Department for
Science, Innovation
& Technology

Cyber Governance Package

Department for Science, Innovation & Technology

National Cyber Security Centre
a part of GCHQ

74%

Of large organisations surveyed identified a breach or attack in 2023. This is broadly **consistent with 2016 figures** (CSBS, 2024).

83%

Indicated the **need for additional solutions** that standardise ‘what good looks like’ for effective cyber risk management (Call for Evidence, 2020).

58%

Of medium and 66% of large businesses surveyed **have a formal cyber security strategy** in place (Cyber Security Breaches Survey, 2024).

55%

Just over half of medium businesses surveyed have a **formal incident response plan** in place, rising to 73% for large businesses (CSBS, 2024).

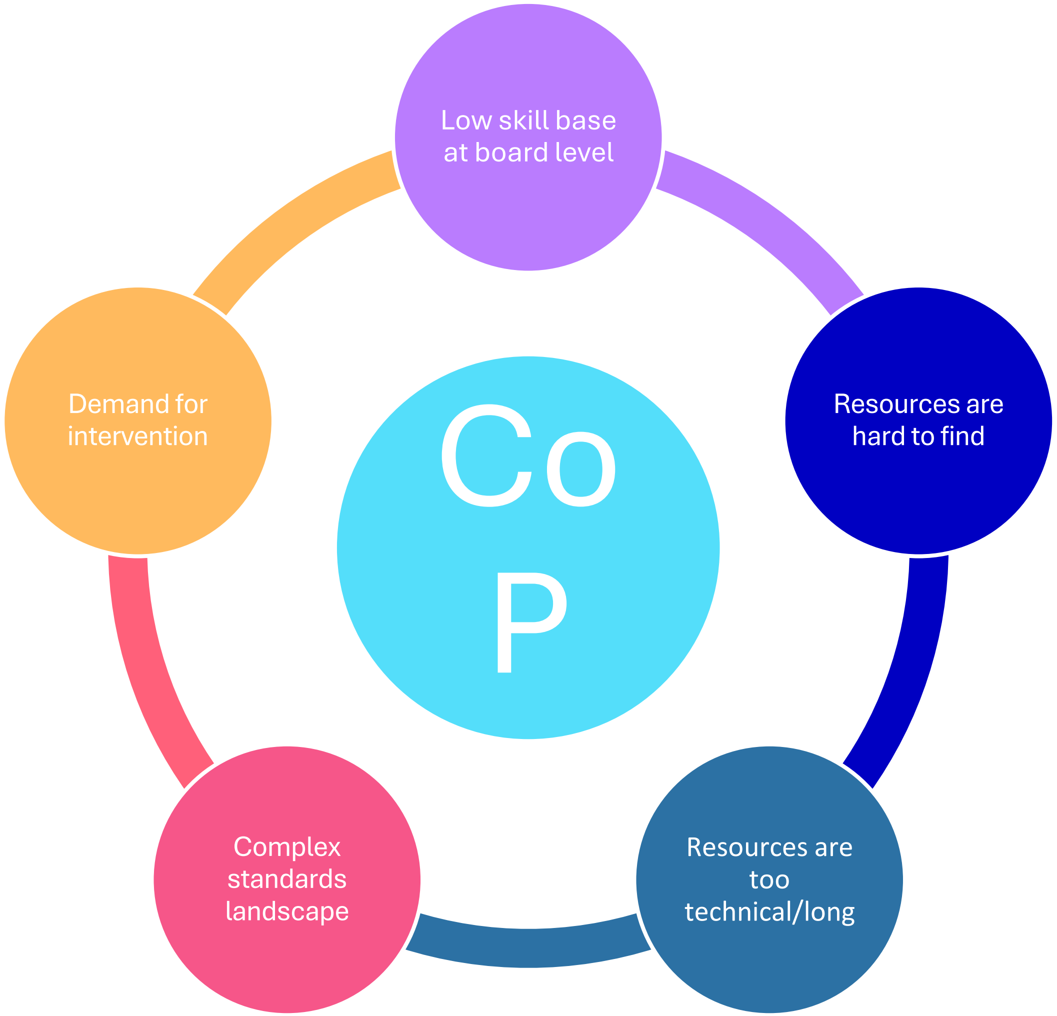
63%

Of medium and 72% of large businesses surveyed, **had undertaken a cyber security risk assessment** in the last year. (CSBS, 2024).

