Ofcom guidance on resilience requirements imposed by or under sections 105A to D of the Communications Act 2003

2022 version

GUIDANCE:

Publication date: 12 December 2022

Contents

Section

Annex

1. Overview

The legislation that applies to telecoms providers requires them to take measures to ensure the security and resilience of their networks and services. We last updated Ofcom guidance telling the relevant providers what we expect them to do to meet their obligations in June 2017 (the "**2017 Guidance**").

Further to the introduction of the Telecommunications (Security) Act 2021 (the "**Security Act**"), we have updated this guidance so that it only applies to the sub-category of security compromises relating to the resilience of networks and services, in terms of availability, performance or functionality.

We have also taken the opportunity to update the guidance to take account of the revised framework, as well as to reflect the changing nature of resilience risks and Ofcom's experience of incident reporting and investigation.

2. Introduction

2.1 This document provides high level guidance to providers of public electronic communications networks or services ("**providers**") on their resilience obligations imposed on them by or under sections 105A to 105D of the 2003 Act, as amended by the Security Act, in the exercise of Ofcom's powers under sections 1(3) and 105Y. It sits within the broader security and resilience framework which was updated by the Security Act. In particular, the revised overarching duties under sections 105A and 105C of the Communications Act 2003 (the "**2003 Act**") (as amended by the Security Act) are complemented by the Electronic Communications (Security Measures) Regulations 2022 (the "**Regulations**") and the Telecommunications Security Code of Practice (the "**Code**")[1] [2].

2.2 The Security Act introduces the definition of a "security compromise". The guidance set out in this document applies to the sub-category of security compromises relating to the resilience of networks and services, in terms of availability, performance or functionality (referred to hereafter as "Resilience Incidents").

2.3 Resilience-related duties under the revised security framework are particularly important because of the increasing extent to which we all depend on communications infrastructure. A major failure within a public electronic communications network has the potential not only to impact large numbers of consumers, but also to have a wider impact on the UK economy. At the same time, the inherently interconnected and global nature of communications services presents challenging vulnerabilities which we must ensure are suitably dealt with.

2.4 Given that the concept of a security compromise in the 2003 Act includes Resilience Incidents, the security duties in that context effectively require that:

- providers must take appropriate and proportionate measures to identify and reduce the risks of Resilience Incidents occurring, and prepare for the occurrence of Resilience Incidents;
- if a Resilience Incident occurs, providers must take appropriate and proportionate measures for the purpose of preventing adverse effects on the network or service arising from the Resilience Incident;
- the provider of the network or service must take such measures as are appropriate and proportionate for the purpose of remedying or mitigating adverse effects resulting from Resilience Incidents;
- network and service providers must report Resilience Incidents to Ofcom, including anything that compromises the availability, performance or functionality, which have a significant impact on the network or service;

[1] The Electronic Communications (Security Measures) Regulations 2022 and Telecommunications Security Code Of Practice.
[2] Ofcom has also issued its general statement of policy under section 105Y of the 2003 Act, providing procedural guidance on the exercise of Ofcom's functions to ensure compliance with the security duties (the "**Ofcom procedural guidance**"), which should be read alongside this document.

- Ofcom may require a network or service provider to submit to, and pay for, an assessment of the measures they are taking to comply with their security duties under the framework, including in respect of resilience;
- Ofcom can use the information gathering, compliance assessment and enforcement provisions in the 2003 Act to assess, investigate, rectify, and penalise any infringement of their security duties, including in respect of resilience.

2.5 In the first instance, it is for providers themselves to determine how their statutory obligations affect their activities and take any necessary measures in order to comply with them. In this context, Ofcom considers in principle that it is important that providers have clear lines of accountability, up to and including Board level, and sufficient technical capability to ensure that potential risks are identified.

2.6 The resilience of Critical National Infrastructure such as the telecommunications sector is currently under scrutiny as part of the UK Government's National Resilience Strategy Review and the Government is also considering the recommendations on resilience made by the National Infrastructure Commission. This may lead to amended approaches to securing the appropriate level of resilience in the sector and we are already in discussion with Government on the options that may be considered. As and when decisions on the way forward are made, Ofcom would expect to review this guidance and update or revoke and replace as appropriate.

