Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003

2017 Version

GUIDANCE

Publication Date: 18 December 2017

About this document

The legislation that applies to telecoms providers requires them to take measures to protect the security and resilience of their networks and services. Ofcom has the power to intervene if we believe a provider is not taking the appropriate measures. In May 2011, we published guidance telling the relevant providers what we expect them to do to meet their obligations. We updated this guidance in 2014.

In June 2017 we consulted on making another update, and we are publishing this 2017 version of the guidance as a result.

In our revisions, we have reflected the changing nature of the security risks faced by communications networks and services. This has resulted in us adding guidance on some additional risks, and updating our guidance on others.

We have also made some changes to the incident reporting process, primarily to increase the consistency of reporting between providers, and to improve the quality of information we receive.

Contents

Section

Annex

1. Introduction

1.1 This document provides high level guidance to providers of public electronic communications networks or services (CPs) on their security and resilience obligations under sections 105A and 105B of the Communications Act 2003 (CA2003).

1.2 These obligations are particularly important because of the increasing extent to which we all depend on communications infrastructure. A major failure within a 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.

1.3 The relevant elements of the legislation help to mitigate these risks by imposing on CPs the following statutory obligations (together with conferring on Ofcom associated powers and duties):

- network and service providers must take appropriate measures to manage risks to security, in particular to prevent or minimise the impact on end users and interconnected networks;
- network providers must take all appropriate steps to protect, so far as possible, network availability;
- network and service providers must report to Ofcom breaches of security or reductions in availability which have a significant impact on the network or service;
- Ofcom must, where we think it appropriate, notify regulators in other Member States, the European Network and Information Security Agency (ENISA[1]), and members of the public, of any reports received;
- Ofcom must send an annual summary of the reports we receive to the European Commission and ENISA;
- Ofcom may require a network or service provider to submit to, and pay for, an audit of the measures they are taking to comply with the obligations; and
- Ofcom can use the information gathering and enforcement provisions in the Act to investigate, rectify, and penalise any infringement of these obligations.

1.4 In the first instance, it is for CPs 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 CPs have clear lines of accountability, up to and including Board level, and sufficient technical capability to ensure that potential risks are identified.

[1] An agency of the European Union (EU), set up to enhance the capability of the EU, the EU Member States and the business community to prevent, address and respond to network and information security problems

Role and Status

1.5 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 security and resilience (statutory) obligations imposed on relevant CPs, thereby ensuring that they properly understand their obligations and enabling potential customers to identify any concerns.

1.6 One of Ofcom's regulatory principles is that Ofcom will regulate in a transparent manner[2]. Guidance can serve as a useful means to achieving this principle and to increasing understanding of Ofcom's policy objectives and approach to regulation.

1.7 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.

1.8 That said, whether or not (and, if so, how) a particular matter is regulated will usually turn on the specific facts in each case. CPs 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.

1.9 This document replaces our previous guidance, which we published in August 2014. 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 in the operation of the reporting scheme, or to incorporate feedback from stakeholders. We will also update the guidance as necessary in response to any relevant changes in the advice and recommendations published by ENISA or the European Commission.

1.10 We note that sections 105A and 105B apply to CPs of all sizes. However, the measures it would be appropriate for a large CP to take to protect security may be different to those appropriate for a smaller company. It is for CPs in the first instance to assess for themselves (taking this guidance into account) the measures which are appropriate in their own particular cases. This guidance is intended to be relevant to CPs of all sizes.

[2] https://www.ofcom.org.uk/about-ofcom/what-is-ofcom

2. Legislative framework

The European & UK Legislative Framework

2.1 The provision of electronic communications networks and services in the UK is regulated under the European Union's common regulatory framework for electronic communications networks and services (the Framework). Originally published in 2002, the Framework comprised five separate Directives[3].

2.2 The Framework was revised in November 2009. Among many other changes, the revisions extended the obligations on Member States, national regulatory authorities and industry in relation to the security and integrity of public electronic networks and services. These new obligations were introduced as Articles 13a and 13b of the Framework Directive[4].

2.3 Member States were required to implement Articles 13a and 13b into national law. In the UK, this was done with revision of the CA2003, principally with the addition of sections 105A to 105D. The relevant sections of CA2003 are included in Annex 2. They came into force on 26 May 2011.

Ofcom's guidance

2.4 We published our original guidance on the security requirements in sections 105A to 105D on 10 May 2011, with a minor revision for clarity following on 3 February 2012, and a further revision in August 2014. We have published this latest version of the guidance after considering the responses we received to our consultation in June 2017.

Scope

2.5 This guidance applies to all providers of Public Electronic Communications Networks[5] (PECN) and Public Electronic Communications Services[6] (PECS). Those providers are referred to as "network providers" and "service providers", respectively, in sections 105A to 105C CA2003.

[3] The Framework Directive (2002/21/EC); the Authorisation Directive (2002/20/EC); the Access Directive (2002/19/EC); the Universal Service Directive (2002/22/EC); and the Directive on privacy and electronic communications (2002/58/EC).
[4] Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services (Framework Directive) as amended by Directive 2009/140/EC.
[5] Section 151(1) CA2003 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.
[6] Section 151(1) CA2003 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.

3. Guidance on s.105A – protecting security

Summary of overall approach

3.1 Section 105A states the following:

Requirement to protect security of networks and services

105A.—(1) Network providers and service providers must take technical and organisational measures appropriately to manage risks to the security of public electronic communications networks and public electronic communications services.

(2) Measures under subsection (1) must, in particular, include measures to prevent or minimise the impact of security incidents on end-users.

(3) Measures under subsection (1) taken by a network provider must also include measures to prevent or minimise the impact of security incidents on interconnection of public electronic communications networks.

(4) A network provider must also take all appropriate steps to protect, so far as possible, the availability of the provider's public electronic communications network.

(5) In this section and sections 105B and 105C—

"network provider" means a provider of a public electronic communications network, and

"service provider" means a provider of a public electronic communications service.

