Department for Science, Innovation & Technology

National Cyber Security Centre
a part of GCHQ

Cyber Governance Code of Practice

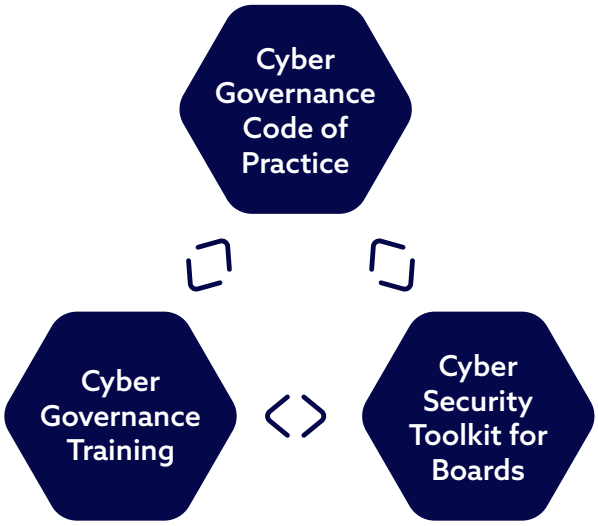
Introduction

What is the Cyber Governance Code of Practice?

The Cyber Governance Code of Practice (the Code) has been created to support boards and directors in governing cyber security risks. The Code sets out the most critical governance actions that directors are responsible for.

The Code forms part of the government's free package of support on cyber governance and should be the first point of reference for board members. It is underpinned by Cyber Governance Training, which helps boards and directors to strengthen their understanding of how to govern cyber security risks, and the Cyber Security Toolkit for Boards, which supports boards and directors in implementing the actions set out in the Code.

- The Cyber Governance Code of Practice sets out what actions boards need to take.
- The Cyber Governance Training confirms why and how board members take those actions.
- The Cyber Security Toolkit for Boards underpins the two, further supporting directors and board members.



Who should use the Cyber Governance Code of Practice?

The Cyber Governance Code of Practice is tailor-made for boards and directors of both public-sector and private organisations. The Code is not intended to be used by those who are responsible for the day-to-day management of cyber security, but can be used to highlight to boards what their responsibilities are.

The Code has been designed for medium and large organisations. However, whilst it has not been specifically created for small organisations, they play a critical role in the resilience of the UK economy and should seek to implement the Code's principles. Small organisations should also refer to the NCSC website for further guidance that is designed for them.

Why should boards and directors use the Cyber Governance Code of Practice?

50% of businesses and 66% of high-income charities report that they have experienced some form of cyber security breach or attack in the last 12 months. The prevalence of attacks is even higher amongst medium businesses (70%) and large businesses (74%) (Cyber Security Breaches Survey 2024).