Role and status

2.7 Guidance has the benefit of contributing to effective regulation by improving transparency and understanding. In particular, this guidance is aimed at encouraging compliance by explaining the resilience (statutory) obligations imposed on relevant providers, thereby ensuring that they properly understand their obligations and enabling potential customers to identify any concerns.

2.8 One of Ofcom's regulatory principles is that Ofcom will regulate in a transparent manner. Guidance can serve as a useful means to achieving this principle and to increasing understanding of Ofcom's policy objectives and approach to regulation.

2.9 Ofcom would normally expect to follow this guidance should it investigate any potential contravention of an obligation discussed in this guidance. If Ofcom decides to depart from this guidance, it will set out its reasons for doing so. As mentioned below, this guidance may also be subject to revision from time to time.

2.10 That said, whether or not (and, if so, how) a particular matter is regulated will usually turn on the specific facts in each case. Providers should seek their own independent advice on specific matters, taking into account the facts in question to answer specific questions on their statutory obligations. Ofcom cannot, as a matter of law, fetter its discretion as to any future decision. Accordingly, although this guidance sets out the approach Ofcom would normally expect to take, this guidance does not have binding legal effect, and each case will be considered on its own merits.

2.11 This document, in conjunction with the Code and the Ofcom procedural guidance, replaces our 2017 Guidance. It should be read alongside these documents. We expect to make further revisions from time to time. These may be to reflect changing threats and vulnerabilities, additional experience from implementing the requirements, for example to incorporate feedback from stakeholders, or to reflect the introduction of further codes of practice under s105E by the Government. We may also update the guidance as necessary in response to any relevant changes in the external sources of guidance referred to in this document.

2.12 We note that the overarching duties in sections 105A and 105C apply to providers of all sizes. However, the measures that would be appropriate for a large provider to take to protect resilience may be different to those appropriate for a smaller company. It is for providers in the first instance to assess for themselves (taking this guidance into account) the measures which are appropriate and proportionate in their own particular cases. This guidance is intended to be relevant to providers of all sizes.

3. Legislative framework

The overarching duties set out in the 2003 Act

3.1 The Security Act amends the 2003 Act, removing existing sections 105A-D and replacing them with strengthened security duties. Section 105A(1) sets out the following overarching duty:

> "The provider of a public electronic communications network or a public electronic communications service must take such measures as are appropriate and proportionate for the purposes of—
>
> (a) identifying the risks of security compromises occurring;
>
> (b) reducing the risks of security compromises occurring; and
>
> (c) preparing for the occurrence of security compromises."

3.2 Further overarching duties are set out in section 105C, which requires providers to take such measures as are appropriate and proportionate to prevent adverse effects arising from a security compromise that has occurred. Where the security compromise has an adverse effect on the network or service, the provider must take such measures as are appropriate and proportionate to remedy or mitigate that effect.

Duties to take specified measures imposed by the Secretary of State by regulations

3.3 The Secretary of State has powers to make regulations under sections 105B and 105D of the 2003 Act which require providers to take certain security measures to meet their security duties set out in sections 105A and 105C of the 2003 Act. In exercise of these powers, the Secretary of State made the Regulations, which came into force on 1 October 2022.

Guidance given by the Secretary of State in codes of practice

3.4 The Secretary of State also has powers to issue codes of practice under section 105E of the 2003 Act giving guidance to providers on the measures to be taken under sections 105A to 105D of the Act. In exercise of these powers, on 1 December 2022 the Secretary of State issued the Code, setting out guidance for providers with relevant turnover in the relevant period of more than or equal to £50m.

Meaning of "security compromise"

3.5 The term "security compromise" is broadly defined in section 105A(2). While it covers aspects such as confidentiality and integrity which are often associated with cyber and

physical security threats, the definition also covers the 'availability, performance or functionality' of networks and services. These aspects are more often associated with threats to availability, reliability and accompanying protective measures to improve network and service resilience such as redundancy and capacity planning, hardware and software maintenance, hardening and change management etc.

General Conditions of Entitlement

3.6 Alongside the revised security framework introduced by the Security Act, providers are separately required to comply with the General Conditions of Entitlement, and in particular General Condition A3 which aims to ensure the fullest possible availability of public electronic communications services at all times, including in the event of a disaster or catastrophic network failure, and uninterrupted access to emergency organisations[3]. Given the degree of overlap between this General Condition and the security duties under the revised security framework, some of the guidance provided in this document is also relevant to General Condition A3. Where this is the case, we have explicitly referred to General Condition A3 in this document.

