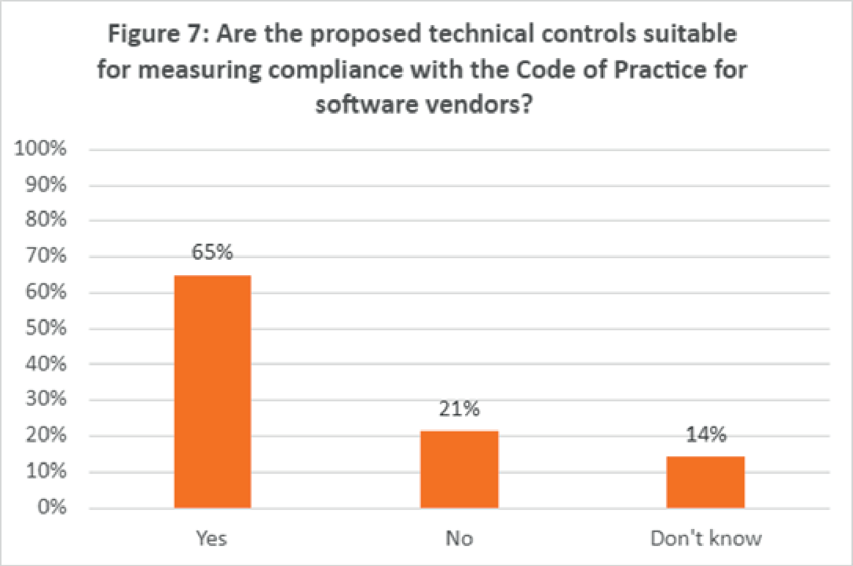
Overall, software vendors and procurers think that the code is feasible to implement, although some barriers (most notably cost) are expected by organisations if they were asked to request that software suppliers meet the code. Furthermore, implementation guidance was requested by these organisations to assist with uptake of the code.

More broadly, in qualitative feedback throughout the call for views, interest in more detailed implementation guidance was a common theme. Feedback on each principle, and particularly for Principles 1 and 3, requested more detailed explanations of how to meet the principles, which could include case studies or examples of what processes could look like for organisations.

c. Support for proposed technical controls

Draft technical controls to be implemented as part of the code were provided in the call for views. Respondents generally provided positive feedback; Figure 7 shows that 65% of respondents thought the proposed technical controls are suitable for measuring compliance with the code. 21% said that they are not suitable, and 14% stated that they don't know.

Figure 7 – Are the proposed technical controls suitable for measuring compliance with the Code of Practice for Software Vendors?



Base: 71

Those who considered the technical controls unsuitable were asked to expand on their response. Most of those who answered this follow up question suggested that more detail and/or some amendments are needed in the technical controls. Similar to feedback on the code's principles, some respondents also requested that further implementation guidance would be helpful.

Government response

The government will address this by developing revised technical controls and full implementation guidance in close collaboration with the National Cyber Security Centre (NCSC). Technical controls and implementation guidance will form accompanying material to the code. The technical controls will set out the minimum set of actions that a software vendor would need to demonstrate to provide confidence in the baseline resilience of their software or software service. The implementation guidance serves as additional support to enable organisations to identify the best implementation options based on their needs. Together they will help vendors meet the requirements outlined in the code's actions.

The revised technical controls will cover all provisions of the code of practice, and they will be more detailed. They will also contain a subset of more specific outcomes ('claims') consistent with the NCSC's Principles Based Assurance approach. The claims will provide additional specifics on the individual measures that organisations need to take to demonstrate each provision. They bring together what is widely considered good practice in software development and should be achievable for organisations of any size and sector. 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.

The technical controls are objective and outcome-focused to give organisations the flexibility to innovate while keeping their products and services secure. They are expected to reduce vulnerabilities in software, providing basic resilience against the most common threats and vulnerabilities. At the same time, demonstration of the code's technical controls will enable customers to gain confidence that the software and software services they purchase and use will not expose them to avoidable risk.

The draft code of practice presented in the call for views contained a sample extract of the implementation guidance for Principle 1 (see Annex B of the Call for Views on the Code of Practice for Software Vendors). This gave respondents an indication of the accompanying material the government will provide to organisations selling and developing software. Work on the final implementation guidance is ongoing with the NCSC and a full version covering all provisions will be published alongside the code of practice and the updated technical controls. Feedback on the sample provided and comments highlighting which aspects of the code will be more challenging for vendors will be used to refine the implementation guidance.

Recognising that the type of measures organisations choose to adopt is a business decision that will vary according to the size, sector and type of business, the implementation guidance will signpost towards existing technical guidance, frameworks and standards where appropriate. This is to avoid being prescriptive in the contents of the code and to allow the necessary flexibility for organisations to choose the implementation options that best suit their organisational culture, risk assessments and risk management processes. Working level teams within software vendor organisations can refer to cited guidance, frameworks and standards to implement the principles of the code of practice and demonstrate the technical controls are in place. In this way, vendors can determine the correct coverage and most appropriate way to achieve the outcomes of the code for their organisation.

