Network and Service Draft Resilience Guidance for Communications Providers

Proposed guidance for communications providers on resilience related security duties under the Communications Act 2003

Published 08 December 2023

Contents

1. Introduction

1.1 Document Purpose

This document provides guidance to communications providers to ensure the resilience of communications networks and services used by UK citizens; including consumers, businesses, and all other organisations.

This guidance describes a range of good practices in the architecture, design, and operational models that underpin robust and resilient telecommunications networks and services. It sets out our key expectations in these areas while taking input from 'Resilience Incidents' reported to us within Ofcom's security compromise reporting function. This guidance is intended to be flexible enough to apply to all types of communications providers offering networks and services in the UK, while allowing for continued technology evolution and innovation. We have set out our expectations in terms of 'outcome-based principles' alongside more specific measures including examples where needed.

This guidance is produced under sections 105Y and 1(3) of the Communications Act 2003 (as amended) and sets out the measures we expect communications providers to take in relation to the availability, performance, and functionality (or *'resilience'*) of their networks and services, as part of their security duties under s105A-D of the Act. This includes duties imposed under the Electronic Communications (Security Measures) Regulations 2022 made by the Secretary of State under sections 105B and 105D of the Act. We note that communications providers' obligations with respect to resilience under s105A-D sit alongside those contained in Ofcom's General Conditions of Entitlement concerning the availability of services and access to emergency organisations and those contained in the Telecommunications Security Code of Practice.

We will use this guidance as a practical reference both:

- in information gathering and monitoring of network and service resilience when engaging with communications providers and the wider industry and;
- as a starting point for considering compliance as part of any enforcement activities in relation to resilience issues.

This guidance supersedes and replaces Ofcom's 2022 Resilience guidance document.[1]

The Telecommunications Security Code of Practice dated December 2022 focuses primarily on measures to address cyber-security aspects of the security duties imposed under Section 105A-D; whereas this guidance focuses on other aspects of network and service resilience. As such, this document is intended to be read in conjunction with the Security Code of Practice, and we refer to it where appropriate.

The guidance in this document is not the only way for communications providers to comply with their resilience-related security duties under s105A-D. A communications provider may choose to comply with their resilience-related security duties by adopting different technical solutions or approaches to those specified here. What is appropriate and proportionate will depend on the particular circumstances of the provider. However, this guidance is intended to set out the general approach which we would normally expect to take in investigating compliance with resilience-

[1] Ofcom, 2022. *Guidance on resilience requirements imposed by or under sections 105A to D of the Communications Act 2003*

related security duties under s105A-D as appropriate. Where a provider has taken a different approach to that set out in this guidance, we would expect them to be able to explain their reasons for doing so.

1.2 Background Factors Related to Network Resilience and Reliability

The following sections outline some of the key concepts and drivers related to resilience and reliability of communications providers' networks and services.

1.2.1 Reliability Concepts

A number of conceptual thematic layers need to be considered in the overall pursuit of ensuring reliable networks and services that people can depend on.

- Infrastructure - The underlying physical components and transmission media; how reliable they are, as well as how they are connected, are among some key factors to consider.
- Processes - Ensuring robust processes are in place to support the full lifecycle of networks and services from inception, through delivery, in-life, to decommissioning[2]
- Availability – Infrastructure and processes directly impact network and service availability and must be engineered to meet appropriate levels for the services provided.

This document provides guidance on infrastructure, processes, and mechanisms to ensure network and service availability and reliability.

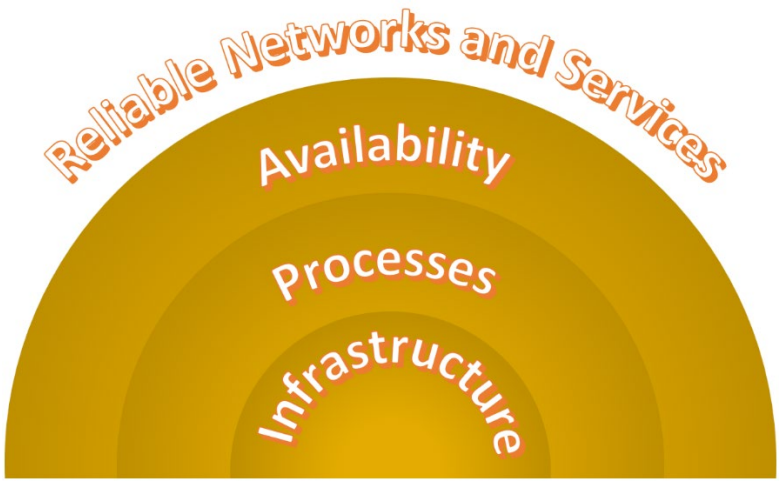

Figure 1: Reliable Networks and Services

1.2.2 Technology and Service Evolution

Technology evolution continues to change the way that networks operate and how services are built and delivered.

[2] This includes appropriate tools and systems to support and monitor those processes.

There has been, and continues to be, a rapid pace of technology evolution. This applies across the whole landscape from the digitisation of services, the Internet, providers' networks, and connected devices. Some of these developments can improve network resilience and overall service reliability. But some of them create new risks to network and service resilience and reliability, partly due to immaturity and complex dependencies.[3]

The technology evolution includes the development of the consumer and industrial Internet of Things (IoT), increased usage of virtual private networks and encryption, augmented and virtual reality, cloud computing, 5G, and other future emerging technology and services.

There are many different service use cases in the provision of communications services, involving a variety of different ecosystems, some utilising the internet and others not. Many use cases are enabled by the digitisation of services (Internet Protocol 'IP' based) along with the evolution from the use of proprietary hardware to the use of virtualised network services based on cloud-native principles.[4]

5G standards and implementation methodologies directly make use of these principles to enable further service innovation and differentiation, and can be combined with network slicing, automation, and data analytics. Furthermore, evolution to software and cloud across different technology domains (fixed, mobile, Wi-Fi, etc) presents some convergence opportunities which can enable further innovation and network infrastructure efficiencies.

Transformative shifts, such as the increasing use of cloud-native concepts, substantially alter the way services are built, using new approaches and operating mechanisms. This can bring about efficiencies to providers, where fixed and mobile core networks can be consolidated onto commercial off-the-shelf (COTS) IT hardware. While this can be beneficial for the operator, with lower cost equipment and theoretically better supply chain competition, the increased consolidation of services due to the combination of convergence and more efficient use of hardware can lead to an increased risk of wider impact when failures do occur.

Some of these shifts result from industry driven programmes or technology lifecycles, such as the move to 'All-IP' where the PSTN, 3G, and 2G networks are to be switched off. In the case of the PSTN, this has inherently provided an amount of power backup due to the nature of the technology. This has meant a telephone service has potentially been available during power failures for a number of days, whereas with broadband and mobile services, this may be significantly less. Therefore, further steps are required to provide a suitable level of availability.

In addition, novel access mechanisms are proliferating in the telecommunications sector, such as the use of Low Earth Orbit (LEO) satellites and Fixed Wireless Access (FWA) technologies that provide additional coverage and access options.

1.2.3 Climate Change and Severe Weather

Climate change is leading to more uncertain and severe weather conditions.

Over recent years, we have seen changes in our climate having increasing impacts on telecoms infrastructure. Weather conditions are more uncertain, and we have seen severe weather (typically

[3] Immaturity in both the technology itself, and the skills and understanding of the technology.

[4] Cloud-native refers to the concept of building and running applications to take advantage of distributed computing offered by cloud computing. Cloud computing can be provided in several ways, offered by a third-party provider or in-house by the communications provider, shared or dedicated hardware, remote or on the providers premises, and where remote over the internet or dedicated links.

storms and flooding), such as Storm Arwen, which could significantly disrupt or damage telecommunications networks.[5] For example, it could cause a mains power loss, or direct physical damage to telecoms infrastructure resulting from storm damage such as downed overhead cables. Without appropriate action, it could become increasingly likely that we experience significant telecoms outages, that could threaten human life. In these cases, the resilience of UK networks to maintain services, particularly emergency services, is made more important.

1.2.4 Societal Dependence on Telecoms

Over the last two decades, we have seen dramatic changes in how people communicate and what they expect from telecoms services. We have also seen shifts to new technologies and a changing climate, which all factor in on the importance of resilience and new challenges around the resilience of networks.[6]

The Internet and user device evolution have dramatically changed how people communicate, make purchases, and interact with the world.

This is also reflected in changes to how people access the emergency services. Statistics published in 2021 showed that 74% of calls made to the emergency services were via mobile.[7] Additionally, the more recently launched emergency video relay service is primarily a mobile device-based service.[8]

More broadly, a variety of safety critical systems are becoming increasingly dependent on telecommunications. Some of the 5G technical capabilities are targeted at safety critical use cases.

1.2.5 UK Critical National Infrastructure Resilience

Resilient infrastructure systems are seen by government as being important, not just for telecoms, but for all Critical National Infrastructure (CNI) sectors. The Cabinet Office has published the National Risk Register and the UK Government Resilience Framework.[9, 10]

Additionally, the UK National Infrastructure Commission (NIC) published a report called 'Anticipate, React and Recover' Report in 2020 in which it presented a framework for resilience with recommendations for UK Government, regulators, and operators of CNI. The NIC framework is illustrated in Figure 2.[11]

[5] EC-RRG, 2022. *2021/2022 Severe Storms Post-Incident Report*
[6] For example: 4G/5G, smartphones and other smart devices
[7] DCMS, DHSC, HO, 2023. *999 and 112: the UK's national emergency numbers.* https://www.gov.uk/guidance/999-and-112-the-uks-national-emergency-numbers [accessed 5 December 2023].
[8] Ofcom, 2021. *Statement: Emergency video relay*. https://www.ofcom.org.uk/consultations-and-statements/category-2/further-consultation-emergency-video-relay [accessed 5 December 2023].
[9] HMG, 2023. *National Risk Register*.
[10] HMG, 2022. *The UK Government Resilience Framework*.
[11] NIC, 2020. *Anticipate, React, Recover - Resilient infrastructure systems*.

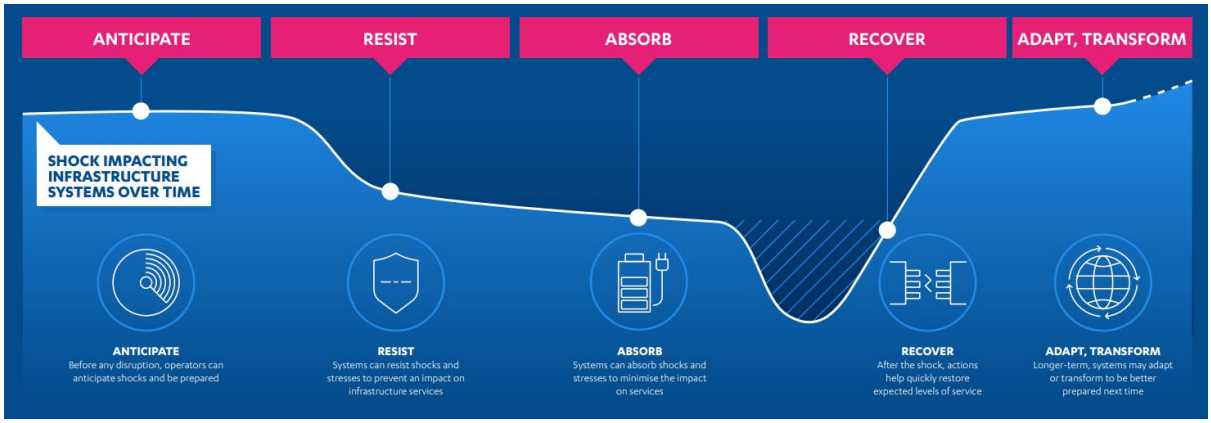

Figure 2: NIC Resilience Framework

The NIC report recommends focusing on three main points; setting clear standards of resilience, demonstrating resilience, and continued drive of improved resilience longer term.