Ofcom's guidance

3.7 As noted above, we published the previous version of our guidance on the security requirements in sections 105A to 105D of the 2003 Act (before the changes introduced by the Security Act) in June 2017. We have updated this guidance to take account of the revised legislative framework, in particular recognising that much of the 2017 guidance has been superseded by the Code. In effect, this means that we have retained the 2017 guidance only insofar as it relates to Resilience Incidents. We have also updated this guidance to reflect the changing nature of resilience risks and Ofcom's experience of incident reporting and investigation.

Scope

3.8 This guidance applies to all providers of Public Electronic Communications Networks (PECN)[4] and Public Electronic Communications Services (PECS)[5].

3.9 We note that the majority of the provisions in the Regulations, and the associated measures in the Code of Practice, address risks that would generally be considered to fall into the category of "cybersecurity". There is less coverage of availability risks and resilience measures, although these remain within the scope of the overarching security

[3] See also Ofcom's 2018 guidance on Protecting access to emergency organisations when there is a power cut at the customer's premises – Guidance on General Condition A3.2(b).
[4] Section 151(1) of the 2003 Act defines "public electronic communications network" as meaning an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to members of the public.
[5] Section 151(1) of the 2003 Act defines "public electronic communications service" as meaning any electronic communications service that is provided so as to be available for use by members of the public.

duties in the Act as well as some of the duties set out in the Regulations and associated measures in the Code. This document provides guidance in relation to the sub-category of Resilience Incidents (as explained above, we use this term throughout this document to refer to security compromises relating to the resilience of networks and services, in terms of availability, performance or functionality). The Secretary of State may choose to issue additional Regulations and codes of practice addressing these aspects in the future.

3.10 For further details on the revised legislative framework, please refer to Section 2 ("Introduction") of the Ofcom procedural guidance. We also set out some of the most relevant aspects of the Regulations for resilience in Section 3 (Our approach to resilience). Links to the 2003 Act, the Regulations, the Code and relevant Ofcom guidance on telecoms resilience are also provided at Annex 2.

4. Our approach to resilience

Summary of overall approach

4.1 This section describes how we will use our powers and sets out the sources of guidance which we will consider when carrying out our functions in relation to resilience.

How we will use our powers

Ofcom's general policy on ensuring compliance with resilience-related security duties

4.2 Ofcom's general policy on ensuring compliance with providers' resilience-related security duties is set out in the Ofcom procedural guidance. In particular, the Ofcom procedural guidance explains how we will use our powers under the revised security framework, both in the context of compliance monitoring and enforcement. These include:

4.3 Our information gathering powers under section 135 of the 2003 Act – see sub-section titled "Information-gathering powers (section 135)" in section 3 of the Ofcom procedural guidance;

4.4 Our power to direct providers to explain any failure to act in according with a code of practice under section 105I of the 2003 Act – see sub-section titled "Power to direct providers to explain any failure to act in accordance with a code of practice (section 105I)" in section 3 of the Ofcom procedural guidance;

4.5 Our assessment powers under sections 105N and 105O of the 2003 Act – see subsection titled "Powers to assess compliance – Assessments and assessment notices (sections 105N-105Q)" and sub-section titled "Powers to assess compliance – Power to enter premises (section 105O and 105R)" in section 3 of the Ofcom procedural guidance; and

4.6 Our enforcement powers under sections 105S to 105V of the 2003 Act – see section 6 of the Ofcom procedural guidance.

Ofcom's Enforcement guidelines for regulatory investigations

4.7 In addition to the Ofcom procedural guidance, Ofcom publishes Enforcement guidelines for regulatory investigations[6], which set out how we investigate compliance with, and approach enforcement of, regulatory requirements across a range of areas, including security duties in a resilience context.

4.8 Where incidents are not resolved to our satisfaction through engagement with providers, we may consider the use of enforcement powers. When assessing whether to open a

[6] As per paragraph 1.10 of the Enforcement Guidelines, in light of the new powers introduced under the Telecommunications (Security) Act 2021, the Enforcement Guidelines are subject to review. Ofcom has consulted on an updated draft and has published revised guidelines on Ofcom website.

formal enforcement investigation, we will consider the specific circumstances of the case to decide on the appropriate course of action.