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.

Respondents also highlighted that organisations that procure software will need support. Government intends to explore the development of guidance on how organisations can factor software security into their procurement and supplier management processes. This will help customer organisations, particularly small and medium-sized enterprises with limited cyber and legal expertise. This guidance could be used by organisations when negotiating and shaping contracts or service agreements with software suppliers, helping them to make appropriate demands for software security and resilience measures in a way that is legally binding through contractual obligations. This will encourage customer organisations to assess risks and suppliers in a way that is consistent with their own risk posture, and to seek appropriate advice to ensure their contracts are appropriate.

d. Alignment with other standards, regulation and guidance

Analysis of responses

Across the qualitative feedback, respondents showed some interest in aligning the code with existing standards, regulation and guidance. This included feedback relating to Principle 1 (secure design and development), where respondents pointed to different sectors' existing guidance, international standards and regulation. When asked about potential barriers to the code's implementation, some respondents also suggested organisations may face issues in implementing the code if it lacks sufficient alignment with existing standards and regulations.

Interest in alignment was also evident in the additional qualitative feedback (Q52), where several respondents again suggested that mapping the code against, or signposting to, other information would be a helpful addition to the code of practice.

Government response

One of the key objectives of the Code of Practice for Software Vendors is to help drive the adoption of existing technical guidance and standards. The government's aim is not to impose unnecessary burden on industry, but to remove barriers to the adoption of best practices in software development, distribution, and maintenance. Existing standards will be referenced in the implementation guidance that will accompany the final version of the code.

DSIT will build on the stakeholder engagement conducted during the co-design of the code and will continue to work with experts from industry, academia, and the NCSC to identify where alignment with existing standards, guidance and international approaches is appropriate. Concurrent to this effort, DSIT will conduct further mapping to explore a possible standards equivalence framework to facilitate compliance and future assurance routes. This process will consider those standards and frameworks referenced by respondents to the call for views as we finalise the code of practice.

The code is being designed to be consistent with international policy and standards and, once published, will be periodically reviewed to ensure it remains up to date. The provisions of the code have also been developed with consideration of both the European Union Cyber Resilience Act (CRA) requirements and the United States Secure Software Development Framework and Secure by Design guidance. DSIT has ensured that the Code of Practice for Software Vendors has no contradictions with either approach. The government is continuing to map international policy and standards as they evolve and will collaborate internationally to ensure our approach to incentivising software security is compatible with the global nature of digital supply chains.

e. Demand for an assurance regime

Analysis of responses

Responses to the call for views demonstrated some interest in adding a form of assurance to the code of practice.

Figure 1 shows that 71% agree that there should be an assurance/certification scheme for software. Those responding on behalf of organisations involved in the selling or development of software were also separately asked about what supporting materials would be helpful in enabling their uptake of the code. As Table 4 shows, the most commonly selected answer was for an assurance or certification scheme (70%).

Table 4- As a software vendor, what other supporting materials would be helpful to enable you to follow the code of practice?

Supporting materials	Number of responses	%
An assurance or certification scheme	14	70%
Product security testing labs	10	50%
Further guidance on how to manage the use open-source software in development	9	45%
Skills interventions to secure the talent pipeline in software development	9	45%

Base: 20 organisations that procure software (Q3 = “an organisation that procures software”).

There was some, but more limited, interest in regulation or mandating measures from the code. As shown in Figure 1, 50% agree there should be mandated security regulations for all software. Several respondents also suggested in qualitative feedback that there is scope for regulation or mandating the measures suggested by the code of practice.

Government response

Assurance schemes enable organisations to demonstrate their compliance with specific guidelines or standards. In doing so, they can help software vendors to use software security and resilience as a selling point, but it can also simplify the supplier assessment and management process for clients. In this way they can help to incentivise adoption and accountability across the market.

The government intends to design an assurance regime for the Code of Practice for Software Vendors. The regime will include the publication of an attestation template with the code of practice to ensure that vendors will be able to demonstrate compliance with the code to their business customers, and that business customers will be able to assess suppliers in more depth. This assurance approach will follow the NCSC's Principle Based Assurance (PBA) approach. It will help organisations and their customers feel confident that the technology they use daily is making them more secure and resilient against cyber-attacks.

The code of practice has been designed specifically to be compatible the NCSC's Principles-Based Assurance Approach. The technical controls shared in the call for views will be developed into artefacts called Assurance, Principles & Claims (APCs) as the basis for this assurance approach. APCs are designed to restructure a set of already published security and assurance principles (the code of practice) into a set of scenario claims that, if met, would show that the technology solution is achieving what the principle intends.

