Loss Prevention Standards – Cyber

Cyber Governance for Boards

This Loss Prevention Standard is designed to provide advice on what senior management and Boards can do to ensure they are taking the right steps regarding cyber risk management, with advice taken from the NCSC’s Cyber Governance Code of Practice.

Version: 1.1
Date: 12th August 2025

Cyber Governance for Boards

Introduction

This Loss Prevention Standard is designed to provide advice on what senior management and Boards can do to ensure they are taking the right steps regarding cyber risk management, with advice taken from the NCSC's Cyber Governance Code of Practice.

Ownership of Cyber Governance sits firmly with Board level, and in the face of increasingly complex risks and regulatory requirements, scrutiny is likely to become ever more heightened.

This Loss Prevention Standard includes links to openly available training and advice, as well as actionable steps that organisations can take to manage their exposure.

Background

The role of the Board in an organisation's cyber security approach is an essential part of any risk management programme. The criticality of their involvement is reflected across industry standards too, with ISO 27001, the international standard for implementing an information security management system, dictating that "top management shall demonstrate leadership and commitment with respect to the information security management system"[1]. The National Institute of Standards and Technology's Cyber Security Framework also places a heavy bearing on the necessity of leadership, with an entire section of the framework being dedicated to how organisations "Govern"[2].

Cyber security must be aligned with overall business objectives and must be an enabler for stability and growth. It must permeate and support each area of an organisation, without being a barrier. The National Cyber Security Centre's (NCSC) breaches survey for 2024 reported that 74% of large businesses in the UK suffered some form of cyber-attack, and 37% of medium businesses did not undertake any form of cyber risk assessment[3].

With increased regulatory stances from nations around the world are becoming the norm, it is an area of governance that should be closely monitored. For example, the UK government are implementing the Cyber Security and Resilience Bill, with the aim being to strengthen the UK's cyber defences and build resilience across essential services. As a result, managed service providers and other critical suppliers are expected to have increased requirements around their cyber security controls[4], and it's likely that increased expected levels of cyber controls are going to filter out to medium and larger sized businesses before too long, if not already.

[1] ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements, https://www.iso.org/standard/27001

[2] National Institute of Standards and Technology, Cyber Security Framework, https://doi.org/10.6028/NIST.CSWP.29

[3] Cyber Security Breaches Survey 2024, Cyber security breaches survey 2024 - GOV.UK

[4] Cyber Security and Resilience Bill, Cyber Security and Resilience Bill - GOV.UK

The Cyber Governance Code of Practice

The NCSC have created the Cyber Governance Code of Practice to help "support Boards in governing cyber security risks and set out the most critical actions that Boards need to take ownership of[5]". It is a key part of a three-pronged approach from the NCSC to improve the Board's participation in cyber security discussions, the other's being a Cyber Governance Training course and a Cyber Security Toolkit for Boards.

The Five Pillars

There are five top-level governing principles/sections in the NCSC code of practice:

A. Risk Management
B. Strategy
C. People
D. Incident Planning, Response and Recovery
E. Assurance and Oversight

Each principle encourages the Board to gain assurance that a particular control or action has been implemented. Whilst there is no requirement for the Board to be technical experts, a knowledge of basic concepts of cyber security is useful. Whilst there may be some initial apprehension to the following topics, the principles themselves are not overly technical, and in our advice for each action we've strived to explain the concepts in easy-to-understand terms with key pointers and questions in regard to each action.

Section A: Risk Management

Risk Management in a cyber security context is essentially the process of identifying (e.g. what is the risk), evaluating (e.g. how bad is it) and treating (e.g. what are we going to do about it) cyber risks. There are numerous standards to choose from and apply here. A simple to follow and internationally recognised path is the one outlined by ISO 27005. IT Governance Ltd have a good writeup on the general process of how to work with ISO 27005: What is ISO 27005?

There are five sub-points to consider within the 'Risk Management' arm of the NCSC code, which are explained in more detail below.

Subsection A1: Gain assurance that the technology processes, information and services critical to the organisation's objectives have been identified, prioritised and agreed.

In simple terms: Does the organisation know what their critical processes are, and if so, have they been identified, documented (generally in the form of a Business Impact Assessment) and prioritised?

Critical processes are anything that maintain operational stability. This can include things like paying staff, receiving goods from a supplier, delivering services to a customer, the list goes on. In a cyber security context, this also extends to the IT systems that these processes rely on. This again could take many forms, be it a database on an on-premises server, or a third party hosted Software-as-a-Service platform. It is the Board's responsibility to outline what the businesses core objectives are first, to support personnel in the identification of key processes and systems.

[5] Cyber Governance code of practice, 2025 https://www.ncsc.gov.uk/cyber-governance-for-Boards/code-of-practice

The Board should check for the existence of this process, ensure it is documented, and it is up to date. If this hasn't been completed, a good place to start can be a Business Impact Assessment. There is guidance available in ISO 22317 and from the UK Government Security page to complete this. It should be noted however, the process will require cross collaboration between various departments, including (but not limited to) the Board, HR, legal, finance, IT, and any internal risk and audit functions.

