George Lusty
Enforcement Director

Gerry McQuaid
Telecoms and Internet Security Director

27 November 2026

Open letter to communications providers: identifying and assessing risks of security compromise

The security and resilience of the UK's public communications networks and services depend on providers[1] identifying and reducing the risks of security compromise. In the context of increasing and evolving threats[2], providers' ability to understand the threats relevant to their networks and services, assess the risks they create and take appropriate and proportionate action to reduce them is essential to maintaining secure and resilient networks and services.

The telecoms security framework

The telecoms security framework places overarching security duties on providers under sections 105A and 105C of the Communications Act 2003[3] (the "2003 Act") as amended by the Telecommunications (Security) Act 2021 (the "TSA"). Those duties are supplemented by specific security measures set out in the Electronic Communications (Security Measures) Regulations 2022[4] (the "2022 Regulations"). Together, those provisions require providers to take a risk-based approach to the security of their public electronic communications networks and services.

Specifically, regulations 3(3)(a)-(b) and 11(b) of the 2022 Regulations are important components of that framework. They require providers to identify and record the risks of security compromises and to undertake periodic risk reviews in order to produce a written assessment of the extent of the overall risk of security compromises occurring.[5]

The Telecommunications Security Code of Practice[6] (the "Code") provides technical guidance on the government's preferred approach to demonstrating compliance with the security duties.[7] We have taken that guidance into account in developing the observations set out in this letter.

---

[1] "Providers" refers to providers of a "public electronic communications network" or "public electronic communications service" as defined in section 151 of the Communications Act 2003.
[2] The NCSC Annual Review 2026 describes a "more contested, competitive and technologically accelerated cyber environment", in which Artificial Intelligence ("AI") is already beginning to reshape the cyber threat landscape (see "Understanding the threat", pages 13-29).
[3] The Communications Act 2003
[4] The Electronic Communications (Security Measures) Regulations 2022
[5] See Annex 1 for more detail on providers' legal obligations under regulations 3(3)(a)-(b) and 11(b).
[6] Telecommunications Security Code of Practice, Version 1.1, July 2026. This revision updated the previous version of the Code (Telecommunications Security Code of Practice, December 2022).
[7] In relation to the risk assessment required by regulation 11(b), the Code (Chapter 10, "Reviews", paragraph 10.4) states that providers should refer to the NCSC advice on risk management, pointing to the Cyber Assessment Framework ("CAF") guidance on Principle A.2 Risk Management (NCSC, 2025). Measure M5.01 of

Ofcom's request to see providers' risk records and assessments

In June 2026, as part of Ofcom's ongoing security and resilience supervision programme[8], we requested a sample of communications providers to provide information to support our supervision programme of monitoring compliance with regulations 3(3)(a)-(b) and 11(b).

We required providers to submit:

- the written records and assessments required by regulations 3(3)(b) and 11(b) that were produced in 2024 and 2025;
- explanations of the factors and information considered; and
- the internal processes and functions of persons involved in producing the relevant assessments.

Although the information provided showed that almost all providers had identified some risks, it did not always clearly demonstrate *how* relevant risks of security compromise had been identified and assessed, or how appropriate regard had been given to the factors set out in regulations 3(3)(a)(i)-(iv) and 11(b)(i)-(viii).

We saw evidence of improvement in some of the records and assessments produced in 2025 compared with those produced in 2024. We welcome that progress and the indication that some providers are taking steps to strengthen their approaches, but further and sustained improvement is needed across the sector.

This letter summarises our initial findings and our current view on how providers can strengthen their approaches to identifying and assessing risks of security compromise, and better demonstrate compliance with the relevant requirements of the 2022 Regulations.

Our initial findings and observations

1. Producing written records and assessments that meet the relevant legal requirements

Many providers submitted a large number and variety of documents intended to demonstrate compliance with the relevant regulations. Material relevant to the legal requirements was often spread across multiple documents, which sometimes lacked information necessary to understand their status and purpose, such as accurate dates. As a result, it was often unclear what assessments had been undertaken, when they had been carried out and what conclusions had been reached, including providers' conclusions about their assessments of the "*overall risk of security compromises*" required by regulation 11(b).