As stated in the report, the Commission has considered six aspects of resilience, which together capture the range of possible actions to take to deliver resilient infrastructure systems:

- anticipate – actions to prepare in advance to respond to shocks and stresses, such as collecting data on the condition of assets
- resist – actions taken in advance to help withstand or endure shocks and stresses to prevent an impact on infrastructure services, such as building flood defences
- absorb – actions that, accepting there will be or has been an impact on infrastructure services, aim to lessen that impact, such as building redundancy through a network
- recover – actions that help quickly restore expected levels of service following an event, such as procedures to restart services following an event such as a nationwide loss of power
- adapt – actions that modify the system to enable it to continue to deliver services in the face of changes
- transform – actions that regenerate and improve infrastructure systems

While the NIC report is applicable to all CNI sectors, we feel that the NIC framework and associated continuous cycle contained in the report, apply very well to the telecommunications sector. While not forming part of this guidance, we would expect providers to consider how this might apply to their networks and services infrastructure.

Relating the NIC framework stages to this guidance, providers of communications networks and services are required by s105A to take appropriate and proportionate measures to identify and reduce the risks of, and prepare for the occurrence of, security compromises (including network or service outages) occurring. This aligns with anticipate, resist, and absorb stages of the NIC framework. Providers must also ensure that when outages do occur, actions are taken to restore normal levels of service within a reasonable period appropriate to the severity of the impact. This aligns with the recover stage. These principles should be backed by longer term adaptations and transformations to be better prepared and recover quicker when future shocks occur.

On 18 October 2023, the NIC published the Second National Infrastructure Assessment.[12] Recommendation 28 builds on the framework described above by recommending the publication of a full set of outcome-based resilience standards for digital services, which includes telecommunications.

1.3 Risks to Resilience

There are a wide range of risks that each communications provider needs to assess before deciding on the appropriate and proportionate measures that they need to take to meet their duties under the Act in relation to network resilience and service reliability. These are captured in this section.

In addition, when assessing such risks, communications providers should consider the planning assumptions relevant to national risks contained in the UK National Risk Register.[13]

1.3.1 Physical Threat/Shocks

Physical Threats/Shocks include:

- Natural phenomena – e.g. extreme weather, earthquakes, flooding, lightning, falling trees
- Fire
- Explosions, in particular those caused by gas leaks
- Damage caused by- e.g. accidents, vandalism, internal sabotage and terrorism

1.3.2 Personnel Threats

Personnel Threats include:

- Insider threat (including the supply chain)
- Human error
- Lack of appropriate training, key skills, knowledge or resource availability
- Malicious acts and hostile reconnaissance
- Negligence

1.3.3 Technology, Physical and Cyber Security Vulnerabilities

Technology, Physical and Cyber Security Vulnerabilities include:

- System vulnerabilities (including software and hardware)
- Lack of adequate capacity management/overload controls; including in relation to traffic or signalling loads
- Interworking or cascade vulnerabilities
- Lack of adequate Separation, Segmentation, or Segregation of networks, including control planes, management planes, and user/data-planes – logical, physical, and geographical
- Review, testing and management of change (detection and prevention of misconfiguration)

[12] NIC, 2023. *The Second National Infrastructure Assessment*.
[13] HMG, 2023. *National Risk Register*.

- Electromagnetic Interference (EMI) such as Electromagnetic Pulses (EMP), malicious electronic interference, geomagnetic induced currents and other space weather phenomenon[14]
- Electromagnetic Compatibility (EMC) and Electromagnetic Emissions (including malicious interference)
- Hacking and inappropriate signals or messages injected by users or external parties
- Inappropriate protective controls to protect sensitive assets
- Denial of Service attacks – malicious attempts to damage a service, sometimes by traffic overload, sometimes by the transmission of 'malware'

1.3.4 Loss of Key Dependencies

Telecommunications depends on the continuous availability of many 'key dependencies', amongst which, some of the most critical are:

- Electrical Power
- Timing/Synchronisation
- Fuel (for backup generators and operational staff vehicle fleet)
- Human access (to operational installations)
- Materials for deployment and repair of telecommunications and associated infrastructure

1.3.5 Architecture/Design Vulnerabilities and Failings

Many of the risks listed above could impact key sites or other shared facilities, and therefore any single component instance or sets of functions that share a common underlying facility within a broader overall network architecture.

Many physical and logical component functions of networks can exist as multiple instances in networks for the purpose of resilience. This is particularly important where loss of the network component or function would have a material impact on the network or service. Without careful attention to both physical and logical architecture of network and service functions, loss of key sites or other common facilities could impact multiple instances of a given function if those multiple instances are not implemented with geographical separation, along with the appropriate resilience mechanisms, spare capacity, and connectivity to make effective use of the geographical separation.

There are two common concepts related to this. The first is sometimes referred to as a 'single point of failure'. The second is where multiple physical instances or logical components 'share fate' on another physical or logical facility. For example, if multiple instances or components are all implemented within one site, or connectivity was all provided through one common duct, they would all have shared fate on the single site or duct. If the site or duct fails, they all fail.

[14] Severe Space Weather events include a range of phenomena which have various potential impacts on electronics and communications infrastructure and signals. These phenomena include coronal mass ejections, solar energetic particles, solar flares, solar radio bursts, high speed streams of radiation. Space weather events may also cause disruptions in key dependencies of telecommunications such as electrical power and timing/synchronisation.

Poor architecture/design policy or poor implementation of adequate architecture/design policy can both lead to significant network and service impacts.

1.3.6 Software Failures

Telecommunications networks are reliant on software-controlled equipment, and no software is immune from errors and operational failings. In addition, care should be taken to avoid 'systemic' or 'common-mode' failures, where a software flaw or error in one network node causes the same or a related fault to occur in other connected nodes leading to a 'cascading' failure of an entire network or service.

As networks become more dynamic, 'data-driven', and 'software-controlled', the use of machine learning to analyse network and/or service performance data and change the network has the potential to cause significant network or service outages if the software or logic fails.

1.3.7 Critical Third parties (Managed Service Partners and Wholesale Network/Service Providers)

Over recent years, it has become increasingly common for communications providers to outsource operation of parts of their networks to third parties, sometimes referred to as managed service providers or managed service partners. Additionally, communications providers sometimes use wholesale services provided by other communications providers, who are in turn providing Public Electronic Communications Networks or Services.

In these cases, there is a risk that communications providers relying on third party services lose a degree of control over their network design and oversight which could impact network or service resilience.

2. Legislative Framework and Definitions

2.1 Legislative Framework

This section explains how the security duties in the Communications Act 2003 (CA 2003) are framed in the context of "resilience".

2.1.1 The overarching duties set out in the Communications Act 2003

The CA 2003 was amended by the Telecommunications (Security) Act 2021, which strengthened the security duties imposed on communications providers.

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."*

Further overarching duties are set out in section 105C, which require 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 appropriate and proportionate measures to remedy or mitigate that effect.

2.1.2 "Security compromise" includes 'Resilience Incidents'

The duties imposed by sections 105A and 105C are set by reference to the concept of a "security compromise" which is defined in section 105A(2).

A security compromise includes "*anything that compromises the availability, performance or functionality"* of networks and services, and "*anything that causes signals conveyed by means of the network or service to be lost"*.[15]

This will, therefore, include both "cyber-type" compromises such as those caused by malicious actors, as well as a broad range of other impacts on the resilience of networks and services, such as outages caused by external factors (e.g. floods, cable cuts, or power cuts) or internal factors (e.g. hardware failures, operational process errors, or network design flaws).

These latter aspects are more often associated with threats to network and service availability and 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.

The guidance set out in this document applies to the category of security compromises relating to the resilience of networks and services, in terms of their availability, performance or functionality (referred to hereafter as "Resilience Incidents").

[15] s105A(2)(a) and (d)

2.1.3 Duties to take specific measures imposed by the Secretary of State by regulations

The Secretary of State has powers to make regulations under sections 105B and 105D of the 2003 Act which require communications providers to take specified security measures or measures of a specified description 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. [16]

These Regulations, which also apply in respect of Resilience Incidents, supplement the duties imposed on communications providers by s105A and 105C of the CA 2003. They require communications providers to take specified security measures including in relation to: network architecture, the protection of data and network functions, protection of certain tools enabling monitoring or analysis, monitoring and analysis, the supply chain, the prevention of unauthorised access or interference, preparing for remediation and recovery, governance, reviews, patches and updates, competency, testing, and assistance.[17]

2.1.4 Guidance given by the Secretary of State in codes of practice

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, the Secretary of State issued the Security Code of Practice, setting out guidance for providers with relevant turnover in the relevant period of more than or equal to £50m. The Security Code of Practice gives guidance on measures which mainly relate to cyber-type security compromises such as those caused by malicious actors.

It should be noted that the guidance provided in this document applies to communications providers of all sizes regardless of turnover.

2.1.5 General Conditions of Entitlement

Alongside the security duties under the CA 2003, communications 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.

This document does not give specific guidance on the General Conditions. But it acknowledges those obligations where doing so provides clarity.

2.2 Key Definitions

A number of terms used in this guidance are defined in section 151 of the CA 2003 and the Regulations. We set out the key definitions relevant to this guidance below.

[16] The Electronic Communications (Security Measures) Regulations 2022

[17] These provisions do not apply to micro-entities, as defined by s384A of the Companies Act 2006, ie. companies who satisfy two of the following conditions (i) have 10 or fewer employees (ii) have a turnover of not more than £632,000 and (iii) have a balance sheet total of not more than £316,000.

2.2.1 Communications Provider (CP)

The term “Communications Provider” is one of the most recognised and commonly used terms in the telecommunications industry and is common in publications directed toward the public. We use this term in this document for ease of accessibility for a broad range of readers. However, the statutory definition may not be as widely understood. In section 151 of the CA 2003,

"Public Communications Provider" means:

a) a provider of a public electronic communications network

b) a provider of a public electronic communications service

c) a person who makes available facilities that are associated facilities by reference to a public electronic communications network or a public electronic communications service

For the purpose of this document, when we use the term “communications provider”, we specifically refer to points “a” and “b” above because the security duties under the CA 2003 only apply to such providers.

2.2.2 Public Electronic Communications Network (PECN)

"Public Electronic Communications Network" means an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to members of the public.

2.2.3 Public Electronic Communications Service (PECS)

"Public Electronic Communications Service" means any electronic communications service that is provided so as to be available for use by members of the public.

The CA 2003 also provides that *“A service is made available to members of the public if members of the public are customers, in respect of that service, of the provider of that service.”* (see 151(9)).

A publicly available service is one that is available to anyone who is both willing to pay for it and to abide by the applicable terms and conditions. The provider will not have imposed an upper limit on the class of potential customers other than those that arise from technical or capacity constraints. A publicly available service is distinguishable from a bespoke service restricted to a limited group of individual and identifiable customers.

It is also to be understood that the term members of the public requires a broad interpretation; it is not to be read as residential or small business customers. A service that because of its functionality or scale, such as a virtual private network service, is only likely to attract corporate or commercial customers is still considered to be available to members of the public. For example, it can include the provision of wholesale network connectivity or services provided to other communications providers or businesses.[18]

[18] The National Archives (originally Oftel), 2003. *Guidelines for the interconnection of public electronic communications networks – 23 May 2003*. https://webarchive.nationalarchives.gov.uk/ukgwa/20080712143605/http:/www.ofcom.org.uk/static/archive/oftel/publications/eu_directives/2003/intercon0503.htm#chapterthree [accessed 5 December 2023]. See paragraphs 6.1 to 6.5.

2.2.4 Electronic Communications Network (ECN)

"Electronic Communications Network" means:

a) a transmission system for the conveyance, by the use of electrical, magnetic or electro-magnetic energy, of signals of any description; and

b) such of the following as are used, by the person providing the system and in association with it, for the conveyance of the signals:

   i. apparatus comprised in the system;

   ii. apparatus used for the switching or routing of the signals;

   iii. software and stored data; and

   iv. (…)other resources, including network elements which are not active.[19]

2.2.5 Electronic Communications Service (ECS)

"Electronic Communications Service" includes a service consisting in, or having as its principal feature, the conveyance of signals, by means of an electronic communications network, except in so far as it is a content service.[20]

[19] s32(1) Communications Act 2003

[20] s32(2) and 32(2A) Communications Act 2003

3. Scope of CP Networks and Services Resilience

3.1 PECN and PECS Network and Services Scope

This guidance applies to all providers of Public Electronic Communications Networks (PECN) and Public Electronic Communications Services (PECS) (“communications providers") in the context of their security duties under the CA 2003.