3.2 The legislation does not, however, define the term "security". Ofcom's understanding of "security" in this context includes the usual meaning given to it in relation to information security, namely protecting confidentiality, integrity and availability. In that regard, we note, in particular, that there is a potential overlap with the requirements to protect the confidentiality of personal data set out in the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426). We note that matters falling specifically under those Regulations are subject to the Information Commissioner exercising his enforcement functions.

3.3 The requirements of section 105A are divided into the following four subsections:

- 105A(1) - management of general security risks;
- 105A(2) - protecting end users;
- 105A(3) - protecting network interconnections; and
- 105A(4) - maintaining network availability.

3.4 The following paragraphs in this Section 3 set out our guidance on the application of section 105A. We start, however, by making some general observations that we urge CPs to take into account. Figure 1, below, summaries the main sources of advice and best practice we refer to in this guidance, and which will expect CPs to consider where relevant to their operations.

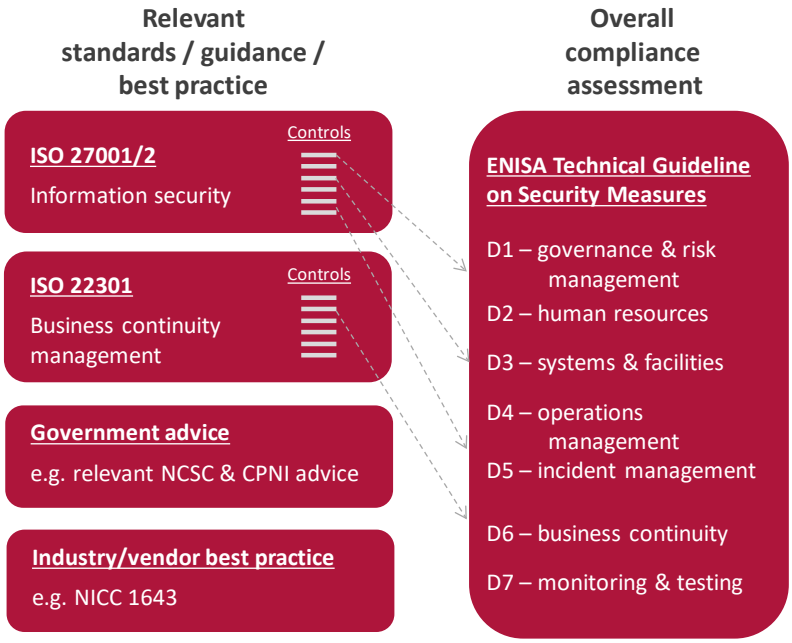

Figure 1: Summary of security advice sources included in this guidance

3.5 When considering compliance with section 105A(1) in relation to a particular matter, we will usually start our investigation by seeking evidence of appropriate risk assessment and ongoing risk management. We consider that ENISA's Technical Guideline on Security Measures[7] sets out good practice which should be considered by CPs to ensure that their activities comply with section 105A(1). We note that ISO 27001[8] is the source of most of these practices and so suitably scoped certification against this standard may encompass many of the considerations set out in the ENISA guideline document.

3.6 A risk assessment is only likely to be effective in driving performance if CPs 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.

3.7 We consider that section 105A(2) requires, in effect, that the approach to security risk management should in particular protect end users. We consider that this can largely be achieved within the approach set out for section 105A(1), 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).

3.8 In relation to the protection of network interconnections, as required by section 105A(3), we encourage CPs to adopt the minimum security controls in ND1643[9] , developed by UK industry specifically for this purpose.

[7] https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures
[8] https://www.iso.org/isoiec-27001-information-security.html
[9] http://www.niccstandards.org.uk/publications/index.cfm

Accountability and expertise

3.9 As noted above, it is important that CPs 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.

3.10 In order to assess this, we suggest that CPs consider the following questions:

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

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

3.12 To be compliant with section 105A, we also consider that CPs must maintain a level of internal security expertise, capacity, and appropriate accountability mechanisms, sufficient to provide proper management of their security risks. This is particularly important in circumstances where a CP has outsourced aspects of its network operations to a third party; responsibility to comply with its s105A-D obligations remains with the CP, and it needs to have sufficient internal capability to do this.

105A(1) – Management of general security risks

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

3.14 Alongside risk assessment, there are many other issues to consider when ensuring appropriate management of security risks. Ofcom's view of relevant issues will be informed by ENISA's Technical Guideline on Security Measures[10]. This document was developed as a guide for use by regulators when assessing compliance with the Framework Directive from which section 105A is drawn.

3.15 That ENISA document is not a technical security standard against which CPs can obtain certification. It is, however, recommended that CPs familiarise themselves with its

[10] https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures

contents, as we consider it covers the security domains relevant for section 105A compliance.

3.16 While not a standard in its own right, we note that ENISA derived six of the seven domains in its document from the ISO 27001:2013[11] domains. As such, a CP with current ISO 27001 certification with a relevant scope is likely to have already considered and achieved most of the security objectives in ENISA's Guideline. The only domain not derived from ISO 27001 addresses business continuity, with ISO 22301 cited as the standard with the closest relationship. Again, CPs with certification against this standard are likely to have already addressed these issues. We stress that neither ISO 27001 nor ISO 22301 certification are a requirement for section 105A compliance.

3.17 We expect that CPs will keep abreast of the range of security 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 security threats. Of particular relevance would be security advice from Government agencies such as NCSC[12] and CPNI[13], industry bodies such as NICC[14] and EC-RRG[15], ENISA[16], and vendors of equipment and software.

3.18 Beyond these general security issues, there are several additional issues, set out below, which CPs should consider.

Certification against technical security standards

3.19 Managing risks involves understanding them and putting in place measures to address them where appropriate. External certification against security standards can form a powerful mechanism to demonstrate that a CP has processes in place to do this. This guidance mentions a number of specific standards and bodies which publish a large number of standards which may be relevant to a particular CP's operations. However, we highlight these standards because we consider that they address issues which are likely to be relevant in considering compliance with section 105A, and not because we require CPs to obtain certification against them. During an investigation, we may ask a CP to provide evidence of the measures they have taken in relation to particular issues. Certification against security standards may usefully form part of this evidence, but it is not required, and indeed may not even be sufficient, to demonstrate compliance.