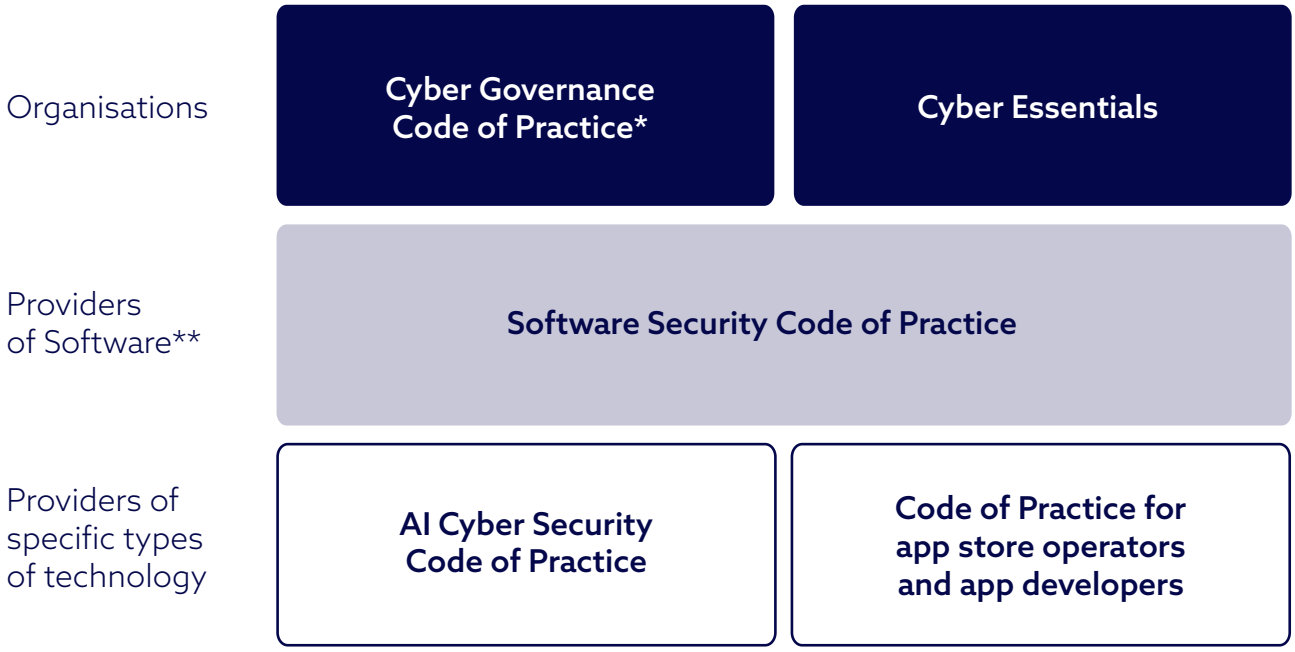
Governing cyber risk requires strong engagement and action at a leadership level. Cyber incidents can disrupt business continuity, reduce an organisation's competitiveness, and damage customer trust. Cyber risk is a material risk for almost all organisations and boards and directors need to be able to govern this risk effectively.

Building and maintaining cyber resilience is therefore crucial to protecting organisations' financial viability. By doing so, organisations are able to take full advantage of digital technologies, like artificial intelligence, to drive the business strategy and improve business performance.

DSIT cyber codes of practice

The Cyber Governance Code of Practice is the foundational code in DSIT's modular approach to cyber security codes of practice. It sets out how boards and directors should govern cyber risk. This is complemented by Cyber Essentials, a government backed certification scheme that helps organisations implement fundamental, cyber security controls. Though it is not a code, Cyber Essentials, together with the Cyber Governance Code of Practice, set out the minimum standard that organisations should have in place to manage their cyber risk.

Organisations that are seeking to implement other DSIT codes of practice, such as the Software Security Code of Practice or the AI Cyber Security Code of Practice, should also follow the Cyber Governance Code of Practice, as well as codes of practice specific to their organisation.



*for medium and large organisations, as well as small tech/AI organisations
**including goods and services that contain software

Cyber Governance Code of Practice

A: Risk management

Action 1	Gain assurance that the technology processes, information and services critical to the organisation's objectives have been identified, prioritised and agreed.
Action 2	Agree senior ownership of cyber security risks and gain assurance that they are integrated into the organisation's wider enterprise risk management and internal controls.
Action 3	Define and clearly communicate the organisation's cyber security risk appetite and gain assurance that the organisation has an action plan to meet these risk expectations.
Action 4	Gain assurance that supplier information is routinely assessed, proportionate to their level of risk and that the organisation is resilient to cyber security risks from its supply chain and business partners.
Action 5	Gain assurance that risk assessments are conducted regularly and that risk mitigations account for recent, or expected, changes in the organisation, technology, regulations or wider threat landscape.

