ARCULUS
CYBER SECURITY
a Bridewell company

Cyber Governance Code of Practice Pilot

Author: Arculus Cyber Security

Contents

List of figures

List of tables

Executive summary

The Cyber Governance Code of Practice Pilot

The Department for Science, Innovation and Technology (DSIT) commissioned Arculus Cyber Security, a Bridewell company ("Arculus"), to deliver user testing of the draft Cyber Governance Code of Practice ("the Code"). The Code brings together critical actions that all directors and their organisations should take to govern cyber risk and formalises government's expectations of directors for governing cyber risk as they would any other business risk.

The implementation phase of the pilot ran for 5 weeks, during which time organisations attempted to implement all or part of the Code. The pilot ended on 15 March 2024.

Participation

27 organisations were accepted to participate in the pilot, of the 33 that applied. Of those 27, 19 completed an assessment of their organisation's cyber maturity and the degree to which they currently carry out activities contained within the Code. 6 participants attended free support sessions with Arculus cyber security consultants, and 12 participants were interviewed about their experiences implementing the Code.

Implementation of the Code

Limited implementation of the Code by participants during the pilot was observed. As such, it is difficult to accurately calculate the true cost and time needed to implement the Code, however the following estimates can be provided based on the qualitative research conducted:

- An estimate of around 6 months to introduce all of the actions outlined in the Code;
- An estimate of around 12 months to fully embed the principles of the Code in business and governance practices, followed by continuous improvement, increasing maturity and evolving organisational culture over time;
- An estimate that Principles C and D are likely to be more costly than others for organisations to implement, due to costs associated with employee training and incident response exercises.

Language used in the Code

Participants stated that the Code successfully avoided use of technical cyber security terminology that could otherwise have made it inaccessible for its intended audience of directors, non-executive directors and senior leadership. However, when implementing the code, participants found that the language was not specific enough for them to understand what was being asked of them. Feedback indicated that business terminology contained in the Code may not be understood, or interpreted inconsistently, across different organisations.

Tools and guidance

Feedback provided about the use of the National Cyber Security Centre (NCSC) Cyber Security Toolkit for Boards[1] ("NCSC Board Toolkit") indicated that it was a helpful supplement to the Code, but participants would benefit from a clear mapping between the Code and the relevant parts of the NCSC Board Toolkit. The same was true for other cyber security standards and frameworks that organisations are currently using to measure and improve their cyber security posture, with participants stating they would find it useful to point to content within those standards that could help them better understand how the Code should be applied. Although the Code did not contradict these standards, participants indicated they would benefit from understanding where they overlap.

Participants expressed that an additional layer of guidance is needed, containing a greater level of detail than the Code itself, in order to effectively implement it. Feedback suggested that participants needed to be able to identify a set of activities that make up the higher-level actions described in the Code, and they would benefit from suggestions, appropriate to the size of their organisation, that would help them achieve this.

Recommendations

This report contains recommendations to:

- Adjust the language of the Code to help users better understand what it is asking of them;
- Map new and existing guidance to the Code that helps organisations of different sizes understand the steps they need to take to implement it;
- Publish the Code on a government website, such as GOV.UK and/or NCSC, and promote awareness of it through industry and professional associations.

[1] Cyber Security Toolkit for Boards - NCSC.GOV.UK

Introduction

In December 2023, the Department for Science, Innovation and Technology (DSIT) commissioned Arculus Cyber Security (Arculus), a Bridewell company, to conduct user testing of a draft Cyber Governance Code of Practice ("the Code"). The testing aimed to explore the feasibility of implementing the Code with directors, non-executive directors and senior leaders from a variety of organisations, and better understand what additional resources or guidance might be needed to support them. Evidence gathered from the user testing phase is intended to help improve the Code, ensuring it is fit for purpose upon publication.

This report details findings from the testing, including quotes from participants and insight gathered from qualitative research activities conducted to date. As with any qualitative findings, these examples are not intended to be statistically representative.

The Cyber Governance Code of Practice

DSIT developed the draft Code in partnership with the NCSC as well as industry leaders including chief executives, non-executive directors and auditors. It is intended to form simple, actions-focused support to make it easier for boards and directors from organisations of all sizes and sectors, both public and private, to understand what they need to do to govern cyber risk effectively and increase their organisation's resilience to cyber threats.

The Code has been developed in the context of existing cyber security frameworks, guidance and standards, including the NCSC Board Toolkit and the NCSC Cyber Assessment Framework (CAF)[2]. The Code includes five principles which have been identified as the critical areas that leaders must engage with:

- **Principle A:** Risk management
- **Principle B:** Cyber strategy
- **Principle C:** People
- **Principle D:** Incident planning and response
- **Principle E:** Assurance and oversight

Each principle is supported by 3 to 5 fundamental actions drawn from best practice and is intended to align with and complement existing government and industry resources. A

[2] Cyber Assessment Framework - NCSC.GOV.UK

copy of the draft Code, in the format it was given to participants, is provided at Annex 1: Draft Cyber Governance Code of Practice.

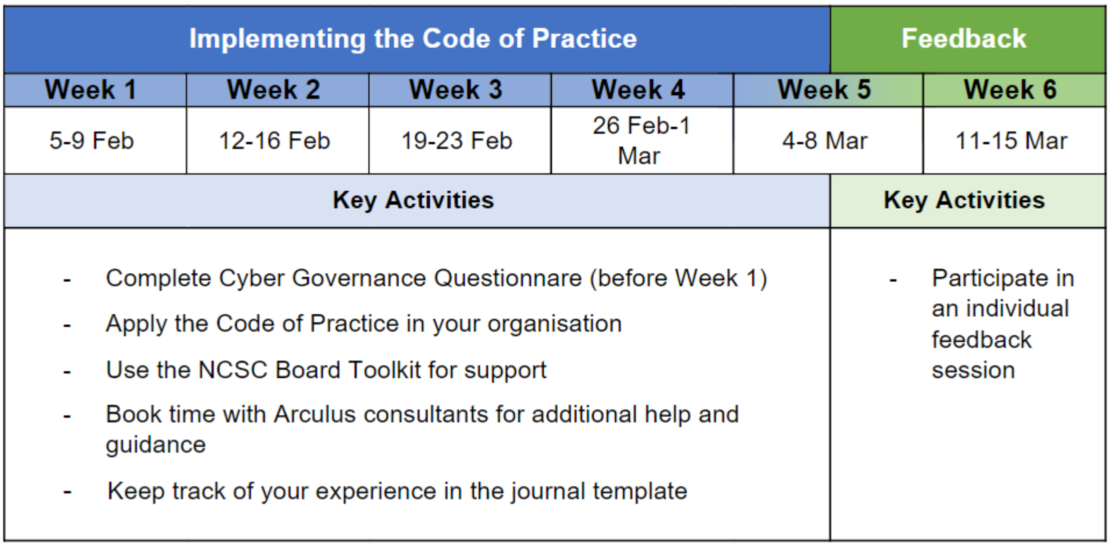
Pilot design

User testing of the Code has been conducted in the form of an implementation pilot, consisting of:

1. **A planning phase**, where pilot objectives and deliverables were agreed.
2. **A recruitment phase**, where suitable participants were identified and shortlisted to conduct user testing of the Code.
3. **An onboarding phase**, where participants were provided with a copy of the Code, signposted to the NCSC Board Toolkit and introduced to the planned research activities. During this phase participants were asked to complete a Cyber Governance Questionnaire to capture their organisation's existing level of cyber maturity and approach to governing cyber risk.
4. **An implementation phase**, where participants were asked to implement all or part of the Code in their organisation over a 5-week period. During this phase participants were issued with a journal template to track their experiences and offered support sessions with cyber security consultants where they could receive one-to-one advice and guidance. The journal template provided participants with a place to record the actions they took, what went well, what didn't go well, resources they used, time taken and costs incurred during the pilot.
5. **A feedback phase**, where participants were interviewed to provide feedback about their experience implementing the Code. Participants were encouraged to review their journals ahead of their interview, and some submitted their completed journals to researchers, although this was not a requirement.

The following timeline was shared with participants during the onboarding phase:

Figure 1: Pilot timeline



Implementing the Code of Practice					Feedback
Week 1	Week 2	Week 3	Week 4	Week 5	Week 6
5-9 Feb	12-16 Feb	19-23 Feb	26 Feb-1 Mar	4-8 Mar	11-15 Mar
Key Activities					Key Activities
- Complete Cyber Governance Questionnare (before Week 1) - Apply the Code of Practice in your organisation - Use the NCSC Board Toolkit for support - Book time with Arculus consultants for additional help and guidance - Keep track of your experience in the journal template					- Participate in an individual feedback session

Methodology

The user research involved a mixed methods approach using both quantitative and qualitative data collection. The following table shows the different strands of data collection and the sample sizes achieved for each. A detailed overview of the methodology is provided at Annex 2: Methodology.

Table 1: Data collection and sample sizes

Data collection	Sample achieved
Screener forms	27 participants selected (out of 33 applications)
Maturity assessment (Cyber Governance Questionnaire)	19
Support session notes	6
Interviews with participants	12
Journals	4

Reporting

This report draws on data from all sources identified in Table 1: Data collection and sample sizes and aims to address the key research questions outlined in both the initial invitation to tender and subsequent discussion with DSIT. A full list of research questions is provided in Annex 3: Research questions.

The analysis in this report is intended to provide DSIT with a profile of pilot participants and their associated organisations, including organisation size, sector, region and cyber maturity before implementing the Code. It aims to provide actionable insight from the pilot and recommendations for improvements to the Code, supporting tools, and guidance to help organisations adopt the Code upon its publication.

Data limitations

This section outlines in brief the main data limitations relating to the qualitative and quantitative findings described in this report.