Relevant sources of resilience guidance

4.9 In addition to the guidance set out in this document, Ofcom will consider the sources of guidance set out below where appropriate.

Guidance under the revised security framework

4.10 As set out in the Legislative framework section above, the security duties set out in the 2003 Act are complemented by further legally binding measures specified in the Regulations. The Secretary of State has also issued the Code, which gives guidance as to some of the measures to be taken by providers to meet the security duties imposed by or under sections 105A to 105D.

4.11 While as noted above, the majority of the provisions in the Regulations, and the associated measures in the Code, address risks that would generally be considered to fall into the category of "cybersecurity", some of the provisions and measures are also relevant to ensuring the resilience of networks and services, in particular, Regulations 3, 6, 7, 9, 10, 11, 12, 13, 14 and 15.

4.12 The Code provides further guidance on the Regulations. In particular, Section 2 of the Code explains the key concepts that need to be understood by providers when applying the specific security measures contained within the Regulations and when applying the technical guidance measures within Section 3 of the Code.

Guidance on General Condition A3

4.13 As noted in the Legislative framework section above, alongside the revised security framework introduced by the Security Act, providers are separately required to comply with the General Conditions of Entitlement, and in particular General Condition A3 which aims to ensure the fullest possible availability of public electronic communications services at all times, including in the event of a disaster or catastrophic network failure, and uninterrupted access to emergency organisations.

4.14 In situations involving access to emergency services, where relevant, Ofcom will also take account of its guidance in relation to General Condition A3.2(b) regarding protecting access to emergency organisations when there is a power cut at the customer's premises.

Additional sources of resilience guidance

4.15 When considering compliance with the duties imposed by or under sections 105A to 105D in relation to a particular resilience matter, we will seek evidence that a provider has taken account of industry standard resilience best practices in their approach to the development and maintenance of their network and services.

4.16 The list below summarises the main sources of further advice and best practice we refer to in this guidance, and which we will expect providers to consider where relevant to their operations. While the advice set out in such publications is relevant to resilience more generally, these documents do not themselves form part of the guidance provided by this document.

ENISA's Technical Guidance on Security Measures

4.17 In relation to appropriate risk assessment, ongoing risk management, operations and business continuity management; we consider that ENISA's Technical Guideline on Security Measures sets out good practice which should be considered by providers, in addition to taking account of the risk assessment and management measures set out in the Regulations and associated Code guidance.

ENISA's Enabling and Managing End-to-End Resilience

4.18 In relation to industry standard resilience best practice, providers should take note of the ENISA report, Enabling and Managing End-to-End Resilience. Although published in 2011, we consider the advice provides a broad and comprehensive introduction to both technical and organisational requirements for developing and maintaining resilient networks and services.

The EC-RRG Guidelines

4.19 We would encourage providers to review the current issue of the EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure, published in 2021, as these guidelines include further technology updates to the above ENISA guidance for areas such as All IP Networking, Virtualisation and 5G.

NICC's Guidelines on the minimum security and overload controls for interconnecting providers

4.20 In relation to the protection of network interconnections, providers should take note of the NICC ND1643 Guidelines on the minimum security controls for interconnecting communications providers as developed by UK industry and published by the NICC specifically for this purpose. This is in addition to complying with the assistance measures set out in Regulation 15 of the Regulations and considering the associated Code guidance.

4.21 At the time of publication of this document, NICC is updating its guidance related to SIP Overload Controls for network interconnections in a new document, ND1657[7].

[7] See para 5.27

5. Ofcom's resilience guidance

5.1 In this section we make some general observations and cover some specific incident scenarios which will inform our approach to resilience.

General observations

5.2 The general observations below will inform our approach to resilience and are therefore provided as guidance to assist providers to comply with resilience-related security duties.

Accountability and expertise

5.3 As noted above, and to be compliant with the duties imposed by or under sections 105A to 105D (including those set out in accompanying Regulations) related to network and service availability, performance and functionality, it is important that providers have clear lines of accountability, up to and including Board or company director level, and sufficient technical capability to ensure that potential risks are identified and appropriately managed.