Subsection A2: 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.
In simple terms: In the risk register, are members of the Board ultimately responsible for certain risks, even if they are delegated to the correct technical specialist?

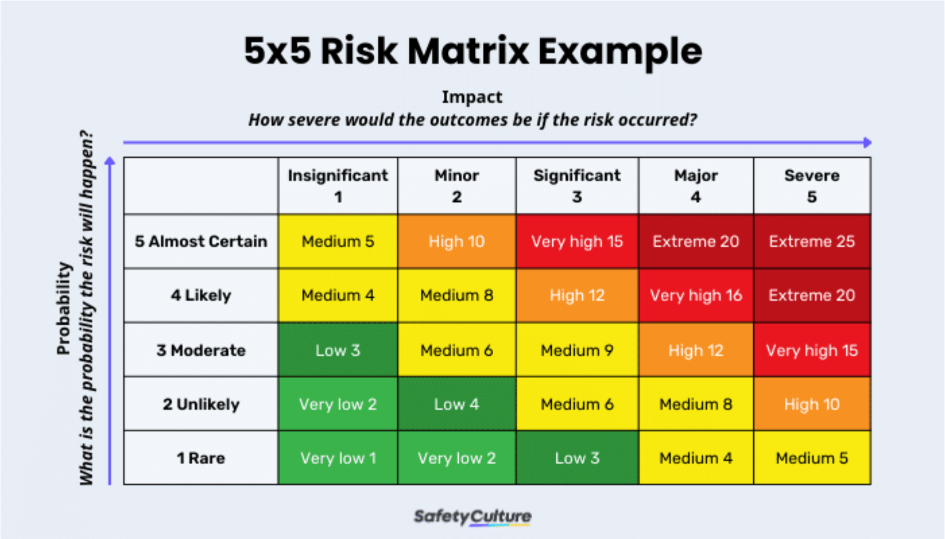
Members of the Board should have overall responsibility for certain risks that are identified as part of the risk management process. Whilst they may not have direct day-to-day influence on mitigating a specific risk, there should be documented evidence (e.g. within a Risk Treatment Plan) as to who the overall risk owner is and what the delegations and actions are. Some organisations create different "Levels" of risk owner to assist with this. For example, the Level 3 owner may be a Board member (strategic direction), the Level 2 owner may be a senior manager (policy creator), and the Level 1 may be a technical analyst (control implementer).

Subsection A3: 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.
In simple terms: Has the Board clearly determined (and documented) what level of cyber risk the organisation is able to tolerate?

Cyber security must support business objectives; it can never be the other way around. The most secure system in the world may not allow anybody access to it and is thus operationally redundant. The Board is responsible for setting the level of cyber risk appetite. Functionally though, what does this look like?

There are four general approaches to treating a risk. They can be mitigated, avoided, transferred or accepted.

For risk assessments whereby the primary assessment mechanism is a traditional 5x5 risk matrix (as seen in figure one) it may be that the Board decides anything above a score of fifteen is seen as an 'unacceptable' risk verses anything below that being 'acceptable'. Anything deemed 'unacceptable' should be treated by the remaining three methods (what are these?).



5x5 Risk Matrix Example

Impact
How severe would the outcomes be if the risk occurred?

Probability
What is the probability the risk will happen?

	Insignificant 1	Minor 2	Significant 3	Major 4	Severe 5
5 Almost Certain	Medium 5	High 10	Very high 15	Extreme 20	Extreme 25
4 Likely	Medium 4	Medium 8	High 12	Very high 16	Extreme 20
3 Moderate	Low 3	Medium 6	Medium 9	High 12	Very high 15
2 Unlikely	Very low 2	Low 4	Medium 6	Medium 8	High 10
1 Rare	Very low 1	Very low 2	Low 3	Medium 4	Medium 5

SafetyCulture

Figure 1 - 5x5 matrix example - https://safetyculture.com/topics/risk-assessment/5x5-risk-matrix/

Boards can also communicate the level of tolerable risk by other means too. The burgeoning field of cyber risk quantification allows a Board to communicate what level of total exposure they are comfortable with, where to invest funds, and can help to assess levels of insurance purchased. For example, if following an analysis, the total level of risk an organisation faces is thought to be in the range of £50m - £70m, the Board could set an 'acceptable' level of tolerance for them to be at £20m - £35m. This could influence decisions on which of the larger perceived risks require investment to reduce their potential exposure down, and the remainder could be transferred away in the form of a cyber insurance policy.

Whilst more complicated to navigate, this field is continuously growing with considerable inputs from the [FAIR Institute]() (as seen in Figure 2 below) and [The Open Group]() . If you're interested in learning more on the risk quantification approach, please reach out to [armscyber@aviva.com]().

