Chartered IIA
Office 202
Alliance House
12 Caxton Street
London SW1H 0QS

Chartered Institute of Internal Auditors – Telecommunications Security Code Of Practice Consultation – Department for Science, Innovation and Technology – Consultation Response

Question 2.1 Do you agree with the thematic areas targeted through the proposed amendments in Section 2? If no, explain why.

The Chartered Institute of Internal Auditors (Chartered IIA) supports the proposed amendments in Section 2; however, we do not agree that the targeted thematic areas are sufficient. In particular, Chapters 9 (Governance) and 10 (Reviews) need to be updated to reflect the important role of internal audit in providing independent and objective assurance on telecoms providers' security risks.

We agree with the intention behind the amendments and the need for the code to reflect evolving security threats to telecoms providers, but this must be accompanied by strengthening oversight and governance arrangements. These proposed amendments are especially timely given the recent high-profile cyber-attacks affecting UK businesses, such as the recent incidents at Jaguar Land Rover, Co-Op and Marks & Spencer, which highlight the impact on critical operations and services. As the UK becomes increasingly reliant on telecommunications infrastructure, the risks of security breaches causing widespread disruption are on the rise.

The Chartered IIA is the professional body for internal auditors in the UK and Ireland, representing 10,000 members working across all sectors, including telecoms. Internal audit provides independent assurance to boards and senior management that governance, risk management and internal controls are working effectively to help protect organisations from threats and deliver long-term resilience.

While the proposed amendments provide important technical and operational updates, there remains a governance gap that the Telecommunications Security Code of Practice does not adequately or explicitly address. Boards must not only oversee the implementation of the measures in the code of practice, but also be able to demonstrate, through independent assurance, that these measures are effective in practice. Internal audit plays an important role here, providing boards with independent assurance and risk assessments on security risks, including cyber, data, fraud, technology, third-party suppliers and broader business resilience.

Our research into the UK broadband sector revealed that six of the thirteen major UK broadband providers do not have internal audit capabilities. This leaves boards without the independent assurance needed when managing security risk. By contrast, regulators in other critical sectors take a more robust approach to oversight and governance: Ofgem's Financial Responsibility Principle requires energy providers to explain their internal audit capability or justify its absence, while the FCA and PRA embed internal audit requirements within governance expectations for financial services through the FCA Internal Controls Handbook and PRA Rulebook. Without setting similar expectations for telecom providers, the sector risks lagging in governance measures despite its critical role in national infrastructure and the digital economy.

As the proposals are currently devised, we cannot fully agree with the thematic areas targeted in Section 2. We recommend that the code of practice be strengthened by encouraging providers to consider their internal

Chartered Institute of Internal Auditors

Chartered IIA
Office 202
Alliance House
12 Caxton Street
London SW1H 0QS

audit capability as part of their governance and assurance arrangements. This would bring telecoms into line with best practice across other regulated sectors and help ensure that boards receive the independent assurance they need to help protect themselves against increasingly sophisticated security threats.

Question 2.2 - Do you agree with the specific amendments proposed in Section 2? If no, explain why and propose alternative suggestions (if possible).

The Chartered IIA does not agree that the specific amendments in Section 2 are sufficient as drafted. While we broadly support the proposed changes and recognise that they provide helpful clarification across a number of technical areas, they do not explicitly recognise the role of internal audit in giving boards and senior management assurance that governance and review processes are functioning as intended. Without this, there is a risk that the code strengthens security requirements without ensuring that boards and senior management have the independent assurance they need over their effectiveness.