This represents a proven method for measuring compliance that will be consistent with future technology security assurance regimes developed by the NCSC. Having an assurance regime in place will also enable us to develop future policy options that would require reliable attestations of compliance, enabling us to explore options such as government procurement requirements. Depending on the evolution of the sector, the threat landscape, and international policy, the government may assess the need for harder levers in the future if voluntary guidance does not drive sufficient uptake of good practice in the market.

f. Language and terminology

Analysis of responses

Another common suggestion made in the call for views feedback was that the code requires more clarity in language. Comments in the qualitative feedback on Principles 1, 2 and 3 showed interest in adding clearer definitions to the code. For example, several respondents thought it would be helpful to define the meaning 'trust' as used in Principle 2 and 'timely' in Principle 3.

Government response

To address this, the revised version of the code of practice will include minor changes to the wording to provide greater clarity and ensure the terminology is accessible and actionable to senior leadership in software organisations.

The government will also draft a glossary for the code of practice. The glossary will include terms and expressions highlighted by respondents such as secure by design, secure by default, secure development framework, development lifecycle, and build environment. This will serve as a complement to the technical controls and implementation guidance that will ensure the code is outcome focused, adaptable, and implementable by any organisation selling and developing software (see section on technical controls and implementation guidance above).

4. Next steps

The call for views has confirmed that government intervention to ensure a more consistent level of best practice adoption for security and resilience in software development, distribution, and maintenance is necessary. It also demonstrates that the proposed Code of Practice for Software Vendors would be a useful tool to help enhance software security practices and better secure digital supply chains across the UK and the digital economy.

The views expressed in the call for views demonstrated a need for minor revisions to the code of practice before publishing. Responses also helped to identify next steps for developing future policy to build on the code of practice. DSIT and the NCSC will therefore take the following actions:

1. **The government will make minor edits to the Code of Practice for Software Vendors before publishing the code in 2025.** The revised version will reflect feedback on both the content and wording of the code, on achievability for small organisations, and clarity. The government will also provide a glossary of key terms to aid understanding of the final code of practice.

2. **The NCSC and DSIT will further refine the technical controls and implementation guidance to publish alongside the code of practice.** To meet the need for more detail, further content and specific claims will be added to the examples provided in the call for views to better support organisations. Particular attention will be paid to the provisions that respondents thought would be more challenging for smaller organisations.

3. **The NCSC and DSIT will develop an attestation method and assurance regime to allow software vendors to demonstrate compliance with the code.** This will be based on the technical controls using the NCSC's Principles Based Assurance Approach. The tool is intended as a market incentive for both software vendors and their customers, to facilitate accountability, market differentiation and supplier assessment methods.

4. **The government will continue to map the code of practice against other standards, regulation and guidance.** This mapping will allow DSIT and the NCSC to explore the potential for demonstrating equivalence between existing standards or frameworks and aspects of the code of practice. The government will also continue to monitor the evolving international landscape to monitor the interaction of this voluntary code with evolving standards and regulatory approaches such as the CRA and US guidance, and the impact

international approaches will have on the UK market. We will use this information and collaborate internationally to ensure that the proposed measures and future policy will not place undue burden on businesses in the software supply chain.

Annex A: First draft of code of practice (as shared in call for views)

The following is the draft of the Code of Practice for Software Vendors as shared for comment in the call for views. This version will be revised before publication.

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.

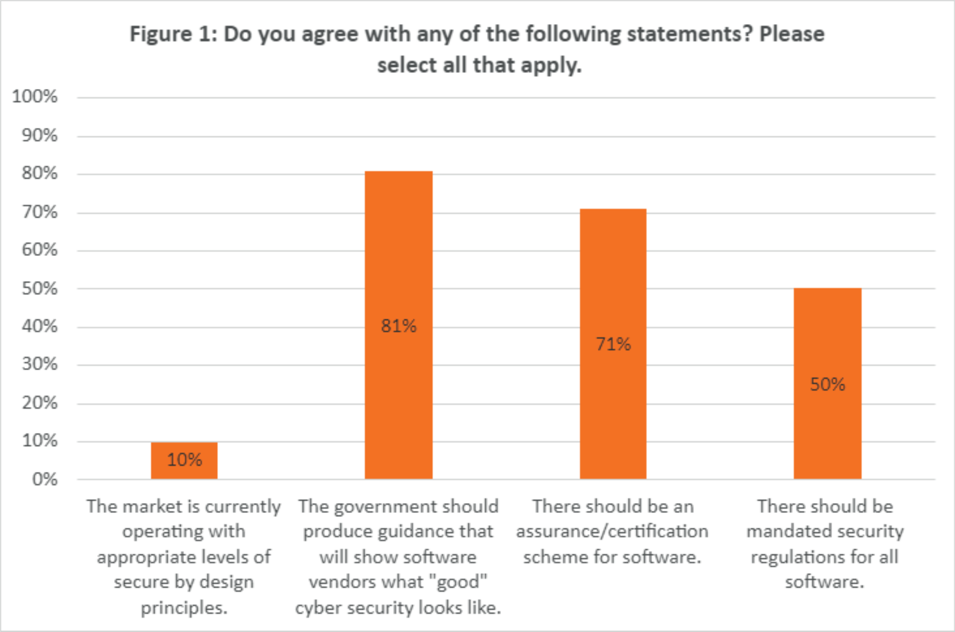
4.6 Provide customer organisations with guidance on how to use, integrate, and configure the software product or service securely.