The key data limitations relating to the findings are:

- **Small sample size:** Small sample sizes should be interpreted with caution. At the conclusion of the pilot, complete datasets were available for 12 participants. As participants were given a different order in which to implement the principles of the Code during the pilot, and some did not complete all principles, the number of participants who provided feedback for each principle ranged from 8 to 9.
- **Self-selection:** Participants volunteering to take part in research activities are likely to have different characteristics from the general population of interest, which can introduce volunteer bias. In the case of this pilot, this may include organisations that had a higher existing level of cyber maturity, were more engaged with the topic of cyber security or deemed themselves to have sufficient capacity, such as through greater availability of time or resources, to participate in activities beyond their usual day job.
- **Attrition:** Participants who withdrew during the course of the pilot may have systematic differences to those who continued, which can introduce attrition bias. For example, some may have needed to spend more time, effort and money during the pilot to reach the same outcomes as others. This may disproportionately impact smaller organisations or those with lower existing cyber maturity and affect how those characteristics are represented in the findings. As the draft Code was not publicly available, participants did not have sight of it prior to the start of the pilot. As such, it may have been difficult for them to judge the level of effort that would be required to implement the Code during the pilot before making the decision to volunteer. The withdrawal of participants during the pilot also led to uneven collection of data across the different principles of the Code.
- **Self-reported maturity, activity and outcomes:** Assessment of organisations' cyber maturity, evidence of implementation of the Code and the resulting

outcomes is based on subjective, self-reported data. This may lead to bias, for example participants might over or underestimate the maturity of their current approach to managing cyber security risk prior to implementing the Code, as they are not aware of gaps in their approach or areas of comparatively high maturity until these are highlighted through use of the Code.

- **Pilot duration:** The implementation phase of the pilot was 5 weeks or less, depending on the point at which participants joined. Participants who joined later in the pilot or were moved from the waitlist had a shorter implementation period. The activities conducted and outcomes achieved by participants may therefore differ according to the point at which they began implementation and the remaining time available to them in the pilot. Marginal improvements over a short time period may be difficult to detect.
- **Limited implementation:** Minimal implementation of the Code was observed during the pilot. Participants broadly expressed either:
    - They reviewed the Code and found they were already carrying out the majority of actions. In many cases they were already using one or more existing cyber standards or frameworks, and sense-checked that these aligned with the Code, or;
    - The pilot duration was too short to effect change. Some participants stated adoption of the Code would require significant cultural change within their organisation, and that this is likely to take months or years to achieve.
- **Interview timings:** Participant interviews were conducted at a fixed point in time. In some cases, interviews took place before participants had completed implementation of all or part of the Code, so only early outcomes were able to be captured.

Pilot participation

This section reports pilot participation numbers and diversity across key organisation demographics such as size, sector and existing cyber maturity. This section also draws on feedback from participants about motivations for volunteering to participate in the pilot and challenges they anticipated they would face while implementing the Code.

Recruitment

The opportunity to participate in user testing of the Code was publicised through a variety of routes:

- Engagement with 35 trade bodies and industry associations who communicated the opportunity to their members. This included sector-specific organisations, membership organisations for directors, non-executive directors and governance professionals, and groups focused on small businesses and charities.
- Publication of a page about user testing of the Code on GOV.UK[3].
- Use of cyber security-focused networks such as regional cyber resilience centres and professional networks such as LinkedIn.
- Direct approaches to organisations known to DSIT and Arculus that met the criteria for participation.

Applicants were asked to complete a screener form (detailed in Annex 2: Methodology), and a selection was made using the process outlined in Annex 4: Participant selection process.

Applications to the Cyber Governance Code of Practice pilot

- 33 applicants completed the screener form
- 30 suitable participants were shortlisted
- 27 participants were invited to join the pilot, after adjusting for organisation demographics
- 48% of applicants heard about the pilot through the page published on GOV.UK (16 out of 33)
- 27% of applicants were referred by membership bodies and trade associations (9 out of 33)

[3] UK cyber governance project - GOV.UK (www.gov.uk)

Participant engagement

Contact with participants during the implementation phase of the pilot consisted of:

- Provision of pilot materials, instructions and links to book support sessions;
- A live online briefing session introducing the pilot and planned research activities, with a recording circulated afterwards;
- A weekly email reminder to complete implementation and research activities;
- Online support sessions providing additional advice and guidance;
- Prompts to book interview sessions.

Of the 27 shortlisted participants, 8 attended the live briefing session. A recording of the session received 13 views, although these views were anonymous, and it is therefore not possible to determine whether they were unique.

19 of the 27 shortlisted participants (70%) completed the Cyber Governance Questionnaire and were therefore able to be assessed for their existing level of cyber maturity.

6 participants utilised support sessions with Arculus cyber security consultants to receive advice and guidance on the interpretation and implementation of the Code.

12 participants were interviewed, and 7 participants declined to be interviewed. Although not required to do so, 4 participants shared their completed journal templates with researchers, including one who was unable to attend an interview.

Reasons for withdrawal

8 participants (30%) withdrew after receiving a copy of the Code and instructions for implementation during the pilot, and before completing the Cyber Governance Questionnaire.

Participants who withdrew during the onboarding phase belonged to one of two groups:

- Those who said their participation in the pilot would not provide value to their organisation, as they determined they were already carrying out the actions described in the Code;
- Those who, upon reviewing the pilot timeline, found it unachievable due to capacity or time constraints and competing business priorities.

Participants who declined to be interviewed stated they had not attempted to implement the Code during the pilot due to competing business priorities, or were unavailable during the interview phase.

Profile of participants

This section outlines findings about the profile of active participants (n=19) in the Cyber Governance Code of Practice pilot and refers to data gathered through the screener form and Cyber Governance Questionnaire. These findings provide context to the emerging insights discussed later in this report.

Organisation size

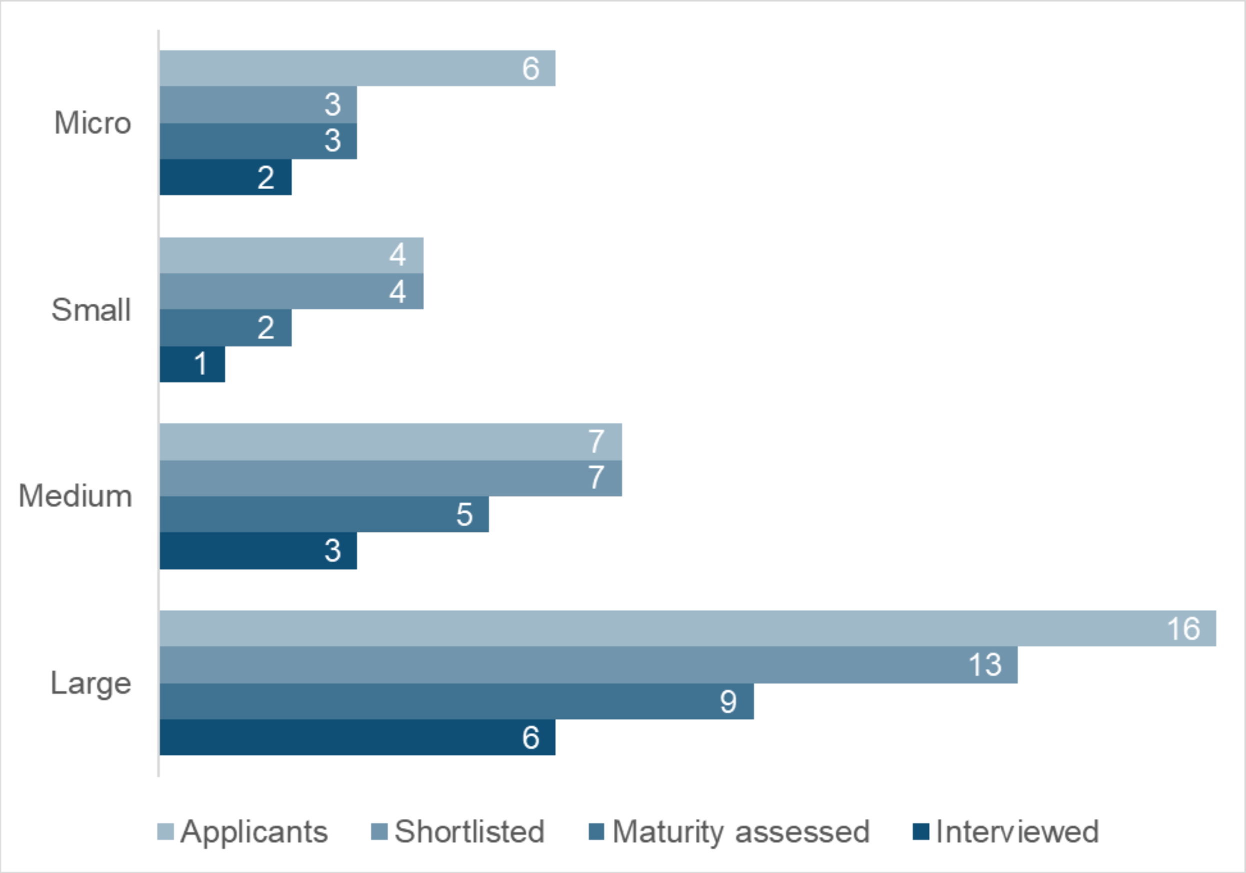
The table below shows the proportion of active participants by organisation size, compared with the target sample. The sample was below the target for medium-sized organisations, and above the target for micro, small and large organisations.

Table 2: Organisation sizes against sample target

Size (number of employees)	Target	Achieved
Micro (1 to 9)	10%	14% (n=3)
Small (10 to 49)	10%	14% (n=2)
Medium (50 to 249)	50%	24% (n=5)
Large (250 or more)	30%	48% (n=9)

The chart below demonstrates the split of sizes in the sample at different stages of the pilot. The highest rate of attrition between shortlisting and interviews was among small organisations (67%) and the lowest was among micro organisations (33%), although smaller sample sizes in these groups meant withdrawal of a single organisation had a greater impact on attrition rate. Additional charts demonstrating the split of organisation sectors and regions can be found in Annex 4: Participant selection process.

Figure 2: Cohort composition by organisation size throughout the pilot



Motivations for participating in the pilot

Organisations expressed varying motivations for participating in the pilot:

- Some participants from organisations with a higher level of cyber maturity sought to cross-reference the Code against existing cyber standards they have achieved or are working towards. Some wanted to find out whether the Code outlined any additional actions they should consider, and they viewed the Code as an additional layer of assurance that they are on the right track.
- Some participants wanted early sight of the Code so they could prepare to demonstrate that they adhere to it, as they anticipated their customers would demand this of them once the Code is published.
- Some participants who ran micro and small businesses expressed a desire to ensure they were managing cyber risk appropriately and following government guidance.