5.4 In order to assess this, we suggest that providers consider the following questions:

- Who at Board level is responsible for resilience matters?
- Who is responsible for advising the Board about resilience matters?
- Who is the most senior member of technical staff responsible for pro-actively managing resilience matters?

5.5 Regulation 10 of the Regulations sets out specified measures to be taken in relation to governance which are relevant to the question of accountability. Providers should refer to Regulation 10 and associated Code guidance for further details.

5.6 In the event that we assess compliance with, or investigate a potential breach of, resilience-related security duties, we will usually seek evidence of the relevant risk management processes and decisions that were used. We will expect to find evidence that relevant resilience risks are regularly considered and have appropriate owners at all levels. We may request specific evidence, such as copies of risk assessments and resilience plans, and their approvals, up to and including Board level.

5.7 To be compliant with the duties imposed by or under sections 105A to 105D (including those set out in accompanying Regulations), we also consider that providers must maintain a level of internal resilience expertise, capacity, and appropriate accountability mechanisms, sufficient to provide proper management of their resilience risks. Regulation 13 of the Regulations sets out specified measures to be taken in relation to the competency of persons given responsibility for the taking of measures on behalf of the provider. Providers should refer to Regulation 13 and associated Code guidance for further details.

5.8 This is particularly important in circumstances where a provider has outsourced aspects of its network operations to a third party. Responsibility to comply with its security duties, including those related to resilience, remains with the provider, and it needs to have sufficient internal capability to do this. Regulation 7 of the Regulations sets out specified measures to be taken in relation to supply chain arrangements. Providers should refer to Regulation 7 and associated Code guidance for further details.

Management of general resilience risks

5.9 We expect that providers will take a risk-based approach to managing the resilience of their networks and services. This means that providers need to consider what resilience risks they face, and how best to manage them, given their own particular circumstances. At an early stage in any compliance assessment or investigation, we are likely to seek evidence that an appropriate assessment of any significant risks to resilience has been undertaken. Appropriate risk management would typically consist of both the initial risk assessment and mitigation, along with an ongoing risk management process.

5.10 A risk assessment is only likely to be effective in driving performance if providers have clear lines of accountability, up to and including Board level, and sufficient technical capability to ensure that potential risks are identified and properly understood. We also consider that providers' approach to resilience risk management should in particular protect end users. We consider that this can largely be achieved, provided that end user risk is taken into account during risk assessment, and that end users have appropriate information (see further about end user information below).

5.11 A number of measures set out in the Regulations are relevant to the assessment and management of resilience risks. These include, in particular, Regulations 3, 7, 9, 10, 11, 12 and 14. Providers should refer to the Regulations and associated Code guidance for further details.

5.12 Alongside risk assessment, there are many other issues to consider when ensuring appropriate management of risks. Ofcom's view of relevant issues will also be informed by ENISA's Technical Guideline on Security Measures. It is recommended that providers familiarise themselves with its contents, as we consider it covers domains relevant for ensuring compliance with the duties imposed by or under sections 105A to 105D of the 2003 Act.

5.13 We expect that providers will keep abreast of the range of resilience related guidance, best practice and standards that are relevant to their networks and services. This will be an ongoing exercise due to the dynamic nature of many availability threats. Of particular relevance would be resilience advice from industry bodies such as NICC and EC-RRG, ENISA, and vendors of equipment and software.

Supply chain and outsourcing

5.14 A provider will generally deal with supply chain risks by extending its resilience controls to the third parties it works with. However, some arrangements may present resilience risks

which need additional mitigations. In particular, the outsourcing of network or service design, build, operation or maintenance has the potential to introduce new resilience risks.

5.15 Providers should undertake and act upon an appropriate resilience risk assessment for any significant arrangements of this type. Suitable processes should be in place for the ongoing management of identified risks.

5.16 Regulation 7 of the Regulations sets out specified measures to be taken in relation to supply chain arrangements. Providers should refer to Regulation 7 and associated Code guidance for further details.

5.17 We strongly encourage providers to discuss with us at an early stage any planned new arrangements that may have significant resilience implications. This early engagement with Ofcom might minimise the risk of any future compliance concerns, and the associated risk that additional costs will need to be incurred as a result of mitigations having to be put in place after the event.

5.18 We provide further guidance on the use of third parties in the "Resilience guidance in relation to specific scenarios" sub-section below.