Annex B - Full findings and charts for closed questions from the call for views Survey

This annex contains charts and quantitative data from responses to the closed questions in the call for views survey. They are provided in this annex to demonstrate full transparency of the quantitative data.

Q8: Do you agree with any of the following statements? Please select all that apply.

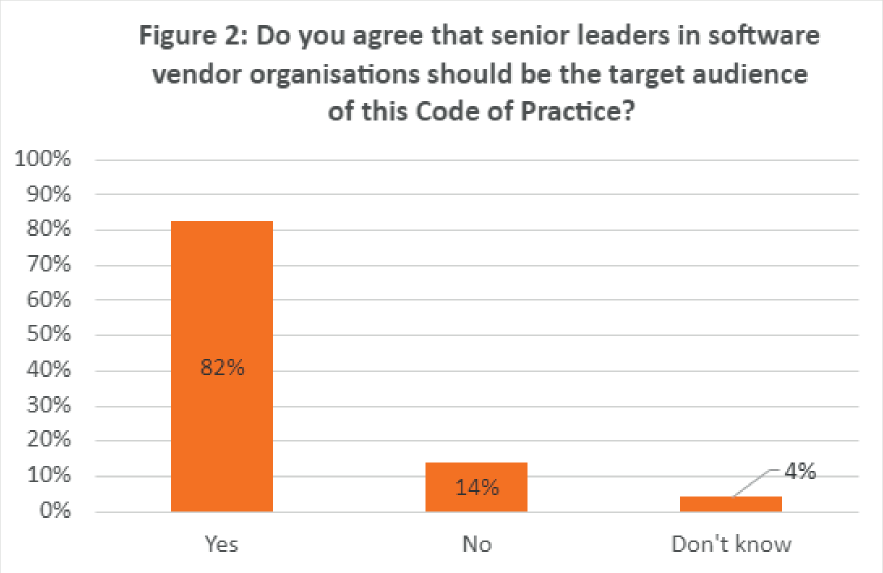
Figure 1: Do you agree with any of the following statements? Please select all that apply.



Base: 72

Q10: Do you agree that senior leaders in software vendor organisations should be the target audience of this code of practice?

Figure 2: Do you agree that senior leaders in software vendor organisations should be the target audience of this code of practice?



Base: 73

Q14a: If one was available, how likely would your organisation be to use a voluntary Code of Practice for Software Vendors to inform procurement?

Table 1.1: If one was available, how likely would your organisation be to use a voluntary Code of Practice for Software Vendors to inform procurement?

Response	Number of responses	%
Very likely	31	46%
Likely	18	27%
Neutral	9	13%
Not likely	5	7%
Definitely won't use	1	1%
Don't know	3	4%

Base: 67

Q14b: If one was available, how likely would your organisation be to use a voluntary Code of Practice for Software Vendors to inform supplier management processes?