Cyber maturity

Data about the cyber maturity of participating organisations was collected through the screener form and Cyber Governance Questionnaire.

Existing standards, frameworks and regulations

79% of screener form respondents (26 out of 33) and 95% of Cyber Governance Questionnaire respondents (18 out of 19) reported they meet an existing cyber security standard or hold an existing cyber security certification.

The most frequently cited certifications were Cyber Essentials (including Cyber Essentials Plus)[4] and ISO 27001[5]. Some organisations in the research cohort are also complying with or working towards the NHS Data Security and Protection Toolkit (DSPT)[6], NCSC's CAF and the National Institute of Standards and Technology (NIST) Cyber Security Framework[7]. Organisations in the health and social care sector regulated by the Care Quality Commission stated they are required to comply with the NHS DSPT, and a small number of organisations cited industry-specific regulations such as the Telecommunications (Security) Act 2021[8] that apply to their sectors.

Use of standards and frameworks

95% of Cyber Governance Questionnaire respondents (18 out of 19) reported they meet an existing cyber security standard or hold an existing cyber security certification, and 61% of those (11 out of 18) were meeting or working towards more than one.

Cyber-related activities

The table below summarises participants' responses to questions about the cyber security-related activities currently conducted by their organisation.

[4] About Cyber Essentials - NCSC.GOV.UK

[5] ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements

[6] Data Security and Protection Toolkit (dsptoolkit.nhs.uk)

[7] Cybersecurity Framework | NIST

[8] Telecommunications (Security) Act 2021 (legislation.gov.uk)

Table 3: Cyber-related activities

Activity	Number of organisations	Percentage of cohort
Processes personal data	18	95%
Takes measures to protect personal data from unauthorised access, loss destruction or damage	17	89%
Has cyber security policies in place	18	95%
Provides cyber security awareness training to all members of staff	16	84%
Puts technical controls in place to protect against cyber attacks, such as firewalls or security monitoring	16	84%
Has someone at board level who is responsible for cyber risk	15	79%
Employs or contracts staff with cyber technical skills	14	74%

Data from 19 respondents

26% of respondents (5 out of 19) reported their organisation has previously experienced a cyber security breach.

Board engagement with cyber security

74% of questionnaire respondents (14 out of 19) stated that cyber is discussed at board level on a regular basis. 16% (3 out of 19) said this occurs on an ad-hoc basis, and 11% (2 out of 19) stated cyber is never discussed at board level. This is similar to figures reported in DSIT's Cyber Security Breaches Survey 2024[9], which found that four-fifths of medium and large businesses updated their senior team about cyber security at least once a year, with 63% of medium businesses and 78% of large businesses doing this at least quarterly.

As a group, participants in this pilot could be deemed to be more cyber mature overall than organisations in the Cyber Security Breaches Survey due to their greater adoption of cyber security standards and frameworks such as Cyber Essentials. 47% of participants in this pilot report adhering to Cyber Essentials or Cyber Essentials Plus, compared to 3% of medium and large businesses in the Cyber Security Breaches

[9] Cyber security breaches survey 2024 - GOV.UK (www.gov.uk)

Survey. However, when it comes to cyber governance practices, the level of maturity is broadly similar.

Accountability for cyber security

95% of questionnaire respondents (18 out of 19) said that they, as a director or C-level executive, were ultimately responsible for their organisation's cyber security.

Barriers to cyber maturity

Budget and financial constraints were the most commonly cited barrier to improving cyber security. Participants from small organisations highlighted that security solutions are expensive and often require minimum licensing volumes or 'enterprise tier' products that are aimed at larger organisations, putting them out of their reach or requiring disproportionate investment. 26% of respondents (5 out of 19) referenced a lack of technical expertise within their organisation that impacts their ability to understand the risk and proportionate solutions, along with difficulty recruiting and retaining technical staff, and another 26% (5 out of 19) cited a lack of time. 11% (2 out of 19) referenced competing business priorities and low staff engagement.

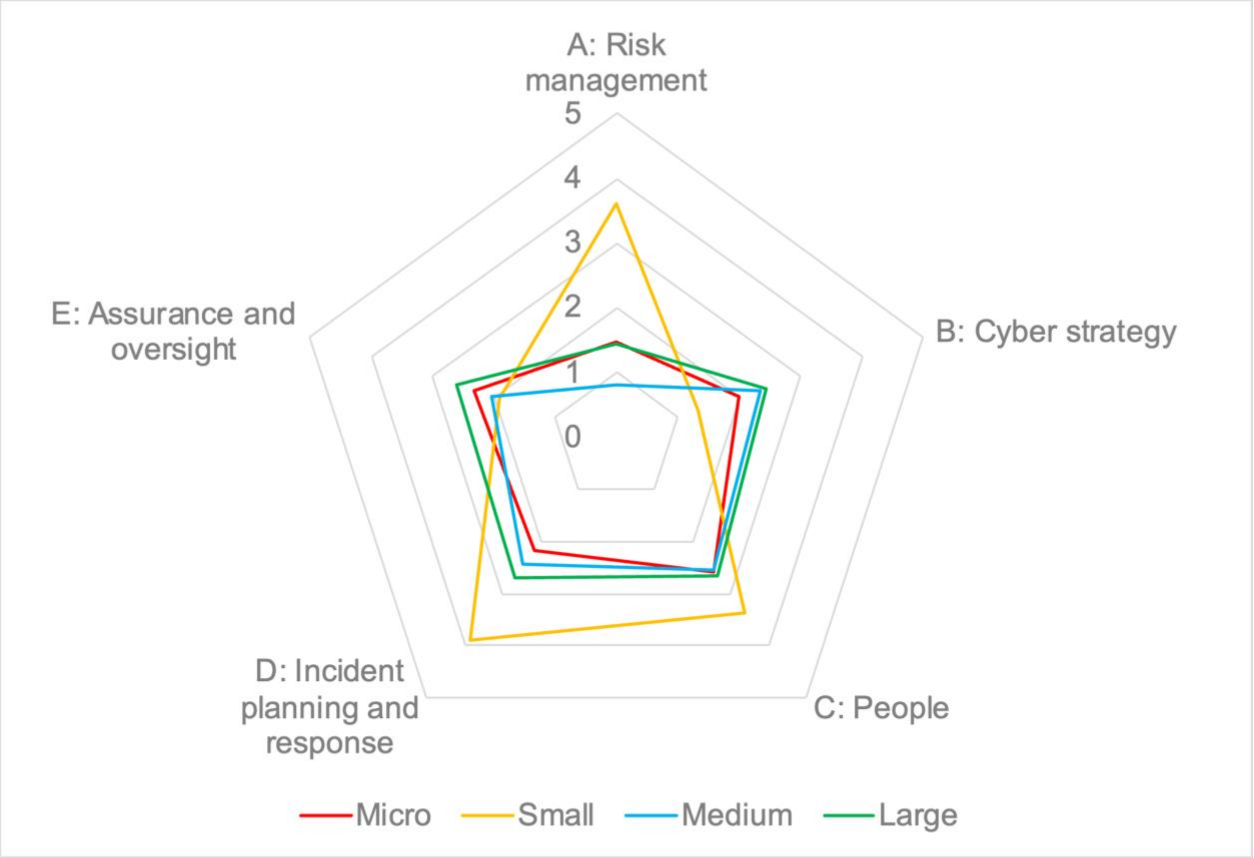
Maturity against the Cyber Governance Code of Practice

In the Cyber Governance Questionnaire, participants were asked to rate the degree to which they currently carry out the activities detailed within the Code. Further detail about the approach and scoring is detailed in Annex 5: Maturity assessment. Maturity is rated on a scale of 0 (lowest) to 5 (highest).

Low to medium maturity

The mean maturity score for each principle across all organisation sizes and sectors was between 2 (managed) and 3 (defined). This indicates that the principles of the Code were generally already being applied to some degree across the majority of participant organisations, albeit in an ad-hoc manner and not embedded in formalised processes.

Figure 3: Maturity by organisation size



Data from 19 respondents

Maturity ratings were reasonably consistent across different sized organisations, with the exception of small organisations, who reported a higher level of maturity for Principles A, C and D, and a lower level of maturity for Principle B. The small sample size of small organisations among questionnaire respondents (n=2) is likely to make this result unreliable.

As shown in the chart above, for micro, medium and large organisations, maturity for Principle A: Risk management was rated lowest, with the remaining principles being rated at a similar level of maturity.

Action 5 of Principle A: Risk management, relating to assessing supplier information, received the lowest mean maturity score overall. 37% of questionnaire respondents (17 out of 19) stated they don’t currently do this, are unable to do this, or haven’t implemented it yet

Action 4 of Principle A received the highest mean maturity score overall. This action relates to addressing cyber risks and establishing risk ownership. 84% of respondents (16 out of 19) stated they were already doing this, with 56% of those (9 out of 16) stating they are doing this in a proactive and adaptive manner.

The table below shows mean maturity scores across the different actions contained within each principle of the Code.

Table 4: Mean maturity scores

Principle	Mean score	Action 1	Action 2	Action 3	Action 4	Action 5
A: Risk management	2.58	2.74	2.47	2.79	3.05	1.84
B: Cyber strategy	2.23	2.11	2.16	2.42	N/A	N/A
C: People	2.70	2.79	2.58	2.95	2.47	N/A
D: Incident planning and response	2.67	2.74	2.26	2.68	3.00	N/A
E: Assurance and oversight	2.34	2.42	2.21	2.79	2.16	2.11

Data from 19 respondents

Table 5: Definition of maturity scores

Score	Survey response	CMMI Maturity level
0	I don't know/I'm unsure *or* I don't do this or am unable to do this	N/A
1	I'm aware of this but haven't implemented it yet	Initial
2	I've done this but it's not embedded yet	Managed
3	I consistently do this	Defined
4	I'm proactive in doing this and adapt to changes	Quantitatively managed
5	I'm proactive in doing this, measure progress and find ways to improve	Optimising

Participants who reported their organisation had previously experienced a cyber security breach reported slightly lower maturity scores than the cohort as a whole, with the exception of Principle D where they assessed themselves slightly higher. Their mean score for Action 4 of Principle D, which relates to lessons learned after an incident, was 3.2. The mean score across all participants for this action was 3.0.