Supply chain and outsourcing

3.20 A CP will generally deal with supply chain risks by extending its security controls to the third parties it works with. However, some arrangements may present security risks which

[11] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
[12] National Centre for Cyber Security
[13] Centre for the Protection of National Infrastructure
[14] The UK telecoms sector's technical forum which develops interoperability standards
[15] Electronic Communications Resilience and Response Group
[16] European Network and Information Security Agency

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

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

3.22 The range of possible supply chain and outsourcing scenarios means it is not possible to generalise about the risks and what might constitute "appropriate measures" to manage them. We therefore strongly encourage CPs to discuss with us at an early stage any planned new arrangements that may have significant security 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.

3.23 We note that beyond section 105A, changes to supply chain arrangements might also have implications under other relevant legislation, such as the Investigatory Powers Act 2016[17] and the Data Retention Regulations[18]. CPs should also discuss such changes with the relevant agencies, and do so well in advance of finalising them.

Network monitoring

3.24 CPs need to have sufficient oversight of their networks and services to quickly identify significant security and availability incidents. This oversight may involve the monitoring of internal signals, such as from equipment fault alarms, and also external signals, such as customer complaints.

Cyber security

3.25 Cyber security is a top tier national security priority for the UK Government. The National Cyber Security Centre (NCSC) was launched in October 2016 to be the authority on the UK's cyber security environment. Government has made it clear in the National Cyber Security Strategy[19] that it considers regulation will have a role to play in ensuring cyber security is appropriately addressed, particularly by companies operating critical national infrastructure.

3.26 We consider that, as an important threat to security, measures to manage cyber threats, such as cyber attack, are in principle included within the obligations set out in section 105A. As we note above, managing security, and hence cyber security, in this context includes protecting confidentiality, integrity and availability.

3.27 CPs to which section 105A applies have a particularly important role in relation to the UK's cyber security because they are responsible for a significant proportion of the UK's relevant

[17] http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted/data.htm
[18] Data Retention (EC Directive) Regulations 2009
[19] https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

digital infrastructure. Furthermore, it is often while using the services provided by the telecoms industry that other organisations are exposed to cyber threats.

3.28 The central role of telecoms in cyber security means CPs generally have high levels of awareness compared to businesses in some other sectors. For example, a number of CPs are members of the Cyber Security Information Sharing Partnership (CISP), which facilitates the sharing of threat and vulnerability information. We encourage all qualifying CPs to join this partnership.

3.29 There is a large and rapidly expanding body of advice and technical standards relating to cyber security, and no single standard which addresses all relevant controls that a given CP should consider. We expect that CPs will ensure they are abreast of the available standards and advice, and implement relevant controls without undue delay. NCSC is a particularly important source of guidance in this area, from the general, such as "10 Steps to Cyber Security"[20], through to information about measures to protect against specific active threats. We are likely to seek evidence that a CP has taken due account of relevant advice during any cyber-related investigation.

3.30 Cyber Essentials[21] is a specific example of an NCSC-backed scheme which sets out basic technical controls to mitigate common internet based threats, and also provides for third party certification (known as Cyber Essentials Plus). We expect that CPs will put in place security measures to comply with section 105A which build on and go well beyond the baseline level of cyber threat management covered by the scheme.

3.31 Nonetheless, the controls in Cyber Essentials represent basic cyber security hygiene factors that all CPs should implement where possible. Obtaining Cyber Essentials Plus certification is a powerful way to demonstrate this has been done. However, the complex range of systems in use by some CPs go beyond the IT systems typically in use by the smaller organisations that the scheme was initially targeted at. Some CPs have told us that this can make obtaining third party certification against the scheme difficult to achieve, and the costs of doing so may become disproportionate. In the event we conduct a relevant investigation into a CP in this position, we will expect it to explain why obtaining Cyber Essential Plus is not proportionate. We will also continue to expect, among other things, to see evidence that the CP has taken the steps required by Cyber Essentials where appropriate.

Cyber vulnerability testing

3.32 At the time of publication, DCMS is leading a project involving Ofcom, NCSC and industry to develop a cyber vulnerability testing framework for the telecoms sector. The intention is that detailed intelligence on the threats faced by the CP undergoing testing would be gathered, and would form the basis for various penetration tests undertaken on their operational networks. As well as assessing how well defended the CP's network is against

[20] https://www.ncsc.gov.uk/guidance/10-steps-cyber-security
[21] https://www.cyberessentials.ncsc.gov.uk/

such attacks, the testing would also show how well it could detect and respond to any attempts.

3.33 We believe that this type of intelligence-led vulnerability testing should be an integral part of any approach to appropriately managing cyber risks. With such a fast-changing and complex threat, such testing is an important part of a CP's approach to developing and maintaining effective security measures. We are aware that many CPs already undertake various forms of vulnerability testing, but consider that this scheme offers some unique features. As such, we think it has the potential to provide powerful evidence that a CP is taking appropriate security measures in relation to cyber security, in the event that we undertake an investigation.

105A(2) – Protecting end users

3.34 Section 105A(2) requires that the measures to manage security risks should, in particular, minimise the impact of incidents on end users. We therefore expect that risk assessments should consider the risk to end users, not just the CP's own business risks.

3.35 The risk appetite of end users will vary, so we expect CPs to provide information about the security of their services to allow customers to make informed purchasing choices. CPs should attempt to match the delivered network and service security performance levels to the customer expectations that have been set.

3.36 We consider that the section 105A(2) requirement to "minimise the impact of security incidents on end-users" includes minimising the loss of availability. In relation to providers of networks, we note there is potential overlap with the availability requirement in section 105A(4). We consider the availability requirements placed on network providers in the section addressing section 105A(4) below.