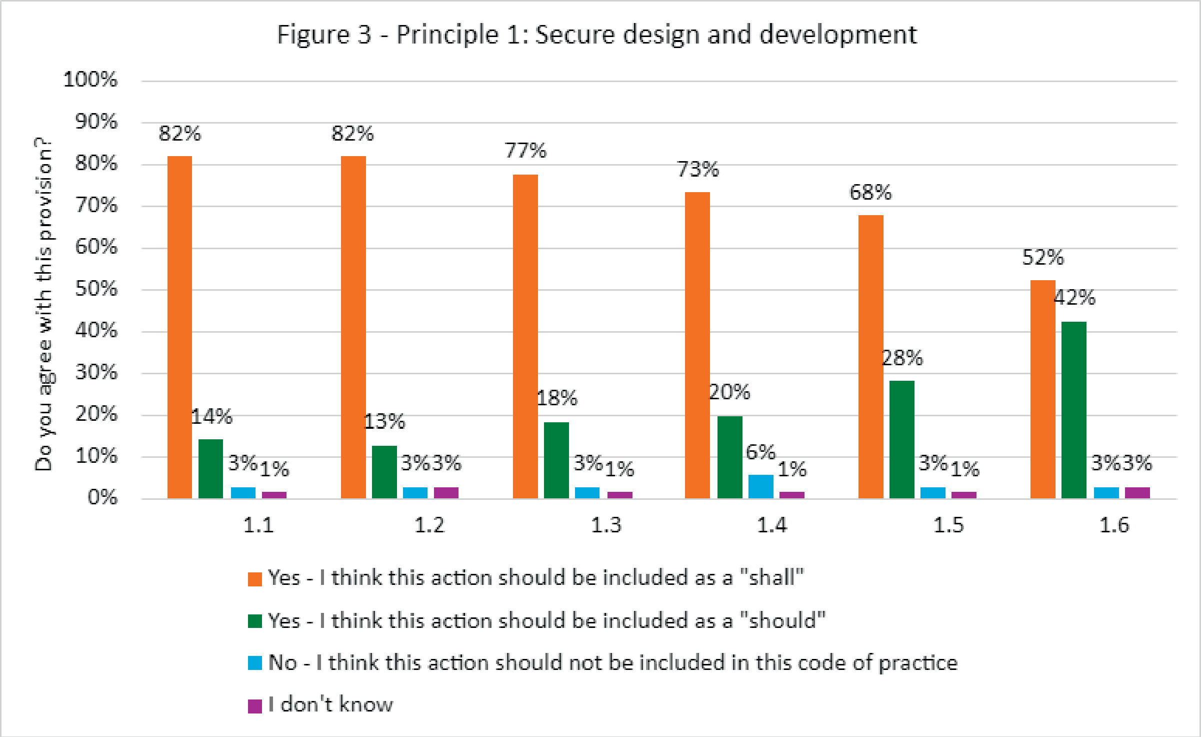
Table 1.2 - If one was available, how likely would your organisation be to use a voluntary Code of Practice for Software Vendors to inform supplier management processes?

Response	Number of responses	%
Very likely	29	43%
Likely	24	35%
Neutral	8	12%
Not likely	4	6%
Definitely won't use	0	0%
Don't know	3	4%

Base: 68

Q15a –15f: Do you agree with this provision?

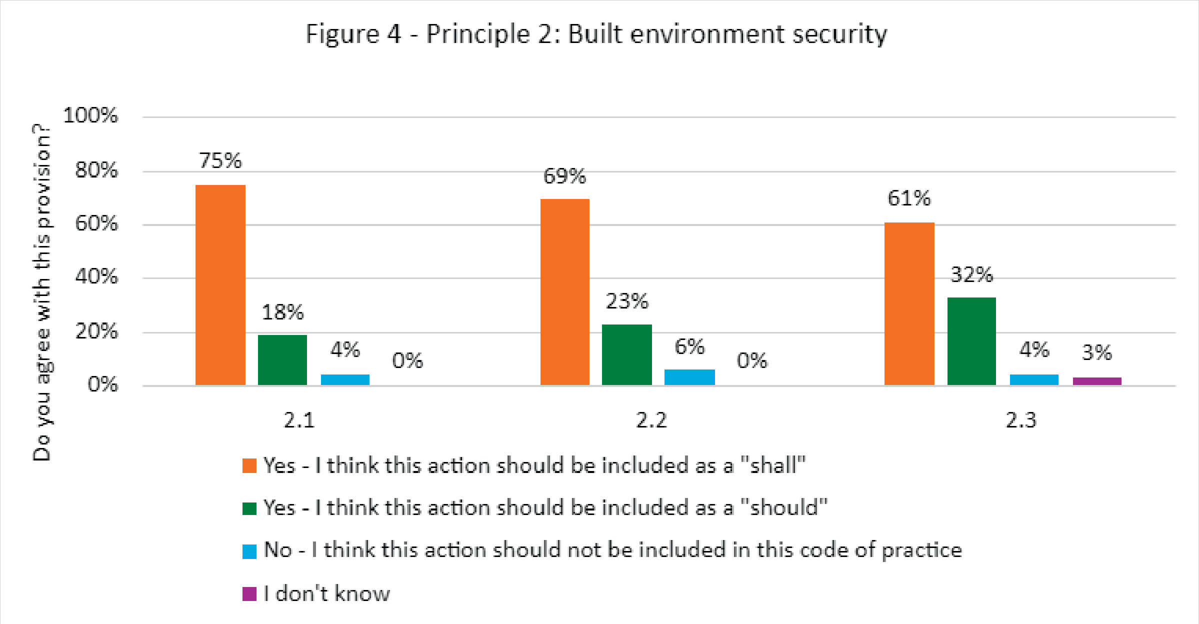
Figure 3: Support for Principle 1 (secure design and development)



Bases: Action 1.1 - 71, Action 1.2 - 71, Action 1.3 - 71, Action 1.4 - 71, Action 1.5 - 71, Action 1.6 - 71

Q18a – 18c: Do you agree with this provision?