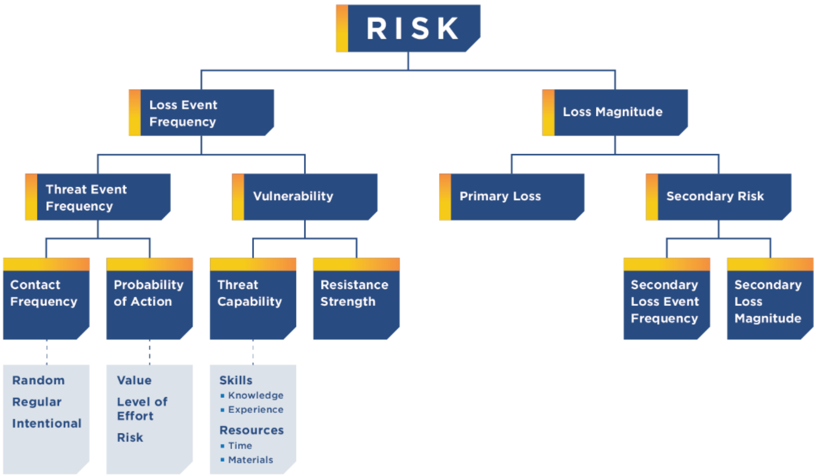


Figure 2 - FAIR Model for Risk Quantification - Source: FAIR Institute - https://www.fairinstitute.org/blog/fair-model-on-a-page

Subsection A4: 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
In simple terms: Does the organisation place any minimum-security standards on its key suppliers and third parties?

Cyber security supply chain risks are fast growing. It's imperative for organisations to know what their core processes are (following the advice of A1) and where they're reliant on third parties. If a business allows third parties access to their data or systems, it's critical to know how they're considering and mitigating their own cyber risks too. A weak link in a chain can cause disruption and losses. An important initiative for an organisation could be to ensure minimum security controls are in place across core suppliers. For example, this could be mandating the implementation of Cyber Essentials certification or creating a security questionnaire that a supplier must adhere to, including audits.

The NCSC has further guidance on securing the Supply Chain and what practically organisations can do.

Subsection A5: 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.
In simple terms: Does the organisation conduct cyber security risk assessments, and if so, are they done (at least) every year?

This one is simple enough and is all about consistency. ISO 27001 dictates that risk assessments are completed at least annually, or when there is a significant change within the business. This could be an acquisition, an extrinsic shock to the trading environment, a change in the external threat landscape, the list goes on.

It is considered best practice to ensure they're updated annually and that the Board gets **at least** an annual presentation on how the risk assessment process is progressing, updates on the most critically identified risks and the outcome of any risk treatment plans.

Section B: Strategy

A well-defined cyber strategy provides a clear roadmap for managing cyber risks, integrating security measures into every aspect of the business. This isn't necessarily a line-by-line approach to exactly how you're going to achieve each goal but encapsulates high level actions that an organisation could take to achieve its objectives. The NCSC advises it should include areas such as:

- Planning your response to an incident.
- Exercising incident response procedures.
- Detecting, responding to and recovering from a cyber-attack.
- Employee cyber awareness training.

It helps to ensure that cyber security is not an afterthought but a fundamental component of strategic planning and decision-making. By adopting a proactive approach, organisations can enhance their cyber resilience, maintain stakeholder trust, and achieve sustainable growth.

There are four sub-points to consider within the 'Strategy' arm of the NCSC code, which are explained in more detail below.

Subsection B1: Gain assurance that the organisation has developed a cyber strategy, and this is aligned with, and embedded within, the wider organisational strategy.
In simple terms: Does your organisation have a cyber strategy, and does this link in with your wider organisational strategy?

To answer this question, drawing up a documented outline of your strategy is a useful place to start. Are there certifications, such as Cyber Essentials, the organisation wants to work towards? Do you want to get 100% staff completion rate on awareness training? In practice, this means having a clear, long-term plan that spans three to five years. This plan should outline how your organisation will manage cyber risks, including the allocation of resources and the implementation of necessary controls. It should also include a process for monitoring and responding to changes in the threat environment and regulatory requirements.

The Local Government Association in the UK has put together an example strategy template, which can be adapted for organisation's needs and is found here.

B2: 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).
In simple terms: Does your strategy encompass a three-to-five-year plan? Also, as part of the strategy, have you considered any laws or regulations that your organisation is affected by?

Ensuring that your cyber strategy aligns with your organisation's risk appetite is crucial for maintaining a balanced approach to cyber security. This means that the strategy should reflect the level of risk your organisation is willing to accept and manage. It's not just about setting high-level goals but also about making sure these goals are realistic and achievable within the agreed risk parameters.

Your strategy must also consider any relevant regulatory obligations. This involves staying up to date with laws and regulations that impact your industry and ensuring that your strategy addresses these requirements. Regular reviews and updates to the strategy are essential to account for any changes in the regulatory landscape. Some relevant areas to consider could be:

- UK GDPR.
- Data Protection Act 2018.
- (Upcoming) Cyber Security and Resilience Bill.
- EU AI Act.
- NIS Directive.