Anticipated challenges

Some patterns were observed between the maturity levels provided by participants and the challenges they anticipated in implementing the Code:

- Participants who rated their maturity highest were more likely to have concerns about the time it would take to implement the Code. 43% of participants with an overall maturity score of 3.0 or higher (3 out of 7) expressed this as their main concern.
- Participants who rated their maturity lowest were more likely to express concerns about a lack of technical capability within their organisation. 42% of participants with an overall maturity score lower than 3.0 (5 out of 12) thought a lack of technical expertise would impact their ability to implement the Code.

Organisations that do not currently employ or contract staff with cyber technical skills had an overall lower maturity than organisations that do, with the biggest difference in maturity being seen in Principles C, D and E, as shown in the table below.

Table 6: Comparison of cyber maturity between organisations with cyber-skilled staff and those without

Principle	Organisations employing or contracting staff with cyber technical skills (mean score, n=14)	Organisations not employing or contracting staff with cyber technical skills (mean score, n=5)
A: Risk management	2.88	2.06
B: Cyber strategy	2.44	1.86
C: People	3.22	1.79
D: Incident planning and response	3.38	1.46
E: Assurance and oversight	2.92	1.34

Data from 19 respondents

Qualitative insight

This section outlines the insight drawn from 6 support sessions and 12 user interviews.

Adoption of the Code was frequently included in business-as-usual discussions and governance activities.

> “We did this review as part of our normal activities, when we are reviewing our [operations] plan and various activities as we go throughout the year. We just built this in as an action point […] I think all told, on and off, we have probably spent about three or four days [on one principle of the Code].”

Time and cost of implementation

As implementation of the Code during the pilot was limited, participants found estimates of the time and cost required to adopt all or part of the Code difficult to make.

- Time spent on implementation ranged from a few hours to a week over the 5-week pilot period. An estimate of around 6 months to a year to implement the entirety of the Code was common, with participants stating it could take a number of years to fully embed.
- No participants reported any direct costs associated with their implementation of the Code during the pilot, aside from utilisation of staff time, which was not quantified. However, participants also explained that the process of allocating budget to this work and procuring supporting resources or services would have taken longer than the time available in the pilot.
- Participants estimated that Principles C and D would be most expensive to implement, due to the cost of staff training and incident response exercising.

Presentation and content of the Code

Participants noted the format of the draft Code was simple to navigate, of an appropriate length, and aligned with what they would expect from a cyber security standard or framework.

Language

Participants stated the language used in the Code was pitched at the right level from a cyber security perspective. However, some expressed that the Code used business and governance terminology that was not familiar to them. Some noted the actions could be made clearer and more concise to better explain what is expected.

> "It's not that there are words there that I don't understand from a dictionary definition perspective, but the actual action or intent. What are you [the person implementing the Code] actually trying to achieve? This was not evident from the Code of Practice."

> "[Interpreting the actions in Principle B] is where I spent what was probably an hour or so trying to untangle what the actual intention was."

Terminology

Participants from small and micro organisations interpreted the Code as being aimed at larger organisations with more formalised roles and governance structures, but said they are practiced at translating similar guidance aimed at larger businesses. However, even participants from medium and large organisations pointed at references to a CISO (Chief Information Security Officer) in Principles A and E of the Code, and stated that:

- The acronym CISO is not explained in the Code.
- The role is not present in many organisations, and although there may be someone senior with day-to-day responsibility for cyber security, this may not be reflected in their job title or a core part of their job description.

> "[Internal cyber security] resource is split between three or four IT people and then up to a CIO (Chief Information Officer). Now, maybe they are quote unquote a 'CISO' as well, but they don't see themselves as that. They see themselves as the CIO or the IT Director or something like that."

Publication of the Code

Most participants would expect to find the Code on a government website, such as GOV.UK, NCSC.gov.uk, or the ICO website. A preference was expressed for the Code to be located alongside other corporate governance and risk management guidance as opposed to other cyber security guidance, standards or frameworks.

Positioning the Code

Multiple participants expressed that the intended audience, purpose and benefits of implementation were not clear from the Code alone. They would benefit from additional positioning content, such as a statement introducing the Code.

Participants would expect industry associations to signpost this information to their members as they do with other emerging government policy and cyber security matters. Accountants were commonly mentioned as a source of advice and guidance to business owners and directors on many of their obligations, and recommended as a suitable route to make directors aware of the existence of the Code.

One participant, who had recently set up their business, referred to a letter received from the ICO when they registered their business with Companies House. They stated including information about the Code in this letter would help new business owners understand what they should be doing to manage their organisation’s cyber risk.

Another participant drew parallels between the Code and the UK Corporate Governance Code published by the Financial Reporting Council[10]. They suggested the Code could be incorporated into existing corporate governance principles rather than having something separate for cyber security, which less cyber mature organisations might be unlikely to seek out.

Mandating the Code

A small number of participants from medium and large organisations stated that the Code would need to be mandatory for their organisations to engage with it in the future. They cited existing standards that their industry requires them to comply with that would be prioritised over meeting the requirements in the Code, unless the Code was given similar priority through a legal requirement to meet it.

Other participants stated that the Code effectively becomes mandatory when their customers begin requiring it, and described the difficulties in needing to meet various different standards that their customers demand. If the Code were to be added to existing procurement frameworks, for example, this would create a requirement for their organisations to meet it.

Interacting with the Code

The steps carried out by participants after receiving the Code generally included:

1. **Conducting a gap analysis:** Comparing their organisation’s current cyber governance and risk management practices with the activities set out in the Code. Participants described reviewing their current activity against the code to identify

[10] UK Corporate Governance Code (frc.org.uk)

additional activities they should be engaging in, or to determine whether they were already carrying out the recommended actions.

2. **Prioritisation:** Identifying an area of the Code to focus on first (where they were attempting to implement the entirety of the Code during the pilot), or an action described within a principle of the Code (where they asked to implement one principle). Prioritisation was based on one, or a combination of:
    - Activity they thought could be completed during the pilot timescale.
    - “Low-hanging fruit” i.e. actions that could be addressed with minimal time, cost and effort.
    - Outcomes they believed would have the most immediate impact on their organisation’s cyber resilience, such as putting in place a cyber incident response plan or gaining assurance that sufficient technical controls were in place to defend against cyber incidents.
3. **Identifying actions:** For each action in the Code, participants said they needed to identify a subset of contributing actions that they would carry out during the pilot. For example, a participant seeking to gain assurance that their organisation’s supply chain was resilient against cyber risks identified an action to speak with their critical suppliers, and a further action to create a list of suitable questions ahead of those conversations in order to help them gather the right information. “Working backwards” from the actions in the Code in this way was described by multiple participants, and this was frequently the stage where additional guidance was sought, by referring to the NCSC Board Toolkit and other sources.

Delegating responsibility

Despite strict selection criteria targeting only directors and equivalent roles, it was observed at various points during the pilot that participants had delegated research activities, such as responding to questionnaires, to others in their organisation, such as members of IT or cyber security teams. Some participants described their perceived role during the pilot as that of a “sponsor” and did not expect to be directly involved in implementing new cyber governance activities themselves. Researchers intervened to ensure research activities were carried out by the intended audience of directors and equivalent roles.

This is a key barrier to effective governance, where cyber risk is viewed as an IT-specific issue and an objective for IT and security teams to deliver, rather than being treated as an enterprise risk owned and managed by directors.

Tools and guidance

The majority of participants referred to external guidance to help them understand how they could complete the actions contained in the Code. Most participants referenced the NCSC Board Toolkit, which was provided to them alongside the Code, but others also referred to existing standards or frameworks used by their organisation such as ISO 27001, Cyber Essentials, the NIST Cyber Security Framework and NCSC's CAF.

An existing standard, where in use, was generally the first choice of resource for participants due to a desire to maintain alignment between their work on the Code and other standards they are already meeting or working towards.

NCSC Cyber Security Toolkit for Boards

Participants reported the NCSC Board Toolkit was a useful supplement to the Code and matched well with the Code's principles and actions, but many said they skim-read it due to its length.

Mapping to the NCSC Board Toolkit

Some participants noted that because the NCSC Board Toolkit was provided alongside the Code, they expected it to map directly to the Code's principles. They expressed a need to be more explicit about where to find relevant information in the NCSC Board Toolkit, or elsewhere, to support implementation of each Code action.

Mapping of guidance to the Code

Along with the NCSC Board Toolkit, participants would like to see other relevant guidance mapped to the Code and signposted directly. Participants described a need to quickly identify relevant parts of existing standards or guidance when planning actions to implement a specific part of the Code and that it would be helpful to have these stated against each action within the Code.

2 participants referred to the NCSC CAF and stated that the use of letters to identify principles of the Code and outcomes of the CAF was confusing as they did not align with one another.

Understanding the action required

Although participants initially considered the level of detail in the Code appropriate for an audience of directors or equivalent roles, when it came to implementation, they found that further detail was needed.

> “It was probably almost slightly too high level, and more supporting resources and implementation guidance would have been helpful on that […] What was probably less clear was the actual steps to implement it in practice.”

Participants expressed difficulty in interpreting what good practice would be, based on the Code alone. Some had used the NCSC Board Toolkit to explore this further but still felt unclear about what they were working towards and wanted specific examples.

> “Where it says in [Principle B] Action 1 ‘monitor and review the cyber resilience strategy’ you think well, what do you mean by monitor and review? What’s the guidance on monitoring and reviewing, what’s the expectation? Because it was very much open to interpretation.”

Some participants made comparisons to existing standards and the supporting information available for them, such as the ISO 27002 supporting standard for ISO 27001, which provides guidance on how the information security controls detailed in ISO 27001 can be implemented.

Level of detail

It was generally expressed that the high-level nature of the actions contained in the Code was a positive, as it means the Code is simple and easy to engage with, however an additional layer of detail is required to support implementation.

Participants from organisations with a higher level of cyber maturity expressed that they preferred a less prescriptive approach as it enabled them to decide what activity they would undertake, however lower maturity organisations occasionally struggled to understand what was required of them.