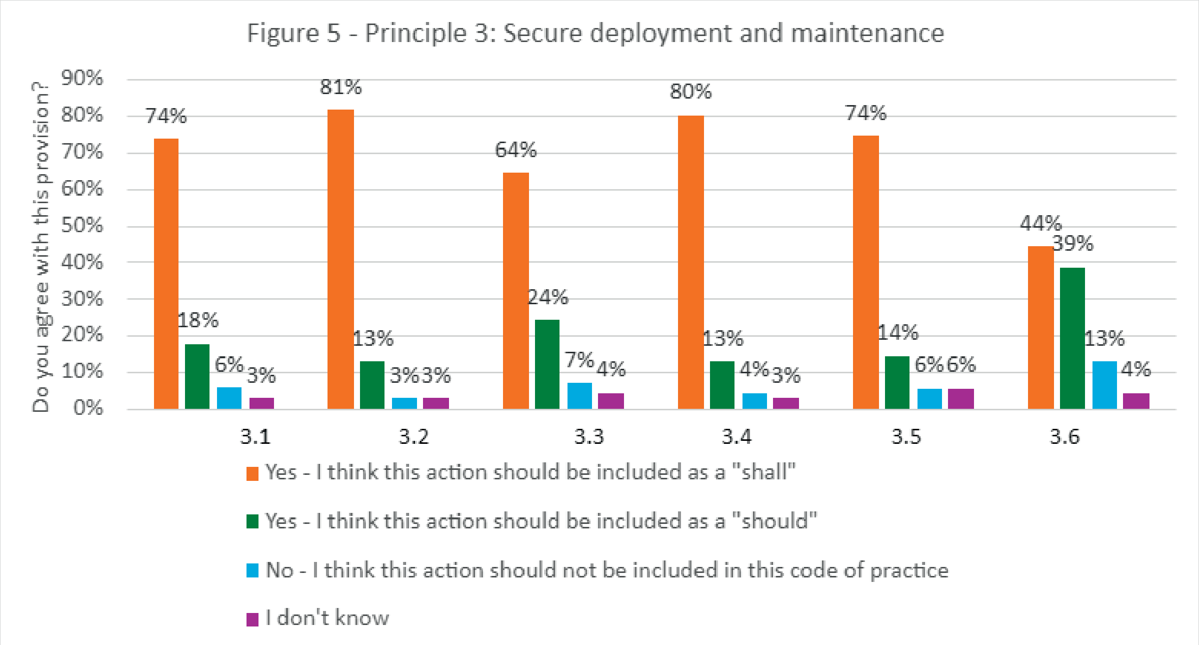
Figure 4: Support for Principle 2 (built environment security)



Bases: Action 2.1 - 71, Action 2.2 - 71, Action 2.3 - 71

Q21a – 21e: Do you agree with this provision?

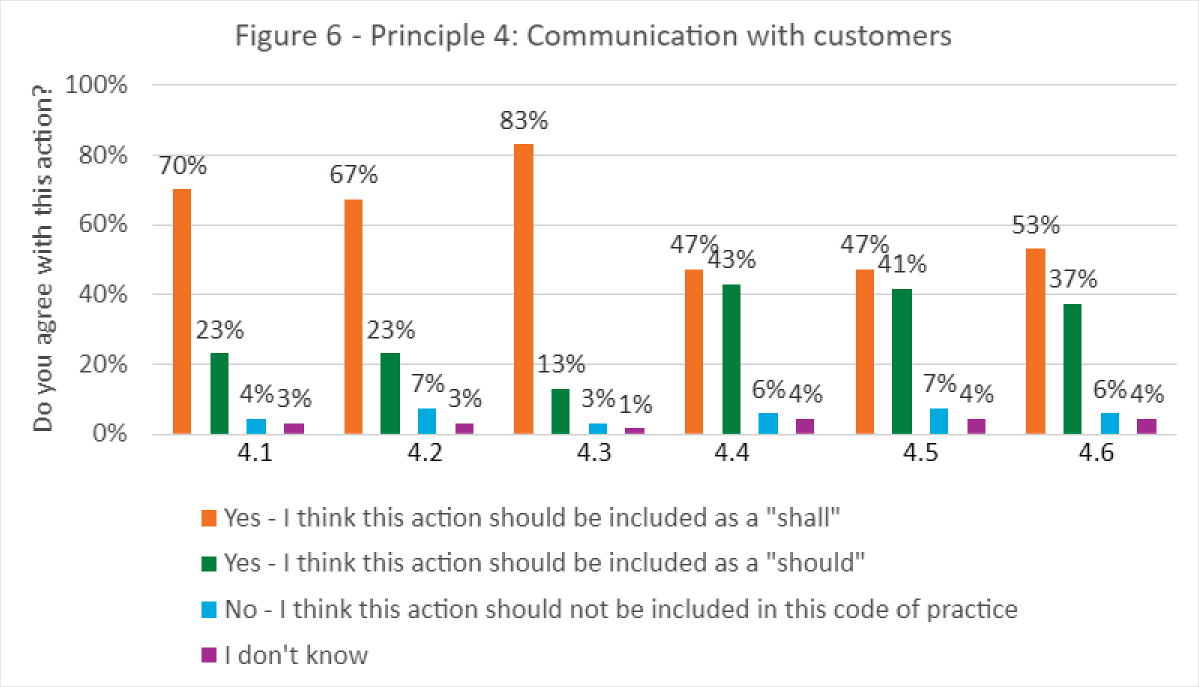
Figure 5: Principle 3 (secure deployment and maintenance)