For example, if new data protection regulations are introduced, your strategy should include steps to ensure compliance, such as updating policies and training staff. Similarly, if your organisation's risk appetite changes, the strategy should be adjusted accordingly to reflect this new direction.

Subsection B3: Gain assurance that resources are allocated effectively to manage the agreed cyber risks (Action A3 and A5).
In simple terms: Have you got a budget, and resources set aside for Information and Cyber Security investment?

Once the Board has agreed a risk treatment plan, how do they make sure that the actions are followed through with the correct resource allocation?

This doesn't have to be all about money and securing new technologies (although having serious investment plans can help). It might take the guise of refocusing or upskilling a member of the team to another area, (e.g. moving someone from Vulnerability Management to Threat Intelligence). Does the organisation have someone who's responsible for cyber security provisions? If the IT team believe they require a new managed detection and response service, who approves this spend?

Having someone on the Board whose core focus is digital and cyber resilience, can result in organisations experiencing less disruption from cyber-attacks.

Subsection B4: Gain assurance that the cyber strategy is being delivered effectively and is achieving the intended outcomes.
In simple terms: Are you measuring the success of your cyber security programme to see if it is being run effectively and improving?

There are several common statistics you can look toward for confirmation of an improving cyber strategy. These can include (and are not limited to) things such as:

- The click rate on Internal Phishing Campaigns. (Related to point C4 later).
- Reporting rate on phishing campaigns.
- Increasing scores on cyber maturity assessments against cyber security frameworks and outlined controls.
- Percentage compliance with industry standards.
- Staff training completion rates.
- Falling exposure levels on cyber risk quantification exercises.
- Reductions in vulnerabilities identified across the organisation.
- Reductions in time to patch vulnerabilities across the organisation.

Any areas the business chooses to assess should be reported on at least annually to measure progress.

Section C: People

There are two schools of thought in Cyber security surrounding 'people' in an organisation. One is that 'people' are the biggest exposure to any cyber security strategy, and the other, is that they're an organisation's biggest strength.

Wherever you sit on this spectrum, there's no doubting that an organisation's people are a **critical** element of cyber resilience. People are undoubtedly the first, largest and most complex attack vector. It's essential that everyone related to an organisation knows the dangers they face each day and how entire businesses can be brought down due to a lack of awareness.

There are four sub-points to consider within the 'People' arm of the NCSC code, which are explained in more detail below.

Subsection C1: 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).
In simple terms: How often does the organisation communicate with all staff on the importance of cyber security?

Here, simple regular training and messaging is essential. It's unlikely a complex message regarding threat actors and responding to industry trends is going to resonate with everyone. Simple and clear to follow instructions that are backed by technological controls are usually thought to be the way to go.

Information on the wider strategy, industry news (such as hacking events) and any relevant threat intelligence should be on the regular updates that go out to all staff.

Subsection C2: Gain assurance that there are clear policies that support a positive cyber security culture.
In simple terms: Does the organisation have a set of information security policies, that staff are aware of and are trained on?

Policies are generally the area in which most businesses are lacking. But for organisations that have a comprehensive set, it can be difficult to get staff to adhere to the outlines of each. Do all staff really know the ins and outs of an information security policy programme?

When it comes to culture, the NCSC have put it best here:
"If your organisation is developing a positive cyber security culture, it should be possible for your security team to demonstrate how security policies and processes have been designed in collaboration with HR and training teams to really address the problem and improve the culture. If it is hard to point to ways in which policy or process has been shaped by the wider organisation (including business process owners), this may indicate a less mature cyber security culture."

Subsection C3: Undertake training to improve your own cyber literacy and take responsibility for the security of the data and digital assets that you use.
In simple terms: How clued up are you personally (and as a Board) on cyber security?

The NCSC have put together a hand training module for Boards here , but the learning never stops. Encourage presentations from technical staff on the threat landscape, read industry reports and even enrol in a free online class on an Introduction to Cybersecurity from Cisco's Networking Academy (NetAcad).

Aviva have cyber risk management courses on our Aviva Risk Training Solutions platform, for policyholders. Get in touch if you'd like to know more.

Subsection C4: Gain assurance, using suitable metrics, that the organisation has an effective cyber security training, education and awareness programme.
In simple terms: Are statistics on cyber security training across the organisation made available to the Board?

Linking in with action B4 above, there are two main areas when it comes to measuring metrics of "People".

The first step could be to aim for a 100% completion rate on cyber awareness training from staff. Some cyber insurance policies even mandate this as a condition of cover, so it may be worth double checking your own policy.

The second step could be regarding phishing statistics. Phishing simulations are an excellent way to test your staff's resilience against social engineering, and they are a worthwhile investment as part of any cyber resilience regime. Areas to keep an eye on will be the click-rate (e.g. staff clicking on potentially dangerous links) and the reporting rate (staff reporting the phishing email). If there are staff regularly putting their credentials into fake websites (following clicking on any provided links), this is something that should set alarm bells off and swiftly addressed with additional training. It is key however, to not create a blame culture, and instead focus on how they are the first line of crucial defence for the business.