Uptake of support

Support sessions with Arculus cyber security consultants were made available for all participants free of charge during the pilot, and 26% of participants (6 out of 19) utilised these. Common themes discussed during these sessions were:

- **How to get started:** Participants sought help identifying steps that would help them begin working towards meeting the principles of the Code. In some cases participants had identified steps they thought appropriate for their organisation size and existing level of cyber maturity, and sought reassurance that these were in line with the “spirit” of the Code.
- **Alignment with other standards:** Participants who were already using cyber standards and frameworks to assess their organisation’s cyber security, or working

towards meeting these, wanted to determine which parts of the Code they were already achieving, or where implementing the Code would support them in meeting those other standards. Participants wanted reassurance that work on the Code would not be duplicative of, or contradictory to, existing efforts to assess and improve their cyber security posture.

> "Like a lot of standards, there are common elements, and so as soon as I rationalised it as, it's more of a governance framework rather than what ISO 27001 attempts to do, or NIST, or any of those sorts of standards… which is good in a way because I'm seeing a lot more standards pop up and it's concerning me greatly […] that we may end up with too many standards and lots of confusion."

Despite a relatively low take-up of these sessions, during user interviews many participants expressed that they would expect to spend money on consultancy services to help them implement different elements of the Code.

Insight by principle

This section outlines insight gathered specific to the individual principles and actions contained within the Code.

Principle A: Risk management

Participants said risk management was a good starting point and this was a logical topic to introduce first in the Code.

> "I've decided that we have the right level of risk at the appropriate level of resources and investment. And so I did nothing new on that, but I spent some time trying to work out whether that was the case or not."

Some participants stated they would need external support to conduct the risk assessments outlined in Action 2, and this would likely be the largest cost associated with implementing Principle A.

Participants also found Action 5 challenging to implement, particularly where they had entirely outsourced IT services or used software-as-a-service and needed to gain assurance from third parties in their supply chain. Participants stated they would benefit from understanding how assurance could be gained, such as recommended questions to ask suppliers to understand the level of risk in their supply chain and how suppliers would respond to cyber incidents. Small and micro organisations cited challenges around a lack of leverage with their suppliers due to their low spend compared to larger organisations, and that it was difficult to get the answers they needed as a result.

Some participants found it difficult to gauge how frequently actions in Principle A should be reviewed for an organisation of their size.

Principle B: Cyber strategy

Participants who focused on implementing this principle said it was missing an action to first put a cyber strategy in place. The actions in this principle begin with monitoring and reviewing the cyber resilience strategy, and participants thought these actions were written with the assumption that such a strategy already exists, which was not the case for some.

> "You need the strategy before you can even start on [Principle B], and I think some work in the area of helping organisations develop that strategy because, for example, we didn't have a strategy simply because what you would classify as strategy is probably spread across multiple policy documents and statements of intent and things like that."

Participants also stated they would benefit from additional guidance on creating an effective cyber strategy and had attempted to use the NCSC Board Toolkit for this, but had not found the information they needed. They recognised that a cyber strategy would likely be specific to an individual organisation, but thought it would be possible to provide some broad guidance such as tips on what the strategy should cover, or questions it should seek to answer.

One participant found it difficult to determine the difference between Actions 1 and 2 of Principle B, and pointed to this as an example of where clearer and simpler wording could help draw out the difference in meaning between the two.

> "I understand every single one of those words. But would really struggle, without giving quite a lot of thought and actually trying to go back to the individual definitions of all those words, to pull apart what the difference is between those two."

It was generally expressed that the cyber strategy could be developed, implemented and reviewed by internal staff, and as such cost estimates were relatively low compared to other principles, mainly consisting of existing staff time.

Principle C: People

Participants wanted greater clarity on Action 1 in order to understand what good sponsorship of communications might look like in practice.

> "[If it were] a Teams message or email from the CFO saying, by the way, do your security training, it's important, full stop. Send. Is that really achieving what they want out of Action 1? […] It's not really improving cyber governance. I think there's an opportunity to be clearer on the actual outcomes."

Implementing effective cyber security training, education and awareness for staff as described in Action 4 was viewed as a high-cost activity due to costs associated with training platforms and software. Free solutions such as NCSC's 'Top Tips for Staff' e-learning package[11] were not identified by participants and would therefore benefit from being signposted alongside the Code in future.

Principle D: Incident planning and response

Immediate impact

Participants who implemented Principle D during the pilot said that it started conversations that were valuable to their organisation and the actions they had taken to implement this principle had an immediate effect on their organisation's cyber posture, particularly where they did not previously have a cyber incident response plan in place.

For those who already had an incident plan in place, this principle highlighted additional ways they could increase their preparedness, although they would find it difficult to justify increased investment in these activities.

> "We have an incident response plan […] but it's the overall kind of how you might respond to an incident. It doesn't contain the specifics around if X goes down, or if X is lost, this is what you need to do, and those playbooks that go along with it. Knowing how long it would take to properly document and come up with those playbooks, we would struggle to justify taking people off their day-to-day to write them. There's probably eight, nine, ten different things that you could argue we – by the intent of that action – should have a playbook for. […] I would struggle to justify investing in the time it takes to develop those playbooks."

Testing incident response plans, as detailed in Action 2, was deemed to have a number of costs associated with it that varied according to the interpretation of what the testing might involve. Some participants were uncertain whether to interpret this as a tabletop exercise, such as using a scenario to step through their incident response plan and

[11] NCSC's cyber security training for staff now available - NCSC.GOV.UK

identify improvements, a live exercise involving switching off systems, or a technical test of the ability to restore a system from a backup by conducting a full restore or rebuild. Some participants stated they would rely on a third party, such as a supplier or incident response specialist, to help them conduct this testing. Considerably higher costs were associated with technical testing than for conducting a tabletop exercise.

Participants were concerned that testing came with a risk that operational systems could be impacted and there may be further costs involved with downtime. As such, it was suggested that a distinction between tabletop exercising of response plans and technical testing of systems could be made in the Code. NCSC's Exercise in a Box[12] was cited as a useful resource to engage the business in testing its incident response plans.

Principle E: Assurance and oversight

Participants implementing Principle E stated they found it useful to think about their governance and reporting processes from an external assurance perspective, and this helped them identify areas where they could document some of these more clearly in order to demonstrate that they were carrying out the activity described in the Code.

> "Having something that we can do to demonstrate that governance, that's not cost prohibitive, would be really great and I think would really drive take-up."

Small and micro organisations said this principle was less relevant to them as they did not have formal reporting structures in place, such as reporting to shareholders or mandatory finance reporting, which meant doing this for their cyber security seemed disproportionate. However, they did find Action 4 prompted them to think about how they monitor their cyber resilience. One participant created a spreadsheet that they would use to track some identified metrics and data on a monthly basis to support this action.

Impact

Participants generally reported it was too soon to have achieved a noticeable impact on their organisation's overall cyber governance and risk management, but spoke positively about actions that had been started and others that they plan to work on in future.

> "I think it'll be a more coordinated and a better understood implementation of our strategy […] so what they will see is that there is a top risk and a strategy to make us more resilient, which in turn will direct activities to mitigate that top risk."

[12] Exercise in a Box - NCSC.GOV.UK

When does implementation end?

Some participants commented that it was unclear when an action in the Code would be considered "done" and said they would benefit from a clearer description of the "end state" they were aiming to reach, so they could know when they reached it.

Others determined that the activities in the Code are continuous and would never be "done", however there would be a period of implementation while new processes are established, followed by a period of embedding the changes until they become part of business-as-usual activity.

Recommendations

Based on the findings described throughout this report, this section contains recommendations for improvements to the Code and further testing.

Presentation of the Code

The following recommendations are made in terms of the Code itself and how it is presented:

- **Language:** Simplify the wording of the Code, using plain English for actions to help users interpret them consistently. Consider addressing the target audience directly using "you" to communicate their individual responsibility, rather than that of their organisation, for carrying out actions.
- **Naming of principles:** Consider removing letters from the names of principles to avoid confusion with NCSC's CAF which also uses a lettering system for its objectives.
- **Positioning:** Publish content alongside the Code that helps readers understand its intended audience, purpose and benefits. This could take the form of an executive summary or introductory web page.
- **Publication:** Publish the Code on a government website such as GOV.UK or NCSC.gov.uk, and engage with Companies House, the ICO, industry associations and the accountancy community to publicise it. This would support awareness of the Code among organisations of all sizes and levels of cyber maturity, especially organisations of lower maturity who would be less likely to proactively seek out guidance on effective governance of cyber risk.

Help users implement the Code

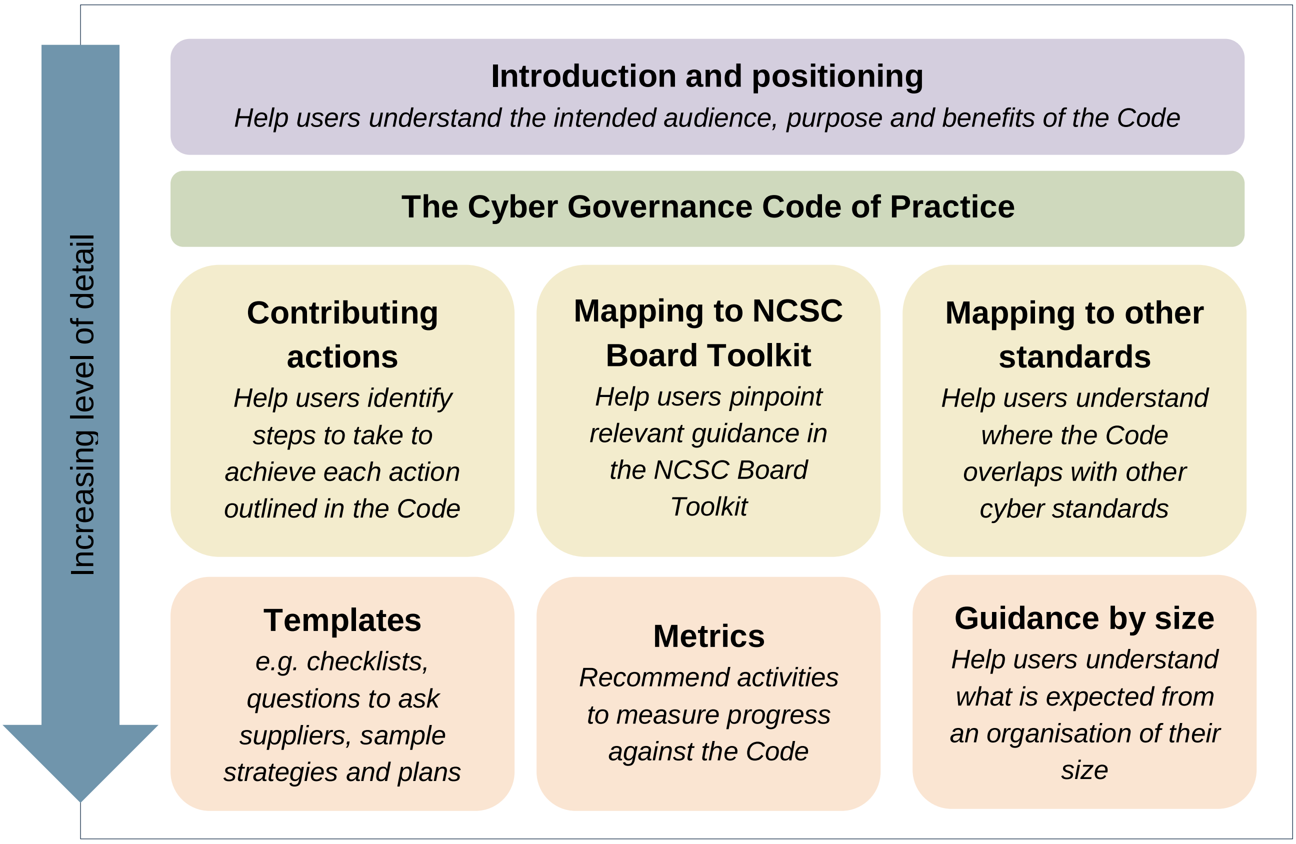
The following recommendations are made to help users better understand the actions they need to take to implement the Code:

- **Map the Code to the NCSC Board Toolkit** to direct users to specific guidance contained in the NCSC Board Toolkit that would help them implement the Code.
- **Map the Code to existing standards and frameworks** such as ISO 27001, Cyber Essentials, NIST Cyber Security Framework and CAF, to help users understand where they may already be implementing parts of the Code under these standards, or where carrying out the actions contained in the Code may help them to meet other standards in future.

- **Provide checklists** with a breakdown of recommended steps that will help users achieve the top-level actions contained in the Code.
- **Provide examples of good practice** for each action to help users identify an achievable target state. Consider providing tailored examples for small, medium and large organisations. This could include providing recommended steps to take, describing how frequently an action should be carried out, suggesting questions that could be asked of suppliers and signposting to free or low-cost resources that could be used.

- **Test supporting information and guidance with users** to ensure it meets user needs prior to publication. Supporting information and guidance should be structured around the Code to help organisations understand who it is aimed at, what its purpose is, and the benefits to organisations of implementing it. Guidance should provide a greater level of detail beyond the Code and help users identify a set of actions to carry out to support them in achieving the higher-level actions contained in the Code. An outline of these suggested layers is provided below.

Figure 4: Suggested layers of support and guidance



Increasing level of detail

Introduction and positioning
Help users understand the intended audience, purpose and benefits of the Code

The Cyber Governance Code of Practice

Contributing actions
Help users identify steps to take to achieve each action outlined in the Code

Mapping to NCSC Board Toolkit
Help users pinpoint relevant guidance in the NCSC Board Toolkit

Mapping to other standards
Help users understand where the Code overlaps with other cyber standards

Templates
e.g. checklists, questions to ask suppliers, sample strategies and plans

Metrics
Recommend activities to measure progress against the Code

Guidance by size
Help users understand what is expected from an organisation of their size

Annex 1: Draft Cyber Governance Code of Practice

The draft Code in the format provided to participants in this pilot.

Cyber Governance Code of Practice				
Action 1	Action 2	Action 3	Action 4	Action 5
A: Risk management				
Ensure the most important digital processes, information and services critical to the ongoing operation of the business and achieving business objectives have been identified, prioritised and agreed.	Ensure that risk assessments are conducted regularly and mitigations account for changes in the internal, external and regulatory environments, which are more rapidly changing than in traditional risk areas.	Establish confidence in and take effective decisions on the level of cyber security risk that is acceptable to the organisation and how much will need to be managed to achieve the business objectives.	Ensure that cyber security risks are addressed as part of the organisation's broader enterprise risk management and internal control activities, and establish ownership of risks with relevant seniors beyond the CISO.	Gain assurance that supplier information is routinely assessed and reviewed commensurate to their level of risk, and that the organisation is resilient against cyber security risks associated with suppliers, stakeholders and business partners.
B: Cyber strategy				
Monitor and review the cyber resilience strategy in accordance with the level of accepted cyber risk, the business strategy, and in the context of legal and regulatory obligations.	Monitor and review the delivery of the cyber resilience strategy in line with current business risks and in the context of the changing risk environment.	Ensure appropriate resources and investment are allocated and used effectively to develop capabilities that manage cyber security threats and the associated business risks.		
C: People				
Sponsor communications on the importance of cyber resilience to the business, based on the organisation's strategy.	Ensure there are clear cyber security policies that support a positive cyber security culture, and satisfy themselves that its culture is aligned with the cyber resilience strategy.	Take responsibility for the security of the organisation's data and digital assets by undertaking training to ensure cyber literacy and by keeping information and data they use safe.	Ensure the organisation has an effective cyber security training, education and awareness programme and metrics are in place to measure its effectiveness.	
D: Incident planning and response				
Ensure that the organisation has a plan to respond to and recover from a cyber incident impacting business critical processes, technology and services.	Ensure that there is regular, at least annual, testing of the plan and associated training, which involves relevant internal and external stakeholders. The plan should be reviewed based on lessons learned from the test and broader external incidents.	In the event of an incident, take responsibility for individual regulatory obligations, and support executives in critical decision making and external communications.	Ensure that a post incident review process is in place to incorporate lessons learned into future response and recovery plans.	
E: Assurance and oversight				
Establish a governance structure that aligns with the current governance structure of the organisation, including clear definition of roles and responsibilities, and ownership of cyber resilience at Executive and Non-Executive Director level.	Establish a regular monitoring process of the organisation's cyber resilience and review of respective mitigations and the cyber resilience strategy.	Establish regular two way dialogue with relevant senior executives, including but not limited to the CISO or relevant risk owner.	Establish formal reporting on at least a quarterly basis and have agreed a target range for each measurement on what is acceptable to the business.	Determine how internal assurance will be achieved and ensure the cyber resilience strategy is integrated across existing external and internal assurance mechanisms.

Annex 2: Methodology

This annex provides an overview of the main elements of data collection for the Cyber Governance Code of Practice pilot, which form the basis of this report.

Surveys

Two separate surveys were issued to participants during the course of the pilot:

1. Screener form
2. Maturity assessment (Cyber Governance Questionnaire)

The screener form received 33 responses. Respondents were asked to provide demographic characteristics such as job role, organisation size, sector and region, as well as questions to establish a basic understanding of the organisation's current cyber maturity, such as whether the organisation holds any existing cyber security certifications. The data also identifies how respondents heard about the pilot and their agreement to implement the Code. Survey responses were used to shortlist suitable organisations, where the respondent was a member of the target audience for the Code (a director, non-executive director or senior leadership equivalent), and the size and sector of the organisation supported a diverse and balanced cohort. 3 respondents were rejected on the basis of eligibility; 2 due to not being members of the target audience and one due to the organisation being located outside of the United Kingdom. 27 respondents were selected to participate in user testing, with 3 remaining in-scope respondents held on a waiting list due to similarity in the size and/or sector of their organisations to that of already accepted participants.

A maturity assessment was conducted using the Cyber Governance Questionnaire. This questionnaire received 19 responses, achieving a response rate of 70% (19 out of 27 invites).

Survey data analysis

Data collected by the above activities was analysed using the following methods:

1. **Demographic analysis**: understanding the demographic profile of respondents and their organisations.
2. **Analysis on secondary questions**: secondary questions were asked across both surveys, for example on how respondents heard about the pilot and whether they anticipated specific support requirements.

3. **Qualitative analysis of open text responses and notes:** in some cases, respondents were asked to elaborate on their answers with text, which was analysed and interpreted along with other qualitative and quantitative evidence.
4. **Maturity assessment:** qualitative scoring of questions relating to participants' current maturity against the Code was conducted using a simplified version of the Capability Maturity Model Integration (CMMI) maturity levels[13]. Further detail about the maturity assessment approach is detailed in Annex 5: Maturity assessment.

All analysis and data visualisation in this report was made using Microsoft Excel and Power BI.

Support sessions

Notes were taken during support sessions with participants to record the principle(s) of the Code and/or action(s) they needed support with, the challenges or barriers they were facing, external sources of guidance and support they had utilised and any feedback relating to their implementation of the Code. 6 support sessions were conducted, consisting of 5 half-hour sessions and one hour-long session.

Participant interviews

This report draws on feedback from 12 interviews conducted between 6 and 22 March 2024. Interviews were conducted remotely using Microsoft Teams and explored participants' feedback about the Code itself, the feasibility of implementing the Code in their organisation, the actions they carried out during the pilot, any challenges or barriers they faced, and tools and guidance they used or needed. A discussion guide was developed based on the research questions identified in the invitation to tender and further discussions with DSIT during the planning phase of the pilot. An outline of the research questions can be found in Annex 3: Research questions, and the discussion guide can be found in Annex 6: Discussion guide.

[13] CMMI Institute - CMMI Levels of Capability and Performance

Annex 3: Research questions

This annex outlines the research questions identified in the invitation to tender and developed through further discussions with DSIT during the planning phase of the pilot. The research questions informed the design of surveys and the development of the discussion guide for user interviews.

Table 7: Research questions

Theme	Primary questions	Secondary questions
Context	How is cyber risk currently governed and managed?	What existing standards or frameworks are in use?
		Who is responsible for managing cyber risk?
		Has the organisation previously experienced a cyber incident?
		Are there currently technical controls in place to manage cyber security risk?
		What barriers do participants face when addressing cyber risk?
Feasibility	How feasible is the Code to implement?	What is the cost of implementing the Code?
		What time is required to implement the Code?
		Is there anything that can't be implemented?
	What was needed in order to implement the Code?	Who was involved?
		What resources were used within the organisation?
		What discussions did it prompt?
		Was it able to be done in house?
		What technical skills were required?
	Is the Code easy to understand?	Is the language appropriate?
		Is there anything in the Code that doesn't apply to their organisation?
		How should the Code look?
Challenges	What challenges do users experience when implementing the Code?	What was easiest?
		What was most difficult?
		What barriers were faced during implementation?
	How does the Code align with existing standards and frameworks?	Does the Code contradict other advice?
Tools and guidance	What support is required?	What external support was used?
		How was the NCSC Board Toolkit used alongside the Code?