Bases: Action 3.1 - 68, Action 3.2 - 70, Action 3.3 - 70, Action 3.4 - 70, Action 3.5 - 70, Action 3.6 - 70

Q24a – 24e: Do you agree with this provision?

Figure 6: Support for Principle 4 (communication with customers)



Bases: Action 4.1 - 70, Action 4.2 - 70, Action 4.3 - 70, Action 4.4 - 70, Action 4.5 - 70, Action 4.6 - 70

Q41: As a software vendor/developer/reseller, do you consider this code of practice feasible to implement?

Table 6.1: As a software vendor/developer/reseller, do you consider this code of practice feasible to implement?

Response	Number of responses	%
Yes	16	84%
No	3	16%
Don't know	0	0%

Base: 19 organisations/businesses involved in the sale or development of software (Q3 = “organisation/business that is involved in the sale or development of software”).

Q42: What barriers would your organisation face if asked to implement this code as a software vendor?

Table 6.2: What barriers would your organisation face if asked to implement this code as a software vendor?

Barrier	Number of responses	%
No barriers. The actions listed in this code of practice are within my organisations' capability	13	68 %
This code of practice would be too expensive to implement.	0	0%
Staff do not have the required skills to implement this code of practice.	1	5%
The actions in this code of practice are too difficult to scale up across the organisation.	0	0%
My organisation does not have the necessary staff to implement this code of practice.	1	5%
Senior leaders in my organisation are not likely to engage with this code of practice.	1	5%
N/A - my organisation does not develop or sell software.	1	5%
Other	2	11 %

Base: 19 organisations/businesses involved in the sale or development of software (Q3 = "organisation/business that is involved in the sale or development of software").

Q43: As a software vendor/developer/reseller, would this code cause excessive hindrance to innovation?

Table 6.3: As a software vendor/developer/reseller, would this code cause excessive hindrance to innovation?

Response	Number of responses	%
Yes	3	14%
No	14	67%
Don't know	3	14%
N/A my organisation is not a software vendor, developer or reseller	1	5%

Base: 21 organisations/ businesses involved in the sale or development of software (Q3 = "organisation/business that is involved in the sale or development of software").

Q44: As an organisation procuring software, do you consider that it would be feasible to use this code of Practice in your procurement processes?

Table 6.4 - As an organisation procuring software, do you consider that it would be feasible to use this code of practice in your procurement processes?

Responses	Number of responses	%
Yes	14	64%
No	8	36%
Don't know	0	0%

Base: 22 organisations/businesses involved in the sale or development of software (Q3 = "organisation/business that is involved in the sale or development of software").[4]

[4] Please note that this question (Q44) was originally written for organisations procuring software, however, the survey was incorrectly routed so this question appeared for organisations/businesses involved in the sale or development of software (based on responses to Q3).

Q45: What barriers would your organisation face if asked to request that software suppliers to your organisation meet this code of practice?

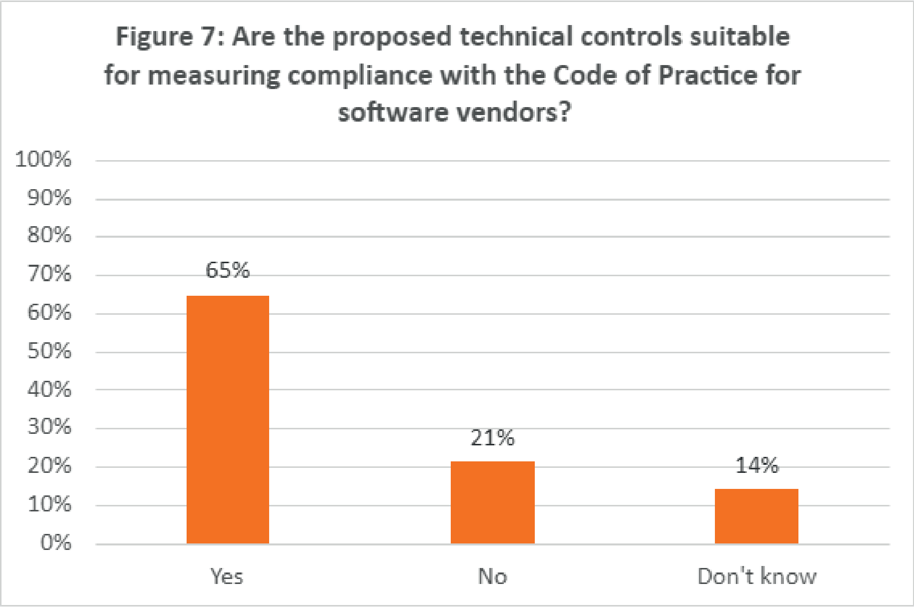
Table 6.5 - What barriers would your organisation face if asked to request that software suppliers to your organisation meet this code of practice?