5.19 We note that beyond the duties imposed by or under sections 105A to 105D, changes to supply chain arrangements might also have implications under other relevant legislation, such as the Investigatory Powers Act 2016. Providers should also discuss such changes with the relevant agencies and do so well in advance of finalising them.

Network monitoring

5.20 Providers need to have sufficient oversight of their networks and services to quickly identify significant network and service availability, performance and functionality incidents. This oversight may involve the monitoring of internal signals such as from equipment fault alarms and network and service key performance indicators (KPIs), and also external signals such as customer complaints.

5.21 Regulation 6 of the Regulations sets out specified measures to be taken in relation to monitoring and analysis of the security critical functions of a provider's public network or service. Providers should refer to Regulation 6 and associated Code guidance for further details.

Protecting end users – risk assessment and provision of information

5.22 Section 105C(2) requires providers to take such measures as are appropriate and proportionate "for the purpose of preventing adverse effects (on the network or service or otherwise)" arising from a security compromise that has occurred. We therefore expect that resilience risk assessments should consider the risk to end users, not just the provider's own business risks. As noted above, a number of measures set out in the Regulations are relevant to the assessment and management of resilience risks. These include, in particular, Regulations 3, 7, 9, 10, 11, 12 and 14. Providers should refer to the Regulations and associated Code guidance for further details.

5.23 The risk appetite of end users will vary, so we expect providers to provide information about the resilience of their services to allow customers to make informed purchasing choices. Providers should attempt to match the delivered network and service availability and performance levels to the customer expectations that have been set. More broadly, providers have a duty to inform users about certain risks of security compromise (section 105J). Providers should refer to Section 5 (Reporting security compromises) of the Ofcom procedural guidance for further details.

Protecting network interconnections

5.24 The security duties under the 2003 Act also apply in relation to security compromises that affect other networks or services (referred to as a "connected security compromise")[8]. This is relevant in the context of protecting network interconnections.

5.25 Regulation 15 of the Regulations sets out specified measures to be taken in relation to providers providing information and assistance to each other in the event that a security compromise may cause a connected security compromise. Providers should refer to Regulation 15 and associated Code guidance for further details.

5.26 We will continue to use ND1643 as a reference point when determining if a provider has taken appropriate measures in relation to connected security compromises concerning resilience.

5.27 At the time of publication of this document, NICC is updating its guidance related to SIP Overload Controls for network interconnections. It is likely that Ofcom will use the future NICC ND1657 guidance on SIP Overload Control as a reference when determining if a provider has taken appropriate measures for the purposes of identifying, reducing and preparing for risks, and where a Resilience Incident has occurred, of preventing, remedying or mitigating adverse effects arising from it.

Relevant considerations in the event of a Resilience Incident

Adverse effects

5.28 Under section 105C, providers must take such measures as are appropriate and proportionate for the purpose of preventing adverse effects arising from Resilience Incidents. If a Resilience Incident has an adverse effect on the network or service, the provider must take such measures as are appropriate and proportionate for the purpose of remedying or mitigating that adverse effect.

5.29 A Resilience Incident occurs as the result of the loss of availability, performance or functionality of a network or service. Such a loss of availability, performance or functionality would be expected to lead to an effect on the network or service which is

[8] The definition of "security compromise" under section 105A(2) includes "anything that occurs in connection with the network or service and causes a connected security compromise" (section 105A(2)(g)). The term "connected security compromise" means, in relation to a public electronic communications network or service, a security compromise that occurs in relation to another public electronic communications network or service (section 105A(5)).

adverse. Therefore, Ofcom will typically consider that where there is a Resilience Incident, there will be an adverse effect for the purpose of section 105C.

5.30 In general, when considering the appropriateness and proportionality of measures to take under section 105C for the purposes of preventing, remedying or mitigating adverse effects arising from a Resilience Incident, providers should take due account of the needs of their customers.

Public access to emergency services

5.31 For networks offering public access to the emergency services, GC A3[9] imposes specific and strict requirements for maintaining availability, performance and functionality.