CYBER GOVERNANCE CODE OF PRACTICE

Department for
Science, Innovation
& Technology

Why?



CoP

Low skill base at board level

Resources are hard to find

Resources are too technical/long

Complex standards landscape

Demand for intervention

CYBER GOVERNANCE CODE OF PRACTICE

Department for Science, Innovation & Technology

The Code

The principles focus on the most critical areas that directors must engage with, rather than being an exhaustive list, and will articulate specific actions against:

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

Department for Science, Innovation & Technology

National Cyber Security Centre
a part of GCHQ

CYBER GOVERNANCE CODE OF PRACTICE

Overview of critical cyber governance areas

Tailored specifically to directors, particularly non-cyber specialists

Simple to engage with

Practical and actions-based

Formalise government's expectations of directors for governing cyber risk

Department for Science, Innovation & Technology

National Cyber Security Centre
a part of GCHQ

CALL FOR VIEWS

Proposed code of practice published in a call for views in January 2024

DSIT sought feedback on:

- The design and content of the code
- How to drive uptake and barriers to implementation
- The need for an assurance process

Department for Science, Innovation & Technology

National Cyber Security Centre
a part of GCHQ

Leadership Training Pack

Purpose

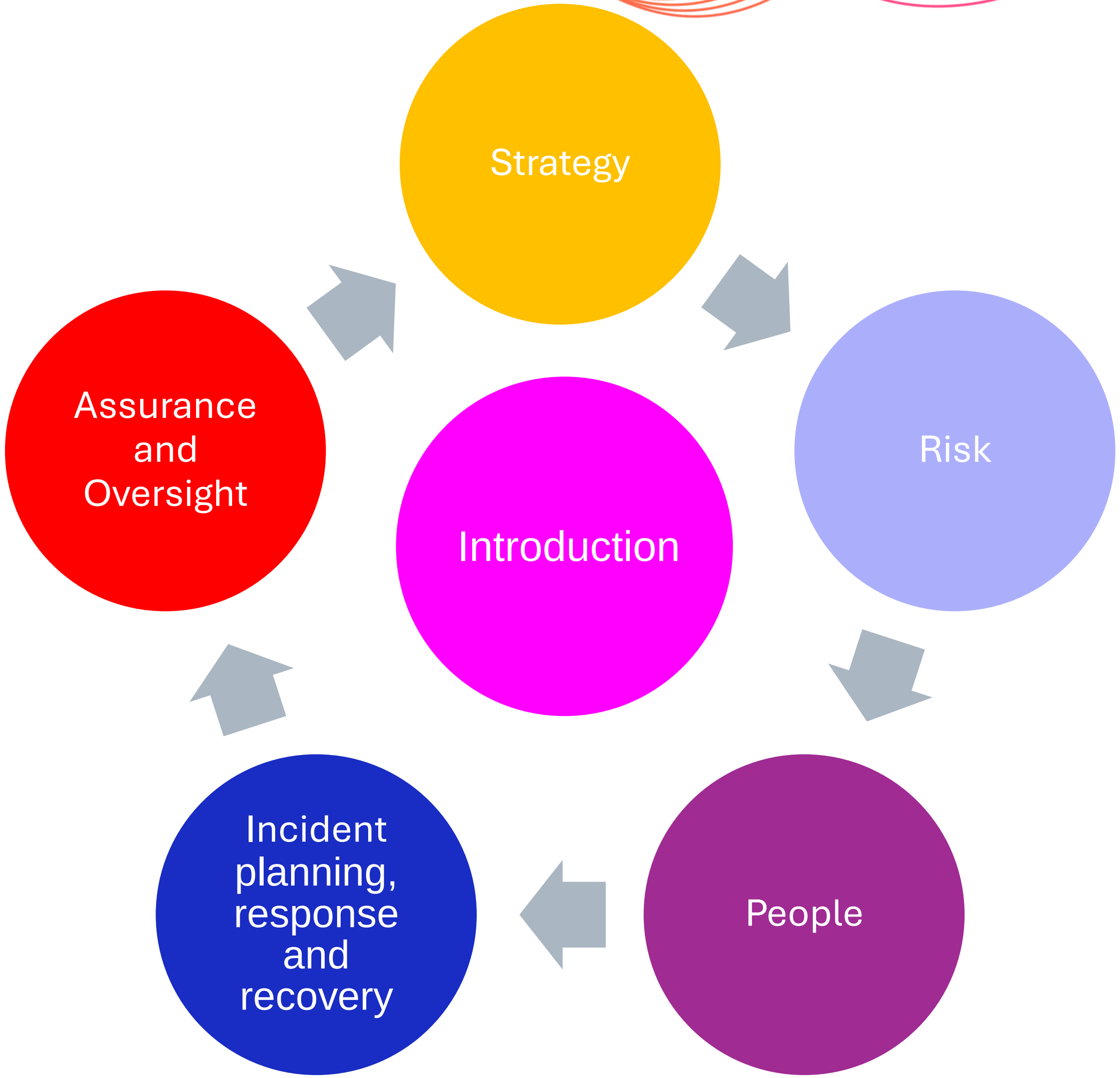
- Explains how to implement the actions from the code
- Supports boards in integrating cyber risk management into governance
- Sets expectations for leadership accountability in cybersecurity.