B: Strategy

Action 1	Gain assurance that the organisation has developed a cyber strategy and this is aligned with, and embedded within, the wider organisational strategy.
Action 2	Gain assurance that the cyber strategy aligns with the agreed cyber risk appetite (Action A3), meets relevant regulatory obligations, and accounts for current or expected changes (Action A5).
Action 3	Gain assurance that resources are allocated effectively to manage the agreed cyber risks (Action A3 and A5).
Action 4	Gain assurance that the cyber strategy is being delivered effectively and is achieving the intended outcomes.

C: People

Action 1	Promote a cyber security culture that encourages positive behaviours and accountability across all levels. This should be aligned with the organisation's strategy (Action B1).
Action 2	Gain assurance that there are clear policies that support a positive cyber security culture.
Action 3	Undertake training to improve your own cyber literacy and take responsibility for the security of the data and digital assets that you use.
Action 4	Gain assurance, using suitable metrics, that the organisation has an effective cyber security training, education and awareness programme.

Cyber Governance Code of Practice

D: Incident planning, response and recovery

Action 1	Gain assurance that the organisation has a plan to respond to and recover from a cyber incident impacting business critical technology processes, information and services.
Action 2	Gain assurance that there is at least annual exercising of the plan involving relevant internal and external stakeholders and that lessons from the exercise are reflected in the incident plan (Action D1) and risk assessments (Action A5).
Action 3	In the event of an incident, take responsibility for individual regulatory obligations, such as reporting, and support the organisation in critical decision making and external communications.
Action 4	Gain assurance that a post incident review process is in place to incorporate lessons learned into future risk assessments (Action A5), response and recovery plans (Action D1) and exercising (Action D2).

E: Assurance and oversight

Action 1	Establish a cyber governance structure which is embedded within the wider governance structure of the organisation. This should include clear definition of roles and responsibilities, including ownership of cyber at executive and non-executive director level.
Action 2	Require formal reporting on at least a quarterly basis, set suitable metrics to track, and agree tolerances for each. These should be aligned to the cyber strategy (Action B1) and based on the agreed cyber risk appetite (Action A3).
Action 3	Establish regular two-way dialogue with relevant senior executives, including but not limited to, the chief information security officer (or equivalent).
Action 4	Gain assurance that cyber security considerations (including the actions in this code) are integrated and consistent with existing internal and external audit and assurance mechanisms.
Action 5	Gain assurance that senior executives are aware of relevant regulatory obligations, as well as best practice contained within other Codes of Practice.

Glossary

Term	Definition
Chief Information Security Officer (or equivalent)	A senior-level executive who is responsible for an organisation's information, cyber and technology policies and security.
Cyber literacy	The ability to understand, discuss and engage with matters relating to cyber security.
Cyber resilience	The overall ability of systems, organisations and citizens to withstand cyber events and, where harm is caused, recover from them.
Cyber security	The protection of internet-connected systems (to include hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so.
Cyber security culture	The values that determine how people are expected to think about and approach security in an organisation. These are shaped by the goals, structure, policies, processes, and leadership of the organisation.
Cyber strategy	A plan of high-level actions of how the organisation will use cyber security to support and enable organisational goals and objectives.
Data and digital assets	The digital resources, files, technologies, information and intellectual property that an organisation owns, stores or manages.
Gain assurance	Obtain and maintain confidence or verification that systems, processes or controls are effective, reliable, and meet required standards, often through audits, reviews, or third-party validations.
Internal controls	The policies, processes, tasks, and behaviours designed to safeguard an organisations assets, minimise risk, and ensure business continuity.
Risk appetite	The level of risk that an organisation is prepared to take in pursuit of its objectives.
Risk owner	A person who is accountable for a risk within an organisation.
Threat landscape	The collection of current and potential cyber security threats that could impact an organisation, sector, or other group. The threat landscape is dynamic and can change rapidly.

Resources

These resources will support boards and directors in implementing the Code.