The 2022 Regulations do not prescribe any particular format or methodology that providers must follow when identifying, assessing or documenting risks of security compromise.[9] Notwithstanding

---

the Code provides that public telecoms providers shall implement appropriate business processes and have regard to implementing specific parts of the CAF contained within Annex C of the Code. The measure should be completed by 31 March 2024 (Tier 1 public telecoms providers) or by 31 March 2025 (Tier 2 public telecoms providers). Annex C includes extracts from the CAF 4.0. CAF Principle A2 concerns the identification, assessment and understanding of security risks and an organisation's overall approach to risk management. The CAF indicators of good practice are intended to inform expert judgement and are not an inflexible or exhaustive checklist.

[8] Further detail on our security and resilience supervision programme is set out in Ofcom's Plan of Work 2026/27.

[9] Providers may choose to draw upon recognised industry standards, frameworks and guidance when developing their approach to identifying, assessing and recording risks of security compromise, such as ISO/IEC 27005 or NIST SP 800-30.

that flexibility, we do not consider that an approach in which relevant risk information is spread across multiple documents, without clarity as to their status and purpose, enables providers to demonstrate clearly that they have identified and assessed the relevant risks in accordance with the regulations.

Providers should adopt an approach which is appropriate and proportionate to their networks, services and organisational arrangements. Whichever approach is adopted, the resulting records and assessments must meet the requirements of the relevant regulations and enable providers to clearly demonstrate compliance.

Producing clear and effective records and assessments

Providers may operate continuous and dynamic risk management processes, which draw on multiple sources of information and are updated in light of relevant changes.[10] However, this does not remove the requirement to produce the specific written records and assessments required by regulations 3(3)(b) and 11(b). Whatever approach is adopted, providers should ensure the material produced:

- meets the requirements of the applicable regulations;
- demonstrates that the applicable requirements have been met at least once during any 12 month period;
- sets out the conclusions reached, including the assessment of the extent of the overall risk of security compromises required by regulation 11(b); and
- communicates those conclusions in a clear and comprehensive manner which can be understood by relevant internal decision-makers and enable compliance to be demonstrated to Ofcom.[11]

In one case, a provider was unable to provide any written assessments required by regulation 11(b) for two consecutive years (2024 and 2025). We have opened an investigation into that provider.[12]

Distinguishing between the requirements of regulations 3(3)(a)-(b) and 11(b)

Some providers did not clearly distinguish between the written record required by regulation 3(3)(b) and the written assessment under regulation 11(b). These requirements serve different but related purposes. Regulation 3(3)(b) requires network providers to make a written record of the risks identified under regulation 3(3)(a). Regulation 11(b) requires network and service providers to undertake a forward-looking review in order to produce a written assessment of the extent of the overall risk of security compromises occurring within the following 12 months.

Some providers also supplied limited evidence that their assessments under regulation 11(b) had taken account of all the factors applicable to their network or service under regulations 11(b)(i)-(vii), together with any other relevant information under regulation 11(b)(viii).[13] The assessment should

---

[10] Annex C of the Code includes the following indicator of good practice, extracted from the CAF: *"Your risk assessments are dynamic and readily updated in the light of relevant changes which may include technical changes to network and information systems supporting your essential function(s), change of use, the introduction of new or emergent technologies or new threat information."*

[11] Annex C of the Code includes the following indicator of poor practice, extracted from the CAF: *"Risk assessment outputs are too complex or unwieldy to be consumed by decision-makers and are not effectively communicated in a clear and timely manner."*

[12] Enforcement Bulletin: Investigation into Daisy's compliance with duties to assess telecoms security risks

[13] The factors contained in regulations 11(b)(i) and 11(b)(iii) relate to providers of a public electronic communications network and are therefore not applicable to providers of a public electronic communications service only.

bring all the relevant matters together in reaching a conclusion about the extent of the overall risk of security compromises occurring within the following 12 months.

The factors specified in regulation 11(b) include risks identified, reviews undertaken and testing carried out under other provisions of the 2022 Regulations.[14] Those underlying requirements remain separate legal obligations, but their results must be taken into account in the regulation 11(b) assessment where applicable.