Each communications provider, whether at the wholesale or retail level, or both, remains responsible for taking appropriate and proportionate measures in respect of the resilience of the network and services they are providing. This includes parts of the operational network operated by third parties on behalf of the communications provider, including as part of managed service arrangements.

This guidance applies to the provision of PECN and PECS at all points between the end-user equipment and the service application being provided by the communications provider, meaning Communications Providers' networks and services. This also includes interconnections from the Communications Provider’s network with third parties. For providers of PECNs, this tends to be from the customer premise, across the network they provide, and either to services that the PECN hosts within their network (such as Voice-over-LTE or Voice-over-Broadband) or to the demarcation (peering/interconnect) interfaces with content providers, application providers, Content Delivery Networks (CDNs), internet transit providers, or other Communications Providers.

PECSs can take a variety of forms. Where a provider offers a communications service, they are responsible for the reliable and secure operation of the service over the end-to-end network path to end-customers.

3.2 Resilience in the context of Communications Providers

As explained above, 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 their availability, performance or functionality, which we refer to as Resilience Incidents.

We interpret this in the broadest sense as the ability of an organisation, resource, or structure to be resistant to a range of internal and external threats, to withstand the effects of a partial loss or degradation of platform, system, or service, and to recover and resume service with the minimum reasonable loss of performance.

As reflected in the EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure, resilience can be seen to include[21,22]:

a) Good network design and deployment practices

b) Effective operational processes for network deployment, operations, management, and maintenance

c) Appropriate processes to respond to a range of contingent risks

d) Business continuity planning and disaster recovery

e) Appropriate review processes of previous incidents

We expect all communications providers to maintain an ongoing programme of risk assessment and to make plans and investments commensurate with the identified risks, taking into account both the likelihood of events and the impact of their occurrence. Communications providers should take a holistic view of resilience, so that it is seen as an integral part of a set of wider company processes. In addition to the measures contained in the Security Code of Practice, we would expect that communications providers would be mindful of and incorporate measures derived from appropriate international standards such as:

a) Overall company Risk Management (ISO 31000)

b) Quality Management (ISO 9001)

c) Information Security (ISO 27001)

d) Business Continuity Management (ISO 22301)

e) Asset Management (ISO 55001)

The Information Technology Infrastructure Library (ITIL) framework provides a useful basis to consider the many processes within the various stages of a communications service's life cycle. [23] Section 5 takes key parts pertinent to the processes supporting the availability of communication services.

In some cases, communications providers might not operate all component parts of the network or service that they provide. For example, a communications provider may rely on interconnecting networks to reach its customers or for its customers to reach other people or applications; or be reliant on some common external facilities (e.g. the Internet Domain Name System 'DNS'); or may

[21] The Electronic Communications Resilience & Response Group (EC-RRG) is a cross government and telecoms industry forum whose aim is to ensure the telecoms sector remains resilient to threats and risks to services. The EC-RRG Resilience Guidance is not formally part of this guidance. DSIT, DCMS, 2022. *Electronic Communications Resilience & Response Group (EC-RRG).* https://www.gov.uk/guidance/electronic-communications-resilience-response-group-ec-rrg [accessed 5 December 2023].

[22] EC-RRG, 2021. *EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure*

[23] ITIL is a library of best practices for managing IT services and improving IT support and service levels. One of the main goals of ITIL is to ensure that IT services align with business objectives, even as business objectives change. IBM. *What is IT Infrastructure Library (ITIL)?.* https://www.ibm.com/topics/it-infrastructure-library [accessed 5 December 2023].

procure underlying network services or infrastructure from other providers. In such cases, the overall resilience of their services inherently depends on these other parties.

However, as stated in section 3.1, overall responsibility remains with the communications provider to take appropriate and proportionate measures to ensure the security and resilience of the networks and services they are providing, where they are providing a PECN or a PECS.

Communications providers may seek Service Level Agreements and contractual arrangements to meet their overall resilience requirements. But it is potentially more effective to ensure that all such external suppliers take a similar and complementary approach to resilience management.

Endeavours should be made to regularly review the following topics with suppliers, partners, or peers with an objective to jointly understand risks and agree the optimal management of those risks.

a) Security and Resilience

b) Business Continuity

c) Disaster Recovery

d) Quality of Service management

e) Emergency Planning

3.3 Infrastructure – Network Domains Overview

The following section provides a high-level overview of the key network domains that typically form part of a communications provider's network. Section 4 then provides technical guidance for each of these domains.

Network Infrastructure Domains

The network infrastructure within Communications Providers' networks can usually be broken down into the following four areas or domains:

- Access / Last Mile: Wireless/Mobile Air Interface and Fixed Access
- Aggregation / Backhaul: Mobile Backhaul and Fixed Aggregation
- Core / Metro
- Peering and Interconnect

In addition to the physical infrastructure-oriented domains above, there is a partially logical domain or 'plane' which spans them. This is:

- Network Management (including Out-of-Band Management)

Figure 3 illustrates a high-level representation of the typical network domains within an end-to-end communications network, and their relative scale for a UK national network.

Note that even in smaller networks, the domain names are often still used, but with smaller quantities of some types of sites.

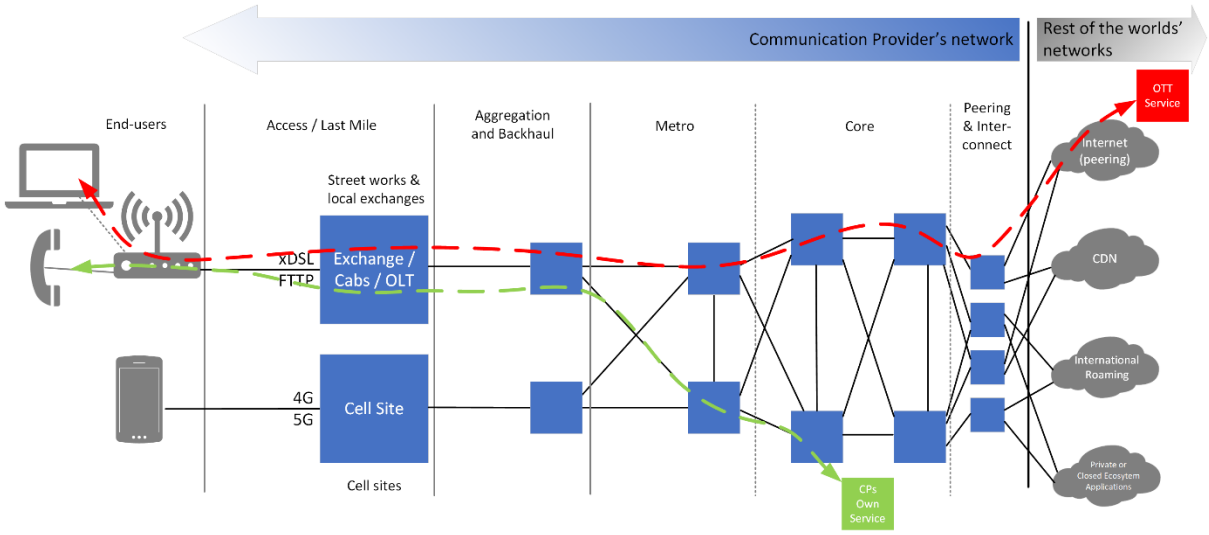

Figure 3: Typical CP Network Infrastructure Domains

3.3.1 Access / Last mile

The access / last mile sub-domains discussed in this section include (but are not limited to)[24]:

- 3GPP Mobile/wireless RAN (Radio Access Network) Air Interface – spectrum/carriers, antennas, and the cell sites to support it
- Fixed Access Network – e.g. xDSL, G.fast, Hybrid Fibre Coax (HFC), FTTP (xPON) to the customer premises
- Non-3GPP wireless access – Fixed Wireless Access and Non-Terrestrial-Networks such as Low Earth Orbit satellites[25,26]

The last mile domain significantly contributes to customers' quality of experience including resilience and general service reliability.

The biggest resilience challenge in this domain is that it often contains a number of single points of failure due to cost and a variety of other technical and practical barriers. However, in cases where greater resilience is needed, it is possible to improve resilience and reliability in Access networks through a variety of means.

The resilience and reliability of the access/last mile portion of networks are subject to a number of key factors. These include:

- Technical/practical challenges resulting in single points of failure
- Technology evolution cycles

[24] Examples of additional access network types include terrestrial broadcast TV/radio

[25] Fixed-Wireless-Access networks typically have similar network topology domains as Fixed or Mobile networks as shown in Figure 3. As such, this guidance will apply to FWA networks.

[26] Non-Terrestrial-Network topologies can vary from the topology in Figure 3 due to the nature of the connectivity from satellites to associated ground stations, and onward to core and peering. NTN based CPs should consider how the resilience principles in this guidance apply to their networks and services to maintain the overall objectives.

- Cost/investment & associated risk
- Spectrum availability, propagation conditions, & cost (for wireless technologies)
- Regulatory environment
- Competition landscape
- Planning permissions limitations

Some of these factors are not within a communications provider's direct control, nor under Ofcom's current regulatory remit.

See section 4.2.1 for specific guidance on this domain.

3.3.2 Aggregation / Backhaul

Aggregation/backhaul networks are different to the core/metro and 'last mile' domains for a variety of reasons. The number of sites and geographical spread of the aggregation/backhaul domain are far greater than the core domain; typically by a factor of 100 to 1000 times greater. As such, the level of physical connectivity resilience may be less than the core/metro domain. But aggregation/backhaul sites are expected to be built with an appropriate degree of physical resilience regarding equipment, physically separate/diverse connectivity, and power backup.

The two variants of this domain with the largest amount of deployment are:

- Fixed aggregation network – This includes connectivity between customer premises or street cabinets and more central sites where subscriber sessions are logically terminated (i.e. an IP address being assigned). Technically, this domain includes switching and routing nodes and transmission links to aggregate the traffic from various fixed access technologies.
- Mobile RAN backhaul – This aggregates and connects cell-sites to exchange or core sites. Technically, this domain consists of various technologies including switching and routing nodes, microwave, passive and active optical transmission, and satellite connectivity.

In these sub-domains, locations like mobile base stations and street cabinets are often connected to a single 'parent' aggregation site without resilient connectivity. But in cases where greater resilience has been deemed necessary by the communications provider, mobile base stations or cabinets may be equipped with resilient connectivity to an additional 'parent' site. [27]

Communications providers (at all levels of the supply chain) make architectural topology choices about how many end locations/nodes (and customers) to aggregate to intermediate aggregation sites, and if those aggregation sites have resilient dual parented connections back to different core sites. This equates to the quantity of aggregation sites that are built in a network. These choices significantly affect how many customers suffer connectivity loss when there are physical failures in certain types of sites.

See section 4.2.2 for specific guidance on this domain.

[27] A CP may deem greater resilience is necessary for a variety of reasons, potentially including things like providing connectivity to hospitals, transport hubs such as airports, shipping ports, or a range of other commercial contracts.

3.3.3 Core / Metro

The core network domain is sometimes broken down further in to core and metro in larger networks. These sites typically have physically separate and diverse connectivity paths to cater for physical failures of network nodes or links (including cable bundles and ducts). These resilient paths are sometimes called 'redundant' paths/links/nodes.

Core sites are where the bulk of the key network control plane functions and communications providers' own services and applications reside. This will often include the mobile core, IMS[28]/Voice platforms, subscriber authentication databases, policy control functions, DNS resolvers, and content caching. In other words, the core sites contain the communications providers' most critical network and service functions, and are typically built to the highest levels of resilience practically and economically possible.