3.37 In relation to the availability of services, CPs should take all appropriate steps to minimise the loss of availability, to the extent technically and commercially feasible. Feasibility will vary depending on whether the service provider has direct ownership of, a contractual relationship with, or no contractual relationship wit,h the underlying network.

105A(3) – Protecting network interconnections

3.38 To ensure compliance with section 105A(3), we strongly encourage CPs to consider, and where relevant, apply the controls in ND1643[22].

3.39 ND1643 was previously published by the UK telecoms industry standards group, NICC, as a compliance standard setting out the minimum security controls expected of interconnecting operators. NICC has reviewed and updated the document, and is expected to publish the revised version shortly, in the form of guidance, rather than a standard against which independent certification can be sought.

[22] Information about NICC documents can be found here: http://www.niccstandards.org.uk/publications/index.cfm

3.40 Despite the change of status of ND1643, the obligation on CPs to take measures to prevent or minimise the impact of security incidents on network interconnections remains. In that regard, we note that, as required by Article 13a(1) of the Framework Directive, the measures to be taken by CPs must ensure a level of security appropriate to the risk presented "having regard to the state of the art" and therefore we would ourselves have regard to the state of the art of such measures in any compliance assessment.

3.41 We will continue to use ND1643, in its revised form, as a reference point when determining if a CP has taken appropriate measures to comply with 105A(3).

105A(4) – Maintaining network availability

3.42 We note that section 105A(4) sets a high bar for compliance with its obligation to protect availability:

3.43 "*A network provider must also take all appropriate steps to protect, so far as possible, the availability of the provider's public electronic communications network.*"

3.44 In general, network providers should take measures to maintain availability appropriate to the needs of their direct customers. An important exception to this principle is for networks offering public access to the emergency services. For these networks, and the services they support, GC3[23] imposes specific and strict requirements for maintaining availability and will continue to apply.

3.45 We recognise the excellent work to improve the resilience of networks, and the management of emergencies, which is carried out by the members of the Electronic Communications Resilience and Response Group (EC-RRG).

Single points of failure

3.46 By single point of failure, we mean the configuration of a network or networks 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.

3.47 We consider that avoiding single points of failure, where it is reasonably possible to do so, is an "appropriate step" within the meaning of s105A(4). We consider that the extent to which avoiding single points of failure is reasonably possible 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 (so that, for example, it is less likely to be proportionate to deploy protection paths in the access network

[23] General Conditions of Entitlement - http://stakeholders.ofcom.org.uk/telecoms/ga-scheme/general-conditions/ Note that revised General Conditions are due to come into force on 1 October 2018. After this data, General Condition A3 will apply in place of the current GC3. Please see our website for further information - https://www.ofcom.org.uk/consultations-and-statements/category-1/review-general-conditions

whereas this is increasingly likely to be a reasonable step to take in a CP's backhaul and core networks); and

- geographic and physical constraints which limit the CP's scope to avoid single points of failure or make it disproportionately expensive.

3.48 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). When investigating such incidents, we expect to seek evidence that the CP has assessed the risks involved in their network design choices, and has met their obligations to take all appropriate steps to protect availability.

Flood Resilience

3.49 Flooding is an increasingly important risk that CPs need to manage appropriately as part of their compliance with section 105A(4). We note that, even where sites are identified as being at a lower risk of flooding, CPs 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. Following a significant flood incident, we expect to closely examine the mitigation steps taken by CPs, and will launch formal investigations if appropriate.

Power Resilience

3.50 Even for 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 CPs will manage the risk of power loss appropriately as part of the measures they take to comply with section 105A(4). Following a significant incident caused by a loss of power, we expect to closely examine the mitigation steps taken by CPs, and will launch formal investigations if appropriate.

Outsourcing

3.51 Many CPs now make extensive use of third parties to provide infrastructure for, and to design and operate, their networks. It is therefore conceivable that a CP 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.

3.52 We do not consider that outsourcing to third parties in this way excuses CPs from their obligations under 105A(4). Put simply, a CP cannot contract out of its statutory obligations. As such, they should have sufficient levels of contractual control over third parties in place to ensure they continue to comply with their obligations. We also expect CPs to continuously and rigorously check that actions undertaken on their behalf do not put them in breach of their obligations.

4. Guidance on s.105B – breach notification

4.1 Section 105B states the following:

Requirement to notify OFCOM of security breach

105B – (1) A network provider must notify OFCOM –

(a) of a breach of security which has a significant impact on the operation of a public electronic communications network, and –

(b) of a reduction in the availability of a public electronic communications network which has a significant impact on the network.

(2) A service provider must notify OFCOM of a breach of security which has a significant impact on the operation of a public electronic communications service.

(3) If OFCOM receive a notification under this section, they must, where they think it appropriate, notify—

(a) the regulatory authorities in other member States, and

(b) the European Network and Information Security Agency ("ENISA").

(4) OFCOM may also inform the public of a notification under this section, or require the network provider or service provider to inform the public, if OFCOM think that it is in the public interest to do so.

(5) OFCOM must prepare an annual report summarising all notifications received by them under this section, and any action taken in response to a notification.

(6) A copy of the annual report must be sent to the European Commission and to ENISA.

General comments on reporting

4.2 It is important that CPs have adequate processes in place to ensure that reporting is routinely performed and that this reporting continues even when experienced staff are absent from work.

4.3 In relation to the initial notification of an urgent incident, we accept that, particularly out of hours, this will be a best efforts activity and not always possible given timing and resource constraints. In the event that we have not received a notification from a CP, and become aware of an incident appearing to us to be urgent, we will normally seek to make enquires via the contact point we have been given by the CP.

How

4.4 Notifications about "urgent" incidents should be made via the agreed contacts, or the 24/7 reporting number outside of office hours. Details of Ofcom's specific contact points will be provided separately to relevant CPs.

4.5 Incident reports should be submitted to incident@ofcom.org.uk.

4.6 If CPs require a more secure method of communication, for example an e-mail address with enhanced security, this can be arranged.