Internal audit provides independent assurance that the governance, risk management, and control processes supporting compliance with the code are being applied effectively. For example, in the current telecommunication code of practice, **9.2(d)** and **9.6**, which require security risks to be escalated to an appropriate governance level and that a person or committee at board level (or equivalent) has overall responsibility and accountability for security. Internal audit can assess whether these escalation and reporting arrangements operate effectively in practice and whether the board receives accurate and timely information to discharge its oversight responsibilities. In relation to **9.8** (learning from incidents), internal audit can review whether post-incident lessons are reviewed and solutions/changes are embedded into future processes. In **10.2** and **10.3** (annual reviews and risk assessments), internal audit can provide assurance that these risk assessments and reviews are complete, evidence-based, and take into account the entire threat landscape faced by telecom providers.

To reflect the important role internal audit can play here, we propose the following wording, which would complement the other changes in Section 2:

Chapter 9 – Governance

(An additional sentence at the end of the amended version of paragraph 9.3 – highlighted in bold below)

"Having an effective security governance framework ensures that procedures, personnel, physical and technical controls continue to work through the lifetime of a network and across the entire business. Without effective governance, it is likely that security improvements will not be sustained or consistent and are likely to leave gaps that can be exploited. Any technical controls deployed outside of an effective security governance framework will be fundamentally undermined and could constrain the business in the future. ***"The security governance framework should integrate and be consistent with internal and external audit and assurance mechanisms, including the assurance over security improvements and technical controls. "***

(A new paragraph after paragraph 9.9 – called 9.10. Chapter crossover paragraph will become 9.11):

"Telecoms providers should explain how the effectiveness of their governance framework is subject to independent assurance. Where appropriate, this may be delivered through an internal audit function. Where no internal audit capability exists, providers should explain how equivalent assurance is achieved"

Chartered Institute of Internal Auditors

Chartered IIA
Office 202
Alliance House
12 Caxton Street
London SW1H 0QS

Chapter 10 – Reviews (A new additional paragraph after 10.6 – called 10.7. Chapter crossovers paragraph will become 10.8.):

"Telecoms providers should ensure that the reviews required under Regulation 11 have independent assurance via internal audit to confirm that governance, risk management and control measures for managing security risks are operating as intended. Where no internal audit capability exists, providers should explain how equivalent assurance is achieved"

These additions and amendments would be proportionate and could be incorporated alongside the government's other updates to Section 2. Making these small refinements to the code of practice and ensuring that security measures are underpinned with strong and independent assurance will contribute to strengthening resilience and security across the telecoms sector.

The Cyber Governance Code of Practice already explicitly references the role of internal audit in providing boards with assurance over cyber security considerations. Referencing this within the Telecommunications Security Code of Practice would ensure greater consistency across government guidance — with the CAF setting the technical baseline, the Cyber Governance Code addressing board oversight, and the Telecommunications Code bridging both. This alignment would help ensure that providers not only implement measures but can also demonstrate through independent assurance that they are effective.

Question 2.3 - Do you have any more feedback on the proposed amendments to Section 2 (Question 2.1 and Question 2.2)? If yes, provide details.

The Chartered IIA welcomes the government's proposed amendments to Section 2, but we remain concerned that the governance and assurance arrangements are not adequately reflected. Strengthening operational security requirements is important, but boards must also have independent assurance that these requirements are being applied and operating effectively.

Experience from other regulated sectors illustrates the risks of neglecting this. In the energy sector, of the 30 or so suppliers that collapsed since 2021 — including Bulb, the UK's 7th largest — none had an internal audit function. The absence of independent scrutiny of significant risks — such as that offered by an internal audit function — may have undermined governance and played a role in the firm's collapse, with notable consequences for consumers.

Telecoms providers, just like energy suppliers, form part of the UK's critical national infrastructure. Failures of governance and oversight in this sector, particularly in relation to cybersecurity and other telecommunications security risks, could have equally profound implications for the economy and public trust. We therefore recommend that the final Telecommunications Security Code of Practice explicitly reference the role of internal audit in supporting board oversight of governance, resilience, and security risks. Such a reference would not be prescriptive, but it would bring telecoms into line with regulatory practice in other sectors and ensure that boards give due consideration to how they obtain independent assurance.