Ideally over time, the business has an increasing training and reporting rate, and a decreasing click rate.

There are details of our Specialist Partner for Phishing and how they can help at the end of this document.

Section D: Incident Planning, Response & Recovery

The question for businesses is no longer if an incident will occur, but when. For Boards overseeing cyber governance, this reality demands a proactive and structured approach to incident planning, response, and recovery. A well-prepared organisation doesn't just react to cyber incidents—it anticipates them, plans for them, and recovers from them with resilience and speed.

Effective incident management is not just a technical exercise; it's a strategic imperative.

It requires clear governance, defined roles and responsibilities, and rehearsed procedures that span the entire organisation. From the Boardroom to the server room, everyone must understand their role in the event of a breach or disruption.

This section explores how Boards can ensure their organisations are not only prepared to withstand cyber incidents but are also equipped to emerge stronger from them. It covers the essential components of incident readiness, the importance of timely and coordinated response, and the critical steps to achieving full recovery—both operationally and reputationally.

There are four sub-points to consider within the 'Incident Planning, Response & Recovery' arm of the NCSC code, which are explained in more detail below.

Subsection D1: 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.

In simple terms: Does the organisation have an incident response plan and process?

An incident response plan is a living document that contains:

- Classification of what is an incident is (e.g. thresholds).
- Who's in the cyber incident response team (CIRT).
- Roles and responsibilities.
- The technical response (how to contain, eradicate and recover).
- The communications strategy throughout.
- Details of cyber insurance.

The plan is an essential part of any organisations approach to cyber risk management. The Board should ensure that this plan has been reviewed in the last year, and if there are any contacts, details of insurance or playbooks (these are documents that have prescribed technical responses to specific incidents, e.g. ransomware deployed at a data centre) that they have been suitably updated with relevant information.

It's also key to identify where external expertise will be required. Not burning out (protecting the mental health, wellbeing and resistance of?' internal people resources is imperative to a successful and swift resolution from a cyber-attack. This can be completed by partnering with external incident response teams, legal firms and public relations companies. Cyber Insurance is a useful product which provides cover for the provision of services to aid of a response to a cyber-attack. Learn more about cyber insurance here.

Subsection D2: 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 simple terms: Is this Incident response plan tested with key members of the team and the Board?

An incident response plan is only as effective as its execution. Regular exercising (through risk free tabletop exercises, or live technical drills) is essential to ensure that everyone involved knows their role and can act swiftly and confidently under pressure.

These exercises should:

- Involve all relevant internal stakeholders, including IT, legal, communications, and executive leadership.
- Include external partners where appropriate, such as managed service providers, regulators, or law enforcement.
- Test both technical and non-technical aspects of the plan, including decision-making, communication, and escalation procedures.
- Be realistic and based on current threat scenarios (e.g. ransomware, data breach, supply chain compromise).

The National Cyber Security Centre has several resources dedicated to supporting businesses in creating effective tabletop exercises. Find out more here.

Subsection D3: 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.
In simple terms: In the Incident Response plan, are there clear instructions for who is responsible for what?

Similar in tone to Action B2, does the organisation know what regulatory obligations it must comply with? For loss of personal data, the ICO mandates a reporting of this within 72 hours[6]. For legal firms or who lose client money or data, you must tell the Solicitors Regulatory Authority (SRA) immediately[7]. Any incident response plan should reference who is responsible for leading the reporting element to the relevant regulatory authority.

[6] Personal Data Breaches: A guide https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/

[7] The Law Society, What to do after a cyber attack, https://www.lawsociety.org.uk/topics/cybersecurity/what-to-do-after-a-cyber-attack

Communications are a large part of the incident response process as well. What do you tell your staff? What about the media, or your key contracts? Should an organisation be as detailed as possible, or only reveal limited information about the attack and its effects? A solid public relations strategy will pay dividends for years after any incident, as if handled correctly it can show competent leadership. The opposite could be catastrophic.

Again, having access to external experts before any incident is imperative.

Subsection D4: 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).
In simple terms: Within the Incident Response plan, are "lessons learned" and reflection meetings scheduled?

A cyber incident doesn't end when systems are restored and operations resume. The most resilient organisations treat each incident as a learning opportunity.

A structured post-incident review process ensures that mistakes aren't repeated, blind spots are addressed, and the organisation becomes stronger with each challenge.

This review process should:

- Be scheduled as a formal step in the incident response plan.
- Involve all relevant stakeholders, including technical teams, legal, communications, and executive leadership.
- Capture what went well, what didn't, and what needs to change.

Section E: Assurance & Oversight

Cyber security is not a one-time investment or a static policy—it's a continuous process of vigilance, improvement, and accountability. For Boards, assurance and oversight are about more than just asking if the right controls are in place. It's about knowing whether those controls are effective, whether they're being followed, and whether they're keeping pace with a rapidly evolving threat landscape.