4.7 CPs should provide Ofcom with a contact point for urgent enquiries about major incidents which we become aware of but which have not yet been reported.

When

4.8 Initial notifications of "urgent incidents" should be made by CPs as soon as possible, and ideally within 3 hours of the CP becoming aware of them.

4.9 Incidents should be reported, whenever possible, within 72 hours of the CP becoming aware of them.

4.10 Where a CP has a significant number of 'non major' incidents (typically those meeting only the lowest fixed numerical threshold), they may be reported in batches.

4.11 All batched incidents which commenced in a calendar month must be reported to Ofcom before the second Monday of the following month.

4.12 To facilitate Ofcom's annual reporting to the European Commission and ENISA, CPs should keep incident data for no less than 18 months following incident resolution.

What

4.13 Section 105B requires CPs to satisfy themselves that they report all incidents having a significant impact on their networks and services. The qualitative criteria and numerical thresholds in this section set out our view of the level at which incidents are likely to be significant and should therefore definitely be reported. Figure 2 describes the process to follow. If any one of the criteria or thresholds is met, the CP should submit an incident report. We would expect that CPs will not adopt an unduly restrictive approach to interpreting these criteria – if there is doubt as to whether a criterion is met, CPs should submit a report.

4.14 For the avoidance of doubt, we consider that major security breaches resulting from cyber attacks are reportable under section 105B. The consequences of a major cyber incident can include a loss of personal data, a loss of other types of data, loss of integrity, and loss of availability. In our view, a major cyber breach resulting in *any* of these consequences is likely to have "a significant impact on the operation of a… network or service" and is therefore reportable. In other words, we consider such an incident is reportable even if end customer service availability has not been affected.

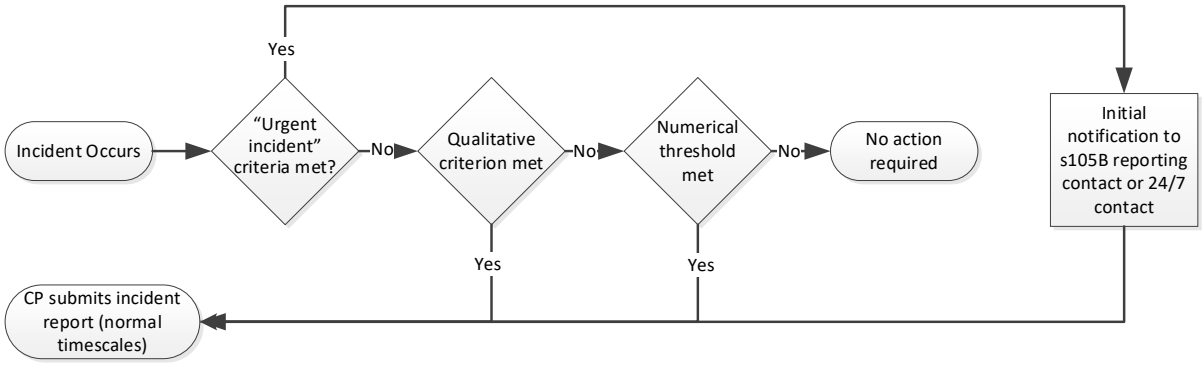

Figure 2: Incident reporting process

Qualitative criteria

Urgent incidents

4.15 Incidents should be notified as "urgent" if they meet any of the following criteria:

- All incidents involving major cyber security breaches that are reportable under the criteria in "Reportable Incidents" in paragraph 4.16 below.
- Incidents affecting services to 10 million end users.
- Incidents affecting services to 250,000 end users, and expected to last 12 hours or more.
- Incidents attracting national mainstream media coverage.
- Incidents affecting critical Government or Public Sector services (e.g. wide spread impact on 999, 3-digit non-emergency numbers, emergency services communications).

Reportable incidents

4.16 Reportable incidents are as follows:

i) General

- Any incidents reported to other Government agencies or departments.
- Any incidents that CPs are aware of being reported in the media (local, national or trade news sources).
- Any incidents involving major cyber security breaches, which meet any of the criteria in this list.

ii) Repeat incidents

- Repeat incidents are considered to be those which reoccur within four weeks, or are separate incidents affecting the same services in the same areas over a four week period.
- For repeat incidents, the CP should combine the impacts of the individual incidents in determining whether they meet the numerical thresholds.

iii) Outages affecting the ability of the customer to contact the emergency services

- Any incident affecting central services involved in connecting emergency calls (e.g. Call Handling Agent platforms, emergency call routing etc.) and leading to a reduction in the usual ability to answer or correctly route calls.
- Any incident that the CP is aware of that has a link to a potential loss of life.

Fixed network numerical thresholds

Network/service type	Minimum number of end customers affected[1]	Minimum duration of service loss or major disruption
Fixed network providing access to the emergency services	1,000	1 hour
Fixed network providing access to the emergency services	100,000	Any duration
Fixed voice or data service/network offered to retail customers	10,000 or 25%[2]	8 hours
Fixed voice or data service/network offered to retail customers	100,000	1 hour

Table 1: fixed network numerical thresholds

4.17 Notes on Table 1:

1. A customer is affected if the main functions of a network or service are not available to them due to the incident.
2. This threshold should be interpreted as either 10,000 end customers or 25% of the CP's total number of end customers on the affected service, whichever is the lowest number.