A risk register simply listing individual risks will not, without further analysis and an assessment of the overall risk, ordinarily be sufficient to demonstrate compliance with regulation 11(b). Other material, including outputs from threat-intelligence, testing or other security activities, may inform the assessment but do not, by themselves, constitute the written assessment required by regulation 11(b).

The number of risks recorded will necessarily vary according to the nature and complexity of a provider's network or service and is not, by itself, an indicator of the completeness of its assessment. However, providers should be able to demonstrate that they have considered the relevant scope of their network or service and the range of risks of security compromise to which it may be exposed.

2. Ensuring assessments are informed by relevant threats and developments

An effective assessment of security risk needs to be informed by the significant threats facing the provider and the sector, including new and emerging threats. In our review, providers' assessments under regulation 11(b) considered these threats to varying degrees, including risks associated with nation-state activity and emerging technologies.

Regulation 11(b)(vi) requires providers to take account of the results of reviews carried out in accordance with regulation 11(a), including relevant developments relating to the risks of security compromises occurring. We consider that relevant developments are likely to include, but are not limited to technological developments, changes in the national threat landscape and developments affecting supply-chain risks.

Regulation 11(b)(viii) also requires providers to take account of any other relevant information. Depending on the circumstances, this may include information derived from security incidents and "near misses". The Code explains that incidents which did not amount to security compromises may nevertheless be relevant to assessing future risks where, for example, they reveal similar root causes.[15]

Relevant threat intelligence, threat modelling, vulnerability information, testing results and incident information may all inform a provider's assessment. These sources can help providers identify and understand relevant threats, vulnerabilities and potential attack vectors.[16] However, their outputs

---

[14] Regulation 11(b) refers to risks identified under regulations 3(3)(a), 5(2), 6(1), 7(1) and 10(4), reviews carried out in accordance with regulation 11(a), and tests carried out in accordance with regulation 14.

[15] See Chapter 10 of the Code, "Reviews", which explains that "*any other relevant information*" may include event-correlation analysis of security incidents which did not amount to security compromises, but which may be relevant to assessing future risks, including where incidents show similar root causes.

[16] Measure M24.03 of the Code, which was introduced in the July 2026 version of the Code (version 1.1), states that public telecoms providers should conduct threat modelling to inform their risk assessments, including by identifying relevant threats, vulnerabilities and potential attack vectors. The implementation timeframe for this measure is 31 December 2029. The Code states this does not preclude public telecoms providers from implementing the measure before this date where it is prudent to do so, and this should be actively encouraged where possible (see page 119 of the Code).

do not, by themselves, constitute the written assessment required by regulation 11(b). Providers should undertake the further analysis required by that regulation and reach a conclusion about the extent of the overall risk.

Providers' written assessments should therefore record how relevant information about existing and emerging threats has informed their conclusions about the overall risk of security compromise.

3. Acting on risk assessments to reduce risks

Identifying and assessing risks are not the end point. Within the wider telecoms security framework, the conclusions reached through those processes should inform decisions and action to reduce risks of security compromise.[17]

Our information-gathering focused on the identification, assessment and recording of security risks and did not seek comprehensive evidence about how providers subsequently managed the risks identified. Nevertheless, within the wider telecoms security framework, identified risks and the conclusions reached through assessment processes should be appropriately communicated and inform decision-making and action.

The 2022 Regulations contain specific governance requirements relevant to this process. In particular, regulation 10(2)(d) requires providers to ensure that their security policy *"provides channels through which risks identified by persons involved at any level in the provision of the network or service are reported to persons at an appropriate governance level"*. The Code explains that this requirement *"aims to ensure (among other things) that public telecoms providers' policies include a way to communicate security issues and risks to the top of the organisation, without risk of dilution."*[18]

Providers should therefore ensure that identified risks are reported to the appropriate governance level in accordance with regulation 10(2)(d), and that the conclusions reached through their assessment processes inform appropriate decisions and action in response to those risks.