Different services and applications used by end-users and devices have differing dependencies on the network functions mentioned above. It is important to note that communications providers' level of Quality of Experience (service reliability) is heavily dependent on a communications providers' ability to forecast capacity demands on the network, often including a full annual budget cycle.

See section 4.2.3 4.2.3 for specific guidance on this domain.

3.3.4 Internet Peering and non-Internet Interconnection

Communications providers typically have connections from their networks to other networks for 'internet' traffic or content, as well as 'non-internet' traffic or content.

The ecosystems for internet peering' versus other types of non-internet interconnect are different in a number of ways including significantly differing processes, commercial models, service level agreements, and quality of service capabilities.

Non-internet interconnections include use cases like voice telephony interconnects and international carriage, international mobile roaming, and other private connectivity. The scale and the approach to resilience between these different cases can vary significantly. Therefore, we distinguish between internet-related connectivity (including peering) and non-internet-related interconnection types. See section 4.2.4 for specific guidance on this domain.

3.3.5 Network Management

Network and device management is a logical plane, typically augmented by some additional physical equipment, which cuts across the rest of the physical network infrastructure domains described in this section. Figure 4 provides a pictural representation of this cross-cutting aspect.

The management plane carries traffic relating to the upkeep of the network and services, with the key purposes being configuration and software maintenance, and monitoring of performance and status/health.

[28] IP Multimedia Subsystem (IMS) is a set of network and device functions and capabilities which support voice, messaging, and other services in IP based networks. As per 3GPP and GSMA standards, IMS provides the basis for integrated Voice over LTE (VoLTE), Voice over WiFi (VoWiFi), messaging, and potentially other services.

Figure 4 shows the concept of managing network equipment across the physical infrastructure domains along with appropriate segregation and security between network elements and network management systems referred to as Network Oversight Functions in the Security Code of Practice.

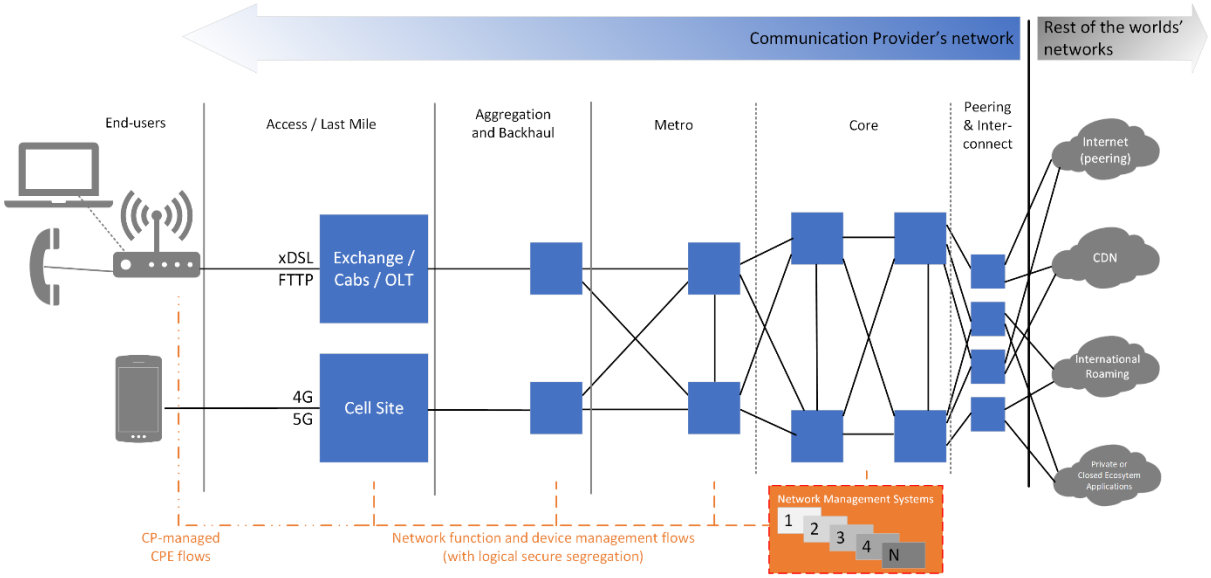

Figure 4: Network Management 'logical domain'

There are two key variations to the connectivity path of the management plane: in-band management and out-of-band management.

In-band management means managing the network and functions via the primary network itself. It is typically used for managing most network functions and devices across a network most of the time.

Out-of-band management means managing the network via means other than the primary network such that the out-of-band management connectivity would remain available when failures impact the availability of the primary network.

It is often used as an additional way to manage key network infrastructure components which underpin the connectivity for the rest of the network functions. The set of key devices tends to include transmission equipment, routers, and switches. However, the key underpinning components can vary depending on the network technologies and services provided. See section 4.4 for specific guidance on this topic.

Communications providers should also refer to the Security Code of Practice which contains cyber-security guidance and measures surrounding the management plane including: privileged user access, privileged access workstations, and Network Oversight Functions (including network management systems as shown in Figure 4).

4. Network and Service Implementation Resilience Guidance

In this section, we set out our guidance on the expected measures to be taken by communications providers for network and service architecture, design, and implementation under sections 105A to 105D.

Basic principles and approach of the guidance

As stated previously, the main objective of this guidance is to achieve a good level of resilience and reliability of communications networks and services in the UK by promoting good practices to be adopted by all types, and sizes of communications providers.

This guidance has been written with flexibility in mind, in order to be applicable to all communications providers and to allow for continued technology evolution. We have set out our expectations in terms of 'outcome-based principles' alongside more specific measures including examples where they are needed based on evidence, including from incidents reported to Ofcom under section 105K of the CA 2003 and gathered through exercising our enforcement functions.

As already discussed, the CA 2003 and Electronic Communications Security Measures Regulations provide overarching obligations on providers related to network and service resilience. Regulation 3 in particular requires network providers to take appropriate and proportionate measures to ensure the network is designed and constructed in a manner which reduces the risks of security compromises occurring, including resilience incidents as previously discussed.

We provide guidance below on measures to be taken relating to network architecture, design, and implementation.

4.1 Network infrastructure general physical guidance

We expect communications providers to take measures to ensure the general resilience of physical aspects of electronic communications networks, including giving appropriate consideration to best practices which apply to the resilience of network infrastructure, and incorporate such best practices into their networks where appropriate.

Examples of such best practices include the EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure which captures a wide range of considerations and best practices in the design and operation of networks. In particular, see the section of the EC-RRG Resilience Guidance on design recommendations related to generic physical aspects of communications network resilience.[29]

Physical security of network infrastructure is also an important factor in ensuring network and service resilience. For further guidance on appropriate and proportionate measures to be taken, communications providers should refer to the Security Code of Practice.

We also expect communications providers to adopt measures on risks around the loss of energy supply as a key input. For example, see the related section of the EC-RRG Resilience Guidance.

[29] EC-RRG, 2021. *EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure*

Additionally, the Building Digital UK – environmental resource guide (see section 6.2.2.4) contains network planning guidance for physical network infrastructure related to a range of power, weather, and other geographical hazards. Communications providers should also adopt measures which factor climate change implications into their network planning and decision making in order to maintain network and service reliability.

We list more specific expectations on the measures which communications providers should take regarding loss of power in the following infrastructure domains sections.

4.2 Network infrastructure domains guidance

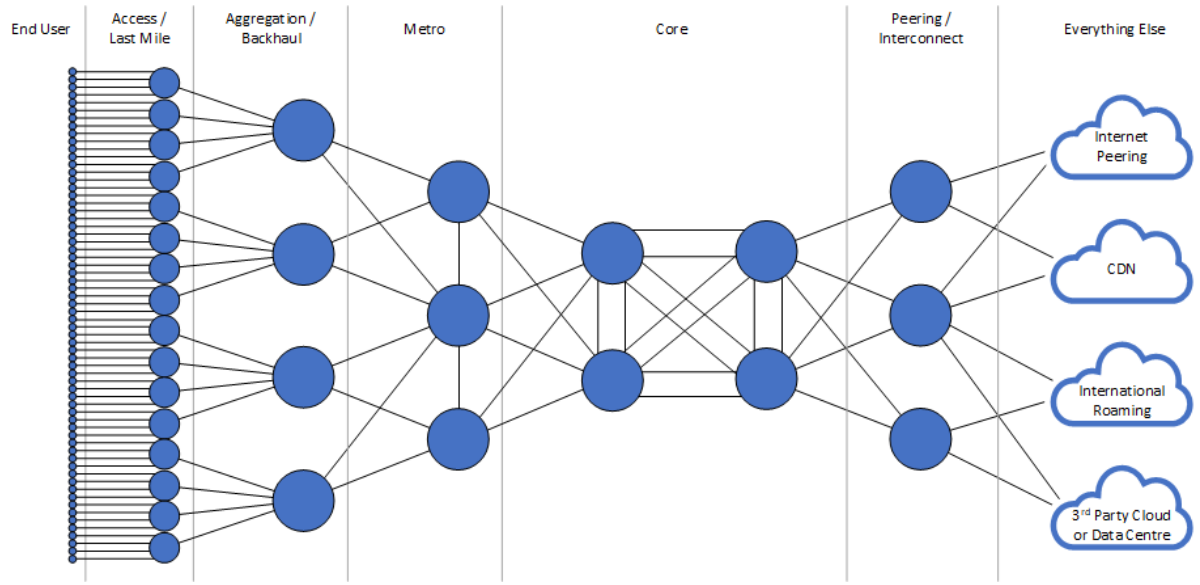

Figure 5: Example of CP Network Infrastructure Domains

4.2.1 Access / Last mile

As described in section 3.3.1, the access/last-mile domain typically consists of the following examples:

- Mobile air interface – spectrum/carriers, antennas, and the mobile cell site equipment
- Fixed access network – xDSL, Hybrid Fibre Coax (HFC), FTTP (xPON) to the customer premises

Different access technologies have different factors related to their overall resilience and reliability such as: propensity to fail, typical time-to-repair of that technology, geographical location distribution of equipment and maintenance field staff, and the number of customers impacted during different types of failures.

All these factors (and more) combine to result in varying levels of customer disruption when there is a network or services failure.

Therefore, when considering network architecture, design, and operational models, communications providers should put in place measures which specifically consider all these factors.

Given the scale and geographical reach of network assets within access networks, it can become costly to create highly resilient access networks. Ofcom is aware that this domain is likely to have

single points of failure, but also understand that the customer concentration should be significantly lower in comparison to the core of networks.

Access network equipment or locations such as mobile base stations and street cabinets are often connected to a single 'parent' site without resilient connectivity. In cases where greater resilience is appropriate, communications providers should equip mobile base-stations or cabinets with resilient connectivity to an additional 'parent' site.

Additionally, in order to provide appropriate resilience to core site failures, we would expect communications providers to take measures to ensure that network equipment within the access sites supports automatic failover from one core site to another, and services should be maintained or re-established automatically.[30] This capability needs to be supported by the upstream aggregation or backhaul network connectivity.

On sites and equipment where a number of customers' last-mile connections are aggregated, resilience of the equipment and all key dependencies should be considered in the site and equipment design (see section 1.3.4). Where possible, communications providers should seek to eliminate loss of key dependencies, including mains power and network timing/synchronisation, for a significant period of time bearing in mind that citizens depend on the access network for access to emergency services. For 3GPP-mobile-based networks, over-reliance on a single source (or path) of network timing/synchronisation is a weakness.

To overcome the loss of mains power, the measures that communications providers are expected to implement include the following power backup provision for different access network types.

In the case of fixed access networks, we expect powered 'active' components in street cabinets to have a minimum of 4hrs of power backup (except where these are planned to be replaced or discontinued within five years of the date of this Guidance). As the number of customers served by a site increases, we would expect that site to be able to survive power losses for longer, potentially with permanent back-up electricity generators on site which can be re-fuelled while in operation.