Mobile network numerical thresholds

Network/service type	Minimum number of end customers affected[1]	Minimum duration of service loss or major disruption

Mobile network providing access to the emergency services[2]	1,000	1 hour
Mobile network providing access to the emergency services[2]	100,000	Any duration
MVNO voice or data service/network offered to retail customers [3]	25%[4]	8 hours
MNO voice or data service/network offered to retail customers	See notes[5]	

Table 2: mobile network numerical thresholds

4.18 Notes on Table 2:

1. A customer is affected if the main functions of a network or service are not available to them due to the incident.
2. Where a CP expects emergency roaming will have allowed customers in the affected area to retain 112/999 access, it is not required to report the incident under this threshold.
3. A Mobile virtual network operator (MVNOs) should report incidents affecting its end customers, even where incidents are the result of a failure in its host mobile network operator's (MNO's) network. In this case, the third party's details should be provided.
4. This threshold should be interpreted as 25% of the CP's total number of end customers on the affected service.
5. Due to the complexity of mobile networks and the inherent difficulty in determining the exact number of end customers affected by an incident, Ofcom has agreed a reporting process with each of the four UK mobile operators which is based on their individual definitions of a major service failure (MSF). Network MSFs are incidents which have a significant impact on the network and are raised to senior management within the MNO. The exact details of an MNOs MSF criteria are commercially sensitive so will not be discussed here. The ultimate intention is to ensure reporting of mobile incidents which cause similar levels of customer disruption to those reportable on fixed networks.

   At the time of publication of this guidance, we are still in discussions with MNOs about revising these agreements, in order address the concerns about the current levels of reporting which we set out in our June 2017 consultation[24]. In summary, the revised agreements are intended to result in more consistency between MNOs in reporting

[24] See paragraphs 3.7 – 3.25 of the consultation found on our website here: https://www.ofcom.org.uk/consultations-and-statements/category-1/review-security-guidance

and in the calculation of customer impact, which for most MNOs will represent a significant increase in the number of incidents they report.

Broadcast network numerical thresholds

Network/service type	Minimum number of end customers affected[1]	Minimum duration of service loss or major disruption
Broadcasting service/network for reception by the general public	100,000	12 hours

Table 3 – broadcast network numerical thresholds

4.19 Notes on Table 3:

1. A customer is affected if the main functions of a network or service are not available to them due to the incident.

4.20 We will keep the numerical and qualitative thresholds under review and may revise them from time to time, for example as a result of CP feedback or our own experience. As such, we welcome discussion of these reporting arrangements with CPs and industry groups.

Data required

Urgent incidents - initial notification

4.21 For "urgent incidents", CPs should inform us as quickly as possible. We expect this initial notification to simply acknowledge that the CP is aware of a major incident, and give an indication of its nature. Any other information that is readily available will be welcomed.

Incident reports

4.22 All other incident reports should include the information described in the rest of this section. Where full or final information is not available at the time of reporting, updated reports can be provided at a later date.

1. CP name

4.23 The full name of the communications provider.

2. CP incident reference number

4.24 A unique reference number that can be used to identify the incident in communications with the CP.

3. Date and time of occurrence

4.25 The date and time that the incident commenced.

4. Date and time of resolution

4.26 The date and time that the incident was resolved completely. Where the incident is ongoing at the time of reporting, the resolution time may be provided when it is available.

5. Location

4.27 Location information should describe the geographical location of the impact of the incident. Where possible, a UK postcode should be provided which describes the geographical area where service interruption was experienced.

4.28 Where the geographical impact of an incident is not easily attributable to a single or small number of complete postcodes, the CP should provide a single or series of summary postcodes which will contain only the 'outward' part of the postcode.

4.29 Where an issue has regional or national impact the CP should provide the name of the region or nation in lieu of a postcode.

4.30 In the case of mobile incidents resulting in the loss of a technology (e.g. 2G, 3G, or 4G) or service (e.g. voice, data) at specific cell sites, a full list of the affected sites should be provided.

4.31 Use the following examples as a guide:

Failure location examples	**Location expectation**
Service interruption due to failure at a single or small number of cell sites	The full post code of the cell site(s)
Service interruption due to failure at a single or small number of street cabinets	The full post code of the street cabinet(s)
Service interruption due to issues associated with a single or a small number of exchanges	The full post code of the exchange(s)
Service interruption to the whole of Leeds city centre	The 'outward' part of the Leeds city centre post code. In this example 'LS1' would be appropriate.
Service interruption with impact across the whole of Manchester	In this case the CP should report the location as 'Manchester'.
Service interruption with impact across an entire county/region	In this case the CP should report the name of the county/region.
Service interruption with national impact	'UK', 'England', 'Scotland', 'Wales', 'Northern Ireland', with 'north', 'south,

	'east' and 'west' designations as appropriate. E.g. Northwest England.

Table 4: providing location information

6. Brief description of incident

4.32 Provide a short summary of the incident, including any relevant information not captured elsewhere on the template.

7. Impact

a) Services affected

4.33 Provide full details of the services affected. This should identity services as understood by the subscriber, for example telephony, broadband, 2G, 3G, 4G, etc.

b) Number/proportion of users affected

4.34 Provide details of the number of subscribers affected by the incident. The information provided should be as accurate as is technically feasible at the time of reporting. If a reporting threshold was met under one of the 'percentage of users affected' criteria the CP should provide the number affected and the percentage of the CP's end customers for this service that this represents.

4.35 The CP should provide details of the total number of affected customers against every service associated with an incident, even where that service did not meet specific thresholds. For example, for an incident which exceeds a voice threshold and also affects data customers – but does not exceed a data threshold – the number of data end customers affected should be included in the report.

4.36 Where the impact of an incident varies over time effort should be made to explain how this was the case.

4.37 Where exact numbers are not available (for example due to a mobile cell site failure) we expect the CP to use historical data to estimate the number of end customers affected.

4.38 CPs which offer wholesale products to other CPs may have little or no visibility of the number of end customers affected by an incident with their network or service. We do not expect a CP to alter their monitoring or reporting systems to obtain this information. However, where it is clear to the CP that an incident is likely to result in service loss to end customers which will exceed the reporting thresholds, we would encourage them to report this.

4.39 A CP should report qualifying incidents affecting any service it sells, even if another CP fulfils the service. However, where a CP's customers use additional services over the top of the network or service it provides, but without its direct involvement, we would not expect the CP to monitor or report any incidents affecting such additional services.

c) Networks & assets affected

4.40 The CP should provide an overview of the networks and assets that were affected during the incident. At this stage the overview should be brief. If we decide to investigate the incident further, network and asset information may be required to a level of detail commensurate with the current ENISA Article 13a Technical Guideline on Threats and Assets[25].