5.32 Where a provider has concluded any change management activity with potential to affect access to the emergency services, we expect that provider to conduct an actual test call to an Emergency Services Access call handling centre for all affected routes. Where a single test call is carried out on a call handling centre's live platform, it should include an in-call announcement making clear to the call handling agent that the call is a test call. Where multiple test calls are required to a call handling centre's live platform, a provider should contact the call handling centre to schedule the test calls in advance in order to preserve capacity for emergency services access. The provider should maintain a record of any change management activity that has the potential to affect access to the emergency services, including the results of all test calls.

5.33 We note that BT, the current provider of Emergency Services Access call handling centres, has developed a set of test call handling procedures. We expect to publish an outline of these procedures on Ofcom's website in the future.

5.34 More generally, providers should ensure that they comply with Regulation 9 and Regulation 10(2)(a), and take due account of associated guidance in the Code.

Resilience Incident reporting and Ofcom assessments

5.35 As covered in the Ofcom procedural guidance, the occurrence of a Resilience Incident that has had a significant effect on the operation of a network or service will need to be reported to us by the affected provider as a security compromise under section 105K. Please refer to Section 5 (Reporting security compromises) of the Ofcom procedural guidance for further details.

5.36 In our analysis of any Resilience Incident reported to us, we will seek evidence to understand:

- if the provider has taken appropriate and proportionate measures to identify, reduce and prepare for the risk associated with the cause of the Resilience Incident, and

[9] See Ofcom's General Conditions of Entitlement.

- if the provider has taken appropriate and proportionate measures to prevent, remedy or mitigate any adverse effects in response to the occurrence of the Resilience Incident.

Resilience guidance in relation to some specific scenarios

5.37 The following is a non-exhaustive list of Resilience Incident causes that we have previously encountered, and is included here to provide some examples of the evidence we may seek to obtain in any future Resilience Incident analysis or assessment:

- Malicious acts (including theft)
- Single points of failure
- Physical damage (including fire, flood, severe weather or other natural phenomena)
- Loss of power
- Hardware failure
- Software failure
- Human error
- Policy or procedure error
- Overload
- Third-party action

Single points of failure

5.38 By single point of failure, we mean the configuration of a network or service resulting in significant amounts of traffic passing over a single route, a single point of handover, and/or the routing of traffic through a single site (such as a building), thereby leaving the service vulnerable in the event of a failure adversely affecting that part of the network.

5.39 We consider that avoiding single points of failure, where it is proportionate to do so, is an "appropriate" measure to take within the meaning of sections 105A and 105C. We consider that the extent to which avoiding single points of failure is proportionate is likely to vary at different points in the network. Factors that will be relevant to the assessment include:

- the volume of traffic conveyed over the single point of failure;
- whether the traffic being conveyed comprises or includes emergency calls;
- the number of customers relying on the single point of failure; for example:
  - it is less likely to be proportionate to deploy protection paths in the access network
  - for a provider's backhaul, core, and interconnect/peering network domains, in most cases, providers will be expected to have protection paths and resilient network functions with fully automatic failover such that all services and internet destinations continue to have reasonable and appropriate service levels
- geographic and physical constraints which limit the provider's scope to avoid single points of failure or make it disproportionately expensive.

5.40 In some cases, a loss of service to a significant geographical area, potentially isolating whole communities, can occur as a result of damage to transmission route optical fibres at a single location, or disruption to a single building (for example as a result of flooding).

5.41 When conducting an assessment of the measures taken by a provider, we expect to seek evidence that the provider has assessed the single points of failure risks involved in their network design choices.

5.42 In this context, our assessment would include considering compliance with the Regulations and take account of associated Code guidance, and is likely to have particular regard to Regulations 3, 9 and 11.

Physical damage (fire, flood and severe weather)

5.43 Flooding is an increasingly important risk that providers need to manage appropriately as part of their compliance with the duties imposed on them by or under sections 105A to 105D. We note that, even where sites are identified as being at a lower risk of flooding, providers should still consider whether additional measures are required for other reasons, for example because they represent a potential single point of failure for a significant number of customers.

5.44 When conducting an assessment of the measures taken by a provider, we expect to closely examine the provider's assessment of the physical damage risks involved in their network design choices.

5.45 In this context, our assessment would include considering compliance with the Regulations and take account of associated Code guidance, and is likely to have particular regard to Regulations 3, 9 and 11.

Loss of power

5.46 Even for Resilience Incidents linked to severe weather or flooding, it is often the associated loss of power that is the actual cause of the communications outages. We expect providers will manage the risk of power loss appropriately as part of the measures they take to comply with their security duties imposed by or under sections 105A to 105D.