This section explores how Boards can gain that confidence. It covers how to ask the right questions, how to interpret the answers, and how to ensure that cyber security is embedded into the organisation's governance structures, just like financial or legal risk. It also highlights the importance of external validation, threat intelligence, and a culture of transparency and continuous improvement.

There are five sub-points to consider within the 'Assurance & Oversight' arm of the NCSC code, which are explained in more detail below.

Subsection E1: 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.
In simple terms: Is it clear who is responsible for cyber security decisions at the top of the organisation?

The work undertaken here should not sit in isolation, it must be fully integrated into the organisation's overall governance framework. This means clearly defining where cyber risk sits within the organisation's risk management structure and ensuring that both Board members and non-executive leaders understand their roles in overseeing it.

A robust cyber governance structure should include:

- Clear ownership of cyber risk at both the executive and Board level.
- Defined roles and responsibilities, including who is accountable for strategy, operations, risk, and incident response.
- Regular reporting lines into Board committees (e.g. audit, risk, or technology committees).
- Alignment with other governance areas, such as financial, legal, and operational risk.

If there's anything to be taken from this document, it's that cyber security is a Board-level issue, not just an IT concern. Boards should ensure that cyber is a standing agenda item, that there is sufficient expertise to challenge and support cyber decisions, and that governance structures enable timely escalation and decision-making in the event of a cyber incident.

Embedding cyber into the wider governance framework ensures it is treated with the same rigour and oversight as other critical business risks.

Subsection E2: 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).
In simple terms: Does the Board have a quarterly update on how the organisation is managing their cyber risks?

Boards need regular, structured updates to maintain effective oversight. Quarterly reporting ensures that cyber security remains visible at the highest level and that the organisation's posture is being measured against its strategic goals and risk appetite.

Effective reporting should include key metrics aligned to the cyber strategy (Action B1), such as:

- Cyber training completion rates (see Action C4 for further examples)
- Phishing simulation results (click rates, reporting rates)
- Number and severity of incidents, notable events or near misses
- Patch management and vulnerability remediation timelines
- Third-party risk indicators
- Agreed tolerances for each metric, so the Board can quickly identify when performance is outside acceptable limits.
- Trend analysis to show whether the organisation is improving or regressing over time.
- Contextual insights, not just raw data (e.g. what the numbers mean, what's driving them, and what actions are being taken)

Subsection E3: Establish regular two-way dialogue with relevant senior executives, including but not limited to, the chief information security officer (or equivalent).
In simple terms: Is there a technical person who regularly meets with the Board as a whole?

This dialogue should not be occasional or informal. It needs to be structured and consistent, giving the Board the opportunity to ask informed questions, challenge assumptions, and understand the broader implications of cyber risks.

At the same time, it ensures that the CISO (or equivalent) has a direct line to the Board, allowing critical issues to be raised without delay or distortion.

Through this relationship, the Board stays informed about emerging threats, trends in incidents, capability gaps, and resource requirements. It also helps ensure that the organisation's cyber risk appetite and strategy are well understood and aligned across leadership. (a key marker to hit for any firm looking to implement IASME or ISO 27001).

Ultimately, this regular engagement builds trust, strengthens decision-making, and ensures that cyber security is treated as a strategic priority, not just an operational concern.

Subsection E4: 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.
In simple terms: Do your internal audits consider the actions set out in the code of governance?

This action is self-referential, so it may seem odd. But it still raises an important point. Are the Board doing all the things that this code of governance recommends?

We've put together a checklist, including the NCSC's indicators of success from the Board pack, to aid you in this endeavour. It's at the end of this loss prevention standard as an Appendix, entitled "Governance Action Checklist". Feel free to use this as a basis to see how you compare against the guidance.

Subsection E5: Gain assurance that senior executives are aware of relevant regulatory obligations, as well as best practice contained within other Codes of Practice.
In simple terms: Do senior leaders know what laws and rules they need to follow when it comes to cyber security—and are they keeping up with best practice?

Action B2 goes into some examples of potentially relevant regulations both in place and on the horizon, and it's imperative that senior executives know what's required of the business.

Whichever framework (and the best practice guides contained within) the organisation chooses to align themselves with is entirely down to them. It should be based on numerous factors, such as industry, business objectives, working knowledge of the framework, and potentially other frameworks in use. For example, an organisation with ISO 9001 certification might find it more culturally appropriate to take on ISO 27001, whilst a business with Cyber Essentials Plus under their belt may see IASME Cyber Assurance as the next logical step.

Senior executives should be made aware of these initiatives and any aspirational targets of the business and even engage in their selection based upon the prospective merits. A major selling point of good governance and compliance is boosted trust, and commercial viability.