8. Summary of incident cause and action taken so far

4.41 The CP should provide sufficient detail to enable us to classify the incident against one of the root cause and primary cause categories defined in the current ENISA Article 13a Technical Guideline on Threats and Assets.

4.42 The CP should provide details of action taken to manage and remedy the incident, and any measures taken to mitigate the risk of reoccurrence.

9. Third party details

4.43 If the cause of the incident was the failure of a third party service, provide the name of the third party.

4.44 Additionally, indicate whether a service level or operational level agreement is in place with the third party and whether a breach occurred.

10. Name and contact details for follow up

4.45 Details to enable us to follow up on the incident if required.

Report format

4.46 Annex 3 provides a reporting template.

4.47 The CP may use their own reporting template if they prefer. Where this is the case, the CP should ensure that the template includes all of the data required in the above section.

Incident follow up

4.48 Where it is felt that there are aspects to an incident that require further investigation we will contact the CP to request further details.

4.49 If we require clarification of data provided in the incident report contact will be made by email or telephone. If we believe that a detailed investigation of the incident is required, we will typically invite the CP to an incident follow up meeting. Figure 3 describes this process.

[25] https://www.enisa.europa.eu/publications/technical-guideline-on-threats-and-assets

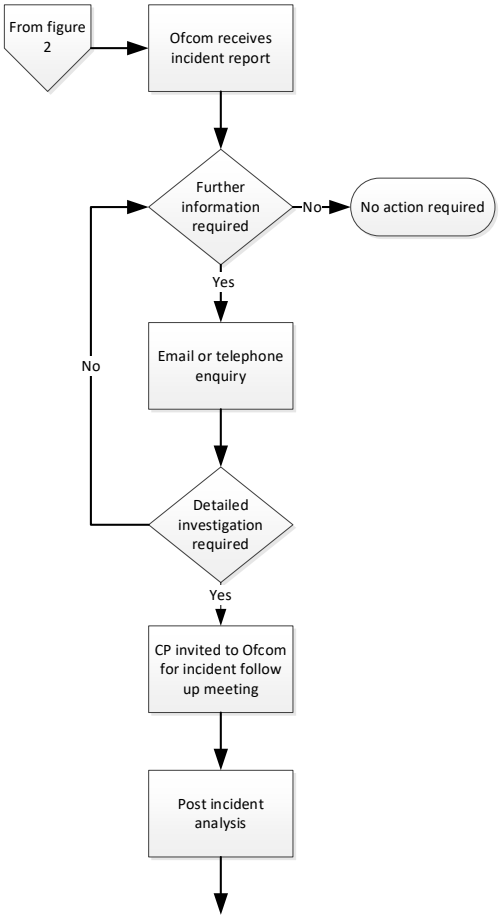

Figure 3: Incident follow up process

4.50 Ofcom will use the incident follow up meeting to examine all aspects of the incident including the CP's approach to security risk management, the incident cause, impact and the remedial actions taken. Where an incident is technically complex and requires a significant understanding of the CP's network architecture, topology and design, Ofcom may request a presentation of this nature. We may use our section 135 powers to gather information if required.

4.51 Post incident measures may include actions or requirements placed on the CP. For example, where an incident remedy requires planned changes to the network we may request regular progress updates.

4.52 In cases where the incident is not resolved to our satisfaction we may consider the use of our auditing and enforcement powers defined in sections 105C and 105D.

Annual incident summary report

4.53 Ofcom provides periodic reports to the UK government on the state of the UK's communications infrastructure, in accordance with section 134A and 134AA of CA2003. These reports include an annual incident summary.

4.54 Additionally, Ofcom will submit a summary of incident reports to ENISA and the EU as required by section 105B. Only incidents which meet the ENISA reporting thresholds set out in the current version of the ENISA Technical Guidance for Incident Reporting[26] will be included in the summary. ENISA will combine data from these incidents with incident data from across the EU to publish its Analysis of Article 13a Annual Incidents report to which UK CPs will have access.

[26] https://www.enisa.europa.eu/publications/technical-guideline-on-incident-reporting

5. Guidance on s.105C & D – auditing and enforcement

5.1 Sections 105C and 105D set out Ofcom's main security and resilience enforcement powers. Under section 105C we can require a network or service provider to undergo an independent audit of their security and resilience arrangements, at the provider's expense. Section 105D extends our powers to enforce compliance with conditions we have set, such as general conditions and significant market powers (SMP) conditions, to the enforcement of sections 105A to C. These enforcement powers include the ability to notify providers of contraventions, to issue directions suspending the entitlement to provide networks or services, and to impose fines up to £2m.

5.2 We can also use our formal information gathering powers when assessing the security and availability of networks and services in relation to compliance with 105A.

5.3 As noted in the previous section, we may need to consider the use of these powers during an investigation of a reported incident or group of reported incidents. However, there are other reasons why we may investigate and need to use these powers. For example:

- following a complaint from a consumer or other stakeholder;
- where we otherwise become aware of a potential security or resilience issue which merits further investigation; or
- where we believe significant incidents may be going unreported.

Audits

5.4 The use of our auditing powers will be specific to the situation we are considering and therefore likely to be different in each case. In general, our objective will be to find evidence of the measures that a CP has taken to manage a particular risk, in order to inform an assessment of whether it has complied with section 105A. The relevant standards and best practice we refer to in this guidance will usually form the basis for an audit where these are relevant to the area of concern.

5.5 To give an example, in which we are considering whether a CP, or group of CPs, had appropriate risk management measures in place, we would be likely to include an assessment of the security objective "SO2: Governance and Risk Management" from the ENISA Technical Guideline[27] in any audit. As such, the auditor might be seeking, among other things, evidence that the CP had a documented risk management methodology which is in line with industry standards, and that it was followed.