In the case of mobile cell sites, in order to meet their duties, MNOs should take at least some measures to mitigate against the risks of power outages and support continued communications services during short term power outages and surges which might reasonably be expected to occur. *Note: This section may be updated following a Call for Input relating to power resilience in mobile radio access networks, published alongside this consultation, and any further consultation as necessary.*

4.2.2 Aggregation / Backhaul

As described in section 3.3.2, there are two main variants of this domain:

- Fixed Aggregation network
- Mobile RAN backhaul (and aggregation)

There are key architectural and design decisions in the aggregation/backhaul portion of networks which have a significant relationship to overall network/service resilience and overall network cost. A key decision is how many customers and/or premises to aggregate onto a given aggregation site

[30] For example, mobile base stations should be configured to fail-over between IPSec Gateways and mobile core functions located at different physical sites in case of core site failure (or more specific functions on those sites). This capability needs to be supported by all relevant functions in the underlying network and backhaul connectivity.

and what resilience measures to include at the aggregation site. This significantly affects the number of aggregation sites and their geographical spread. Aggregating a higher number of customers/premises per aggregation site results in an increased risk of impacting more customers when failures occur.

When architecting and designing a network, we would expect communications providers to take measures to address such risks, including the measures explained below.

Single points of failure are a very important network architecture/design decision when considering the number of customers impacted and the duration of typical impacts (including the typical time to repair). Generally, we would expect communications providers to minimise single points of failure that could lead to a significant impact on network service. Communications providers should consider the 'user-hours lost' reporting thresholds for non-major compromises in Ofcom's Procedural Guidance under section 105Y of the Communications Act 2003, which sets out our view of the level at which service impacts are likely to be significant; see section 5.27 of Ofcom's Procedural Guidance. [31]

As the number of aggregated customers/premises increases at an aggregation point in a network, we would expect communications providers to implement measures to enhance onward connectivity and physical resilience, e.g. through equipment redundancy, physically separate and diverse connectivity, and power backup. In cases where a network is aggregating both fixed and mobile network access, the resulting impact of failures should also be appropriately considered in the network and site designs.

In many cases, it will be expected that onward traffic flows from aggregation sites toward the core/metro will be protected through appropriate resilience mechanisms including fully automatic failover between core/metro sites; e.g. separate resilient transmission links, dual parenting, and any other mechanisms that are appropriate.

Larger aggregation sites are expected to be part of local/regional exchanges (or other similar bespoke facilities) that allow for robust backup of power to be in place; e.g. dual resilient mains electricity power feeds, battery back-up, and electricity generators.

These larger aggregation sites are expected to be able to survive power loss for extended durations with the likely need of permanent electricity generators on site which can be refuelled while in operation to extend operation further if needed.

4.2.3 Core / Metro

See the overview of core and metro sub-domains in section 3.3.3.

Communications providers are expected to take measures to ensure the resilience of core and metro sites, including the measures set out below.

Core and metro sites are expected to have physically separate and diverse transmission connectivity paths to cater for physical failures of network nodes or links (including cable bundles and ducts). These resilient paths are sometimes called 'redundant' paths/links/nodes.

- Core sites are expected to have a significant amount of resilient meshed connections to other core sites using separate and diverse transmission. In large scale networks, this could mean resilient connections to four or more other core sites.

[31] Ofcom. *General statement of policy under section 105Y of the Communications Act 2003*

- In larger networks containing metro sites, they are expected to have resilient connections to at least three other metro or core sites using separate and diverse transmission.

Network functions at core sites, along with the underlying transport network connectivity, should allow network equipment in aggregation and access sites to fail over from one core site to another automatically. This requires all network functions in core sites to be configured and scaled to cater for the loss of a core site including instantaneous load that may result. Networks are expected to be configured to distribute this load across remaining core sites effectively to ensure overall network stability. This applies to all functions including the underlying transport network, user-plane functions, control plane and control plane scaling functions described in section 4.3, and management plane.

Communications providers should implement measures to ensure that their forecasting and capacity planning and network and service resilience mechanisms can survive unexpected loss of a core or metro site with minimal impact to overall network and service reliability. See section 4.5.1.3 for further discussion on resilience mechanism approaches.

Core site locations should be selected considering geographical fibre route diversity and separation, geological hazards like floodplains, extreme weather vulnerability, and a range of other potential hazards as per section 1.3. Where possible, sites which avoid these hazards should be selected. Where avoidance is not possible, appropriate mitigations are expected to be put in place.

Electrical power provision at each core site is expected to include the following as a minimum: dual resilient mains electricity power feeds, battery backup, and fuel-powered electricity generators. These sites are expected to be able to survive power loss for extended durations of a minimum of 5 days, with permanent electricity generators on site which can be refuelled while in operation to extend operation further if needed. [32]

4.2.4 Internet Peering and non-Internet Interconnection

See the overview of the internet peering and 'non-internet interconnect sub-domains in section 3.3.4.

As previously stated, we distinguish between internet-related peering and non-internet-related interconnection types.

We expect communications providers to take measures to ensure that they have resilience across a set of peering and interconnects to third parties providing overall resilience of applications/services hosted beyond their networks.

This means that communications providers are expected to make use of multiple geographically separate paths to third-party networks with appropriate capacity to ensure general reliability of services, applications, and content hosted beyond the communications providers' networks.

As part of this, communications providers should consider physical and logical routes connecting beyond the UK landmass, including subsea cables.

[32] Five days of power backup in a core site would cover the duration specified in the Electricity System Restoration Standard which obligates the Electricity System Operator (ESO) to have sufficient capability and arrangements in place to restore 100% of Great Britain's electricity demand within five days. ESO, *Electricity System Restoration Standard*. https://www.nationalgrideso.com/industry-information/balancing-services/electricity-system-restoration-standard [accessed 5 December 2023].

It is understood that communications providers are not in control of the traffic routing or other policies or practices of third parties, other content and applications providers, or the wider internet.

Regarding non-internet-related interconnects, communications providers are expected to also make use of resilient network elements when connecting to their interconnect partners; as captured in section 4.3.1 for example. Furthermore, as per GSMA IR.77[33] Binding Security Requirements and NICC ND1643[34], voice/VoIP/IMS interconnection between networks should be separate from the Internet.

4.3 Control Plane Resilience

Networks typically have several different categories of logical and physical planes including user planes, control planes, and management planes. [35] This section focuses on the measures we would expect communications providers to take to ensure control plane resilience because control planes are critical to the correct functioning of the network and services. The control plane(s) decide how data is managed, routed, and processed. The user plane is responsible for the actual moving or forwarding of data traffic under the control of the control plane.

Communications networks have control planes of a variety of forms. Depending on the type of services offered by the communications provider, and the associated network functions and infrastructure, there are often multiple control planes.

The guidance contained in this section is not exhaustive in covering every existing or future control plane function or associated protocol. We expect communications providers to take resilience and reliability into account for any control plane function or associated protocol that is part of their networks.

4.3.1 Control Plane Scaling and Overload Resilience

All communications networks have special control plane functions that are needed to increase the scale of the network by eliminating the need for a full mesh of control plane interfaces between all related network functions. This principle applies to, but is not limited to, the following special control plane aggregation or proxy functions in many networks:

- Border Gateway Protocol 'BGP' and BGP Route Reflection
- Signalling Transfer Points (SS7/SIGTRAN)
- Diameter Routing Agents (DRA) and Diameter Edge Agents (DEA)
- Service Communication Proxy (using HTTP2)
- Session Initiation Protocol 'SIP' border controller/gateway/proxy

These functions are critical because the stability and correct functioning of the whole network is dependent on them due to their nature of performing control plane aggregation and distribution.

---

[33] IR.77: InterOperator IP Backbone Security Requirements for Service and Inter-operator IP backbone Providers. GSMA, 2019. *IR.77 InterOperator IP Backbone Security Req. For Service and Inter-operator IP backbone Providers v5.0.* https://www.gsma.com/security/resources/ir-77-interoperator-ip-backbone-security-req-for-service-and-inter-operator-ip-backbone-providers-v5-0/ [accessed 5 December 2023].

[34] NICC Standards, 2009. *ND1643: Minimum security controls for interconnecting communications providers*

[35] User-Plane is sometimes also known as Data-plane or Forwarding-plane.

Therefore, it is imperative that extra care is taken to ensure extreme reliability/resilience in the design of the network control plane(s) including these special functions.

We would expect communications providers to take measures to eliminate any service impacts if one or more of the instances of these special control plane functions was to fail, malfunction, respond with unexpected errors, or become overloaded.

Measures we would expect communications providers to consider include:

- Ensuring multiple geographically separate control plane aggregation function instances (eg DRAs) with multiple parallel active connections with fully automatic switchover between instances.
- Client devices/functions with control-plane interfaces should be designed and implemented with control plane associations with more than one geographically separate instance of the control plane aggregation functions, which should automatically switch between instances when one instance fails, malfunctions, responds with unexpected errors, or becomes overloaded.
- Ensuring sizing and feature-set of instances can handle overload conditions if one or more instances fails, malfunctions, or responds with errors.
- Ensuring all aspects of the instances and their feature set are hardened to be robust against a broad range of abnormal messages and unexpected conditions.
- When interconnecting signalling/messaging protocols (eg Diameter, SIGTRAN, SIP) to untrusted domains including third parties, implementing security and reliability mechanisms as per the Security Code of Practice. When implementing these security capabilities, it is critical to consider the resilience mechanisms of the protocols used, and the overall resilience approach of the network signalling plane(s). Not only is it important that the security functions are aware of the signalling/messaging protocol, but they must be fully compatible with the resilience mechanisms and packet handling operation of the signalling protocols. If not properly implemented, the security function can break the signalling/messaging flows during routine signalling procedures and signalling failover/switch-over events. A robust approach is commonly achieved by using specialised signalling plane functions that embed the security functionality; eg Diameter Edge Agent and SIP Session Border Gateway.
- Implementing BGP optimisations to significantly improve routing reconvergence times with the goal of consistently low reconvergence times, regardless of the number of prefixes in the routing table. Carrier grade IP/MPLS routers support enhancements to the BGP forwarding table entries by organizing the forwarding data structures in a hierarchical manner, introducing an indirect next-hop, which typically dramatically reduces the number of forwarding table changes, and therefor BGP reconvergence times. Vendors typically refer to this capability as Prefix Independent Convergence or next-hop indirection. Additionally, secondary next-hops can be pre-installed in the forwarding table, which further reduce the reconvergence time by simply removing the primary next-hop when it becomes unusable.

Communications providers are also expected to implement appropriate signalling gateway and interconnectivity frameworks and associated overload control mechanisms. Examples of such mechanisms and frameworks are described in the following standards.

Signalling Interconnection - protocol related standards

- NICC ND1657- SIP Overload Control
- GSMA FS.19 – Diameter Interconnect Security
- GSMA FS.21 – Interconnect Signalling Security Recommendations
- GSMA FS.38 – SIP Network Security

Interconnection Connectivity Framework standards

The GSMA documents above should be read together with the following GSMA documents which provide overviews and guidance for the physical and logical interconnections between mobile network operators, fixed operators, and application service providers via 'IPX'. IP packet exchange (IPX) is a global, private, secure, IP network which supports end-to-end quality of service. IR.34 provides technical guidance to Service Providers for connecting their IP based networks and services together to achieve roaming and/or inter-working services between them. IR.77 contains security requirements underpinning IPX connections and interconnection. AA.51 provides an architectural overview of IPX and how component parts of services should be segregated and carried over Interconnects. The same principles apply when providers interconnect directly between themselves instead of via an IPX provider, including in the context of virtual network operators.

- GSMA IR.34 – Guidelines for IPX Provider Networks
- GSMA IR.77 - InterOperator IP Backbone Security Requirements for Service and Inter-operator IP backbone Providers
- GSMA AA.51 – IPX Definition

The NICC has also produced similar guidelines which are aligned to fixed communications provider SIP VoIP telephony, broadband, and IP/Ethernet interconnection.

- NICC ND1643 - Guideline on the Minimum Security Controls for Interconnecting Communications Providers

The Security Code of Practice contains additional cyber-security guidance and measures for incoming and outgoing signalling and control plane protocols which providers should consider.