5.47 When conducting an assessment of the measures taken by a provider, we expect to closely examine the provider's assessment of the loss of power risks involved in their network design choices, as well as measures relating to the identification and reduction of these risks.

5.48 In this context, our assessment would include considering compliance with the Regulations and take account of associated Code guidance, and is likely to have particular regard to Regulations 3, 9 and 11.

Network upgrade and transformation activities

5.49 Service affecting Resilience Incidents caused by failures in change management, asset management, general planning and testing policy or procedures tend to occur as providers

engage in network upgrade or transformation activities. In some examples, these events have not only caused extensive loss of service hours but have also been repeated within a change programme as it has progressed. Other examples have introduced single points of failure in the ability for consumers to access emergency services through implementation of a change followed by lack of adequate testing.

5.50 When conducting an assessment of the measures taken by a provider, we expect to closely examine and seek evidence to understand if failures in Risk, Change, Performance, Capacity or Fault Management have contributed to the loss or degradation in availability, performance or functionality of a network or service.

5.51 In this context, our assessment would include considering compliance with the Regulations and take account of associated Code guidance, and is likely to have particular regard to Regulations 9, 10, 13 and 14.

Third parties

5.52 Many providers now make extensive use of third parties to provide infrastructure for, and to design and operate, their networks. It is therefore conceivable that a provider may have less visibility or control over the level of resilience that is put in place, than it would if it kept these activities in-house.

5.53 We do not consider that outsourcing to third parties in this way excuses providers from their security duties under the 2003 Act, including those relating to network and service availability, performance, and functionality. Put simply, a provider cannot contract out of its statutory obligations. As such, a provider should have sufficient levels of effective control over third parties in place to ensure they continue to comply with their obligations. We also expect providers to continuously and rigorously check that actions undertaken on their behalf do not put them in breach of their obligations. This includes providers being in a position to demonstrate to Ofcom that they have proactively engaged with suppliers and sought specific and appropriate assurances in relation to identifying, reducing and preparing for risks of Resilience Incidents. When conducting an assessment of the measures taken by a provider, we expect to closely examine any contractual arrangements between the provider and relevant third parties, as well as any resilience risk assessment carried out by the provider and any processes in place for the ongoing management of identified risks.

5.54 In this context, our assessment would include considering compliance with the Regulations and take account of associated Code guidance, and is likely to have particular regard to Regulation 7.

A1. Glossary

EC-RRG – The Electronic Communications Resilience and Response Group. This group, formed of the major network operators, the UK and devolved Governments, and Ofcom, is a focal point for cooperation on telecoms network resilience issues.

ENISA – The European Network and Information Security Agency. An agency of the European Union set up to enhance the capability of the European Union, the EU Member States and the business community to prevent, address and respond to network and information security problems.

MNO – Mobile Network Operator, a provider which owns a cellular mobile network.

NICC – a technical forum for the UK communications sector that develops interoperability standards for public communications networks and services in the UK.

Provider – Used to refer to a person providing public electronic communications networks or services.

A2. Links to relevant sources

Communications Act 2003

Communications Act 2003 (as amended by the Security Act)

The key sections of the Communications Act related to network or service resilience are as follows:

Duties and guidance for providers

- Duties of providers to take security measures (including in response to security compromises): sections 105A to 105D
- Secretary of State codes of practice about security measures: sections 105E to 105I
- Duties of providers to inform others of security compromise: sections 105J and 105K
- Civil liability for contravention of security duties: section 105W
- Relationship between security duties and certain other duties: section 105X

Duties and powers of Ofcom

- Duties and powers of Ofcom in relation to securing compliance with security duties: sections 105M to 105V
- Powers of Ofcom to inform others of security compromise: section 105L
- Statement of policy on ensuring compliance with security duties: section 105Y
- Ofcom reports on security: section 105Z

Regulations

The Regulations

Code

The Code

Ofcom's procedural guidance

General statement of policy under section 105Y of the Communications Act 2003

Guidance on General Condition A3

General Conditions of Entitlement

Ofcom 2018 guidance on Protecting access to emergency organisations when there is a power cut at the customer's premises – Guidance on General Condition A3.2(b)