Cyber Governance Training

- Access all the training modules

Cyber Governance Training: Key Takeaways

- Risk management
- Strategy
- People
- Incident planning, response and recovery
- Assurance and oversight

Cyber Security Toolkit for Boards

Principle A: Risk Management

- Identifying the critical assets in your organisation
- Risk management for cyber security
- Collaborating with your supply chain and partners

Principle B: Strategy

- Embedding cyber security into your organisation
- Understanding the cyber security threat
- Implementing effective cyber security measures
- Cyber security regulations and directors' duties in the UK

Principle C: People

- Developing a positive cyber security culture
- Growing cyber security expertise

Principle D: Incident Planning, Response and Recovery

- Planning your response to cyber incidents

Principle E: Oversight and Assurance

- Embedding cyber security into your organisation
- Understanding the cyber security threat

Further Resources

- Responding to a cyber incident - a guide for CEOs
- Questions for the board

DSIT is committed to monitoring and evaluating the cyber governance code of practice. You can provide your feedback through our survey.

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

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

Cyber Governance Code of Practice				
Action 1	**Action 2**	**Action 3**	**Action 4**	**Action 5**
A: Risk management				
Gain assurance that the technology processes, information and services critical to the organisation's objectives have been identified, prioritised and agreed.	Agree senior ownership of cyber security risks and gain assurance that they are integrated into the organisation's wider enterprise risk management and internal controls.	Define and clearly communicate the organisation's cyber security risk appetite and gain assurance that the organisation has an action plan to meet these risk expectations.	Gain assurance that supplier information is routinely assessed, proportionate to their level of risk and that the organisation is resilient to cyber security risks from its supply chain and business partners.	Gain assurance that risk assessments are conducted regularly and that risk mitigations account for recent, or expected, changes in the organisation, technology, regulations or wider threat landscape.
B: Strategy				
Gain assurance that the organisation has developed a cyber strategy and this is aligned with, and embedded within, the wider organisational strategy.	Gain assurance that the cyber strategy aligns with the agreed cyber risk appetite (Action A3), meets relevant regulatory obligations, and accounts for current or expected changes (Action A5).	Gain assurance that resources are allocated effectively to manage the agreed cyber risks (Action A3 and A5).	Gain assurance that the cyber strategy is being delivered effectively and is achieving the intended outcomes.	
C: People				
Promote a cyber security culture that encourages positive behaviours and accountability across all levels. This should be aligned with the organisation's strategy (Action B1).	Gain assurance that there are clear policies that support a positive cyber security culture.	Undertake training to improve your own cyber literacy and take responsibility for the security of the data and digital assets that you use.	Gain assurance, using suitable metrics, that the organisation has an effective cyber security training, education and awareness programme.	
D: Incident planning, response and recovery				
Gain assurance that the organisation has a plan to respond to and recover from a cyber incident impacting business critical technology processes, information and services.	Gain assurance that there is at least annual exercising of the plan involving relevant internal and external stakeholders and that lessons from the exercise are reflected in the incident plan (Action D1) and risk assessments (Action A5).	In the event of an incident, take responsibility for individual regulatory obligations, such as reporting, and support the organisation in critical decision making and external communications.	Gain assurance that a post incident review process is in place to incorporate lessons learned into future risk assessments (Action A5), response and recovery plans (Action D1) and exercising (Action D2).	
E: Assurance and oversight				
Establish a cyber governance structure which is embedded within the wider governance structure of the organisation. This should include clear definition of roles and responsibilities, including ownership of cyber at executive and non-executive director level.	Require formal reporting on at least a quarterly basis, set suitable metrics to track, and agree tolerances for each. These should be aligned to the cyber strategy (Action B1) and based on the agreed cyber risk appetite (Action A3).	Establish regular two-way dialogue with relevant senior executives, including but not limited to, the chief information security officer (or equivalent).	Gain assurance that cyber security considerations (including the actions in this code) are integrated and consistent with existing internal and external audit and assurance mechanisms.	Gain assurance that senior executives are aware of relevant regulatory obligations, as well as best practice contained within other Codes of Practice.