4.3.2 CPE / Device signalling overload avoidance

We expect communications providers to take measures to avoid customer premise equipment (CPE)/device signalling overload. In particular, CPE and other user equipment devices which are attached to communications providers' networks should be configured to prevent mass synchronisation of connection/reconnection attempts to the communications providers' network functions to avoid network signalling overload. This configuration can take a variety of forms. It is best done before connection or registration. But messages can also be sent to client devices after connection or registration establishment.

The Security Code of Practice contains additional cyber-security guidance and measures for customer premise equipment which communications providers should consider.

4.3.3 Real-Time Charging Resilience

Many mobile networks have moved to real-time charging for their complete mobile subscriber base; both pre-paid and post-paid subscriptions. One of the results of this transition is that the ability for the end-user services to function depends on continuous reachability of the real-time charging solution with correct and timely responses. Therefore, we would expect communications providers to take measures to ensure that network functions with real-time charging interfaces, and the rest of the real-time charging solution, should take resilience and reliability into account in their designs and testing.

This should include implementation of geographic separation of resilient instances with multiple parallel logical connections between components. To avoid end-user service impact, client network functions should support fully automatic switchover between real-time charging instances in cases that they fail, malfunction, become overloaded, or respond with unexpected errors.

4.3.4 Policy Control Resilience

There are a variety of approaches to implementation of policy control in mobile networks; applied to user plane-functions via the control plane. In some more sophisticated scenarios, Policy Control Functions are used to support more granular and/or dynamic policy control than what may have traditionally been used. In cases where network functions depend on the reachability and correct and timely responses from the Policy Control Function in order for end-user service to function, we expect communications providers to take measures to ensure that resilience and reliability are included in the designs and testing of all aspects of the policy control solution and connectivity.

This should include implementation of geographic separation of resilient instances with multiple parallel logical connections between components. To avoid end-user service impact, client network functions (such as a User Plane Function) should support fully automatic switchover between policy control instances in cases that they fail, malfunction, become overloaded, or respond with unexpected errors.

4.3.5 Network Authentication/Authorisation Resilience

End-user-device authentication/authorisation on to a network to use services is a critical component for both fixed and mobile networks. Connectivity and reliability of the platforms (or service functions) which provide the authentication/authorisation function are critical as a result. This typically includes RADIUS/Diameter/AAA/HLR/HSS/SDM/UDM platforms/function in networks.

We would therefore expect communications providers to take measures to implement network authentication/authorisation resilience. Implementation of these functions should include geographic separation of resilient instances with multiple parallel logical connections between relevant components. To avoid end-user service impact, client network functions should support fully automatic switchover between instances in cases that they fail, malfunction, become overloaded, or respond with unexpected errors.

4.3.6 Domain Name System (DNS) Resilience

In its most basic form, the Domain Name System (DNS) is used to resolve IP addresses from human readable domain names or Uniform Resource Locators (URLs). In modern networks, DNS is often used for multiple different purposes with different requirements for scalability, resilience, and security. There are typically at least two different DNS uses cases for implementation within communications providers networks, those being:

- Customer Facing DNS – This includes resolving of internet destination IP addresses (both IP version 4 and IP version 6) for applications residing on customer devices. This can also include resolving of IP addresses of services hosted and operated within the communications provider's network estate.
- Infrastructure DNS – This includes resolving of internal infrastructure IP addresses that are not related to the Internet and are not exposed to end customers or the wider internet.

A number of control plane protocols and network infrastructure and service solutions have become dependent on 'infrastructure DNS' residing within internal private portions of communications providers' network infrastructure. Examples include: the 5G core Service Based Architecture control plane interfaces, IMS network function interfaces, and the internal underlying infrastructure addressing used within Network Functions Virtualisation Infrastructure (NFVI). In these cases, the availability and performance of the infrastructure DNS becomes as critical as the rest of the control plane, and the infrastructure DNS is effectively subsumed into the control plane as a result. Therefore, we would expect communications providers to take measures to ensure that infrastructure DNS should take resilience and reliability into account in their designs, testing, and operational model.

Regarding customer facing DNS, including for the purposes of resolving internet destination IP addresses, we also expect communications providers to take resilience and reliability into account in their designs, testing, and operational model.

In order to prevent cascading failures between customer facing DNS and infrastructure DNS, we expect communications providers to implement customer facing DNS and infrastructure DNS to make use of separate infrastructure resources with appropriate level of protection or isolation from each other.

4.4 Management Plane Resilience

As per section 3.3.5, the management plane may be provided 'in-band' over the same physical production network as the user and signalling planes with appropriate segregation, or 'out-of-band' (OOB) physically separate from the primary network carrying the user and signalling planes.

Whilst in-band management is typically more cost effective, we would expect communications providers to take measures to ensure sufficient segregation of management traffic and production traffic, including mechanisms to ensure management traffic can neither be impacted by or have an impact on the production traffic. As a minimum, we expect this to include logical separation of management traffic into different VLANs and VPNs/VRFs to limit the potential for problems in one virtual routing or switching domain impacting another.

The sole use of in-band management has the disadvantage that it is possible that a change made to the network remotely via in-band management could inadvertently disconnect the production traffic as well as the management user traffic without a remote method to rectify the mistake, thus requiring on-site local access to the impacted piece of equipment. This risk, at best, adds expense and delay and, at worst, can prolong a catastrophic outage. For example, if a communications provider needed to have field engineers drive to a large number of geographically distributed sites simultaneously to locally restore operation and connectivity of network equipment, this could take a number of days. When architecting, designing, and operating networks and services, communications providers should also consider the measures set out in the Security Code of Practice related to the security and segregation of the management plane and associated management

traffic including: privileged user access, privileged access workstations, network oversight functions, and security critical functions.

4.4.1 Out-of-Band Management

An OOB management network is a separate network used only for network management purposes, such as configuration, troubleshooting, and sometimes monitoring of key network infrastructure components that underpin other network functions.

The OOB network provides a dedicated path for the network management traffic, which is typically encrypted and protected by access controls and other security measures. This allows network administrators to perform network management tasks on key primary network elements when the primary network is not functioning correctly and also without the potential of the management traffic impacting the performance or availability of the primary network.

We would expect communications providers to consider whether it is appropriate to implement OOB management. There are a number of reasons why network architects might consider an OOB management network:

1. Network Management: An OOB management network provides a separate and dedicated network for managing network devices such as switches, routers, and firewalls, which enable network administrators to perform tasks such as firmware upgrades, configuration changes, and monitoring without depending on or affecting the main network.
2. High Availability: An OOB management network provides an alternative network path for network administrators to access network devices if the main production network is down. This helps to ensure the availability and reliability of network management, which in turn enables faster restoration of the production network. This is particularly relevant for networks with a large number of geographically distributed equipment which might otherwise require driving to large numbers of sites simultaneously to restore correct operation.
3. Security: An OOB management network provides a secure path for network management traffic and reduces the risk of malicious attacks or unauthorized access to the main network.
4. Isolation: An OOB management network provides a separate network for management traffic, which can help to minimize the risk of congestion, interference, and other issues that may impact the performance of the main network and the main network on the OOB network.
5. Auditing: An OOB management network provides a separate network for network management traffic, which can simplify network auditing and provide better visibility into network management activities.

In summary, an OOB network can provide additional security, reliability, and visibility for network management, and can help to ensure the availability and performance of the main production network.

4.5 ‘CP-managed’ services – enhancing reliability

Communications providers often design, host, and operate services in a 'fully integrated' manner within their own network footprint so the services are optimised for reliability and security, while also being separate and independent of the functioning of the wider internet. These are often called

CP-managed services and should not be confused with outsourcing service hosting or operation to third parties. Some of these CP-managed services may be consumed by end customers. Others may be internally consumed by other functions within the communications provider's network. For example, the authentication/authorisation and control plane aggregation/distribution functions can be seen as critical internal network-related services.

Communications providers typically choose a CP-managed service model in order to ensure greater operational reliability with complete operational ownership in comparison to applications that are externally hosted and dependent on the operation of the wider internet.

In addition to the security duties under CA 2003, communications providers have obligations to ensure the reliable operation of some specific services under other statutory or regulatory requirements; for example as per Ofcom's General Conditions of Entitlement. Voice services are a key example as they are used for accessing the emergency services; with obligations captured in Ofcom's General Conditions A3. Ofcom's Open Internet (Net Neutrality) Guidance also makes specific allowances for this and other CP-managed services; for example, where they are considered 'Specialised Services'.

While this guidance sets out measures communications providers should take to meet their security duties, we would expect providers to consider more broadly what measures might be required to meet these wider statutory and regulatory obligations. While we do not provide detailed guidance on wider obligations in this document, and what is required will depend on any given case, some general good practices which we consider may be relevant to compliance with these obligations are listed below.

4.5.1 Service implementation independent of the wider Internet

As indicated in Figure 3, customer applications or services accessing the internet and the communications provider’s own services (e.g. Fixed / Wireline Voice calling) often use elements of common infrastructure across several parts of the network.

In cases of critical services, in order to maintain robust and secure service, communications providers are advised to design, host, and operate these services entirely within their own infrastructure and securely separate it from the Internet such that the service is not dependent on the functioning of the wider Internet. Consideration should also be given to how traffic is managed to ensure the appropriate level of service is maintained.

For mobile services, 3GPP standards dictate separation and differentiation between internet and voice services which allows for respective traffic priority to be provided. In the case of fixed-line voice-over-broadband (VoBB), which inherently uses the ‘Internet Protocol’ to carry voice traffic, the separation of voice and internet traffic is not as prescriptively defined in industry standards. However, there are design approaches that should be used to provide prioritisation and separation from internet traffic to enable consistent quality of experience, and protect the voice service from

DDoS and other malicious attacks. [36,37,38] Communications providers should build their VoBB services that are aimed to be 'PSTN replacements' in a manner that maintains these principles.

Furthermore, as stated in section 4.2.4, voice/VoIP/IMS interconnection between networks should be separate from the Internet.

4.5.2 Quality of Service and Prioritisation Mechanisms

The types of services and approaches mentioned in this section will typically be implemented with enhanced traffic prioritisation and failover/handover resilience mechanisms. This can only be done for a limited number of services due to limitations of scalability and complexity of these mechanisms, and increased cost often due to sacrificed efficiency. Furthermore, these enhancements can typically only be applied to services implemented within the communications provider's network infrastructure due to the increased design, testing, and operational burden.

4.5.3 Resilience Mechanisms and approaches

When architecting, building, and operating networks and services, communications providers should assess the criticality of the services running on/over the network. That criticality assessment feeds in to architectural, design, and network platform/function implementation decisions. These implementation decisions apply to the design and engineering of the Application Servers, User Plane Functions, and the associated control plane(s).

Where a network supports critical or important telecommunications services, such as CP-managed-voice services (e.g. VoLTE or VoBB), careful consideration of local, hosting, and end-to-end resilience mechanisms used, and the capabilities and performance of hardware platforms such as servers, switches, routers, and transmission is expected. In the telco world, this stringent set of capabilities, performance, and reliability is often referred to as 'Carrier Grade'.

Communications providers should generally ensure that platforms, solutions, and designs include fast and scalable failure detection and failover mechanisms to minimise impact to services appropriately, with appropriate attention given to services for which they have specific obligations. Furthermore, the failover mechanisms of the platforms, solutions, and designs should be tested in a representative test environment and optimised under load, and fully understood by the relevant technical staff.

---

[36] This assumes that the broadband service is functioning and that the customer's premise has power available to the broadband router which contains the VoBB client. Such services can be prioritised provided they meet the requirements for a 'specialised service' set out in Art 3(5) of retained Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and retail charges for regulated intra-EU communications and amending Directive 2002/22/EC and Regulation (EU) No 531/2012 (Text with EEA relevance). (EUR-Lex, 2020. *Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R2120 [accessed 5 December 2023].

