Public Bill Committee Call for Evidence: Cyber Security and Resilience (NIS) Bill
ISACA Submission

Executive Summary

ISACA welcomes the opportunity to submit evidence to support the Public Bill Committee's scrutiny of the Cyber Security and Resilience Bill. As a global professional association with more than 180,000 members worldwide – including over 10,000 cyber security, audit, governance and risk professionals in the UK – ISACA is well placed to comment on the practical challenges organisations face in building and maintaining strong cyber resilience.

Cyber attacks on UK organisations are rising at an alarming rate. More than 40% of UK businesses experienced an incident last year, costing the economy an estimated £14.7 billion, while the NCSC recorded 204 nationally significant cyber events – more than double the previous year. These trends demonstrate that cyber resilience is not only a security concern but a major economic one. Weaknesses in organisational governance, preparedness, and leadership awareness now have a measurable impact on growth, confidence and investment.

Against this backdrop, the Bill presents a timely and important opportunity to strengthen the UK's approach to cyber resilience. The expansion of the NIS perimeter and the creation of new regulatory powers are welcome steps. However, Parliament now has an important opportunity to ensure the legislation is truly future proof and capable of addressing the real-world risks facing the UK economy.

To achieve this, ISACA recommends targeted improvements in three key areas:

1. **Scope and Governance:** Introduce a statutory review of the uptake and effectiveness of the Cyber Governance Code and give Government the power to make adoption mandatory for economically significant businesses currently outside the Bill's scope, such as major retailers.

2. **Accountability and Competency:** Require organisations to name an accountable individual and meet defined competency standards – similar to other safety-critical sectors – supported by recognised industry training and certifications.

3. **Resilience and Testing:** Extend to all in-scope sectors the principle already applied in financial services by empowering regulators to mandate periodic external resilience assessments, such as penetration tests and scenario-based exercises, to ensure organisations can withstand real-world attacks

These recommendations draw directly from ISACA's global research base, our long-standing partnerships with UK Government, and our role as a founding member of the UK Cyber Security Council. Taken together, they would materially strengthen the Bill and help deliver a more resilient digital environment for UK citizens and businesses. ISACA and our UK membership stand ready to support the Committee with additional technical advice or evidence as the Bill progresses.

---

1. Scope and Governance

The Bill's expansion of the UK's NIS perimeter, particularly to Managed Service Providers and large data centres, is an appropriate and necessary response to the growing concentration of operational and systemic risk. However, several economically significant sectors remain outside scope despite their critical role in the wider economy.

Large retailers are a clear example. Retail is the UK's largest private-sector employer, handles substantial volumes of customer data, and often relies on legacy IT systems. These features make major retailers prime targets for cyber criminals, yet they are not covered by the Bill's core obligations.

The Government plans to promote its new Cyber Governance Code of Practice to improve preparedness in these out-of-scope sectors. ISACA supports this ambition. However, evidence shows that voluntary schemes struggle to achieve meaningful or consistent uptake without monitoring, incentives or the possibility of future enforcement. ISACA's Global State of Cybersecurity 2025 report shows that only 56% of boards adequately prioritise cybersecurity, highlighting a persistent gap in board-level oversight.

If Parliament cannot track uptake of the Code, and if Government cannot escalate to mandatory governance where justified, large parts of the UK economy may remain exposed. This creates the risk of systemic vulnerabilities in sectors that are central to economic stability.

ISACA recommends two practical steps to improve governance maturity across the wider economy:

- First, the Bill should require the Secretary of State to publish an annual assessment of the uptake and effectiveness of the Cyber Governance Code of Practice across medium and large UK enterprises. This will enable Parliament to track progress and identify sectors where voluntary adoption remains low.

- Second, the Bill should provide a reserve power enabling Government to require annual board-level attestation to the Code's principles for sectors where risk is rising or uptake is insufficient. This allows proportionate escalation without imposing technical controls on lower-risk organisations.

Please find a suggested amendment to the Bill in the annex below.

---

2. Accountability and Competency

Unlike other safety-critical sectors, the Bill does not require organisations to name an accountable individual or ensure that those responsible for cyber governance meet appropriate competency standards. In industries such as nuclear and aviation, the principle of "suitably qualified and experienced persons" (SQEP) is a proven mechanism for embedding responsibility and driving high-quality decision making.

The absence of similar expectations in other industries presents a risk that compliance becomes a procedural checkbox rather than a meaningful leadership responsibility. ISACA's global research shows that skills and competency gaps are among the biggest barriers to organisational resilience. Smaller firms often

struggle to secure expertise, and even large organisations frequently lack leaders with the necessary level of cyber literacy.

Introducing competency expectations would help ensure that individuals performing governance and compliance functions under the NIS regime have the skills needed to discharge their duties effectively. These standards could be aligned with frameworks developed by the UK Cyber Security Council and supported by widely recognised industry certifications. Providing regulators with a power to introduce competency requirements would give flexibility to develop expectations gradually, proportionately and in consultation with industry.

Please find a suggested amendment to the Bill in the annex below.

---

3. Resilience and Testing

Mandatory resilience testing is a proven mechanism for improving real-world preparedness. In financial services, regulators have required regular threat-led, intelligence-driven resilience exercises since 2014 through frameworks such as CBEST and TIBER. These exercises expose weaknesses not evident through documentation alone and give boards a realistic understanding of their organisation's resilience.

Despite this success, the Bill does not extend comparable requirements to other essential sectors. ISACA's latest research shows that only four in ten organisations are confident in their incident response plans, and many have not undertaken meaningful scenario-based testing or external assessments. Without structured resilience exercises, organisations may rely on untested assumptions about their ability to respond to sophisticated attacks.

Giving regulators the power to require periodic resilience testing – including scenario-based recovery drills, communications rehearsals, and red-team or penetration testing – would materially strengthen the Bill. These measures would create a cycle of continuous improvement and help ensure essential services can withstand and recover from disruptive cyber event.

Please find a suggested amendment to the Bill in the annex below.

Annex: Suggested Committee Stage Amendments

1. Scope and Governance

Part 3, Chapter 5, Clause 40

- Insert after subsection (4)(d):
    - (e) include an assessment of the uptake and effectiveness of the Cyber Governance Code of Practice among medium and large UK enterprises;

- (f) identify any sectors where uptake is significantly below expectations and set out any steps the Secretary of State proposes to take to improve uptake and effectiveness.

- Insert after subsection (4):

  - (5) Regulations may require specified classes of organisations to attest annually to compliance with the Cyber Governance Code of Practice and to publish a cyber governance statement.
  - (6) Regulations under subsection (5) may make different provision for different classes of organisations and may include enforcement provisions.
  - (7) Before making regulations under subsection (5), the Secretary of State must consult such persons as the Secretary of State considers appropriate.

2. Accountability and Competency

Part 3, Chapter 3, Clause 30

- Insert after subsection (6):

  - (7) Regulations may require regulated persons to ensure that individuals performing compliance and governance functions meet prescribed competence standards, including reference to frameworks adopted by the UK Cyber Security Council and professional pathways aligned with internationally recognised approaches.

3. **Resilience and Testing**

Part 3, Chapter 3, Clause 29

- Insert after subsection (6):

  - (7) Regulations may require regulated persons to conduct periodic resilience exercises and independent testing, proportionate to risk, including scenario-based recovery drills and rehearsals for communications and customer notifications.