Conclusion

The remainder of this decade is likely to bring significant changes to the regulatory and operational landscape for cyber security in the UK. Think about the requirements for FCA regulated firms and the processes now seen as commonplace for businesses in these sectors. With the introduction of new legislation such as the Cyber Security and Resilience Bill, and the increasing expectations placed on organisations by regulators, customers, and insurers alike, cyber governance is no longer a niche concern—it is a Boardroom priority.

This document has outlined the practical steps Boards can take to embed cyber security into their governance structures, strategies, and culture. From identifying critical business processes and setting a clear risk appetite, to ensuring regular incident response exercises and meaningful engagement with technical leaders, the actions outlined here are designed to help Boards move from passive oversight to active leadership.

Cyber security is not just about preventing attacks—it's about building resilience. That means having the right people, processes, and plans in place to respond effectively when things go wrong, and to learn and improve when they do. It also means ensuring that cyber risk is treated with the same seriousness and structure as financial, legal, or operational risk.

Boards don't need to be technical experts, but they do need to ask the right questions, understand the answers, and hold their organisations to account. The NCSC's Cyber Governance Code of Practice provides a strong foundation for doing just that, and this guidance has aimed to translate those principles into clear, actionable advice.

Ultimately, good cyber governance is about protecting the organisation's reputation, operations, and future. It's about leadership, accountability, and making informed decisions in an increasingly digital world.

Checklist

A generic **Cyber Governance Action Checklist** is presented in Appendix 1 which can be tailored to your own organisation.

Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services at preferential rates via our network of Specialist Partners.

Crisis Communications and Business Continuity - **Horizonscan**
Cyber Security Awareness Training - **Phishing Tackle**

For more information please visit: Aviva Risk Management Solutions - Specialist Partners

Sources and Useful Links

- ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements
- National Institute of Standards and Technology, Cyber Security Framework
- Cyber security breaches survey 2024 - GOV.UK
- Cyber Security and Resilience Bill - GOV.UK
- National Cyber Security Centre (NCSC)
- NCSC Cyber Governance Code of Practice
- CISCO Course - Introduction to Cybersecurity
- NCSC Cyber Governance Training course
- NCSC Cyber Security Toolkit for Boards.
- Local Government Association strategy template.
- Personal Data Breaches: A guide
- The Law Society - What to do after a cyber attack

Additional Information

- **Cyber Security: Top 12 Tips to Protect Against Cyber Attacks.**
- **Cyber Security: Respond and Recover.**
- **Cyber Security: The Internet of Things**
- **Ransomware - Cyber Loss Prevention Standard**
- **Cyber Essentials - Accreditation**
- **Cyber - Respond and Recover**
- **Cyber - Incident Response Process**
- **Cyber - Homeworking Security**

To find out more, please visit Aviva Risk Management Solutions **or speak to one of our advisors.**

Email us at riskadvice@aviva.com or call 0345 366 6666.*

*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

Appendix 1 – Cyber Governance Action Checklist

Location	
Date	
Completed by (name and signature)	

	Governance Action	Y/N	Comments
	A: Risk Management		
A1.	Gain assurance that the technology processes, information and services critical to the organisation's objectives have been identified, prioritised and agreed. **Success Indicators** a) Asset Inventories are up to date. b) Change management databases are up to date. c) Business Impact assessments are completed at least annually. d) Critical assets are matched to a business objective.		
A2.	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. **Success Indicators** a) Cyber risks are included in the enterprise risk register b) Named Board-level owners are assigned to key cyber risks. c) Risk Treatment Plans include ownership and delegation levels. d) Cyber risk ownership is reviewed at least annually. e) Cyber risks are discussed at Board or risk committee meetings.		
A3.	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. **Success Indicators** a) Cyber risk appetite is formally documented b) Risk appetite is aligned with business objectives		

	c) Risk treatment thresholds (e.g. via a 5x5 matrix) are clearly defined d) Action plans exist for risks exceeding the defined appetite e) Risk appetite is reviewed and updated regularly by the Board		
A4.	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. **Success Indicators** a) Key suppliers and third parties are identified and risk-assessed b) Minimum cyber security standards are defined for suppliers c) Supplier contracts include security requirements or clauses d) Security questionnaires or assessments are conducted regularly e) Spot audits or reviews are performed on high-risk suppliers		
A5.	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. **Success Indicators** a) Cyber security risk assessments are conducted at least annually b) Risk assessments are updated following significant organisational or technological changes c) Risk assessments consider changes in the regulatory environment d) Risk assessments reflect current threat intelligence and trends e) The Board receives and reviews risk assessment outcomes annually		