[37] Distributed Denial of Service – distributed volumetric attacks against a person, a service, a CP, or even a collection of CPs

[38] Internet-based/OTT VoIP services cannot achieve the same level of reliability, so they should not be considered as a 'primary-line', particularly in relation to making Emergency calls. "VoIP" is an umbrella term for any approach to Voice over the 'Internet Protocol'. It often relates to an 'un-managed' application based on the wider internet; eg an 'Over-The-Top' (OTT) application. Voice over BroadBand (VoBB) is a more specific term which typically refers to a 'CP-managed' 'On-net' solution rather than OTT.

In generalised terms, there are three main approaches to addressing the resilience of services when network failures occur, and each has a different level of impact on users for a given service or application:

1. Not externally visible – 'zero service impact' - typically having increased complexity and requiring more system resources, therefore limiting scalability
2. Limited external visibility with automatic failover - network-initiated or application-initiated session re-establishment – users may be aware of an impact to service for up to a second or two, but do not need to take any action
3. Extensive external visibility - user-initiated session/call re-establishment – users are very aware of the impact and need to take action to re-establish the service

We recognise that there are complexity, scalability, and cost implications to the different failover approaches above. We understand that it is unlikely to be technically feasible or cost effective to support option 1 for all services or traffic types. Aspects relating to how a service recovers from a failure should also be considered.[39] Communications providers must make choices that align with their service design requirements and obligations.

4.5.4 Network Slicing and Telco Cloud

Forms of network slicing have been around in various guises across many different technologies over the last few decades in the forms of logical or virtual private networks using a variety of different Open Systems Interconnection (OSI) layer 1, layer 2, and layer 3 approaches.

In networks using 'cloud-native' network functions and other forms of disaggregated network functions with the addition of slice-capable 5G devices, the notion of network slicing has taken further steps forward that allow significant differences in the build of logical network topologies over common underlying network infrastructure.

These different per-slice topologies can be combined with 5G-slice-specific enhanced radio network capabilities and prioritisation to create on-net services with fundamentally different characteristics for packet latency (delay), jitter (delay variation), and loss. This approach provides the possibility of a new way of building services with enhanced reliability and/or performance.

However, in most cases, these 5G slices are expected to be used for services other than standard consumer end-user internet-related services. As such, regarding Net Neutrality, services built using 5G network slices are expected to be considered 'Specialised Services'.

5G network slicing related standards and implementation approaches continue to evolve across a broad range of different technical domains and ecosystems. Many different international standards bodies underpin those different domains and ecosystems, all of which are needed to realise interoperable end-to-end solutions and implementations that are reliable.

The GSMA publication on End-to-End Network Slicing Architecture (NG.127) provides an overview of the current status of the 5G E2E slicing landscape and a broad set of associated gaps, overlaps, and challenges that may need to be addressed across multiple standards bodies and industry stakeholders to achieve widescale rollout of 5G network slices in a viable and realistic manner.

[39] For example, if a service automatically recovers how are differences in state reconciled, as well as any potential service impact due to additional load or rapid change in state. This can also drive additional availability requirements in specific components and/or their connectivity.

Communications providers should take this into account when considering the implementation of network slicing.[40]

Additionally, at the time of writing this guidance, 'cloud-native' technology and methodologies for its application to telecommunications network functions are still evolving across many different industry groups, organisations, and open-source communities. While a cloud-native 'Telco Cloud' approach has many advantages, there are some drawbacks as well. The associated technology and solutions for control plane and user plane functions are not yet felt to be fully mature for the goal of achieving high levels of resilience, security, scale, and throughput.[41] Additionally, there are multiple different approaches to the infrastructure and operational model including: private cloud (run by the communications provider), public cloud (run by a third party), and hybrid or multi-cloud (where multiple different options are used in combination).[42] There are also multiple different approaches for disaggregated User Plane Function implementations including, but not limited to: software-based (on either x86 or RISC processors), hardware-based 'white-boxes', and a range of hardware acceleration options. As such, it is not currently possible to provide mature guidance on the resilience aspect of cloud-native Telco Cloud implementations.[43]

However, we are aware that communications providers are moving from physical and 'virtualised' network functions towards 'cloud-native' implementations of network functions, including the critical control plane functions listed in this guidance. As part of our Resilience Incident reporting function, we have been made aware of a number of significant network outages that have occurred to virtualised and cloud-native implementations of network functions. Our general assessment is that the root causes of these incidents tend to be related to immaturity and complexity of the new solutions combined with skills gaps of technical and operational staff.

While network slicing typically has the promise of enhanced service reliability and/or performance, where new technologies are used, such as 5G network slicing and cloud-native deployment, there are maturity challenges that need to be addressed.

We expect communications providers to take reliability, resilience, and security into account in their designs, testing, and operational models when using software-based or cloud-native implementations of network functions, regardless of the specific approach. As a reminder, where a provider offers a communications service, they are responsible for the reliable and secure operation of the service over the end-to-end network path to end-customers. This includes any use of cloud infrastructure or supply chain model used.

---

[40] GSMA, 2022. E2E Network Slicing Architecture, Version 2.0.

[41] See Ofcom, "*Maintaining Reliability in Telco Cloud Transformation*" in ITP, 2023. *The Journal*. Vol 17, part 2.

[42] Private cloud computing; A cloud deployment model where computing resources are dedicated to (as opposed to shared between) individual customers. Public cloud computing; A cloud deployment model where cloud services are open to all customers willing to pay, and computing resources are shared between them. Hybrid cloud computing; A cloud deployment model involving a combination of public clouds and private environments (such as private clouds or on-premises resources). which allow workloads to be shared between them. Multi-cloud; A cloud deployment model involving the use of more than one cloud by a single customer, where multiple clouds may or may not be integrated with each other.

[43] The Security Code of Practice provides a range of cyber security focused measures. The EC-RRG Resilience Guidance contains background information on virtualisation including a range of resilience considerations.

5. Processes, Tools, and Training

In this section, we set out our guidance as to the measures to be taken under sections 105A to 105D by communications providers on processes, tools and training.

We focus on a number of aspects relating to the 'operational wrap' around underlying physical and logical deployment (infrastructure) that allows for it to be architected, designed, tested, deployed, and operated in an effective manner and to achieve expected levels of availability. Aspects of the Information Technology Infrastructure Library (ITIL) framework which have a particular bearing on the availability of telecommunications services have been used and adapted as a basis to provide a structure that aligns with industry recognised best practice for the following section.

ITIL does not focus on staff competency (e.g. skills and training), but this section is the logical place to cover that as well.

Where process measures are implemented, in particular, we expect communications providers' management to commit to these, with a clear line of responsibility and chain of command from the Board level down to operational delivery, with clear evidence of this in relevant internal process documentation.

5.1 Network and Service Design

Service Design relates to both development of new services as well as changes and improvements to existing ones.

5.1.1 Processes related to Network and Service Design

5.1.1.1 Service Level Management

The Service Level Management process sets the service level requirements for the services that a communications provider operates and ensures the designs of each service can meet them. In implementing any Service Level Management processes, we would expect that communications providers should consider the operational support impacts, as well as any use of third-party services consumed as part of the service provision.

5.1.1.2 Capacity Management

Capacity Management considers all resources required to deliver the service, and plans for short, medium, and long-term requirements. We would expect communications providers to take measures to ensure that they are adhering to forecasts to allow for the full cost to be recognised and any increase in scale to be understood and planned in a timely manner. Such capacity management measures should:

- include monitoring and forecasting for all User-Plane, Control-Plane, and Management-Plane traffic, as well as other forms of load like routing and forwarding table sizes, rule-base sizes, and control-plane message processing capacity.
- build in the capacity needed to maintain reliable service during significant network failures and high signalling load conditions. For example, capacity planning and failover mechanisms should allow for the loss of a core site or peering/interconnect site during the busy hour without resulting in network congestion or overload that would affect the ability to manage the network or significantly affect the operation of the network or service.

5.1.1.3 Availability Management

Availability Management considers the required service levels and measures the service against these. This can include a number of key performance indicators including the number, and duration of interruptions to service. There could be a variety of reasons that impact the service levels. The quality of the service from the perspective of the users' experience also needs to be considered. We would expect communications providers to take measures to ensure appropriate availability management is implemented. When the normal service levels of a given service are not being met, the cause needs to be identified, and appropriate actions then taken to remediate the issue in order to bring it back up to an appropriate level.

Taking an extreme example, if a voice service is unusable due to a lack of bandwidth in the underlying network, this will often be no different to the voice service itself (e.g. a call server) not being available from a consumer's perspective.

5.1.1.4 Continuity Management

Continuity Management (also often referred to as Business Continuity Management (BCM)) relates to how risks of serious impact to service are mitigated and managed. We would expect communications providers to take measures to ensure that appropriate service levels are met by reducing risks from disaster events as well as having plans for how a business-as-usual service is resumed in a timely manner. This process should also consider maintenance of the processes and procedures including periodic exercises and testing.

5.1.1.5 Supplier Selection, Management, and Spares

Supplier Management is critical for both the supply of equipment and appropriate support arrangements.

We would expect communications providers to take measures to ensure appropriate supplier management is implemented. Selection of supplier hardware, software, or solutions should include assessment based on a suite of testing of reliability and resilience. Using the hardware, software versions, and features relevant to the intended network design, this testing should include:

- Load performance and scalability
- link/card/hardware failure detection and resulting failover performance/speed/stability (while under load)
- IP reconvergence speed and stability for each relevant IP networking protocol used in the network (while under load)

Such measures also include, in some cases, pre-emptively build up dedicated spare equipment stores of hardware stock to meet the service level targets or obligations.

Particular care should be taken to ensure third party support is not invalidated through the use of unsupported configurations, either physically or logically.

5.1.2 Tools related to Network and Service Design

Communications providers are also expected to implement and use tools related to network and service design necessary to support the aforementioned processes. These include:

- Capacity Planning – including modelling of network faults combined with traffic forecasts to determine resulting capacity on an ongoing basis

- Service Modelling to ensure broad understanding of service design and dependencies
- Configuration Management

Note that tools which contain information about the network or services are deemed to be Network Oversight Functions in the Security Code of Practice and should be secured appropriately as indicated in it.

5.2 Network and Service Transition

The ITIL framework groups the functions of network and service *testing*, *deployment*, and *change* under the banner of 'transition'. The build and deployment of both new services and updates to existing services requires careful consideration and planning, all informed and validated by a broad suite of testing. Both the processes and the tools to support the processes need to support the appropriate levels of availability. We would expect communications providers to take the following measures to ensure appropriate network and service transition.

5.2.1 Processes related to Network and Service Transition

5.2.1.1 Change Management

Communications providers are expected to have a robust change management process and set of tools. The main objective is to control and coordinate network and service changes with minimum impact to service availability. Questions to be considered in the implementation of changes include:

- Is the impact of the change understood? E.g. has it been tested in a representative environment at full load?
- Is the change being made at an appropriate day and time? E.g. avoiding busy hours specific to the service potentially being impacted where possible.
- Are successful entry and exit criteria understood? E.g. documented test cases to be carried out both before and after the change.

5.2.1.2 Asset and configuration management

As a part of maintaining network and service resilience, we would expect communications providers to take measures to ensure that they have an accurate up to date record of physical and logical network assets as part of understanding their dependencies and impact on services.

Communications providers should have a 'service-to-asset map' for relevant staff to have a clear and accurate understanding of which services depend on which network assets. This allows the communications provider to clearly understand which services may be impacted when a given asset fails or is changed.

All assets in a network should be uniquely identified in an accurate and effective manner. This record will support several other processes such as planning change and assessing impacts when incidents occur.

This record should include all physical assets that underpin the network including (but not limited to) ducts, cables, patch panels, ODF cassettes, routers, power equipment and feeds, and other network and service infrastructure. It should also include key logical assets, for example a VLAN specific to a service, to aid understanding impacts to key services.

This information should be used as part of ongoing risk assessments of network changes.

Training of all relevant staff in the asset identification methods and systems used is crucial to ensure that the correct information is used when replacing or making changes to network assets.

5.2.1.3 Testing and Validation management

Communications providers should take measures to implement appropriate testing and validation management. The objective is to ensure new services and changes to existing services meet the required service levels.