	What hints and tips would be helpful?	Where should the Code be hosted?
		What advice would participants give to other organisations implementing the Code?
Impact	What has changed since implementing the Code?	How confident are participants at managing cyber risk?
		What actions will they continue?
		How will cyber risk be governed in future?

Annex 4: Participant selection process

The participant selection process was carried out using responses to the screener form, based first on the following set of key eligibility criteria for shortlisting prospective participants:

- **Shortlist:** Respondents in the role of director, non-executive director or equivalent senior leadership within organisations based in the United Kingdom, who had confirmed that they agreed to implement the Code during the pilot and gave consent for researchers to collect and store their data.
- **Decline:** Respondents in roles other than those indicated above, from organisations located outside of the United Kingdom, or those who had declined to implement the Code or did not provide consent for the collection of their data.

Following initial shortlisting, further demographic analysis was conducted to select participants into the research cohort with the aim of maintaining a diverse and balanced cohort so that no single organisation size, sector or existing level of cyber maturity was overrepresented in the research data. Applicants that were shortlisted but not selected into the research cohort, for example where their organisation size and sector was similar to others already selected, were placed on a waiting list for contingency purposes and invited into the cohort when similar organisations withdrew. The agreed target sample is provided in Table 8: Target sample by organisation size, later in this Annex.

Participants and their organisations were kept anonymous throughout the pilot and reporting. Where organisations approached DSIT directly about participating in the pilot, they were referred to the research team and asked to complete the screener form, and no feedback was provided to DSIT as to whether those organisations were selected as participants.

Target sample

A target sample size of 25 organisations was set in the invitation to tender. The Code is targeted primarily towards medium and large organisations, and government has other schemes, such as Cyber Essentials, targeted towards smaller organisations. In order to best try and match the characteristics of the target demographics for the Code, a target split between different organisation sizes in the research cohort was agreed during the planning phase as follows:

Table 8: Target sample by organisation size

Size	Target
Micro	10%
Small	10%
Medium	50%
Large	30%

Although no specific target was set relating to organisation sectors, participant selection was carried out with balance in mind and sought to avoid overrepresentation of any one sector, particularly those most closely associated with cyber security and information technology.

Organisation size

Organisation size was determined using employee size bands, in line with definitions used by the Office for National Statistics (ONS) and in DSIT's Cyber Security Breaches Survey 2024[14]. These definitions were provided to respondents as options in the screener form:

Table 9: Definitions of organisation size

Size	Definition
Micro	Organisations with 1 to 9 employees
Small	Organisations with 10 to 49 employees
Medium	Organisations with 50 to 249 employees
Large	Organisations with 250 or more employees

[14] Cyber security breaches survey 2024 - GOV.UK (www.gov.uk)

Organisation sector

A list of sectors was provided in the screener form for respondents to select from, based on the top level of the UK Standard Industrial Classification (SIC 2007) hierarchy[15]:

- Accommodation and food
- Agriculture, forestry and fishing
- Arts, entertainment and recreation
- Business administration and support
- Charity and non-profit
- Construction
- Education
- Finance and insurance
- Health and social care
- IT and communications
- Manufacturing
- Mining and extractives
- Professional and technical services
- Public administration and defence
- Real estate
- Retail and wholesale
- Transport and storage
- Utilities[16]
- Other

It was observed that some respondents had selected sectors they operate within as opposed to the nature of their own business, for example a provider of IT services to local government identified their organisation as belonging to the public administration and defence sector. A review of self-reported sectors was conducted using Companies House searches to match organisations' registered nature of business (SIC 2007) to the

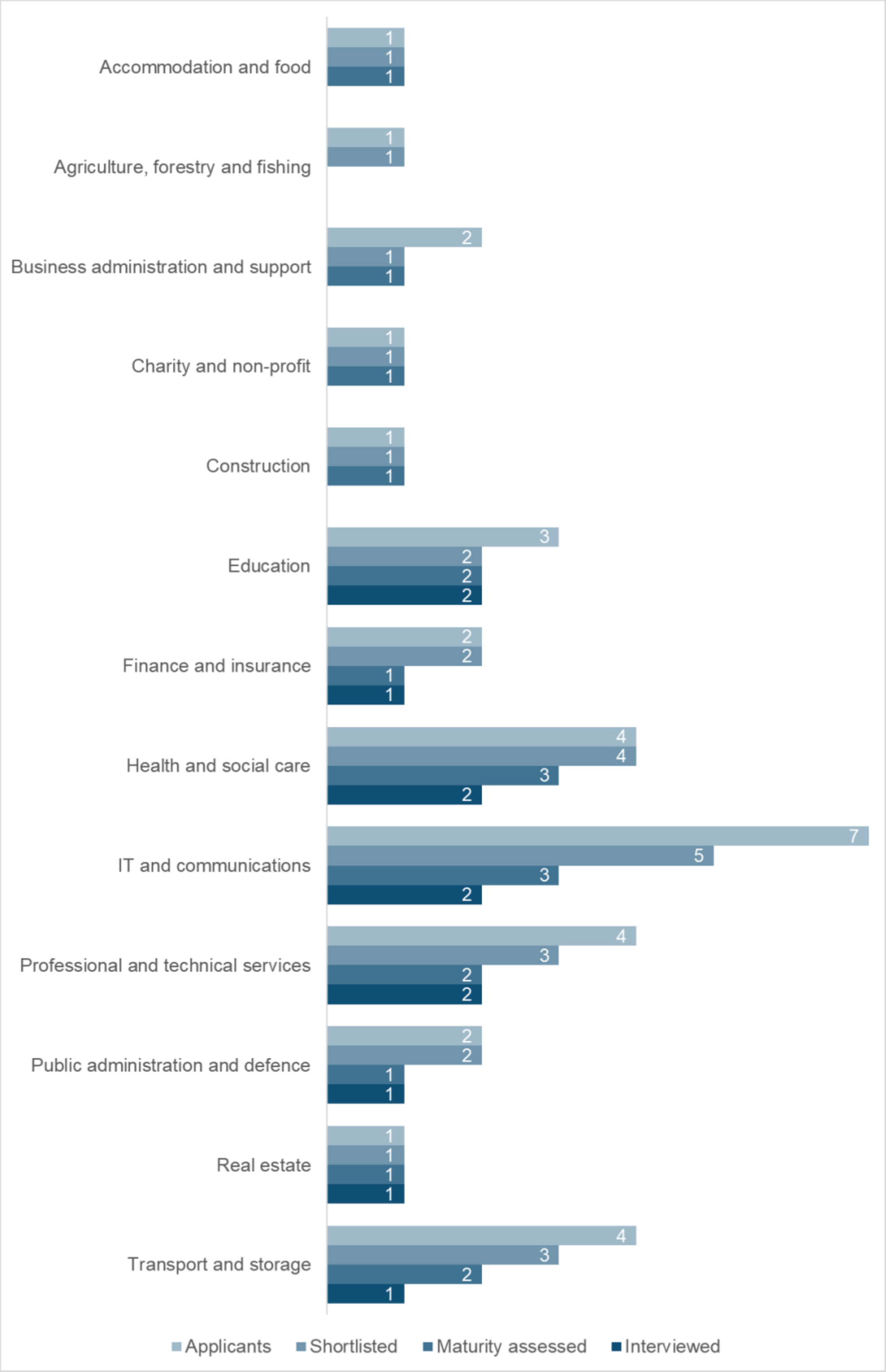
[15] UK Standard Industrial Classification (SIC) Hierarchy (onsdigital.github.io)

[16] Combines SIC Section D: Electricity, gas, steam and air conditioning supply with Section E: Water supply, sewerage, waste management and remediation activities.

relevant top-level groupings in the above list, and this replaced the self-reported sector for all demographic analysis in this report.

The chart below demonstrates the composition of the pilot cohort by organisation sector at different stages of the pilot.