Barriers	Number of responses	%
No barriers. My organisation would not face any significant challenges in using this code of practice in procurement processes.	25	37%
This code of practice would be too expensive to incorporate into procurement processes.	7	10%
This code of practice would be incompatible with my organisation's procurement processes.	4	6%
Staff responsible for procurement would not have the necessary skills to use this code when negotiating with suppliers.	6	9%
Staff do not have the necessary skills to understand any attestation or proof provided by software vendors of adherence to this code of practice.	5	7%
Other (please specify)	20	30%

Base: 67

Q46a: Are the proposed technical controls suitable for measuring compliance with the code of practice for software vendors?

Figure 7: Are the proposed technical controls suitable for measuring compliance with the Code of Practice for Software Vendors?



Base: 71

Q50a: 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?

Table 7.1 - 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?

Supporting material	Number of responses	%
Standardised contractual clauses	7	50 %
Guidance on how to assess suppliers' adherence to the code	11	79 %
Standardised templates for supplier attestation of compliance with the code	9	64 %
Training for non-cyber specialists	6	43 %
An assurance scheme or certification	9	64 %
Product security testing labs	4	29 %
N/A - my organisation does not procure software	0	0%
Other	1	7%

Base: 14 software procurement organisations (Q3 = "an organisation that procures software")

Q51: As a software vendor, what other supporting materials would be helpful to enable you to follow the code of practice?

Table 7.2 - As a software vendor, what other supporting materials would be helpful to enable you to follow the code of practice?

Supporting materials	Number of responses	%
An assurance or certification scheme	14	70 %
Product security testing labs	10	50 %
Further guidance on how to manage the use open-source software in development	9	45 %
Skills interventions to secure the talent pipeline in software development	9	45 %

Base: 20 organisations that procure software (Q3 = "an organisation that procures software").

Annex C – Survey questionnaire

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

Q2a. [if Q2 = "Other"] If Other, please specify. [Free text]

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
- A organisation that procures software
- A cyber security provider
- An educational institution
- Government
- Other

Q3a. [if Q3 = "Other"] If Other, please specify. [Free text]

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

Q6a. [if Q6 = “Other”] If Other, please specify. [Free text]

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

Q7a. [if Q7 = “Other”] If Other, please specify. [Free text]

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

Q14: 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 focused on individual actions asked by the code.

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.

Q15a: 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.

Q15b: 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.

Q15c: 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.

Q15d: 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.

Q15e: 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.

Q15f: 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.

Q16: Do you think there is anything missing from this Principle? If so, what? [Free text]

Q17: 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.

Q18a: 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.

Q18b: 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.

Q18c: 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.

Q19: Do you think there is anything missing from this Principle? If so, what? [Free text]

Q20: 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:

- Ensure that software is distributed securely to customers.

Q21a: 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:

- 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.

Q21b: 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:

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

Q21c: 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:

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

Q21d: 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:

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

Q21e: 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:

- 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.

Q21f: 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.

Q22: Do you think there is anything missing from this Principle? If so, what? [Free text]

Q23: 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:

- 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.

Q24a: 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:

- 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.

Q24b: 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:

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

Q24c: 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:

- 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.

Q25d: 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:

- 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.

Q24e: 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:

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

Q24: 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.

Q25: Do you think there is anything missing from this Principle? If so, what? [Free text]

Q26: 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 organisation's 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/business that is involved in the sale or development of 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

Q45a: If other, please specify. [Free text]

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 do you feel the proposed technical controls are **not** suitable for measuring compliance with the code of practice? [Free text]

Q49: Do you have any other comments about the implementation guidance and technical controls outlined above (found in annex B of the consultation)? [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? [select all that apply]

- 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

Q50b [if Q50 = "Other"]: If other, please specify. [Free text]

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

Survey close

Q52: Do you have any other feedback on our code of practice? [Free text]

E03293157

978-1-5286-5441-8

E03293157

978-1-5286-5441-8