Department for Science, Innovation & Technology

National Cyber Security Centre
a part of GCHQ

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.