5.6 As another example, we might use an audit to seek evidence that a specific technical measure had been undertaken. For example, if we would have concerns about the measures taken to protect a CP's internet connected desktop PCs, we might focus an audit

[27] https://www.enisa.europa.eu/publications/technical-guideline-on-minimum-security-measures/at_download/fullReport

on whether security patches had been applied within 14 days of becoming available, in line with a control in the Cyber Essentials scheme.

Frequency of audits

5.7 We are aware that audits are potentially a significant burden on CPs. This is due both to the direct cost on them of paying for the auditing work, but also the internal resources required to support it. We will consider the appropriateness of auditing carefully in each case. However, under this new guidance, we expect to consider the use of audits more frequently than we have to date.

Enforcement

5.8 Ofcom publishes Enforcement guidelines for regulatory investigations[28], which set out how we investigate compliance with, and approach enforcement of, regulatory requirements across a range of areas, including section 105A-D.

5.9 In relation to specific incidents, rather than launching an investigation, it can be more effective for us to work informally with stakeholders, given that our priority will usually be to ensure that any security incident is addressed by CPs as soon as possible. However, we will not be slow to use our formal enforcement powers where we consider that to be appropriate.

[28] https://www.ofcom.org.uk/consultations-and-statements/category-2/ofcoms-approach-to-enforcement

A1. Glossary

CISP The Cyber-Security Information Sharing Partnership. A joint initiative between industry and Government to share cyber threat and vulnerability information in order to increase overall situational awareness of the cyber threat and therefore reduce the impact upon UK business.

CP Communications Provider. Used to refer to entities providing public electronic communications networks or services.

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.

ISO International Organisation for Standardisation. The largest developer of international voluntary standards. Among many others, it publishes the 27000 series of information security standards.

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

MSF Major Service Failure. A commonly used term within the telecoms industry to signify the most serious service-affecting incidents. Such incidents usually receive senior management attention and trigger the highest level incident management procedures. The term is not universal but most providers will have an equivalent designation.

MVNO Mobile Virtual Network Operator. An organisation which provides mobile telephony services to its customers, but does not have allocation of spectrum or its own wireless network and instead, buys a wholesale service from a mobile network operator.

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

A2. Communications Act 2003 wording

Security of public electronic communications networks and services

Requirement to protect security of networks and services

105A.—(1) Network providers and service providers must take technical and organisational measures appropriately to manage risks to the security of public electronic communications networks and public electronic communications services.

(2) Measures under subsection (1) must, in particular, include measures to prevent or minimise the impact of security incidents on end-users.

(3) Measures under subsection (1) taken by a network provider must also include measures to prevent or minimise the impact of security incidents on interconnection of public electronic communications networks.

(4) A network provider must also take all appropriate steps to protect, so far as possible, the availability of the provider's public electronic communications network.

(5) In this section and sections 105B and 105C—

"network provider" means a provider of a public electronic communications network, and

"service provider" means a provider of a public electronic communications service.

Requirement to notify OFCOM of security breach

105B.—(1) A network provider must notify OFCOM—

(a) of a breach of security which has a significant impact on the operation of a public electronic communications network, and'

(b) of a reduction in the availability of a public electronic communications network which has a significant impact on the network.

(2) A service provider must notify OFCOM of a breach of security which has a significant impact on the operation of a public electronic communications service.

(3) If OFCOM receive a notification under this section, they must, where they think it appropriate, notify—

(a) the regulatory authorities in other member States, and

(b) the European Network and Information Security Agency ("ENISA").

(4) OFCOM may also inform the public of a notification under this section, or require the network provider or service provider to inform the public, if OFCOM think that it is in the public interest to do so.

(5) OFCOM must prepare an annual report summarising all notifications received by them under this section, and any action taken in response to a notification.

(6) A copy of the annual report must be sent to the European Commission and to ENISA.

Requirement to submit to audit

105C.—(1) OFCOM may carry out, or arrange for another person to carry out, an audit of the measures taken by a network provider or a service provider under section 105A.

(2) A network provider or a service provider must –

(a) co-operate with an audit under subsection (1), and

(b) pay the costs of the audit.

Enforcement of obligations under sections 105A to 105C

105D.—(1) Sections 96A to 96C, 98 to 100, 102 and 103 apply in relation to a contravention of a requirement under sections 105A to 105C as they apply in relation to a contravention of a condition set under section 45, other than an SMP apparatus condition.

(2) The obligation of a person to comply with the requirements of section 105A to 105C is a duty owed to every person who may be affected by a contravention of a requirement, and -

(a) section 104 applies in relation to that duty as it applies in relation to the duty set out in subsection (1) of that section, and

(b) section 104(4) applies in relation to proceedings brought by virtue of this section as it applies in relation to proceedings by virtue of section 104(1)(a).

(2) The amount of a penalty imposed under sections 96A to 96C, as applied by this section, is to be such amount not exceeding £2 million as OFCOM determine to be—

(a) appropriate; and

(b) proportionate to the contravention in respect of which it is imposed.

135 Information required for purposes of Chapter 1 functions

(3) The information that may be required by OFCOM under subsection (1) includes, in particular, information that they require for any one or more of the following purposes--

(ie) assessing the security of a public electronic communications network or a public electronic communications service;

(if) assessing the availability of a public electronic communications network

137 Restrictions on imposing information requirements

(2A) OFCOM are not to require the provision of information for a purpose specified in section 135(3)(ie) or (if) unless—

(a) the requirement is imposed for the purpose of investigating a matter about which OFCOM have received a complaint;

(b) the requirement is imposed for the purposes of an investigation that OFCOM have decided to carry out into whether or not an obligation under section 105A has been complied with; or

(c) OFCOM have reason to suspect that an obligation under section 105A has been or is being contravened

A3. Incident reporting template

1	CP name	
2	CP incident reference number	
3	Date and time of occurrence	
4	Date and time of resolution	
5	Location	
6	Brief description of incident	
7	Impact: i) Services affected ii) Number/proportion of users affected iii) Networks & assets affected	
8	Summary of incident cause and action taken so far	
9	Third party details	
10	Name and contact details for follow up	