	Governance Action	Y/N	Comments
	B: Strategy		
B1.	Gain assurance that the organisation has developed a cyber strategy, and this is aligned with, and embedded within, the wider organisational strategy. **Success Indicators** a) A written cyber strategy is in place b) All business units have considered cyber security as a risk c) The cyber strategy contains measurable goals and objectives with timelines in place.		
B2.	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). **Success Indicators** a) Applicable regulations are understood and documented		
B3.	Gain assurance that resources are allocated effectively to manage the agreed cyber risks (Action A3 and A5).		
B4.	Gain assurance that the cyber strategy is being delivered effectively and is achieving the intended outcomes. **Success Indicators** a) Progress against the cyber strategy is tracked through regular reporting (e.g. quarterly updates) b) Key performance indicators (KPIs) and key risk indicators (KRIs) are defined and monitored c) Independent reviews or audits assess delivery of the strategy at least annually d) Lessons learned and feedback from incidents or testing are used to update the strategy e) The strategy is reviewed and refreshed at least every two years or following major changes		

	Governance Action	Y/N	Comments
	C: People		
C1.	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). **Success Indicators** a) Cyber culture is referenced in the organisation's strategy and values b) Staff receive regular, role-specific cyber awareness training c) Leadership visibly supports and models secure behaviours d) Cyber responsibilities are included in job roles and performance reviews e) Positive behaviours are recognised and reinforced (e.g. through rewards or feedback) f) Staff feel confident reporting incidents or concerns		
C2.	Gain assurance that there are clear policies that support a positive cyber security culture. **Success Indicators** a) Cyber policies are easy to understand and accessible to all staff b) Policies reflect desired behaviours and align with organisational values c) Staff confirm understanding of policies through induction or training d) Policies are reviewed and updated at least annually e) Breaches of policy are tracked and addressed consistently		
C3.	Undertake training to improve your own cyber literacy and take responsibility for the security of the data and digital assets that you use. **Success Indicators** a) Senior leaders complete cyber training annually b) Training includes data handling and asset protection c) Leaders demonstrate secure practices in daily work d) Cyber responsibilities are included in leadership objectives		
C4.	Gain assurance, using suitable metrics, that the organisation has an effective cyber security training, education and awareness programme. **Success Indicators**		

	a) Training completion rates are tracked and reported b) Staff understanding is tested through assessments or simulations c) Programme covers all roles and risk areas d) Feedback is collected and used to improve content e) Effectiveness is reviewed at least annually		

	Governance Action	Y/N	Comments
	D: Incident Planning, Response & Recovery		
D1.	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. **Success Indicators** a) A documented incident response and recovery plan exists and is approved b) The plan covers critical systems, data, and services c) Roles and responsibilities are clearly defined d) Contact lists and escalation paths are up to date e) The plan is reviewed and updated at least annually		
D2.	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). **Success Indicators** a) Incident response exercises are held at least once a year b) Exercises involve key internal teams and external partners c) Scenarios are realistic and based on current threats d) Lessons learned are documented and shared e) Plans and risk registers are updated based on outcomes		
D3.	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. **Success Indicators** a) Regulatory reporting duties are clearly assigned b) Leaders understand their legal and regulatory obligations c) Decision-making roles are defined in the incident plan		

	d) Communications plans include internal and external messaging e) Incident logs include actions taken and decisions made		
D4.	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). **Success Indicators** a) Post-incident reviews are conducted after every major incident b) Reviews identify root causes and improvement actions c) Findings are shared with relevant stakeholders d) Risk assessments, plans, and exercises are updated accordingly e) Progress on improvement actions is tracked and reported		

	Governance Action	Y/N	Comments
	E: Assurance and Oversight		
E1.	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. **Success Indicators** a) Cyber governance roles and responsibilities are clearly defined b) Executive and non-executive ownership of cyber is documented c) Cyber governance is integrated into existing committees or forums d) Governance structure is reviewed annually for effectiveness		
E2.	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). **Success Indicators** a) Cyber reporting is scheduled at least quarterly		

	b) Agreed metrics and tolerances are documented and tracked c) Reports align with the cyber strategy and risk appetite d) Deviations from tolerances trigger defined escalation routes		
E3.	Establish regular two-way dialogue with relevant senior executives, including but not limited to, the chief information security officer (or equivalent). **Success Indicators** a) Regular meetings are held with the CISO or equivalent b) Cyber risks and priorities are discussed with senior leaders c) Feedback from executives informs cyber planning and actions d) Dialogue is documented and reviewed for effectiveness		
E4.	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. **Success Indicators** a) Cyber is included in internal and external audit scopes b) Audit findings related to cyber are tracked and acted upon c) Assurance activities align with the cyber governance framework d) Audit outcomes inform updates to cyber policies and plans		
E5.	Gain assurance that senior executives are aware of relevant regulatory obligations, as well as best practice contained within other Codes of Practice. **Success Indicators** a) Senior leaders receive regular updates on cyber regulations b) Awareness of key codes and standards is tested or confirmed c) Regulatory obligations are mapped to internal controls d) Compliance is reviewed at least annually		

Please Note

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise, and Aviva recommend that you obtain specific advice relevant to the circumstances.

31st July 2024

Version 1.0

ARMSGI3322025

Aviva Insurance Limited, Registered in Scotland Number SC002116. Registered Office: Pitheavlis, Perth PH2 0NH.
Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.