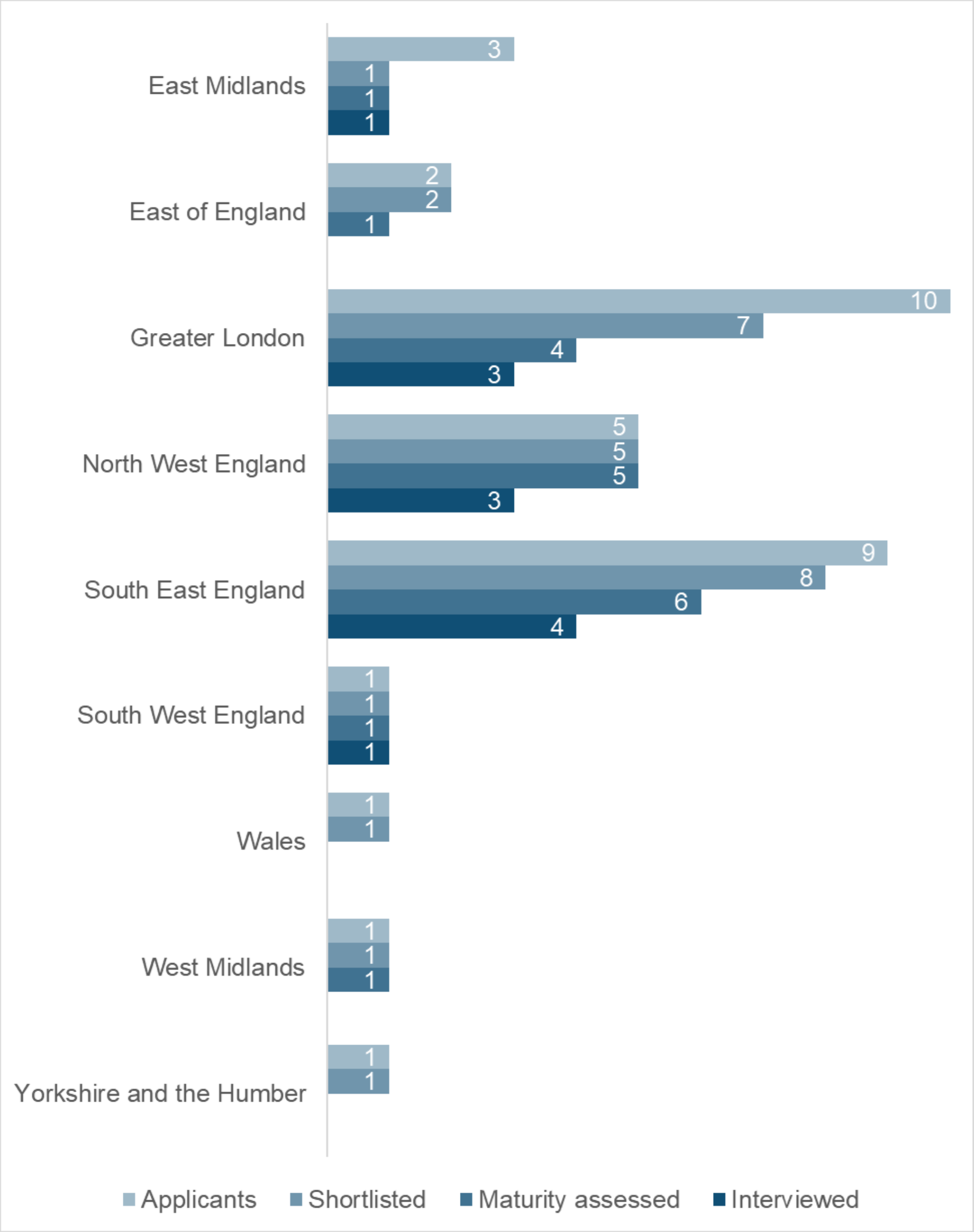
Figure 5: Cohort composition by organisation sector throughout the pilot



Organisation location

The chart below demonstrates the composition of the pilot cohort by organisation location at different stages of the pilot.

Figure 6: Cohort composition by organisation region throughout the pilot



No applications were received from organisations located in North East England, Northern Ireland or Scotland.

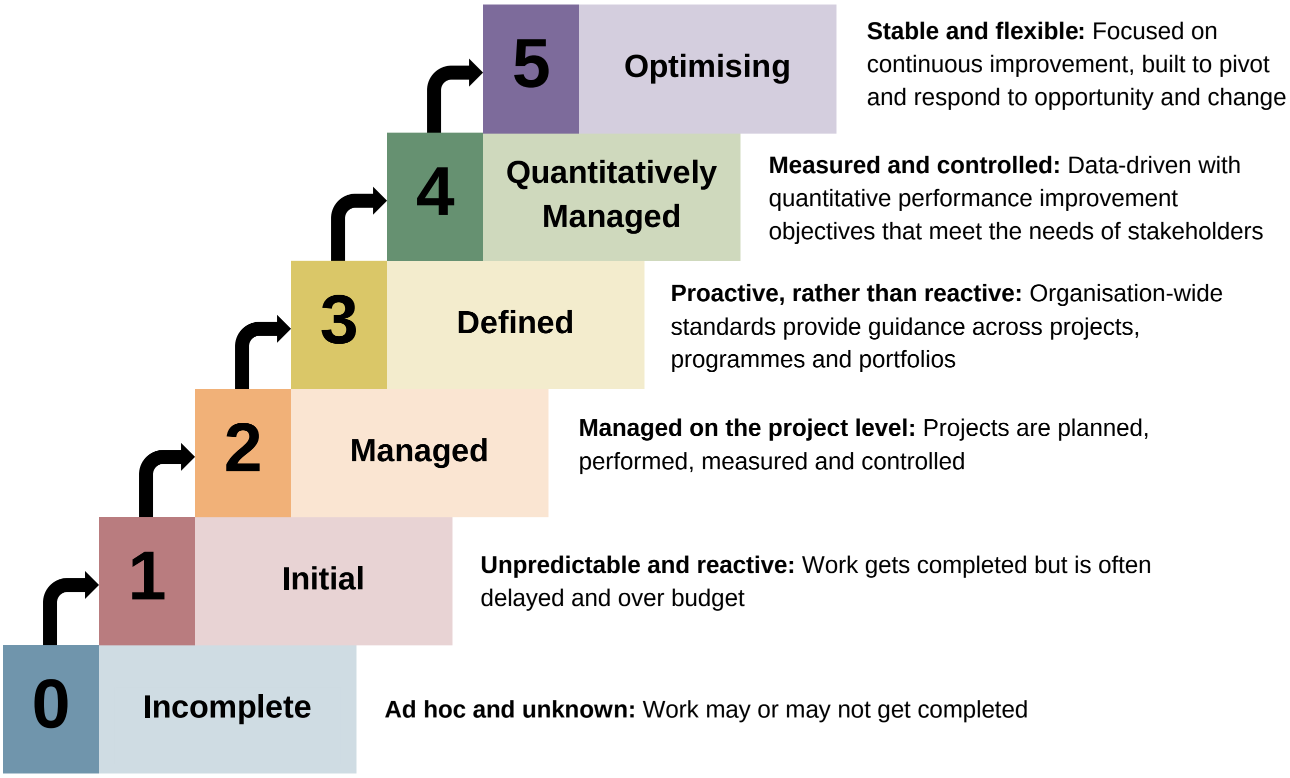
Annex 5: Maturity assessment

The maturity of participants’ current approach to governing cyber risk and their organisation’s cyber risk management activities was self-assessed through the Cyber Governance Questionnaire. The questionnaire sought background information to capture cyber security activities and asked participants to rate the degree to which they currently carry out the governance activities outlined in the Code. The scale was based on the Capability Maturity Model Integration (CMMI)[17] and adapted for survey purposes to include an option for participants who did not know or were unsure.

Capability Maturity Model Integration (CMMI)

The Capability Maturity Model Integration (CMMI) is an established model for representing an organisation’s performance and process improvement efforts across a set of practice areas. The figure below shows the characteristics of each maturity level.

Figure 7: Characteristics of the CMMI maturity levels



Stable and flexible: Focused on continuous improvement, built to pivot and respond to opportunity and change

Measured and controlled: Data-driven with quantitative performance improvement objectives that meet the needs of stakeholders

Proactive, rather than reactive: Organisation-wide standards provide guidance across projects, programmes and portfolios

Managed on the project level: Projects are planned, performed, measured and controlled

Unpredictable and reactive: Work gets completed but is often delayed and over budget

Ad hoc and unknown: Work may or may not get completed

Source: CMMI Institute

[17] CMMI Institute - CMMI Levels of Capability and Performance

For the purposes of this research, the actions contained within each principle of the Code were used as the practice areas and the maturity level definitions were adapted to be easily understood and suit a survey format, as shown in the table below.

Table 10: Adaptation of the CMMI model for the Cyber Governance Questionnaire

CMMI maturity model			Cyber Governance Questionnaire	
Level	**Description**	**Characteristic**	**Maturity score**	**Survey options**
			0	I don’t know/I’m unsure
			0	I don’t do this or am unable to do this
1	Initial	Processes unpredictable, poorly controlled and unreliable. Work may or may not get completed.	1	I’m aware of this but haven’t implemented it yet
2	Managed	Processes characterised for projects and often reactive. Work gets completed but is often delayed or over budget.	2	I’ve done this but it’s not embedded yet
3	Defined	Processes characterised for the organisation and proactive. Projects are planned, measured and controlled.	3	I consistently do this
4	Quantitatively managed	Processes measured and controlled. Data-driven with quantitative improvement objectives.	4	I’m proactive in doing this and adapt to changes
5	Optimising	Focus on process improvement. Able to pivot and respond to opportunity and change.	5	I’m proactive in doing this, measure progress and find ways to improve

Annex 6: Discussion guide

The following discussion guide was developed based on the research questions in Annex 3: Research questions, and used to facilitate interviews with participants.

The code

Question: Tell us what you thought about the code itself

Intent: To find out if the participant found the code clear and understandable, and if any changes might be needed to the code itself

Prompts:

- Was the language used in the code easy to understand?
- Was there anything you needed to look up or ask others in order to understand it?
- Is there anything in the code that doesn't apply to your organisation? Why?
- How would you expect the code to look when it's published?
- Where would you expect to find the code? (Do you currently visit this site for guidance?)
- How does the content of the code compare to other guidance you may have seen or used? Are there any contradictions?

Feasibility of implementing the code

Question: What did you do to implement the code (or part of the code) in your organisation?

Intent: To understand the actions the participant took to implement the code in their organisation and how easy or difficult these were

Prompts:

- What actions did you identify?
- What did you prioritise?
- Who did you involve?
- What costs were associated with the changes?

- How long did it take?
- How much did you oversee yourself?

Question: What will you continue to do after the pilot?

Intent: To understand the actions the participant will continue to take, particularly if they were not able to implement parts of the code during the pilot

Prompts:

- Which part of the code might you move on to next? Why?
- Who will you need to involve?
- What costs might you incur?
- How long do you think it would take to implement the code in its entirety?

Challenges

Question: Tell us about any challenges you faced implementing the code

Intent: To understand any pain points and how these could be addressed

Prompts:

- What did you find most difficult?
- What discussions were prompted?
- Did you need support from elsewhere?
- Is there anything in the code that you think you wouldn’t be able to achieve? Why?
- How did your organisation’s existing structures and processes impact your ability to make changes?

Tools and guidance

Question: What additional sources of information did you use?

Intent: To identify the types of guidance most useful to participants in implementing the code

Prompts:

- Which were most useful?
- Did you use the NCSC Board Toolkit? Which part(s) were most useful?
- How did you identify other sources of information or people who could help?
- What further tools or guidance would be helpful? (Where should they be hosted?)

Reflection

Question: How confident do you feel about governing cyber risk in your organisation?

Intent: To determine the impact of participating in the pilot and implementing the code

Prompts:

- What changes have happened as a result of implementing the code?
- What changes do you think will be most impactful for your organisation's cyber security?
- Would you recommend the code to other organisations like yours? Why or why not?
- What advice would you have for another organisation like yours if they were to begin implementing the code?