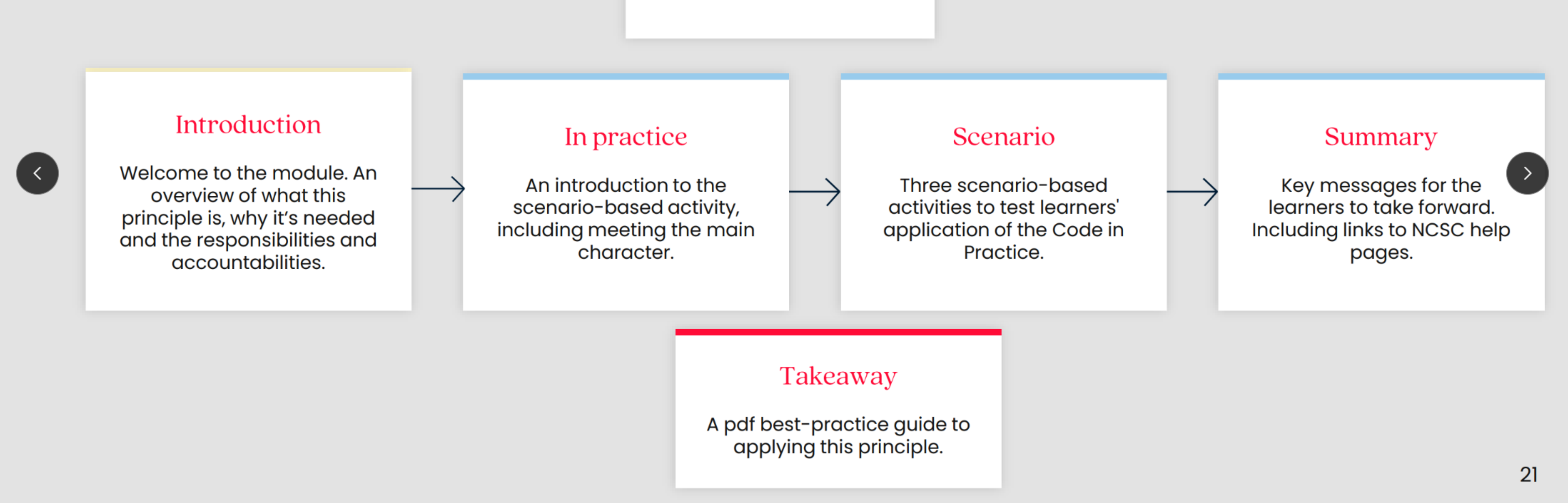
Department for Science, Innovation & Technology

National Cyber Security Centre
a part of GCHQ

Leadership Training Pack

Modules





Introduction

Welcome to the module. An overview of what this principle is, why it's needed and the responsibilities and accountabilities.