- For a given network or service deployment or update, we would expect for there to be an agreed test plan including specific test cases, with results recorded for each test.
- A broad suite of testing should be performed including: functional testing, component resilience testing under load, and end-to-end service testing while inducing component failures by suitably competent people.
- Tests should include mechanisms of deployment as well as back out approach.
- Service acceptance testing - Additional testing is required once a service has been deployed to ensure that what has been deployed meets the requirements and nothing has been broken as a result of the deployment.
- Appropriate service and resilience testing should be repeated any time there is a relevant equipment, software, or configuration change that may have an impact on the network or service performance or reliability.

5.2.1.4 Knowledge management

Communications providers should take measures to implement appropriate knowledge management. The objectives of knowledge management are to gather, analyse, store, and share knowledge and information within the organisation. The primary purpose is to improve efficiency by reducing the need to rediscover knowledge. This is important for a secondary purpose of maintaining appropriate network and service resilience by avoiding errors and incidents that would result from incomplete or inaccurate information. Knowledge management may include the following:

- Process documents for the above purposes
- Network architecture and design documentation
- Service design documentation
- Test plans, test cases, test results, and plans for remediation
- Network and Service performance, availability, and service impact insights resulting from network monitoring and data analysis and correlation

5.2.2 Tools related to Service Transition

Communications providers should take measures to implement appropriate tools related to service transition, such as:

- Asset inventory management
- Service provisioning
- Run book task automation

- Network and service architecture, design, and operational knowledge documentation
- Network and service configuration management

Note that tools which contain information about the network or services are likely to comprise Network Oversight Functions for the purposes of the Security Code of Practice.

5.3 Service Operation

Service operation relates to managing a service through its day-to-day production life. It also includes supporting operations by means of new models and architectures such as shared services, utility computing, web services, and mobile commerce.

We would expect communications providers to take measures on the operational aspects of Service Level Management, Capacity Management, Availability Management, Continuity Management, and Supplier Management and Spares, which are in addition to the network and service design measures which are covered in section 5.1.1. This includes network monitoring and management in order to ensure that the network and service design requirements and planning rules are being met.

As a reminder, outsourcing aspects of network or service operation carries risk, and the operational responsibilities remain with the communications provider. Refer to sections 1.3.7 and 3. Furthermore, oversight of third-parties is covered in the Security Code of Practice.

5.3.1 Processes related to Service Operation

5.3.1.1 Network Control-Plane Monitoring

We would expect communications providers to take measures to ensure appropriate processes are implemented in relation to network control-plane monitoring.

Incoming and outgoing network signalling should be monitored at ingress and egress points of networks in relation to a range of security measures (se also the Security Code of Practice).

Additionally, communications providers are expected to monitor control plane (signalling plane) interfaces across the infrastructure domains within their network for the purposes of more general network and service resilience purposes.

The network control plane aggregation function instances described in section 4.3.1 should be monitored for signs of overload so that appropriate action can be taken to maintain the correct functioning of the function and the wider network. For example, alarms and or telemetry fed into the appropriate tools and alerting staff in the Network Operations Centre.

Communications providers should use data analytics to correlate network, service, and subscriber/device information related to the network and service health. This should allow a communications provider to quickly and pro-actively identify service degradation and accurately identify how many subscribers/devices are impacted during network or service faults which also supports accurate and timely decisions regarding notification and reporting of incidents to Ofcom.

In a mobile network for example, MNOs are expected to log, monitor, and correlate signalling between the radio access network and mobile core network (S1-C for example) in addition to all Diameter, 5G SBA (HTTP2), SIGTRAN/SS7, GTP-C, and SIP signalling messages and associated errors.

5.3.1.2 Network User-Plane Monitoring

The User-Plane is also sometimes called the Data-plane. We would expect communications providers to take measures to ensure appropriate network user-plane monitoring. Monitoring of the

user-plane functions and interfaces of the network is required for capacity planning and purposes as well as understanding the impacts of network faults. It is also useful in understanding quality, consistency, and reliability that will be experienced by users of the network or services.

5.3.1.3 Event Management

We would expect communications providers to take measures to ensure that Infrastructure and services should be constantly monitored. The Event Management process aims to filter and categorise events to decide on appropriate actions required in a timely manner. This is significantly aided by control plane monitoring described in the previous section.

5.3.1.4 Incident Management

We would expect communications providers to take measures to establish a process to manage the lifecycle of all incidents due to unplanned interruptions or reductions in quality or resilience of a service. This process should include among other things, the logging, prioritisation, tracking, reporting, and escalating where necessary. Tools and processes should include the ability to correlate the impact to specific services and provide proactive user information.

5.3.1.5 Problem Management

We would expect communications providers to take measures to establish problem management processes. Problem Management seeks to minimise the adverse impact incidents by preventing the incidents from happening. For incidents that have already occurred, Problem Management tries to prevent these incidents from happening again.

5.3.1.6 Operations Centres and Help Desks

Communications providers are expected to take measures to establish Operations Centres supporting the continuous monitoring of network infrastructure and service performance, functionality, and availability.

As per regulation 15, where it appears to the communications provider that a network or service incident may cause an incident to another communications provider's network or service, the communications provider must so far as is appropriate and proportionate, provide assistance and information to the other communications provider

Communications providers are expected to provide their customer the means to contact them to inform customers about network and service faults and performance; typically referred to as a help desk.

5.3.2 Tools related to Service Operation

Communications providers should take measures to implement appropriate tools related to service operation including:

- Network and Control Plane monitoring and data analytics
- Incident Management
- Event Management
- Run Books

As already noted, tools which contain information about the network or services are likely to comprise Network Oversight Functions for the purposes of the Security Code of Practice.

5.4 Skills Competency and Training

We would expect communications providers to take measures to ensure that the responsible persons have appropriate knowledge and skills to perform their responsibilities effectively, and to ensure that the responsible persons are competent to enable the communications provider to perform their duties.

Therefore, we expect communications providers to ensure that their staff (or others on their behalf) have the appropriate skills, competency, and tools for the full lifecycle of architecture, design, deployment, operation, monitoring, and remediation of their network and services. Attaining an appropriate level of skills, competency, and experience would include relevant training.

This includes any managed service providers or partners as described in 1.3.7.

This is consistent with Regulation 13 which requires communications providers to take such measures as are appropriate and proportionate to ensure that anyone responsible for taking measures to meet the provider's security duties (or other responsible persons on their behalf) are competent to discharge their responsibilities and are given resources to enable them to do so.

5.5 Network Automation

Network automation can include the processes of automating the configuration, management, testing, deployment, and monitoring of physical & virtual devices in a communication provider's network.

Automating the configuration of the network can provide benefits including repeatable and predictable outcomes which can be pre-tested to provide confidence in the outcome.

Network automation can span both Service Transition and Service Operation; see previous sections.

As with other aspects relating to building robust and resilient networks, network automation should be considered at the inception of a design as this can drive the approach of the design; for example, how functional and reusable capabilities are defined. In some cases, this may be counter-intuitive compared to a more bespoke approach which may seem initially more efficient but can lead to additional complexities in non-standard and thus unpredictable outcomes.

For cloud-native network implementations, network automation becomes essential due to the scale and complexities of cloud infrastructure, containers, logical connectivity, and the more dynamic nature of the network and service ecosystem. It would typically not be possible to use historic operational configuration and support models.

As networks become more automated, they will rely more on 'data analytics' and 'software-control'. This is often associated with the use of machine learning to analyse network and/or service performance data and then make automated network changes. This has the potential to cause significant network or service outages if the software or logic fails. Additionally, integration and implementation complexity can often be a contributory factor to failures.

Network automation carries risk, potentially of catastrophic network failure, so it is crucial that network automation is very carefully considered in every aspect. For this reason, we would expect communications providers to take measures to ensure that they apply an appropriate level of diligence when implementing network automation.

6. Our approach to Resilience

This section describes how we will use our powers and sets out relevant industry guidance which communications providers may wish to consider.

6.1 How we will use our powers

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

Ofcom has published a general statement of policy under section 105Y of the CA 2003 setting out procedural guidance on the exercise of its functions to ensure compliance with the security duties, including providers' resilience-related security duties (the Ofcom procedural guidance).[44] 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:

- 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.
- 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.
- Our assessment powers under sections 105N and 105O of the 2003 Act – see subsection titled "Powers to assess compliance – Assessments and assessment notices (sections 105N105Q)" and sub-section titled "Powers to assess compliance – Power to enter premises (section 105O and 105R)" in section 3 of the Ofcom procedural guidance.
- Our enforcement powers under sections 105S to 105V of the 2003 Act – see section 6 of the Ofcom procedural guidance.

6.1.2 Resilience Incident reporting and Ofcom assessments

Section 105K(1) requires communications providers to inform Ofcom as soon as reasonably practicable of any security compromise that: has a significant effect on the operation of the network or service; or involves unauthorised access to, interference with or exploitation of the network or service so that a person is put in a position to bring about a further security compromise that would have a significant effect on the operation of the network or service. This includes the occurrence of a Resilience Incident. Please refer to Section 5 (Reporting security compromises) of the Ofcom procedural guidance for further details.

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

- if the communications provider has taken such measures as are appropriate and proportionate to identify and reduce the risk associated with the cause of the Resilience Incident and prepare for the occurrence of the Resilience Incident.

[44] Ofcom. *General statement of policy under section 105Y of the Communications Act 2003*

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

6.1.3 Ofcom's Enforcement guidelines for regulatory investigations

In addition to the Ofcom procedural guidance, Ofcom publishes Regulatory Enforcement Guidelines for regulatory investigations, 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.[45]

Ofcom has a general duty to ensure compliance with security duties. 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 formal enforcement investigation, we will consider the specific circumstances of the case in accordance with our guidelines to decide on the appropriate course of action.

6.2 Related sources of Resilience Guidance

In addition to the guidance set out in this document, communications providers should consider the sources of guidance set out below where appropriate.

6.2.1 Guidance on General Condition A3

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.

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.

We note that BT, the current provider of Emergency Services Access call handling centres, has developed a set of 999 Test Call Handling Procedures. We have published an outline of these procedures on Ofcom's website here Ofcom: Telecoms industry guidance.

6.2.2 Additional sources of resilience guidance

When considering the measures necessary to comply with the security duties imposed by or under sections 105A to 105D in relation to a particular network or service resilience matter, Ofcom will expect communications providers to have considered industry standard resilience best practices in their approach to the development and maintenance of their network and services.

The list below summarises the main sources of further advice and best practice that we refer to in this guidance. 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.

[45] Ofcom, 2022. *Regulatory Enforcement Guidelines for Investigations*

6.2.2.1 ENISA's Technical Guidance on Security Measures

ENISA's Technical Guideline on Security Measures gives guidance in relation to appropriate risk assessment, ongoing risk management, operations and business continuity management. [46]

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

The ENISA report, Enabling and Managing End-to-End Resilience provides a broad and comprehensive introduction to both technical and organisational requirements for developing and maintaining resilient networks and services.[47]

6.2.2.3 EC-RRG Resilience Guidelines

The EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure, published in 2021, include further technology updates to the above ENISA guidance for areas such as All IP Networking, Virtualisation, and 5G.

6.2.2.4 Building Digital UK Environmental Resource Guide for Digital Infrastructure

Building Digital UK (an executive agency within the Department for Science, Innovation and Technology) published guidance for mobile operators and broadband providers (including satellite solutions) covering environmental design and operational considerations related to network infrastructure resilience. [48] It contains guidance on network infrastructure design and planning considerations related to electrical power dependence, extreme weather events, and other climate change risks and adaptions.

[46] ENISA, 2021. *Guideline on Security Measures under the ECC*.

[47] ENISA, 2011. *Enabling and managing end-to-end resilience*.

[48] Building Digital UK, 2023. *Building Digital UK - environmental resource guide August 2023.* https://www.gov.uk/guidance/building-digital-uk-environmental-resource-guide-august-2023 [accessed 5 December 2023].