Actions for providers

We encourage providers to review their arrangements in light of the above and take action where necessary to ensure compliance with the relevant legal requirements. In particular, providers should:

1. review whether their processes, written records and assessments meet the distinct requirements of regulations 3(3)(a)-(b) and 11(b);
2. consider whether their processes for identifying and assessing risks cover the relevant scope of their network or service and the range of risks of security compromises to which it may be exposed;
3. review whether their assessments under regulation 11(b) take account of relevant threats, developments and other information required by that regulation; and
4. ensure that identified risks are reported to the appropriate governance level in accordance with regulation 10(2)(d), and that assessment conclusions inform appropriate decisions and action.

Providers should also consider the relevant provisions of the Code when reviewing their arrangements. The Code states that providers should refer to NCSC advice on risk management

[17] Section 105A(1)(b) of the 2003 Act places an overarching duty on providers to reduce the risks of security compromises occurring.

[18] Chapter 9 of the Code, "Governance", at paragraph 9.6.

when carrying out the review for the purposes of regulation 11. Measures M5.01 and M22.01[19] of the Code state that providers should have regard to implementing specific parts of the CAF, including "A2.a Risk Management Process" and "A2.b Understanding Threat" respectively. Providers should refer to "A2.b Understanding Threat" for guidance on ways to understand the threat assumptions that inform their risk assessments.

Relevant resources to inform providers' risk assessments include:

- Telecommunications Security Code of Practice, in particular:
  - Chapter 9 – Governance
  - Chapter 10 – Reviews
  - Annex C – Extracts from the Cyber Assessment Framework: Principal A2.a Risk Management Process; Principal A2.b Understanding Threat
- NCSC Risk Management Guidance

Next steps and enforcement action

As noted above, we have opened an investigation into one provider.[20]

We are also writing separately to providers included in this programme where we have identified specific concerns about their records and assessments. We will engage further with those providers where additional information or follow-up action is required.

We will continue to monitor compliance with the relevant security duties and requirements through our supervision programme.

Where we identify concerns that providers may be failing to comply with their security duties, we will take appropriate action, which may include opening an investigation.

Where we conclude (after completion of an investigation) that the relevant statutory requirements have not been met, Ofcom has powers to impose financial penalties of up to 10% of a provider's relevant turnover.[21]

Finally, we would like to thank the providers that responded to our request for their cooperation.

Yours faithfully

George Lusty

Gerry McQuaid

[19] Measure M22.01 of the Code, which was introduced in the July 2026 version of the Code (version 1.1), states that public telecoms providers shall have regard to implementing parts of the CAF contained within Annex C including, among others, "A2b-Understanding Threat". The implementation timeframe for this measure is 31 March 2028. The Code states this does not preclude public telecoms providers from implementing the measure before this date where it is prudent to do so, and this should be actively encouraged where possible (see page 116 of the Code).

[20] Enforcement Bulletin: Investigation into Daisy's compliance with duties to assess telecoms security risks

[21] Further information about how Ofcom exercises its enforcement powers in relation to security duties is set out in our Regulatory Enforcement Guidelines for investigations and our General statement of policy under section 105Y of the Communications Act 2003.

Annex 1: Regulations 3(3)(a)-(b) and 11(b)

Regulation 3(3)(a)-(b)

In summary, regulation 3(1) imposes a duty on network providers to take such measures as are appropriate and proportionate to ensure that the network architecture (including its design or redesign, construction, development and maintenance) reduces the risk of security compromises occurring.

Regulation 3(3)(a) states that the duty for network providers set out in regulation 3(1) includes in particular a duty to *"identify and reduce the risks of security compromises to which the network as a whole and each particular function, or type of function, of the network may be exposed having appropriate regard to the following—*

(i) whether the function contains sensitive data,
(ii) whether the function is a security critical function,
(iii) the location of the equipment performing the function or storing data related to the function, and
(iv) the exposure of the function to incoming signals".

Regulation 3(3)(b) requires network providers *"to make a written record, at least once in any period of 12 months, of the risks identified under paragraph (a)".*

Regulation 11(b)

Regulation 11(b) states that network and service providers must *"undertake at least once in any period of 12 months a review of the risks of security compromises occurring in relation to the network or service in order to produce a written assessment of the extent of the overall risk of security compromises occurring within the next 12 months,"* taking into account the factors listed in regulation 11(b)(i)-(vii) and any other relevant information (regulation 11(b)(viii)).