In practice

An introduction to the scenario-based activity, including meeting the main character.

Scenario

Three scenario-based activities to test learners' application of the Code in Practice.

Summary

Key messages for the learners to take forward. Including links to NCSC help pages.

Takeaway

A pdf best-practice guide to applying this principle.

21

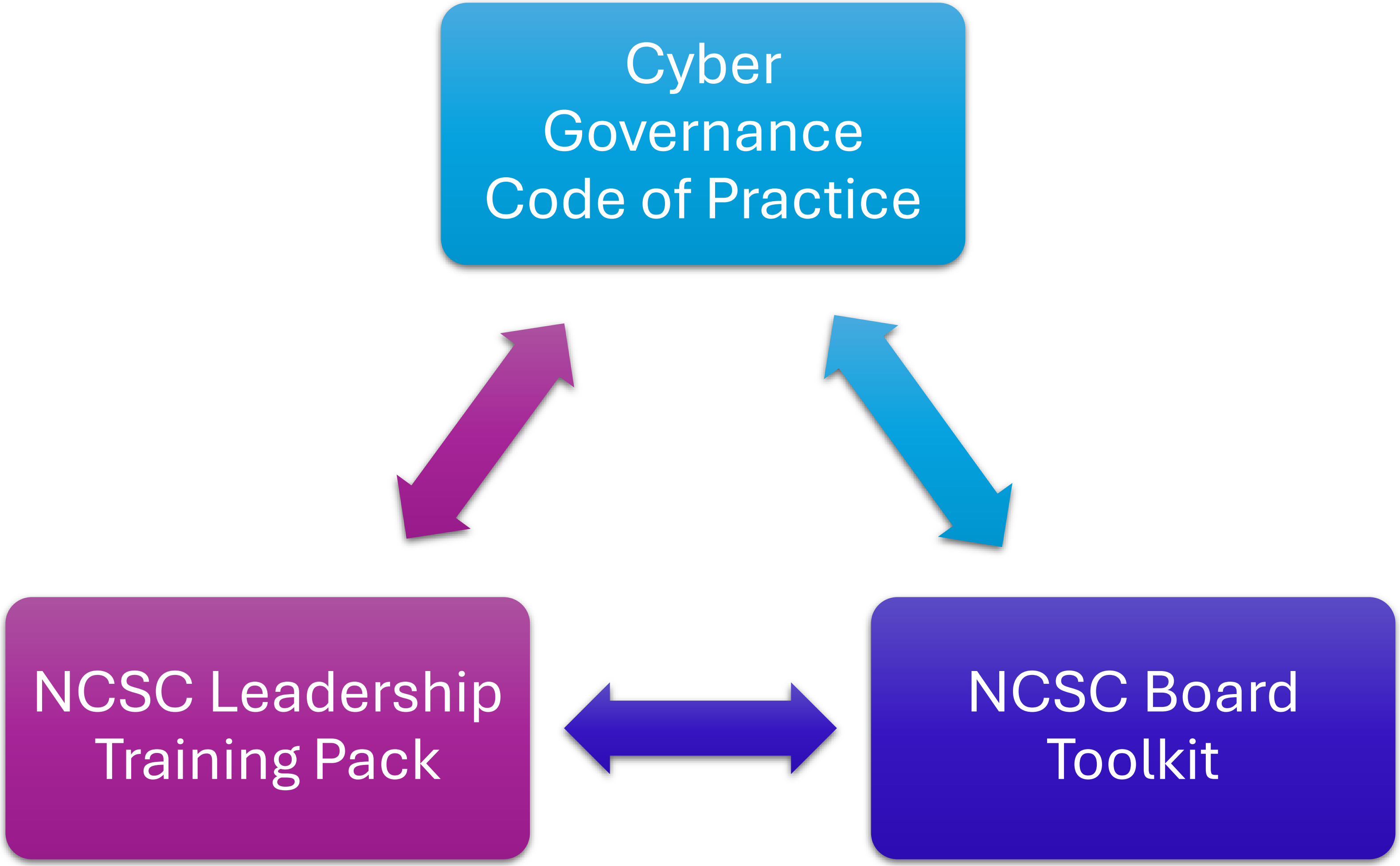
Leadership Training Strategy

NCSC Website Publication

Governance Training Programmes

Business Schools

CYBER GOVERNANCE PACKAGE



Cyber Governance Code of Practice

NCSC Leadership Training Pack

NCSC Board Toolkit

MAPPING THE CODE

National Cyber Security Centre
a part of GCHQ

Department for Science, Innovation & Technology

Government

- NCSC products
- DORA Framework
- ANSSI Risk Management Guide
- NIST CSF 2.0
- CISA Cyber Security Toolkit

Private

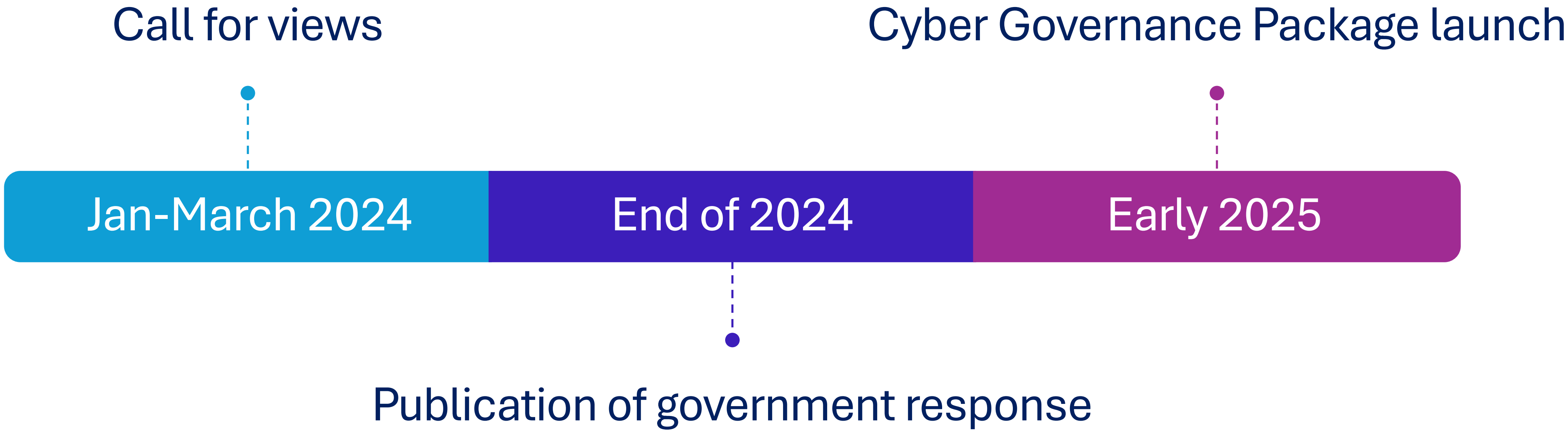
- IASME Cyber Assure
- ISACA COBIT
- ISACA CMMI

International

- ISO27001
- WEF Principles for Board Governance of Cyber Risk
- ISA Director’s Handbook

Department for Science, Innovation & Technology

National Cyber Security Centre
a part of GCHQ



Jan-March 2024

Call for views

End of 2024

Publication of government response

Early 2025

Cyber Governance Package launch

Department for Science, Innovation & Technology

National Cyber Security Centre
a part of GCHQ

Exercise – getting assurance

- Imagine you need to get assurance that your organisation (or an organisation you are assessing) has completed the actions in the Cyber Governance Code of Practice.

- Work together to draft a questions that you could ask for each action which gathers the relevant information to understand if that action has been completed.

- E.g. Risk Management: Action 1 – ‘Do we know what our most important digital processes are? How have we identified these processes?’